Официален вестник L 207

на Европейския съюз

Издание на български език

Законодателство

Година 59

1 август 2016 г.

Съдържание

[1] Текст от значение за ЕИП

BG

Актовете, чиито заглавия се отпечатват със светъл шрифт, са актове по текущо управление на селскостопанската политика и имат кратък срок на действие.

Заглавията на всички останали актове се отпечатват с получер шрифт и се предшестват от звездичка.

II

(Незаконодателни актове)

РЕШЕНИЯ

РЕШЕНИЕ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2016/1250 НА КОМИСИЯТА

от 12 юли 2016 година

съгласно Директива 95/46/ЕО на Европейския парламент и на Съвета относно адекватността на защитата, осигурявана от Щита за личните данни в отношенията между ЕС и САЩ (EU-U.S. Privacy Shield)

(нотифицирано под номер C(2016) 4176)

(текст от значение за ЕИП)

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 г. за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни ([1]), и по-специално член 25, параграф 6 от нея,

след консултация с Европейския надзорен орган по защита на данните ([2]),

1. ВЪВЕДЕНИЕ

(1) В Директива 95/46/ЕО се определят правилата за предаването на лични данни от държавите членки към трети държави, доколкото това предаване попада в приложното поле на директивата.

(2) С член 1 от Директива 95/46/ЕО и съображения 2 и 10 от нейния преамбюл се цели да се осигури не само ефективна и пълна защита на основните права и свободи на физическите лица, по-специално на основното право на зачитане на личния живот при обработването на лични данни, но и висока степен на защита на тези основни права и свободи ([3]).

(3) Значимостта на основното право на зачитане на личния живот, гарантирано от член 7 от Хартата на основните права на Европейския съюз, както и значимостта на основното право на защита на личните данни, гарантирано от член 8 от същия документ, се подчертава в практиката на Съда ([4]).

(4) Съгласно член 25, параграф 1 от Директива 95/46/ЕО от държавите членки се изисква да следят предаването на лични данни към трета държава да се осъществява само ако съответната трета държава гарантира адекватно ниво на защита и ако законите на държавата членка, с които се привеждат в изпълнение други разпоредби от директивата, са спазени преди предаването. Комисията може да установи, че дадена трета държава гарантира такова адекватно ниво на защита чрез националното си законодателство или международните ангажименти, които е поела с цел защита на правата на физическите лица. В такъв случай и без да се засяга спазването на националните разпоредби, приети в съответствие с други разпоредби от директивата, личните данни могат да бъдат предавани от държавите членки, без да са необходими допълнителни гаранции.

([1]) ОВ L 281, 23.11.1995 г., стр. 31.
([2]) Вж. становище 4/2016 относно проект на решение за адекватността на Щита за личните данни в отношенията между ЕС и САЩ, публикувано на 30 май 2016 г.
([3]) Дело C-362/14, *Maximillian Schrems c/y Data Protection Commissioner* („делото *Schrems*“), EU:C:2015:650, точка 39.
([4]) Дело C-553/07, *Rijkeboer*, EU:C:2009:293, точка 47; съединени дела C-293/12 и C-594/12, *Digital Rights Ireland и други*, EU:C:2014:238, точка 53; дело C-131/12, *Google Spain и Google*, EU:C:2014:317, точки 53, 66 и 74.

(5) Съгласно член 25, параграф 2 от Директива 95/46/ЕО нивото на защита на данните, осигурявано от трета държава, следва да се преценява като се вземат под внимание всички обстоятелства, свързани с операцията по предаването на данни или с набора от операции по предаване на данни, включително общите и секторните законови разпоредби, които са в сила във въпросната трета държава.

(6) В Решение 520/2000/ЕО на Комисията ([5]) беше прието, че по смисъла на член 25, параграф 2 от Директива 95/46/ЕО принципите за „сфера на неприкосновеност на личния живот“, прилагани в съответствие с насоките, предоставени с т.нар. „често задавани въпроси“, публикувани от Министерството на търговията на САЩ, осигуряват адекватно ниво на защита на личните данни, предавани от Съюза към организации, установени в Съединените американски щати.

(7) В своите съобщения COM(2013) 846 final ([6]) и COM(2013) 847 final от 27 ноември 2013 г. ([7]) Комисията счете, че основите на схемата за сфера на неприкосновеност на личния живот трябва да бъдат преразгледани и укрепени в контекста на редица фактори, сред които са значителното увеличаване на потоците от данни и изключителното значение на тези потоци за трансатлантическата икономика, бързото нарастване на броя на дружествата в САЩ, които се присъединяват към схемата за сфера на неприкосновеност на личния живот, и новата информация за мащабите и обхвата на някои разузнавателни програми на САЩ, която повдигна въпроси относно нивото на защита, което може да се гарантира. Наред с това, Комисията установи някои недостатъци и пропуски в схемата за сферата на неприкосновеност на личния живот.

(8) На основата на данните, събрани от Комисията, включително информация, получена в резултат от работата на Контактната група ЕС—САЩ по въпросите на защитата на личния живот ([8]), и информацията относно разузнавателните програми на САЩ, получена в Работната група *ad hoc* ЕС—САЩ ([9]), Комисията формулира 13 препоръки за преразглеждане на схемата за сфера на неприкосновеност на личния живот. Тези препоръки са съсредоточени върху укрепване на основните принципи за защита на личния живот, повишаване на прозрачността на политиките за неприкосновеност на личния живот, възприети от самосертифицираните дружества в САЩ, подобряване на осъществявания от органите на САЩ надзор и мониторинг за спазването на тези принципи и на налагането на тяхното спазване, наличието на механизми за разрешаване на спорове на достъпна цена и необходимостта да се гарантира, че изключението, свързано с националната сигурност, предвидено в Решение 2000/520/ЕО, ще бъде използвано само доколкото това е строго необходимо и пропорционално.

(9) В решението си от 6 октомври 2015 г. по дело C-362/14, *Maximillian Schrems c/y Data Protection Commissioner* ([10]), Съдът на Европейския съюз обяви Решение 2000/520/ЕО за невалидно. Без да анализира съдържанието на принципите за сфера на неприкосновеност на личния живот, Съдът счете, че в посоченото решение Комисията не е отбелязала, че Съединените американски щати ефективно „гарантират“ достатъчна степен на защита по силата на националното си законодателство или на международните си ангажименти ([11]).

(10) В тази връзка Съдът поясни, че въпреки че съдържащият се в член 25, параграф 6 от Директива 95/46/ЕО термин „достатъчна степен на защита“ не означава степен на защита, която е идентична на гарантираната в правния ред на ЕС, той трябва да се разбира в смисъл, че от третата държава се изисква да гарантира степен на защита на основните права и свободи, която „по същество е равностойна“ на гарантираната в Съюза по силата на Директива 95/46/ЕО, разглеждана във връзка с Хартата на основните права. Макар да е възможно средствата, до които третата държава прибягва в тази връзка, да са различни от прилаганите вътре в Съюза, все пак е необходимо на практика тези средства да се окажат ефективни ([12]).

(11) Съдът отправи критика относно липсата на достатъчно констатации в Решение 520/2000/ЕО относно наличието в Съединените американски щати на приети федерални правила за ограничаване на евентуалната намеса, засягаща основните права на лицата, чиито данни се прехвърлят от Съюза към САЩ, която намеса държавните структури на тази страна имат право да извършват, ако преследват законосъобразни цели, като например осигуряването на националната сигурност; той отправи също така критика относно липсата на достатъчно констатации относно наличието на ефективна правна защита срещу този вид намеса ([13]).

([5]) Решение 2000/520/ЕО на Комисията от 26 юли 2000 г. съгласно Директива 95/46/ЕО на Европейския парламент и на Съвета относно адекватността на защитата, гарантирана от принципите за „сфера на неприкосновеност на личния живот“ и свързаните с това често задавани въпроси, публикувани от Министерството на търговията на САЩ (ОВ L 215, 28.8.2000 г., стр. 7).

([6]) Съобщение на Комисията до Европейския парламент и Съвета „Възстановяване на доверието в обмена на данни между ЕС и САЩ“, COM (2013) 846 final от 27 ноември 2013 г.

([7]) Съобщение на Комисията до Европейския парламент и Съвета относно функционирането на „сферата на неприкосновеност на личния живот“ („Safe Harbour“) от гледна точка на гражданите на ЕС и дружествата, установени в ЕС, COM(2013) 847 final от 27 ноември 2013 г.

([8]) Вж. напр. Съвет на Европейския съюз, Окончателен доклад на контактната група на високо равнище ЕС—САЩ относно обмена на информация и защитата на неприкосновеността на личния живот и личните данни, документ № 9831/08 от 28 май 2008 г., достъпен на интернет адрес: http://www.europarl.europa.eu/document/activities/cont/201010/20101019ATT88359/20101019ATT88359EN.pdf.

([9]) Доклад относно констатациите на съпредседателите от ЕС на Работна група *ad hoc* ЕС—САЩ по защита на данните от 27 ноември 2013 г., достъпен на интернет адрес: http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf.

([10]) Вж. бележка под линия 3.

([11]) Делото *Schrems*, точка 97.

([12]) Делото *Schrems*, точки 73—74.

([13]) Делото *Schrems*, точки 88—89.

(12) През 2014 г. Комисията започна разговори с органите на САЩ с цел да бъде обсъдено укрепването на схемата за сферата на неприкосновеност на личния живот в съответствие с 13-те препоръки, съдържащи се в Съобщение COM(2013) 847 final. След постановяване на решението на Съда на Европейския съюз по делото *Schrems* тези преговори станаха по-интензивни, с цел да бъде намерено ново решение за адекватността, което да изпълнява изискванията на член 25 от Директива 95/46/ЕО според тълкуването, дадено от Съда. Резултат от тези дискусии са документите, които са включени като приложения към настоящото решение и също така ще бъдат публикувани във Федералния регистър на САЩ. Принципите на неприкосновеност на личния живот (приложение II), заедно с официалните писмени изявления и поети ангажименти на различни органи на САЩ, съдържащи се в документите в приложение I и приложения III до VII, съставляват Щита за личните данни в отношенията между ЕС и САЩ.

(13) Комисията направи внимателен анализ на американското законодателство и практиката на американските власти, включително на посочените официални писмени изявления и ангажименти. Въз основа на констатациите, развити в съображения 136—140, Комисията стигна до заключението, че Съединените американски щати гарантират адекватна степен на защита на личните данни, които се предават съгласно Щита за личните данни в отношенията между ЕС и САЩ от Съюза към самосертифицирани организации в САЩ.

2. **ЩИТ ЗА ЛИЧНИТЕ ДАННИ В ОТНОШЕНИЯТА МЕЖДУ ЕС И САЩ**

(14) Щитът за личните данни в отношенията между ЕС и САЩ се базира на система за самосертифициране, чрез която организациите в САЩ се ангажират да спазват един набор от принципи за неприкосновеност на личния живот — рамковите принципи на Щита за личните данни в отношенията между ЕС и САЩ, включително допълнителните принципи (наричани по-долу общо „Принципите“), — публикувани от Министерството на търговията на САЩ и посочени в приложение II към настоящото решение. Той се прилага за администраторите, както и за обработващите данни (представители), с особеността, че обработващите лични данни трябва да бъдат договорно обвързани да извършват действия само въз основа на указания от администратора от ЕС и да го подпомагат в изготвянето на отговори на лицата, упражняващи своите права по силата на Принципите ([14]).

(15) Без да се засяга спазването на националните разпоредби, приети съгласно Директива 95/46/ЕО, настоящото решение води до това, че са позволени предаванията от страна на администратор или на обработващ данни в Съюза към организации в САЩ, които са се самосертифицирали, че спазват Принципите пред Министерството на търговия и са поели ангажимент да се съобразяват с тях. Принципите се прилагат единствено за обработката на лични данни от организацията в САЩ, доколкото обработването от тези организации не попада в приложното поле на законодателството на Съюза ([15]). Щитът за личните данни не засяга прилагането на законодателството на ЕС, уреждащо обработването на лични данни в държавите членки ([16]).

([14]) Вж. приложение II, раздел III, точка 10, буква а). В съответствие с определението в раздел I.8.в. администраторът от ЕС ще определя целите и средствата за обработка на лични данни. Освен това в договора с представителя трябва да е ясно дали са позволени последващи предавания (вж. раздел III, точка 10, буква а), подточка ii) — 2.)

([15]) Това се прилага също така, когато от Съюза се предават данни за човешки ресурси в контекста на трудовото правоотношение. Докато в Принципите се подчертава „основната отговорност“ на работодателя в ЕС (вж. приложение II, раздел III, точка 9, буква г), подточка i)), те същевременно ясно показват, че поведението му ще бъде в обхвата на правилата, приложими в Съюза и/или съответната държава членка, а не Принципите. Вж. приложение II, раздел III, точка 9, буква а), подточка i), буква б), подточка ii), буква в), подточка i) и буква г), подточка i).

([16]) Това се прилага и за обработването, осъществявано посредством оборудване, намиращо се в Съюза, но използвано от организация, установена извън Съюза (вж. член 4, параграф 1, буква в) от Директива 95/46/ЕО). От 25 май 2018 г. Общият регламент относно защитата на данните (ОРЗД) ще се прилага за обработването на лични данни i) в контекста на дейностите на място на установяване на администратора или обработващия данни в Съюза (дори когато обработването се извършва в Съединените щати), или ii) на субекти на данни, които се намират в Съюза, от администратор или обработващ данни, който не е установен в Съюза, когато дейностите по обработване на данни са свързани със а) предлагането на стоки или услуги, независимо дали от субекта на данни се изисква плащане, на такива субекти на данни в Съюза; или б) наблюдението на тяхното поведение, доколкото това поведение се проявява в рамките на Европейския съюз. Вж. член 3, параграфи 1 и 2 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) (ОВ L 119, 4.5.2016 г., стр. 1).

(16) Защитата на личните данни, осигурявана от Щита на личните данни, се прилага за всеки субект на данни от ЕС ([17]), чиито лични данни се предават от Съюза на организации в САЩ, които са се самосертифицирали, че спазват Принципите пред Министерството на търговия

(17) Принципите се прилагат незабавно след сертифицирането. Едно изключение е свързано с принципа на отчетност за последващо предаване в случаите, в които организация, самосертифицираща се към Щита за личните данни, вече има предварително съществуващи търговски отношения с трети страни. Като се има предвид, че може да е необходимо време, за да се приведат тези търговски отношения в съответствие с приложимите правила съгласно Принципа на отчетност за последващо предаване, организацията ще бъде задължена да направи това във възможно най-кратък срок и във всеки случай не по-късно от девет месеца след самосертифицирането (при условие че то се осъществи в първите два месеца след деня, в който влиза в сила Щита за личните данни). По време на този преходен период организацията трябва да прилага принципа на уведомяването и на избора (като по този начин на субекта на данни се дава възможност за неучастие „opt out“), а в случаите, когато лични данни се предават на трета страна, изпълняваща функциите на представител, трябва да се гарантира, че последният осигурява поне същото ниво на защита, каквото се изисква от Принципите ([18]). Този преходен период осигурява разумен и подходящ баланс между зачитането на основното право на защита на данните и законната необходимост на предприятията да разполагат с достатъчно време, за да се приспособят към новата рамка, в която са зависими и от търговските си отношения с трети страни.

(18) Управлението и мониторингът на тази система ще се осъществяват от Министерството на търговията въз основа на ангажиментите, посочени в писмените изявления на министъра на търговията на САЩ (приложение I към настоящото решение). По отношение на принудителното изпълнение на Принципите на неприкосновеност на личния живот, Федералната търговска комисия (ФТК) и Министерството на транспорта са направили писмени изявления, включени съответно в приложения IV и V към настоящото решение.

2.1. *Принципи на неприкосновеност на личния живот*

(19) Като част от самосертифицирането им съгласно Щита за личните данни в отношенията между ЕС и САЩ, организациите трябва да се ангажират да спазват Принципите на неприкосновеност на личния живот ([19]).

(20) Съгласно принципа „*Уведомяване*“ организациите са задължени да предоставят информация на субектите на данните относно редица ключови елементи във връзка с обработването на техните лични данни (напр. вида на събираните данни, целта на обработването, правата на достъп и избор, условията за последващо предаване и отговорност за причинени вреди). Прилагат се и допълнителни защитни мерки, по-специално изискването организациите да оповестяват публично своите политики в областта на неприкосновеността на личния живот (отразяващи Принципите) и да предоставят електронни препратки към уебсайта на Министерството на търговията (с допълнителна информация относно самосертифицирането, правата на субектите на данните и наличните механизми за защита), списъка към Щита за личните данни (разгледан в съображение 30) и към уебсайта на подходяща организация за алтернативно разрешаване на спорове.

(21) Съгласно принципа „*Пълнота на данните и ограничаване в рамките на целта*“ личните данни трябва да бъдат ограничени до необходимото за целите, за които се обработват, да са надеждни за предвиденото им използване, точни, пълни и актуални. Никоя организация не може да обработва лични данни по начин несъвместим с целите, за които те са били събрани първоначално или за които по-късно е получено разрешение от субекта на данните. Организациите трябва да се гарантира, че личните данни са надеждни за предвиденото им използване, точни, пълни и актуални.

([17]) Настоящото решение има значение за ЕИП. В Споразумението за Европейското икономическо пространство (Споразумение за ЕИП) се предвижда разширяването на вътрешния пазар на Европейския съюз за трите държави от ЕИП — Исландия, Лихтенщайн и Норвегия. Законодателството за защита на данните на Съюза, включително Директива 95/46/ЕО, попада в обхвата на Споразумението за ЕИП и е включено в приложение XI към него. Съвместният комитет на ЕИП следва да вземе решение за включването на настоящото решение в Споразумението за ЕИП. След като настоящото решение започне да се прилага по отношение на Исландия, Лихтенщайн и Норвегия, Щитът за личните данни в отношенията между ЕС и САЩ ще обхване и тези три държави и позоваванията в пакета за Щита за личните данни на ЕС и на държавите—членки на ЕС, се четат като включващи Исландия, Лихтенщайн и Норвегия.

([18]) Вж. приложение II, раздел III.6.e.

([19]) За данните относно човешки ресурси, събирани в контекста на трудовите правоотношения, се прилагат специални правила за осигуряване на допълнителна защита, както е посочено в допълнителния принцип „Данни за човешки ресурси“ от Принципите на неприкосновеност на личния живот (вж. приложение II, раздел III.9). Например работодателите трябва да вземат предвид предпочитанията на заетите лица, що се отнася до неприкосновеността на личния им живот, като ограничават достъпа до личните данни, анонимизират някои от тях, или ги кодират или псевдонимизират. Най-важното е, че от организациите се изисква да си сътрудничат с органите по защита на данните на Съюза и да спазват техните препоръки по отношение на този вид данни.

(22) Когато нова (променена) цел се различава съществено от — но е все още съвместима със — първоначалната цел, принципът „*Избор*“ предоставя на субектите на данни правото на възражение (клауза за неучастие „opt out“). Принципът „*Избор*“ не замества изричната забрана за несъвместимо обработване ([20]). Специалните правила, които по принцип дават възможност за неучастие „по всяко време“ от използването на личните данни, се прилагат за целите на прекия маркетинг ([21]). Когато става дума за чувствителни данни, организациите трябва по принцип да получат утвърдителното изрично съгласие („opt in“) на субекта на данните.

(23) Все още съгласно принципа *Цялост на данните и ограничаване в рамките на целта* личната информация може да се съхранява под форма, която идентифицира или позволява идентифицирането на физическите лица (и по този начин — под формата на лични данни), само доколкото това служи на целта(ите), за която(които) е била събрана първоначално или за която(които) по-късно е дадено разрешение от физическото лице. Това задължение не възпрепятства организациите — участници в Щита за личните данни, да продължат да обработват лична информация за по-дълги периоди, но само в рамките на срок и доколкото тази обработка служи за една от следните конкретни цели: архивиране от обществен интерес, журналистика, литература и изкуства, научни и исторически проучвания или статистически анализ. По-продължителното съхраняване на лични данни за една от тези цели ще подлежи на гаранциите, които се осигуряват от Принципите.

(24) Съгласно принципа „*Сигурност*“ организациите, които създават, поддържат, използват или разпространяват лични данни, трябва да вземат „разумни и подходящи“ предпазни мерки като отчитат рисковете, свързани с обработването, както и характера на данните. Когато обработването се извършва от подизпълнител, организациите трябва да сключат договор с него, който да гарантира същото ниво на защита, което се осигурява от Принципите, и да предприемат мерки да гарантират, че договорът се изпълнява правилно.

(25) Съгласно принципа „*Достъп*“ ([22]) субектите на данните имат правото без да е необходимо обосноваване и срещу такса, която не е прекомерна, да получат от дадена организация потвърждение дали тя обработва лични данни, свързани с тях, и съответните данни да им бъдат съобщени в рамките на разумен срок. Това право може да бъде ограничавано само при изключителни обстоятелства; всеки отказ или всяко ограничаване на правото на достъп трябва да бъдат необходими и надлежно обосновани, като организацията носи тежестта на доказване, че тези изисквания са спазени. Субектите на данни трябва да могат да коригират, изменят или заличават лична информация, когато тя е неточна или се обработва в нарушение на Принципите. В правото на САЩ са предвидени специални средства за защита срещу неблагоприятни решения ([23]) в областите, в които е най-вероятно дружествата да прибягват до автоматизирано обработване на личните данни с цел вземане на решения, засягащи физическите лица (напр. при предоставяне на заеми, оферти за ипотечни кредити, в сферата на заетостта). В тези актове обикновено се предвижда правото на физическите лица да бъдат информирани за конкретните причини в основата на дадено решение (напр. при отказ на кредит), да оспорват непълна или неточна информация (както и използването на неправомерни фактори), както и да потърсят правна защита. Тези правила предлагат защита в по-скоро ограничения брой на случаите, в които автоматизираните решения ще се вземат от самата организация — участник в Щита за личните данни ([24]). Въпреки това предвид нарастващото използване в съвременната цифрова икономика на автоматизирано обработване (включително профилиране) като основа за вземане на решения, засягащи физическите лица, това е една област, която трябва да се следи внимателно. С цел да се улесни този мониторинг, с органите на САЩ беше договорено, че в първия годишен преглед, както и в последващите прегледи, ако е необходимо, ще бъде включен диалог относно автоматизираното вземане на решения, включително обмен на сходства и различия в подхода на ЕС и на САЩ в това отношение.

([20]) Това се отнася до всяко предаване на данни съгласно Щита на личните данни, включително когато те се отнасят до данни, събрани посредством трудово правоотношение. Въпреки че самосертифицираните организации в САЩ може по принцип може да използват данните за човешки ресурси за цели различни от целите, свързани с трудовоправните отношения (напр. за определени маркетингови съобщения), те трябва да спазват забраната за несъвместима обработка, като освен това могат да правят това само в съответствие с принципите „*Уведомяване*“ и „*Избор*“. Забраната на американската организация да предприема наказателни действия срещу даден служител при упражняването на такъв избор, включително всяко ограничаване на възможностите за заетост, ще гарантира, че въпреки връзката на подчиненост и свързаната с нея зависимост служителят няма да бъде подлаган на натиск и по този начин може да упражнява истински свободен избор.

([21]) Вж. приложение II, раздел III.12.

([22]) Вж. също така допълнителния принцип „Достъп“ (приложение II, раздел III, точка 8).

([23]) Вж. напр. Закон за равните възможности за кредитиране (Equal Credit Opportunity Act (ECOA), 15 U.S.C. 1691 и следв.), Закон за оповестяване на информация за кредити (Fair Credit Reporting Act (FRCA), 15 USC § 1681 и следв.) или Закон за справедливото жилищно настаняване (Fair Housing Act (FHA), 42 U.S.C. 3601 и следв.).

([24]) В контекста на прехвърлянето на лични данни, събирани в ЕС, договорното правоотношение с физическото лице (клиент), в повечето случаи ще бъде със — и следователно всяко решение въз основа на автоматизирано обработване обикновено ще се взема от — администратора от ЕС, който следва да се подчинява на правилата на ЕС за защита на данните. Това включва сценариите, при които обработването се извършва от организация — участник в Щита за личните данни, изпълняваща функциите на представител от името на администратора от ЕС.

(26) Съгласно принципа „*Защита, прилагане и отговорност за причинени вреди*“ ([25]) участващите организации трябва да предвидят солидни механизми да гарантират спазването на останалите Принципи на неприкосновеност на личния живот, както и право на защита за субектите на данни от ЕС, чиито лични данни се обработват в нарушение на тези принципи, включително и ефективни средства за правна защита. След като една организация е решила доброволно да се самосертифицира ([26]) съгласно Щита за личните данни в отношенията между ЕС и САЩ, ефективното спазване на Принципите на неприкосновеност на личния живот е задължително за нея. За да ѝ бъде позволено да продължи да се ползва от Щита за личните данни за получаване на лични данни от Съюза, тази организация трябва ежегодно да пресертифицира своето участие в очертаната рамка. Организациите трябва също така да предприемат мерки за извършване на проверка ([27]) дали публикуваните от тях политики в областта на неприкосновеността на личния живот съответстват на Принципите на неприкосновеност на личния живот и дали се спазват реално. Това може да става или посредством система за самооценка, която трябва да включва вътрешни процедури, чрез които да се гарантира, че служителите получават подготовка за прилагането на политиките на организацията в областта на неприкосновеността на личния живот и че периодично се извършва обективен преглед на спазването, или посредством външни проверки за спазването, сред чиито методи може да се включат методите на одитиране или случайни проверки. Освен това организацията трябва да създаде ефективен механизъм за защита, чрез който да се разглеждат жалбите (в тази връзка вж. също съображение 43), и да подлежи на правомощията по разследване и прилагане на ФТК, Министерството на транспорта или друг законоустановен орган, който гарантира за ефективното спазване на Принципите.

(27) За така наречените „последващи предавания“, т.е. предавания на лични данни от организация към трета страна администратор или обработващ данни, независимо дали те се намират в Съединените американски щати или в трета държава извън Съединените американски щати (и Съюза), се прилагат специални правила. Целта на тези правила е осигурят, че няма да бъде подкопана защитата на личните данни на субектите на данни от ЕС и че тя не може да бъде заобиколена чрез прехвърлянето им на трети страни. Това е от особено значение при по-сложните процеси на обработване, които са характерни за съвременната цифрова икономика.

(28) Съгласно принципа *Отчетност за последващото предаване* ([28]) последващо предаване може да се осъществи само i) с ограничена и конкретна цел, ii) въз основа на договор (или подобно споразумение в рамките на дадена корпоративна група ([29])) и iii) само ако в този договор се предвижда същото ниво на защита като тази, гарантирана от Принципите, включващи изискването, че тяхното прилагане може да бъде ограничено само до необходимата степен с оглед на спазване на изискванията за националната сигурност, правоприлагането и други цели от обществен интерес ([30]). Това следва да се разглежда във връзка с принципа *Уведомяване*, а в случай на последващо предаване на администратор на трета страна ([31]) — с принципа *Избор*, според който субектите на данни трябва да бъдат информирани (наред с другото) относно вида/идентичността на всеки получател на трета страна, относно целта на последващото предаване, относно предлагания избор, както и да имат право на възражение (клауза за неучастие „opt out“) или в случай на чувствителни данни да трябва да дадат утвърждаващо изрично съгласие („opt in“) за последващите предавания. С оглед на принципа *Цялост на данните и ограничаване в рамките на целта* задължението да се осигурява същата степен на защита, която се гарантира от Принципите, предполага, че третата страна може да обработва предадената ѝ лична информация само за цели, които не са несъвместими с целите, за които е била събрана първоначално или за които по-късно е дадено разрешение от физическото лице.

(29) Задължението да се осигурява същата степен на защита, която се изисква от Принципите, се прилага за всяка една и за всички трети страни, участващи в обработката на данните, прехвърляни независимо от тяхното местоположение (в САЩ или в друга трета държава), както и в случая, когато първоначалният получател на третата страна предава тези данни на друг получател на третата страна, например за целите на обработване от подизпълнител. Във всички случаи в договора с получателя на третата страна трябва да се предвижда последният да уведоми организацията — участник в Щита за личните данни, ако организацията констатира, че вече не е в състояние да изпълнява посоченото задължение. Когато тази констатация е направена, третата страна администратор ще прекрати обработката и ще трябва да се предприемат други обосновани и съответни мерки за справяне с

([25]) Вж. също така допълнителния принцип „Разрешаване на спорове и прилагане“ (приложение II, раздел III, точка11).
([26]) Вж. също така допълнителния принцип „Самосертифициране“ (приложение II, раздел III, точка 6).
([27]) Вж. също така допълнителния принцип „Проверка“ (приложение II, раздел III, точка 7).
([28]) Вж. също така допълнителния принцип „Задължителни договори за последващите предавания“ (приложение II, раздел III, точка 10).
([29]) Вж. допълнителния принцип „Задължителни договори за последващите предавания“ (приложение II, раздел III, точка 10, буква б). Въпреки че този принцип дава възможност предаванията да се основават също на извъндоговорни инструменти (напр. вътрешно-групови програми за спазване и контро), в текста се пояснява, че тези инструменти винаги трябва да „гарантират непрекъснатост на защитата на личната информация съгласно Принципите на Щита за личните данни“. Освен това предвид това, че самосертифицираните организации в САЩ ще продължат да бъдат отговорни за спазването на Принципите, ще има силен стимул да се използват инструменти, които наистина са ефективни на практика.
([30]) Вж. приложение II, раздел I, точка 5.
([31]) Физическите лица няма да имат право на клаузата за неучастие в случаите, когато личните данни се предават на трета страна, изпълняваща функциите на представител за осъществяване на задачи от името на и съгласно указанията на организацията в САЩ. За това обаче е необходим договор с представителя и организацията в САЩ ще поеме отговорността да гарантира защитата, предоставена по силата на Принципите, като упражни правомощията си за даване на указания.

положението ([32]). При възникване на проблеми със спазването на този принцип по веригата на обработване или при обработване от подизпълнител, организацията — участник в Щита за личните данни, изпълняваща функциите на администратор на личните данни, ще трябва да докаже, че не носи отговорност за събитието, породило вредата, като в противен случай носи отговорност за причинените вреди, както е посочено в принципа „*Защита, прилагане и отговорност за причинени вреди*“. В случай на последващо предаване към трета страна посредник ([33]) се прилага допълнителна защита.

2.2. *Прозрачност, управление и надзор на Щита за личните данни в отношенията между ЕС и САЩ*

(30) В Щита за личните данни в отношенията между ЕС и САЩ се предвиждат механизми за надзор и за прилагане, за да се проверява и гарантира, че самосертифицираните организации в САЩ спазват Принципите и че се отстранява всяко неспазване. Тези механизми са посочени в Принципите (приложение II) и в ангажиментите, поети от Министерството на търговията (приложение I), ФТК (приложение IV) и Министерството на транспорта (приложение V).

(31) За да се гарантира правилното прилагане на Щита за личните данни в отношенията между ЕС и САЩ, заинтересованите страни, като например субектите на данни, износителите на данни и националните органи по защита на данните (ОЗД), трябва да бъдат в състояние да идентифицират организациите, които се придържат към Принципите. За тази цел Министерството на търговията е поело задължението да поддържа и предостави за публичен достъп списък на организациите, които са се самосертифицирали, че спазват Принципите, и които са от компетентността на поне един от правоприлагащите органи, включени в приложения I и II към настоящото решение („списък към Щита за личните данни“) ([34]). Министерството на търговията ще актуализира списъка въз основа на ежегодно подаваните заявления за пресертифициране и при всяко оттегляне или заличаване на дадена организация от Щита за личните данни в отношенията между ЕС и САЩ. Освен това той ще поддържа и предоставя за публичен достъп официален списък на организациите, които са били заличени от списъка, с посочване на причините за заличаването за всеки отделен случай. И накрая, Министерството на търговията ще предостави електронна връзка към списъка на казусите, свързани с Щита за личните данни, с които е сезирана Федералната търговска комисия, който списък се поддържа на уебсайта на ФТК.

(32) Министерството на търговията ще предостави за публичен достъп списъка към Щита за личните данни и подадената от организациите информация за самосертифициране на създаден за тази цел уебсайт. Самосертифицираните организации на свой ред трябва да предоставят интернет адреса на министерството за списъка към Щита за личните данни. Освен това, когато политиката на една организация в областта на неприкосновеността на личния живот е на разположение онлайн, в нея трябва да се предостави хипервръзка към уебсайта на Щита за личните данни, както и хипервръзка към уебсайта или към формуляра за подаване на жалба на независимия механизъм за защита, който е на разположение за разглеждане на нерешени жалби. Министерството на търговията системно ще проверява, в контекста на сертифицирането и пресертифицирането на дадена организация към очертаната рамка, дали нейните политики в областта на неприкосновеността на личния живот са съобразени с Принципите.

(33) Организации, които трайно не се съобразяват с Принципите, се заличават от списъка към Щита за личните данни и трябва да върнат или заличат личните данни, които са получили в рамките на Щита за личните данни в отношенията между ЕС и САЩ. В други случаи на заличаване от списъка, като например доброволно оттегляне от участие или неподаване на заявление за пресетифициране, организациите могат да запазят тези данни, ако ежегодно уверяват Министерството на търговията в ангажираността си да продължат да прилагат Принципите или предоставят адекватна защита на личните данни посредством други разрешени средства (напр. като използват договор, в който изцяло са отразени изискванията на съответните одобрени от Комисията стандартни договорни клаузи). В този случай организацията посочва лице за връзка с нея по всички въпроси от областта на Щита за личните данни.

(34) Освен това Министерството на търговията ще наблюдава организациите, които вече не участват в Щита за личните данни в отношенията между ЕС и САЩ поради доброволно оттегляне или изтичане на сертифицирането, за да провери дали те ще върнат, заличат или задържат ([35]) личните данни, които са получили преди това съгласно прилагането на рамката. Ако те задържат посочените данни, организациите са задължени да продължат да

([32]) Положението е различно в зависимост от това дали третата страна е администратор или обработващ данни (представител). При първия сценарий в договора с третата страна трябва да е предвидено тя да прекрати обработката и да предприеме други обосновани и съответни мерки за справяне с положението. При втория сценарий посочените мерки се вземат от организацията — участник в Щита за личните данни, като администратор на обработването, под чиито указания действа представителят.

([33]) В такъв случай организацията в САЩ трябва при уведомяване да предприеме обосновани и съответни мерки, i) за да гарантира, че представителят ефективно обработва предадената лична информация по начин, който съответства на задълженията на организацията съгласно Принципите; и ii) да преустановят и отстранят последиците от неразрешено обработване.

([34]) Информация относно управлението на личния живот щит списък може да бъде намерена в приложение I и приложение II (раздел I, точка 3, раздел I, точка 4, раздел III, точка 6, буква г) и раздел III, точка 11, буква ж).

([35]) Вж. приложение II, раздел I, точка 3, раздел III, точка 6, буква е) и раздел III, точка 11, буква ж), подточка i).

прилагат Принципите спрямо тях. В случаите, когато Министерството на търговията отстрани организации от рамката поради трайно неспазване на Принципите, то ще гарантира, че тези организации задължително ще върнат или заличат личните данни, които са получили съгласно нейното прилагане.

(35) Когато по някаква причина една организация напусне Щита за личните данни в отношенията между ЕС и САЩ, тя трябва да оттегли всички свои публични изявления, предполагащи, че тя продължава да участва в Щита за личните данни в отношенията между ЕС и САЩ или че се ползва от предимствата на такова участие, по-специално всички упоменавания на Щита за личните данни в отношенията между ЕС и САЩ в публикуваната от нея политика в областта на неприкосновеността на личния живот. Министерството на търговията ще търси неправомерни твърдения за участие в рамката, включително на бивши членове, и ще намира решения ([36]). Всяко погрешно представяне пред широката общественост относно придържането на организацията към Принципите може да подлежи на санкциониране от ФТК, Министерство на транспорта или друг съответен правоприлагащ орган в САЩ; въвеждането в заблуждение на Министерството на търговията подлежи на санкциониране по Закона за неверните твърдения (False Statements Act) (18 U.S.C. § 1001) ([37]).

(36) Министерството на търговията ще осъществява *служебно* наблюдение за евентуални неверни твърдения за участие в Щита за личните данни или за неправомерно използване на сертификационния знак на Щита за личните данни, като ОЗД могат да насочват организациите за проверка към определеното лице за контакт в министерството. Когато една организация се оттегли от Щита за личните данни в отношенията между ЕС и САЩ, не подаде заявление за пресертифициране или бъде заличена от списъка към Щита за личните данни, Министерството на търговията ще проверява периодично дали тя е изтрила от публикациите относно политиката ѝ в областта на неприкосновеността на личния живот всички упоменавания на Щита за личните данни, които може да водят до заключението, че тя продължава да участва в него, и ако тя продължава да прави неверни твърдения, ще отнася въпроса за разглеждане от ФТК, Министерството на транспорта или друг компетентен орган, който да предприеме евентуални действия по санкциониране. Освен това Министерството на търговията ще изпраща въпросници до организациите, чието самосертифициране изтича или които доброволно са се оттеглили от Щита за личните данни в отношенията между ЕС и САЩ, за да провери дали организацията ще започне отново да участва, или ще се отпише или ще продължи да прилага Принципите на неприкосновеност на личния живот за личните данни, които е получила докато е участвала, и ако възнамерява да задържи личните данни, да провери кой в рамките на организацията ще служи за лице за постоянен контакт по въпросите на Щита за личните данни.

(37) Министерството на търговията текущо ще извършва *служебни* прегледи ([38]) за спазването от страна на самосертифицираните организации, включително чрез изпращане на подробни въпросници. Също така той системно ще извършва проверки, когато е получил конкретна жалба (със сериозен характер), когато дадена организация не предоставя задоволителни отговори на запитванията от негова страна или когато има достоверни доказателства, че може да се предполага, че дадена организация не спазва Принципите. Когато е целесъобразно, Министерство на търговията ще се консултира и с ОЗД за такива прегледи на спазването.

2.3. *Механизми за защита, разглеждане на жалби и прилагане*

(38) В принципа „*Защита, прилагане и отговорност за причинени вреди*“ на Щита за личните данни в отношенията между ЕС и САЩ се съдържа изискването организациите да осигуряват защита за физическите лица, които са засегнати от неспазване, и по този начин се дава възможност на субектите на данни от ЕС да подават жалби относно неспазване от страна на самосертифицираните дружества в САЩ и тези жалби да бъдат разрешени, ако е необходимо чрез решение за предоставяне на ефективна правна защита.

(39) Като част от своята декларация за самосертифициране, организациите трябва да отговарят на изискванията на принципа „Защита, прилагане и отговорност за причинени вреди“, като предоставят ефективни и леснодостъпни независими механизми за подаване на жалби, чрез които жалбите и споровете на лицето могат да се разследват и разрешават бързо без разходи за лицето.

(40) Организациите могат да изберат независими механизми за защита в Съюза или в Съединените американски щати. Това включва възможността доброволно да се ангажират да си сътрудничат с ОЗД в ЕС. Този избор обаче не е

([36]) Вж. приложение I, раздел „Търси неверни твърдения за участие и намира решения“.
([37]) Вж. приложение II, раздел III, раздел 6, буква з) и раздел III, точка 11, буква е).
([38]) Вж. приложение I.

налице, когато обработват данни относно човешките ресурси, тъй като сътрудничеството с ОЗД е задължително. Другите алтернативи включват независимото Извънсъдебно разрешаване на спорове (ИРС) и разработените за сектора *програми на неприкосновеност на личния живот за личните данни*, в чиито правила са залегнали Принципите на неприкосновеност на личния живот. Последните трябва да включват ефективни механизми за прилагането им в съответствие с изискванията на принципа „Защита, прилагане и отговорност за причинени вреди“. Организациите са задължени да отстраняват проблеми, свързани с неспазване. Те трябва също така да посочат, че те са предмет на правомощията за разследване и правоприлагане на ФТК, Министерство на транспорта на САЩ или други оправомощени законоустановени орган.

(41) Следователно рамката на Щита за личните данни на неприкосновеността на личния живот предвижда редица възможности за субектите на данните гаранция да упражняват правата си, да подават жалби относно неспазване от страна на самосертифицираните дружества в САЩ и техните жалби да се разрешават, ако е необходимо, чрез решение за предоставяне на ефективна правна защита. Физическите лица могат да предявят жалба директно пред организация, независим орган за решаване на спорове, посочен от организацията, националните ОЗД или ФТК.

(42) В случаите, когато техните жалби не са били разрешени чрез нито един от тези механизми за защита и правоприлагане, физическите лица имат също така право да поискат въпросът да бъде решен чрез правно обвързващ арбитраж съгласно панела на ОЗД (Приложение 1 към приложение II към настоящото решение). С изключение на арбитражния панел, при който има изискването някои средства за правна защита да бъдат изчерпани, преди да бъде използван, физическите лица имат право да упражняват някои или всички механизми за правна защита по свой избор и не са задължени да избират определен механизъм или да спазват определена последователност. Съществува обаче определен логически ред, който е препоръчително да се следва, както е посочено по-долу.

(43) На първо място субектите на данни от ЕС могат да преследват нарушения на спазването на Принципите чрез преки контакти със *самосертифицираното дружество в САЩ*. За да се улесни решаването на споровете, организацията трябва да създаде ефективен механизъм за защита, чрез който да се разглеждат жалбите. Това означава в политиката ѝ в областта на неприкосновеността на личния живот да се предоставя ясна информация на физическите лица за звеното за връзка, независимо дали в рамките на организацията или извън нея, което отговаря за разглеждането на жалбите (включително съответна организация в Съюза, която може да отговаря на запитвания или оплаквания), както и за независимите механизми за разглеждане на жалби.

(44) При получаване на жалба от физическо лице — директно от лицето или чрез Министерството на търговията след сезиране от ОЗД, организацията трябва да предостави отговор на субекта на данните от ЕС в срок 45 дни. В този отговор трябва да се прави преценка по същество на жалбата и да се предоставя информация как организацията ще разреши проблема. Освен това от организациите се изисква да реагират своевременно на запитвания и други искания за информация от ([39]) Министерството на търговията или от орган за защита на данните (когато организацията е ангажирана да си сътрудничи с органа за защита на личните данни) във връзка с придържането им към принципите. Организациите трябва да съхраняват документацията си за прилагане на техните политики за защита на личните данни и да ги предоставят при поискване на независим механизъм за защита или ФТК (или друг орган на САЩ, компетентен да разследва нелоялните и измамни практики) в рамките на дадено разследване или жалба за неспазване.

(45) На второ място организациите трябва да определят *независим орган за разрешаване на спорове* (в Съединените американски щати или в Съюза), който да разследва и разрешава отделните жалби (освен ако те са очевидно необосновани или нямат сериозен характер) и да предоставя безплатно подходяща защита за физическите лица. Санкциите и средствата за правна защита, налагани от този орган, трябва да са достатъчно строги, за да гарантират спазването от организациите на Принципите и да осигуряват отстраняване или поправка от страна на организацията на последиците от неспазването на Принципите, а в зависимост от обстоятелствата — и преустановяване на последващото обработване на въпросните лични данни и/или тяхното заличаване, както и публично оповестяване на констатациите за неспазването. От определените от организацията независими органи за разрешаване на спорове ще бъде изисквано да включват на своите публични уебсайтове съответна информация относно Щита за личните данни в отношенията между ЕС и САЩ и услугите, които извършват съгласно него. Те трябва да публикуват ежегодно годишен доклад с обобщена статистическа информация относно тези услуги ([40]).

([39]) Това е органа, разглеждащ жалбите, определен от панел на ОЗД, предвиден в допълнителния принцип „Ролята на органите по защита на данните“ (приложение II, раздел III, точка 5).

([40]) В годишния доклад трябва да бъдат включени: 1) общият брой на получените през отчетната година жалби във връзка с Щита за личните данни в отношенията между ЕС и САЩ; 2) видът на получените жалби; 3) качествени показатели за решаването на спора, напр. времето за обработването на жалбите; и 4) изходният резултат от получените жалби, а именно броят и видовете средства за правна защита или санкции, които са били наложени.

(46) Министерството на търговията ще проверява също и дали самосертифицираните дружества в САЩ действително са регистрирани към независимите механизми за защита, към които са заявили, че са регистрирани. От организациите и от отговорните независими механизми за защита се изисква да отговарят в кратки срокове на запитвания и искания за информация от страна на Министерството на търговията във връзка с Щита за личните данни.

(47) В случай, че организацията не спази решението на орган по разрешаване на спорове или на саморегулиращ се орган, последният трябва да уведоми за това Министерството на търговията и ФТК (или друг орган на САЩ, компетентен да разследва нелоялни и измамни практики) или компетентния съд ([41]). Ако дадена организация отказва да изпълнява окончателното решение на саморегулираща се организация в областта на неприкосновеността на личния живот, или независим орган по решаване на спорове или на държавен орган, или когато даден орган констатира, че организация често нарушава Принципите, това ще се счита за трайно неспазване. Вследствие на това, след като първо е изпратило на организацията нарушител тридесет дневно предизвестие и е дало възможност за отговор, Министерството на търговията ще заличи организацията от списъка ([42]). Ако след заличаването от списъка организацията продължава да твърди, че е сертифицирана съгласно Щита за личните данни, министерството ще отнесе въпроса пред ФТК или друга правоприлагаща агенция ([43]).

(48) Трето, физическите лица могат да отнесат жалбите си до национален *орган за защита на данните*. Организациите са длъжни да сътрудничат при разследването и разрешаването на жалба от ОЗД или когато става въпрос за обработването на данни за човешките ресурси, събрани в рамките на трудово правоотношение, или когато съответната организация доброволно се е подложила на надзор от страна на органите за защита на данните. По-специално организациите трябва да отговарят на запитвания, да спазват препоръките на ОЗД, включително за корективни или компенсаторни мерки, и да предоставят на ОЗД писмено потвърждение, че са взети такива мерки.

(49) Препоръките на ОЗД ще се предоставят чрез неформален панел на ОЗД, създаден на европейско равнище ([44]), който ще спомага също така за осигуряването на хармонизиран и съгласуван подход. Препоръки ще се дават след като и двете страни по спора са имали подходяща възможност да представят своите забележки и евентуално своите доказателства. Съответният панел на ОЗД ще предоставя препоръките си в най-кратки срокове, доколкото го позволява изискването за справедлив процес, и по принцип най-късно в срок от 60 дни считано от получаването на жалбата. Ако някоя организация не изпълни препоръката в срок от 25 дни след предоставянето ѝ, без да посочи убедително обяснение за закъснението, групата на ОЗД ще оповести намерението си да отнесе въпроса пред ФТК (или друг орган на САЩ, компетентен да предприема действия за принудително изпълнение) или да заключи, че е допуснато сериозно нарушение на ангажимента за сътрудничество. При първия вариант това може да доведе до предприемане на действие по принудително изпълнение съгласно раздел 5 от Закона за Федералната търговска комисия (или други сходни закони). При втория вариант групата ще информира Министерството на търговията, което ще счете отказа на организацията за трайно неспазване на Принципите, в резултат на което тази организация ще бъде заличена от списъка към Щита за личните данни.

(50) Във всички разгледани случаи, ако ОЗД, до който е адресирана жалбата, не предприеме никакви действия или действията са недостатъчни за разрешаване на жалбата, жалбоподателят има възможността да заведе иск срещу това (без)действие в националните съдилища на съответната държава членка.

(51) Освен това физическите лица могат да подават жалби до ОЗД, дори когато за решаване на спорове не е бил определен панел на ОЗД. В тези случаи органът за защита на данните може да отнася такива жалби пред Министерството на търговията или ФТК. За да улесни съвместната работа, Министерството на търговията ще създаде специализирано звено за контакт, което да служи за връзка и да съдейства при запитвания от ОЗД относно спазването от страна на дадена организация на Принципите на неприкосновеност на личния живот ([45]). По същия начин ФТК се е ангажирала да създаде специализирано звено за контакт ([46]) и оказва на ОЗД съдействие чрез разследвания по реда на Закона за безопасен интернет на САЩ (U.S. SAFE WEB Act) ([47]).

([41]) Вж. приложение II, раздел 11, буква д).
([42]) Вж. приложение II, раздел III, точка 11, буква ж), и по-специално подточки ii) и iii).
([43]) Вж. приложение I, раздел „Търси неверни твърдения за участие и намира решения“.
([44]) Правилникът за дейността на неформалната група на ОЗД следва да бъде определен от ОЗД въз основа на правомощието им да организират работата си и да си сътрудничат помежду си.
([45]) Вж. приложение I, раздели относно „Засилване на сътрудничеството с ОЗД“и „улесняване разрешаването на жалби относно неспазване“ и приложение II, раздел II, точка 7, буква д).
([46]) Вж. приложение IV, стр. 6.
([47]) *ibid*.

(52) Четвърто, *Министерството на търговията* се е ангажирало да получава и разглежда жалби относно неспазването на Принципите от дадена организация, както и да полага всички възможни усилия да ги разрешава. За тази цел Министерството на търговията предвижда специални процедури за отнасянето на жалбите от страна на ОЗД до определеното звено за връзка и за проследяването им, както и последващи действия съвместно с дружествата за улесняване на разрешаването. За да се ускори обработването на отделните жалби, звеното за връзка ще си сътрудничи директно със съответния ОЗД по въпросите относно спазването на Принципите, и по специално ще го уведомява за етапа на разглеждане на жалбите в срок до 90 дни след сезирането му. Това позволява на субектите на данни да подават жалби относно неспазването на Принципите от самосертифицираните дружества в САЩ директно до своя национален ОЗД, след което тези жалби ще бъдат насочвани към Министерството на търговията, като органът в САЩ, управляващ Щита за личните данни в отношенията между ЕС и САЩ. Също така Министерството на търговията се ангажира да предоставя при годишния преглед на функционирането на Щита за личните данни в отношенията между ЕС и САЩ доклад, в който да бъдат анализирани в обобщен вид жалбите, получени от него всяка година ([48]).

(53) Когато въз основа на *служебните* си проверки, жалби или друга информация, Министерството на търговията стигне до заключението, че дадена организация трайно не спазва Принципите на неприкосновеност на личния живот, то я заличава от списъка към Щита за личните данни. Отказът да се съобрази с окончателно решение на който и да е саморегулиращ се орган, независима инстанция за разрешаване на спорове или правителствен орган, с компетентност в областта на неприкосновеността на личния живот, включително ОЗД, ще бъде считан за трайно неспазване на Принципите.

(54) На пето място, организацията — участник в Щита за личните данни, трябва да бъде предмет на правомощията за разследване и прилагане от органите на САЩ, и по-специално *Федералната комисия за търговия* ([49]), които ефективно ще гарантират спазването на Принципите. На четвърто място Федералната търговска комисия ще разглежда с предимство случаи на неспазване на Принципите на неприкосновеност на личния живот, за които е била сезирана от независими инстанции за разрешаване на спорове или от саморегулиращи се органи, от Министерството на търговията и ОЗД (по тяхна собствена инициатива или след получени жалби), за да определи дали са нарушени изискванията на раздел 5 от Закона за Федералната търговска комисия (FTC Act) относно забраната за нелоялни или измамни практики ([50]). ФТК се е ангажирала да създаде стандартен процес на сезиране, да определи звено за връзка в нея за сезиранията от страна на ОЗД и да обменя информация относно случаите, за които е била сезирана. В допълнение тя ще приема жалби директно от физически лица и ще предприема разследвания във връзка с Щита за личните данни по своя собствена инициатива, по-специално като част от по-мащабни нейни разследвания по въпроси относно неприкосновеността на личния живот.

(55) ФТК може да налага спазването на Принципите посредством административни заповеди („заповеди за съгласие“) и ще провежда системен мониторинг за изпълнението на такива заповеди. Когато организациите не ги изпълняват, ФТК може да сезира компетентен съд, с цел налагането на граждански санкции и други средства за правна защита, включително за причинени вреди в резултат на неправомерно поведение. Като алтернативна мярка ФТК може да иска налагане на временна или постоянна съдебна възбрана или други средства за правна защита от федерален съд. Всяка заповед за съгласие с адресат организация — участник в Щита за личните данни, ще включва разпоредби за доброволно докладване ([51]), а от организациите ще се изисква да обявяват публично всички релевантни и свързани с Щита за личните данни части от евентуален доклад или оценка за спазването, представени на ФТК. И накрая, ФТК ще поддържа онлайн списък на дружествата, по отношение на които са били издадени заповеди от ФТК или съдебни разпореждания по казуси, свързани с Щита за личните данни.

(56) На шесто място, като механизъм за защита, който е последна възможност, в случай че жалбата на лицето не е получила удовлетворително решение посредством останалите налични средства за правна защита, субектът на данни от ЕС може да поиска въпросът да бъде решен чрез правно обвързващ арбитраж от „Специалната група по Щита за личните данни“ (*Privacy Shield Panel*). Организациите трябва да информират физическите лица за възможността им при определени условия да използват правно обвързващ арбитраж, както и са длъжни да реагират, след като дадено физическо лице е използвало тази възможност, като е изпратило уведомление на съответната организация ([52]).

([48]) Вж. приложение I, раздел „Съдейства за разрешаването на жалби за неспазване“.

([49]) Организация — участник в Щита за личните данни, трябва да обяви публично задължението си да спазва Принципите, да оповестява публично своите политики за неприкосновеността на личния живот и да ги прилага изцяло. Неспазването подлежи на принудително изпълнение съгласно раздел 5 от Закона за Федералната търговска комисия, който забранява нелоялните и измамни практики в търговията или засягащи търговията.

([50]) Според информация от ФТК, тя няма правомощия да извършва проверки на място в областта на защитата на неприкосновеността на личния живот. Той обаче има правомощието да задължи организациите да представят документи и да предоставят свидетелски показания (вж. раздел 20 от FTC), и може да използва съдебната система за принудително изпълнение на такива заповеди в случай на неспазване.

([51]) Със заповеди на ФТК или съдебни разпореждания може да се изиска от дружествата да прилагат програми за неприкосновеността на личния живот и редовно да предоставят на ФТК доклади за спазването на тези програми или оценки от независима трета страна.

([52]) Вж. приложение II, раздел II, точка 1, подточка xi) и раздел III, точка 7, буква б).

(57) Групата включва резерв от най-малко 20 арбитри, определени от Министерството на търговията и от Комисията въз основа на тяхната независимост, почтеност и опита им със законодателството на САЩ в областта на неприкосновеността на личния живот и законодателството на ЕС в областта на защитата на данните. За всеки индивидуален спор страните ще избират от тази група състав от един или трима ([53]) арбитри. Производството ще се ръководи от стандартни правила за арбитраж, които предстои да бъдат договорени между Министерството на търговията и Комисията. Тези правила ще допълнят вече приключената рамка, която съдържа няколко характеристики, подсилващи достъпността на този механизъм за субектите на данни в ЕС: i) при подготвянето на иск пред панела субектът на данни може да получи съдействие от своя национален ОЗД; ii) Тъй като арбитражът ще се провежда в Съединените американски щати, субектите на данни от ЕС могат да изберат да участват чрез видео- или телефонна конферентна връзка, която ще се осигурява безплатно за лицата. iii) въпреки, че езикът, използван в хода на арбитража, е по правило английски, устният превод в хода на арбитражното изслушване обикновено ([54]) ще бъде осигурен въз основа на мотивирано искане от страна на субекта на данните без разходи; iv) И накрая, докато всяка от страните трябва да поеме за своя сметка разходите за хонорара на своя адвокат, ако се представлява от такъв пред арбитражния състав, Министерството на търговията ще създаде фонд, който ще се захранва от годишни вноски на организациите — участници в Щита за личните данни, от който ще бъдат покривани допустимите разходи по арбитражната процедура до един максимален размер, който ще бъде определен от органите на САЩ в консултация с Комисията.

(58) Специалната група по Щита за личните данни ще има правомощия да предписва „специфични за конкретния случай непарични безпристрастни мерки“ ([55]), необходими като корективно действие срещу неспазването на Принципите. Въпреки че при постановяване на решението си специалната група ще взема предвид другите средства за правна защита, получени в рамките на механизмите съгласно Щита за личните данни, физическите лица все пак могат да използват арбитраж, ако счетат тези средства за недостатъчни. Това ще позволи на субектите на данни от ЕС да инициират арбитражно дело във всички случаи, когато в резултат от действие или бездействие от страна на компетентните органи на САЩ (например ФТК) не са получили удовлетворително решение по жалбата. Не може да се инициира арбитражно дело, ако ОЗД разполага със законови правомощия да разреши въпросната жалба срещу самосертифицирано дружество в САЩ, по-специално когато организацията е задължена да съдейства и да спазва препоръките на ОЗД във връзка с обработването на данни за човешки ресурси, събрани в контекста на трудово правоотношение, или доброволно се е ангажирала да направи това.

(59) Седмо, когато една организация не спазва ангажимента си да съблюдава Принципите и обявената от нея политика в областта на неприкосновеността на личния живот, по силата на законодателството на отделните щати в САЩ може да има допълнителни възможности за съдебна защита, които осигуряват средства за правна защита при причинени вреди и в случаи на въвеждане в заблуда с цел измама, нелоялни или измамни действия или практики, или нарушаване на договор.

(60) Освен това, когато при получаване на искане от субект на данни на ЕС ОЗР счете, че прехвърлянето на лични данни на физическо лице към организация в САЩ се извършва в нарушение на законодателството на ЕС за защита на данните, включително когато установеният в ЕС износител на данни има причини да смята, че организацията не се съобразява с Принципите, той може също така да упражнява правомощията си по отношение на износителя на данни и, ако е необходимо, да разпореди спиране на прехвърлянето на данни.

(61) Предвид информацията в настоящия раздел Комисията счита, че Принципите, публикувани от Министерството на търговията на САЩ, като цяло осигуряват степен на защита на личните данни, която е равностойна по същество на гарантираното от основните принципи, установени в Директива 95/46/ЕО.

(62) В допълнение към това ефективното прилагане на Принципите на неприкосновеност на личния живот е гарантирано от задълженията за прозрачност и управлението на Щита за личните данни от страна на Министерството на търговията.

(63) Освен това Комисията счита, че взети заедно механизмите за надзор и защита, предвидени съгласно Щита за личните данни, позволяват нарушенията на Принципите на неприкосновеност на личния живот от организациите — участници в Щита за личните данни, да бъдат установявани и наказвани на практика и осигуряват средства за правна защита на субектите на данни, с възможност за достъп до свързаните с тях лични данни и евентуалното коригиране или заличаване на тези данни.

([53]) Броят на арбитрите в специалната група ще бъде договорен между страните.

([54]) Арбитражният състав може да счете обаче, че при обстоятелствата на конкретното арбитражно дело покриването на разноските би довело до необосновани или непропорционални разходи.

([55]) Физическите лица не могат да предявяват иск за вреди в арбитражно дело, но от друга страна инициирането на арбитражно дело не изключва възможността да се поиска обезщетение за вреди в обикновените съдилища на САЩ.

3. ДОСТЪП И ИЗПОЛЗВАНЕ НА ЛИЧНИ ДАННИ, ПРЕДАВАНИ СЪГЛАСНО ЩИТА ЗА ЛИЧНИТЕ ДАННИ В ОТНОШЕНИЯТА МЕЖДУ ЕС И САЩ, ОТ ПУБЛИЧНИТЕ ОРГАНИ НА САЩ

(64) Съгласно приложение II, точка I.5, спазването на Принципите се ограничава до степента, в която това е необходимо, за да бъдат спазени изискванията в областта на националната сигурност, обществения интерес или правоприлагането.

(65) Комисията направи оценка на ограниченията и гаранциите, които са предвидени в правото на САЩ във връзка с достъпа и използването на лични данни, предавани съгласно Щита за личните данни в отношенията между ЕС и САЩ, от публичните органи на САЩ за целите на националната сигурност, правоприлагането и за други цели от обществен интерес. Освен това правителството на САЩ, чрез Службата на директора на Националното разузнаване (Office of the Director of National Intelligence (ODNI) ([56]), предостави на Комисията подробни писмени изявления и ангажименти, които са поместени в приложение VI към настоящото решение. С писмо, подписано от Държавния секретар и приложено като приложение III към настоящото решение, правителството на САЩ се ангажира също така да създаде нов механизъм за надзор относно намесата за целите на националната сигурност — омбудсман към Щита за личните данни, който е независим от разузнавателните структури. И накрая, в писмено изявление на Министерството на правосъдието на САЩ, поместено в приложение VII към настоящото решение, са разгледани ограниченията и гаранциите, които се прилагат спрямо достъпа и използването на данни от страна на публичните органи за целите на правоприлагането и за други цели от обществен интерес. За да се повиши прозрачността и да се отрази правният характер на тези ангажименти, всеки от посочените и приложени към настоящото решение документи ще бъде публикуван във Федералния регистър на САЩ.

(66) По-долу са разгледани по-подробно констатациите на Комисията относно ограниченията спрямо достъпа и използването от страна на публичните органи на САЩ на лични данни, предадени от Европейския съюз към Съединените американски щати, и наличието на ефективна правна защита.

3.1. *Достъп и използване от публични органи на САЩ за целите на националната сигурност*

(67) Анализът на Комисията показва, че в правото на САЩ се съдържат редица ограничения спрямо достъпа и използването за целите на националната сигурност на лични данни, които се предават съгласно Щита за личните данни в отношенията между ЕС и САЩ, както и механизми за надзор и правна защита, които осигуряват достатъчно гаранции за ефективната защита на тези данни срещу незаконна намеса и рискове от злоупотреби ([57]). От 2013 г. насам, когато Комисията публикува своите две съобщения (вж. съображение 7), тази правна рамка е била значително подсилена, както е описано по-долу.

3.1.1. Ограничения

(68) Съгласно конституцията на САЩ гарантирането на националната сигурност е в правомощията на Президента, в качеството му на върховен главнокомандващ, върховен изпълнителен орган, а по отношение на външното разузнаване — и ръководител на външната политика на САЩ ([58]). Докато Конгресът има правомощията да налага ограничения и е правил това по различни въпроси, в обхвата на така наложените граници Президентът може да направлява дейността на разузнавателните структури на САЩ, по-специално чрез издаване на изпълнителни декрети и президентски директиви. Това се прилага, разбира се, също и за онези области, в които не се осъществява ръководство от Конгреса. Понастоящем двата главни правни инструмента в тази връзка са Изпълнителен декрет 12333 ([59]) и Президентска изпълнителна директива 28.

([56]) Директорът на Националното разузнаване (DNI) изпълнява задълженията на ръководител на разузнавателните структури и функцията на главен съветник на президента и на Националния съвет за сигурност. Вж. Закон за реформа на разузнаването и предотвратяване на тероризма (Intelligence Reform and Terrorism Prevention Act) от 2004 г., публ. L. 108-458 от 17.12.2004 г. Наред с останалото ODNI определя изискванията към определянето на задачите, събирането, анализа, получаването и разпространението на национална разузнавателна информация от страна на разузнавателните структури и ги управлява и насочва, включително чрез разработване на насоки за начините на достъп, използване и споделяне на информация или разузнавателни данни. Вж. раздел 1.3, букви a) и b) от Изпълнителен декрет 12333.

([57]) Вж. *делото Schrems*, точка 91.

([58]) Конституция на САЩ, член II. Вж. също въведението към ПИД-28.

([59]) Изпълнителен декрет 12333: Разузнавателна дейност на Съединените американски щати, Федерален регистър том 40, № 235 (8 декември 1981 г.). Доколкото този изпълнителен декрет е обществено достъпен, той определя целите, насоките, задълженията и отговорностите на разузнавателните усилия на САЩ (включително ролята на различни разузнавателни структури) и установява общите параметри за провеждането на разузнавателната дейност (по-специално необходимостта да се издават конкретни процедурни правила). Съгласно раздел 3.2 от Изпълнителен декрет 12333 Президентът, с подкрепата на Националния съвет за сигурност, и директорът на Националното разузнаване издават укази, процедури и насоки в изпълнение на декрета.

(69) Президентска изпълнителна директива 28 (ПИД-28), издадена на 17 януари 2014 г., налага редица ограничения за операциите по „радиоелектронно разузнаване“ ([60]). Президентските директиви имат задължителна сила за разузнавателните органи на САЩ ([61]) и остават в сила и след промени в администрацията на САЩ ([62]). ПИД-28 е особено важна за лицата, които не са американски граждани, включително за субектите на данни от ЕС. Наред с останалото, в нея се предвижда, че:

а) събирането на радиоелектронна разузнавателна информация трябва да се основава на законови разпоредби или на разрешение от Президента и трябва да се осъществява съобразно с Конституцията на САЩ (по-специално четвъртата поправка) и правото на САЩ;

б) всички лица следва да се третират по достоен начин и с уважение, независимо от тяхното гражданство или местопребиваването им;

в) всички лица имат законни интереси за неприкосновеност на личния живот при обработването на тяхна лична информация;

г) неприкосновеността на личния живот и гражданските свободи следва да бъдат неразделна част от съображенията при планирането на дейностите на радиоелектронното разузнаване на САЩ;

д) следователно дейностите на радиоелектронното разузнаване на САЩ трябва да включват подходящи гаранции за личната информация на всички физически лица, независимо от тяхното гражданство или местопребиваването им.

(70) В ПИД-28 е указано, че радиоелектронна разузнавателна информация може да се събира единствено с цел разузнаването или контраразузнаването да спомага за изпълнението на задания, изпълнявани от национални и министерски органи, но не и с някаква друга цел (напр. за осигуряване на конкурентно предимство на американски дружества). Съгласно тези писмени изявления разузнавателните структури „следва да изискват събирането да бъде съсредоточено върху конкретни разузнавателни обекти или теми, доколкото това е практически възможно, като за целта се използват разграничителни критерии (*напр*. конкретни технически средства, условия за подбор и идентификатори).“ ([63]) Освен това в писмените изявления на ODNI се дават уверения, че вземането на решенията относно „практическата осъществимост“ не се оставя на отделни служители на разузнаването, а е предмет на политики и процедури, които различните разузнавателни структури (агенции) на САЩ трябва да въведат в изпълнение на ПИД-28 ([64]). Също така търсенето и определянето на подходящи критерии за подбор се осъществяват в обхвата на цялостната Рамка на приоритетите в националното разузнаване (National Intelligence Priorities Framework) (NIPF), с която се гарантира, че приоритетите в разузнаването се определят от отговорни за политическите решения лица на високо равнище и редовно се преразглеждат, с цел да може да се реагира на реалните заплахи за националната сигурност, като се отчитат възможните рискове, включително рисковете за неприкосновеността на личния живот ([65]). На тази основа служителите в агенциите търсят и определят конкретни условия за подбор, с които се очаква да бъде събирана разузнавателна информация, отговаряща на приоритетите ([66]). Критериите за подбор трябва редовно да бъдат преразглеждани, за да се проверява дали чрез тях все още се осигурява ценна разузнавателна информация в съответствие с приоритетите ([67]).

([60]) Съгласно Изпълнителен декрет 12333 директорът на Агенцията за национална сигурност (АНС) управлява функционално радиоелектронното разузнаване и ръководи единна организация за дейностите на радиоелектронното разузнаване.

([61]) За определението на понятието „разузнавателни структури“ вж. раздел 3.5, буква h) от Изпълнителен декрет 12333, заедно с бележка под линия 1 от ПИД-28.

([62]) Вж. меморандума на Службата на правния съветник към Министерството на правосъдието до президента Клинтън от 29 януари 2000 г. Съгласно това правно становище президентските директиви имат „същото материално правно действие като изпълнителните декрети“.

([63]) Писмени изявления на ODNI (приложение VI), стр. 3.

([64]) Вж. раздел 4, букви б) и в) от ПИД-28. Според публично обявената информация с прегледа за 2015 г. са потвърдени текущите шест цели. Вж. Реформа на радиоелектронното разузнаване, доклад за напредъка за 2016 г. на ODNI.

([65]) Писмени изявления на ODNI (приложение VI), стр. 6 (във връзка с Директивата за разузнавателните структури 204 (Intelligence Community Directive 204). Виж също раздел 3 от ПИД-28.

([66]) Писмени изявления на ODNI (приложение VI), стр. 6. Вж. напр. Защита на гражданските свободи и неприкосновеността на личния живот за целеви дейности на радиоелектронното разузнаване (SIGINT) съгласно Изпълнителен декрет 12333, 7 октомври 2014 г. на Агенцията за национална сигурност (АНС), Служба за гражданските свободи и неприкосновеността на личния живот (NSA Civil Liberties and Privacy Office (NSA CLPO). Вж. също доклада за състоянието на ODNI за 2014 г. За заявки за достъп съгласно раздел 702 от Закона за упражняване на надзор върху външното разузнаване (Foreign Intelligence Surveillance Act (FISA) запитванията се извършват съгласно процедурите за свеждане до минимум, одобрени от Съда по надзора върху външното разузнаване (Foreign Intelligence Surveillance Court (FISC). Вж. Изпълнение от страна на АНС на раздел 702 от Закона за упражняване на надзор върху външното разузнаване от 16 април 2014 г., на Службата за гражданските свободи и неприкосновеността на личния живот към АНС.

([67]) Вж. Реформа на радиоелектронното разузнаване, юбилеен годишен доклад за 2015 г. Вж. също писмените изявления на ODNI (приложение VI), стр. 6, 8-9, 11.

(71) Освен това предвидените в ПИБ-28 изисквания събирането на разузнавателна информация винаги ([68]) да бъде „съобразено с конкретния случай, доколкото това е практически възможно“ и разузнавателните структури да дават предимство на наличието на друга информация и подходящи и осъществими алтернативи, отразяват общото правило ([69]) за определяне на приоритетите на целевото събиране на масиви от данни пред масовото събиране на масиви от данни. В съответствие с гаранциите, предоставени от ODNI, те гарантират по-специално, че събирането на масиви от данни не е нито „масово“, нито „безогледно“, и че изключението не отменя правилото ([70]).

(72) Въпреки че в ПИД-28 се пояснява, че при определени обстоятелства понякога се налага разузнавателните структури да извършват събиране на масиви от данни при радиоелектронното разузнаване, например за да бъдат идентифицирани нови или възникващи заплахи, в директивата се дават указания на тези структури да отдават приоритет на алтернативни възможности, които биха позволили провеждането на целево радиоелектронно разузнаване ([71]). От това следва, че събирането на масиви от данни ще се осъществява само когато целенасоченото събиране чрез използване на разграничителни критерии — т.е. идентификатор, свързан с конкретния обект на разузнаване (като например негов електронен адрес или телефонен номер) — не е възможно „по технически или оперативни съображения“ ([72]). Това се прилага както за начина, по който се събира радиоелектронна разузнавателна информация, така и за това, което реално се събира ([72]).

(73) Съгласно писмените изявления на ODNI, дори когато разузнавателните структури не могат да използват конкретни идентификатори за целево събиране, те ще се стремят към ограничаване на събирането „във възможно най-голяма степен“. За да се гарантира това, че тя „прилагат филтри и други технически средства за съсредоточаване на събирането до онези съоръжения, за които има вероятност да съдържат комуникации със стойност за външното разузнаване“ (и следователно ще отговарят на изискванията, формулирани от създателите на политики на САЩ съгласно процеса, обяснен в по-горе в съображение 70). Вследствие на това към събирането на масиви от данни ще се подходи по поне два начина: Първо, то винаги ще се отнася до конкретни цели на външното разузнаване (напр. за придобиване на радиоелектронна разузнавателна информация относно дейностите на терористична група, която действа в даден регион) и ще бъде съсредоточено върху съобщения, които имат такава връзка. Съгласно гаранцията, осигурена от ODNI, това е отразено във факта, че „радиоелектронните разузнавателни дейности на Съединените американски щати САЩ обхващат само много малка част от комуникациите, преминаващи по интернет“ ([73]). Второ, в писмените изявления на ODNI е обяснено, че филтрите и другите технически средства ще бъдат проектирани така, че събирането да е концентрирано „възможно най-точно“, за да се гарантира, че ще се сведе до минимум количеството на събираната „нерелевантна информация“.

(74) И накрая, дори когато Съединените американски щати считат за необходимо да събират обща радиоелектронна разузнавателна информация при условията, посочени в съображения 70—73, ПИД-28 ограничава използването на такава информация до един конкретен списък с шест цели на националната сигурност, за да бъдат защитени неприкосновеността на личния живот и гражданските свободи на всички лица, независимо от тяхното гражданство и местопребиваване ([74]). Тези разрешени цели включват мерки за откриване и противодействие на заплахи, произтичащи от шпионска дейност, тероризъм, оръжия за масово унищожение, заплахи за киберсигурността, отправени към въоръжените сили или военни служители, както и заплахи от презгранична престъпна дейност,

([68]) Вж. писмените изявления на ODNI (приложение VI), стр. 3.

([69]) Следва също да се отбележи, че съгласно раздел 2.4 от Изпълнителен декрет 12333 елементите на разузнавателните структури „следва да използват на територията на Съединените щати техники на събиране, които са с най-малка намеса, доколкото това е практически осъществимо“. По отношение на ограниченията за заместването на цялото събиране на масиви от данни с целенасочено събиране, вж. резултатите от оценката от Националния съвет за научни изследвания по данни на Агенцията на Европейския съюз за основните права, Надзор от страна на разузнавателните служби: Гаранции и правни средства за защита на основните права в ЕС (2015 г.) на стр. 15—16.

([70]) Писмени изявления на ODNI (приложение VI), стр. 4.

([71]) Виж също раздел 5, буква d) от ПИД-28, в който се дават указания на директора на Националното разузнаване, в координация с ръководителите на съответните разузнавателни структури и Службата за научна и технологична политика (Office of Science and Technology Policy), да предоставят на президента „доклад с оценка на практическата осъществимост относно създаването на софтуер, с който да се позволи на разузнавателните структури по-лесно да извършват целево придобиване на информация, вместо събиране на масиви от данни“. Съгласно публично обявената информация заключението от този доклад е, че „не съществува софтуерно базирана алтернативна възможност, която да позволява да бъде заместено изцяло събирането на масиви от данни при откриването на някои заплахи за националната сигурност“. Вж. Реформа на радиоелектронното разузнаване, юбилеен годишен доклад за 2015 г.

([72]) Вж. бележка под линия 68.

([73]) Писмени изявления на ODNI (приложение VI). Това отговаря в частност на загрижеността, изразена от националните органи за защита на данните в тяхното становище по проекта на решение относно адекватността. Вж. становище 01/2016 на работната група по защита на данните по член 29 относно проекта на решение за адекватността на Щита за личните данни в отношенията между ЕС и САЩ (прието на 13 април 2016 г.), стр. 38, № 47.

([74]) Вж. раздел 2 от ПИД-28.

свързана с другите пет цели, като поне веднъж годишно се извършва преглед на тези цели. Съгласно писмените изявления на правителството на САЩ разузнавателните структури са укрепили своите аналитични практики и стандарти за първичен анализ на непотвърдена радиоелектронна разузнавателна информация с цел да отговорят на тези изисквания; използването на целеви първични анализи „е гаранция, че за задълбочено проучване от анализаторите се предава само тази информация, за която може да се счита, че има потенциална разузнавателна стойност“ ([75]).

(75) Тези ограничения са особено релевантни за предаването на лични данни съгласно Щита за личните данни в отношенията между ЕС и САЩ, по-специално когато събирането на лични данни се осъществява извън територията на Съединените американски щати, включително по време на преноса им по трансатлантическите кабелопроводи от Съюза до САЩ. Както беше потвърдено от органите на САЩ в писмените изявления на ODNI, посочените в тях ограничения и гаранции, включително по силата на ПИД-28, се прилагат за този вид събиране ([76]).

(76) Въпреки че не са формулирани със същата правна терминология, тези принципи отразяват същността на принципите на необходимост и пропорционалност. Отдава се ясен приоритет на целевото събиране, докато събирането на масиви от данни е ограничено до (изключителни) случаи, когато целевото не е възможно по технически или оперативни причини. Дори когато не може да се избегне *събиране на масиви от данни*, последващото „използване“ на такива данни чрез достъп е *строго ограничено* до конкретни правомерни цели на националната сигурност ([77]).

(77) В качеството на директива издадена от Президента като главен изпълнителен орган, тези изисквания са обвързващи за всички разузнавателни структури и са въведени с допълнителни правила и процедури на агенциите, с които общите принципи са транспонирани в конкретни указания за всекидневната работа. Освен това Конгресът, за който указ ПИД-28 няма обвързваща сила, също е предприел стъпки за гарантиране, че събирането и достъпът до лични данни в Съединените американски щати стават целенасочено, а не се извършват на „общо основание“.

(78) От наличната информация, включително писмените изявления, получени от правителството на САЩ, следва че след като данните са предадени на организации, установени в Съединените щати и самосертифицирани съгласно Щита за личните данни в отношенията между ЕС и САЩ, разузнавателните агенции на САЩ могат да поискат лични данни само ([78]) когато техните искания са съобразени със Закона за упражняване на надзор върху външното разузнаване (ЗУНВР) (Foreign Intelligence Surveillance Act (FISA)) или са отправени от Федералното бюро за разследвания (ФБР) въз основа на т.нар. писмо във връзка с националната сигурност (ПНС) (National Security Letter (NSL) ([79]). Съгласно ЗУНВР има няколко правни основания, които могат да бъдат използвани за събиране (и последващо обработване) на лични данни на субекти на данни от ЕС, предадени съгласно Щита за личните данни

([75]) Писмени изявления на ODNI (приложение VI), стр. 4. Вж. също Директива за разузнавателните структури № 203 (Intelligence Community Directive 203).

([76]) Писмени изявления на ODNI (приложение VI), стр. 2. По същия начин се прилагат и ограниченията, установени с Изпълнителен декрет 12333 (напр. необходимостта събраната информация да отговаря на определените от Президента приоритети на разузнаването).

([77]) Вж. *делото Schrems*, точка 93.

([78]) В допълнение към това събирането на данни от ФБР може да се основава също така и на разрешения, издавани за целите на правоприлагането (вж. раздел 3.2 от настоящото решение).

([79]) За допълнителни пояснения относно използването на писма във връзка с националната сигурност (ПНС) вж. писмените изявления на ODNI (приложение VI), стр. 13—14 с бел. под линия 38. Както е посочено там, ФБР може да използва писма във връзка с националната сигурност (ПНС) само при искания за несъдържателна информация във връзка с разрешено разследване в сферата на националната сигурност за защита срещу международния тероризъм или секретни разузнавателни дейности. По отношение на предаванията на данни съгласно Щита за личните данни в отношенията между ЕС и САЩ най-релевантното правно основание за разрешаване изглежда е Законът за неприкосновеност на електронните съобщения (Electronic Communications Privacy Act) (18 U.S.C. § 2709), съгласно който се изисква всяко искане за информация за абонат или за справка за операции да съдържа „понятие, което определя по специфичен начин дадено лице, субект, телефонен номер или сметка“.

в отношенията между ЕС и САЩ. Освен раздел 402 от ЗУНВР ([80]), отнасящ се за традиционното индивидуализирано електронно наблюдение, и раздел 402 от ЗУНВР ([81]), отнасящ се за инсталирането на електронни устройства за регистриране или проследяване, двата главни инструмента са раздел 501 от ЗУНВР (предишен раздел 215 от Закона за обединяване и укрепване на САЩ (U.S. PATRIOT ACT) и раздел 702 от ЗУНВР ([82]).

(79) В тази връзка със Закона за свободата в САЩ (*USA FREEDOM Act*), който влезе с сила на 2 юни 2015 г., се забранява общо събиране на данни на основание раздел 402 от ЗНЧРС (електронни устройства за регистриране или проследяване), раздел 501 от ЗНЧРС (предишен: раздел 215 от Закона за обединяване и укрепване на САЩ (U.S. PATRIOT ACT)) ([83]) и с използване на писма във връзка с националната сигурност (ПНС), а вместо това се определя изискване за използване на конкретни „критерии за избор“ ([84]).

(80) Въпреки че в Закона за упражняване на надзор върху външното разузнаване (ЗУНВР) се съдържат допълнителни правни основания за разрешаване на провеждането на дейности на националното разузнаване, включително на радиоелектронното разузнаване, оценката на Комисията показва, че доколкото се отнася за лични данни, предавани съгласно Щита за личните данни в отношенията между ЕС и САЩ, тези правни основания също така и ограничават намесата на органите на публична власт в целенасоченото събиране и достъп.

(81) Това е ясно що се отнася до традиционното индивидуализирано електронно наблюдение съгласно раздел 104 от ЗУНВР ([85]). Доколкото се отнася до раздел 702 от ЗУНВР, в който са предвидени основанията за две важни разузнавателни програми, по които работят разузнавателните агенции на САЩ (PRISM и UPSTREAM), търсенията се извършват целево чрез използване на индивидуални критерии за подбор, които служат за идентифициране на конкретни технически средства за връзка, като например адрес на електронна поща или телефонен номер на целта, но не и ключови думи, нито дори имена на лицата, към които е насочено търсенето ([86]). Следователно, както отбелязва Надзорният съвет по въпросите на неприкосновеността на личния живот и гражданските свободи (Privacy and Civil Liberties Oversight Board (PCLOB), наблюденията по раздел 702 „се изразяват изцяло в

([80]) 50 U.S.C., § 1804. Докато този правен инструмент изисква „обявяване на фактите и обстоятелствата, на които се основава заявителят за обосноваване на своето убеждение, че А) целта на електронното наблюдение е чужда сила или служител на чужда сила“, последното може да се отнася за лица, които не са американски граждани и участват в международен тероризъм или в международно разпространение на оръжия за масово унищожение (включително в подготвителни действия) (50 U.S.C. § 1801 (b)(1)). Все пак съществува само теоретична връзка с личните данни, предавани съгласно Щита за личните данни в отношенията между ЕС и САЩ, предвид това, че обявяването на фактите трябва също така да обосновава убеждението, че „всяко от средствата или местата, към които е насочено електронното наблюдение, се използва или предстои да бъде използвано от чужда сила или служител на чужда сила“. Във всички случаи позоваването на този инструмент налага да се подаде заявление до Съда по надзора върху външното разузнаване (СНВР), който ще направи преценка, наред с останалото, дали въз основа на посочените факти съществува вероятна причина случаят наистина да е такъв.

([81]) 50 U.S.C. § 1842 заедно с § 1841(2) и раздел 3127 от дял 18. Този инструмент не се отнася за съдържанието на съобщенията, а по-скоро има за цел получаването на информация за клиента или абоната, който използва дадена услуга (напр. име, адрес, абонатен номер, продължителност/вид на получената услуга, източник/механизъм на плащане). За целта се изисква да се подаде заявление за издаване на разпореждане до Съда по надзора върху външното разузнаване (СНВР) (или до магистрат към окръжен съд (U.S. Magistrate Judge) и да се използва специален критерий за подбор по смисъла на § 1841(4), т.е. понятие, което определя по специфичен начин дадено лице, сметка и др. и се използва за ограничаване в максимално възможната разумна степен на обхвата на исканата информация.

([82]) Докато с раздел 501 от ЗУНВР (предишен раздел 215 от Закона за обединяване и укрепване на САЩ) се дават правомощия на ФБР да иска съдебно разпореждане с цел получаването на „материални вещи“ (по-специално телефонни метаданни, както и търговски справки) за цели във връзка с чуждото разузнаване, в раздел 702 от ЗУНВР на разузнавателните структури на САЩ се разрешава да искат достъп до информация, включително съдържание на съобщения в интернет, на територията на Съединените щати, но по отношение на лица, които не са американски граждани и се намират извън Съединените щати.

([83]) На основание тази разпоредба ФБР може да отправя искане за „материални носители“ (напр. записи, хартиени носители, документи), ако докаже пред Съда по надзора върху външното разузнаване (СНВР), че са налице разумни основания да се счита, че те са релевантни за целите на конкретно разследване на ФБР. При извършване на търсенето си ФБР трябва да използва одобрени от Съда по надзора върху външното разузнаване критерии за подбор, за които са налице „основателни и доказуеми подозрения“, че са свързани с една или няколко чужди сили или техни служители, участващи в международен тероризъм или в подготвителни действия за такъв. Виж доклад на Надзорния съвет по въпросите на неприкосновеността на личния живот и гражданските свободи, раздел 215, стр. 59; Служба за гражданските свободи и неприкосновеността на личния живот на АНС, Доклад за прозрачност: Закон за свободата в САЩ, търговски регистър, в изпълнение на ЗУНВР, 15 януари 2016 г., стр. 4—6.

([84]) Писмени изявления на ODNI (приложение VI), стр. 13 (бел. под линия 38).

([85]) Вж. бележка под линия 81.

([86]) Доклад на Надзорния съвет по въпросите на неприкосновеността на личния живот и гражданските свободи, раздел 702, стр. 32—33 с допълнителни препратки. Според службата по въпросите на неприкосновеността на личния живот на АНС тази агенция трябва да удостовери, че е налице връзка между целта и критерия за подбор, да документира външноразузнавателна информация, които се очаква да бъдат получени, данните трябва да бъдат разгледани и одобрени от двама старши анализатори на АНС и целият процес да бъде проследен с цел последващи прегледи за съответствие от страна на ODNI и Министерството на правосъдието. Вж. Изпълнение от страна на АНС на раздел 702 от ЗУНВР от 16 април 2014 г. на Службата за гражданските свободи и неприкосновеността на личния живот към АНС.

целенасочено разследване на конкретни лица [които не са американски граждани], за които е направено индивидуализирано определяне“ ([87]). Поради клаузата за изтичане на срока на действие, през 2017 г. ще трябва да се направи преглед на раздел 702 от ЗУНВР, като по същото време Комисията ще трябва отново да направи преценка относно гаранциите, които са налице за субектите на данни от ЕС.

(82) Освен това в своите писмени изявления правителството на САЩ даде на Европейската комисия изрични уверения, че разузнавателните структури на САЩ „не извършват безразборно наблюдение на който и да било, включително на обикновени европейски граждани“ ([88]). По отношение на личните данни, събирани на територията на Съединените щати, това изявление е придружено с емпирични доказателства, които показват, че *исканията за достъп* чрез писма във връзка с националната сигурност (ПНС) и по силата на ЗУНВР, поотделно и взети заедно, се отнасят само за относително малък брой цели, в сравнение с целия поток от информация по интернет ([89]).

(83) По отношение на *достъпа* до събраните данни и *сигурността на данните* в ПИД-28 е установено изискване достъпът да „бъде ограничен само до упълномощения персонал, за който е необходимо да разполага с информацията, за да осъществи мисията си“ и личната информация „да се обработва и съхранява при условия, осигуряващи адекватна защита и възпрепятстващи достъпа на неоправомощени лица, които са съвместими с гаранциите, приложими за чувствителната информация“. Разузнавателният персонал преминава през съответно подходящо обучение относно установените в ПИД-28 принципи ([90]).

(84) И накрая, по отношение на *съхранението* и последващото *разпространение* на лични данни на субекти на данни от ЕС, събрани от разузнавателните органи на САЩ, в ПИД-28 се посочва, че всички лица (включително лицата, които не са граждани на САЩ) следва да бъдат третирани по достоен начин и с уважение, че всички лица имат легитимни интереси за неприкосновеност на личния живот при обработването на тяхна лична информация, и че следователно разузнавателните структури трябва да възприемат политики, осигуряващи подходящи гаранции за такива данни, „които са разумно проектирани да свеждат до минимум [тяхното] разпространение[то] и запазване[то]“ ([91]).

([87]) Доклад на Надзорния съвет по въпросите на неприкосновеността на личния живот и гражданските свободи, раздел 702, стр. 111. Вж. също писмените изявления на ODNI (приложение VI), стр. 9. („Събирането по силата на раздел 702 от [ЗУНВР] не е „масово и безразборно“, а тясно съсредоточено върху събирането на разузнавателни данни за индивидуално идентифицирани законни цели“) и стр. 13, бел. под линия 36 (във връзка със становище на Съда по надзора върху външното разузнаване от 2014 г.); Доклад на Надзорния съвет по въпросите на неприкосновеността на личния живот и гражданските свободи на АНС: Изпълнение от страна на АНС на раздел 702 от Закона за упражняване на надзор върху външното разузнаване от 16 април 2014 г. Дори в случая на програмата UPSTREAM АНС може да изисква само прихващане на електронните съобщения до, от, или за определените за задачата критерии за подбор.

([88]) Писмени изявления на ODNI (приложение VI), стр. 18. Вж. също и стр. 6, където е посочено, че прилаганите процедури „доказват ясния ангажимент да бъде предотвратено произволното и безразборно събиране на радиоелектронна разузнавателна информация и от най-високите нива на нашето правителство да бъде въведен принципът на разумността“.

([89]) Вж. доклада за прозрачността на статистическата информация по отношение на използването на основанията за национална сигурност от 22 април 2015 г. За целия поток от информация по интернет вж. напр. Агенция за основните права, Наблюдения от страна на разузнавателните служби: Гаранции и правни средства за защита на основните права в ЕС (2015 г.) на стр. 15—16. По отношение на програмата UPSTREAM, според разсекретеното становище на Съда по надзора върху външното разузнаване от 2011 г. над 90 % от електронните съобщения, получени по силата на раздел 702 от ЗУНВР, са били от програмата PRISM, докато под 10 % са от програмата UPSTREAM. Вж. СНВР, становище меморандум 2011 г. WL 10945618 (FISA Ct., 3.10.2011), бел. под линия 21 (на адрес: http://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf).

([90]) Вж. раздел 4, буква а), подточка ii) от ПИД-28. Вж. също ODNI, Гаранции за личната информация на всички лица: Доклад за състоянието относно развитието и прилагането на процедурите съгласно Президентски изпълнителен указ от 28 юли 2014 г., стр. 5, според който „Политиките на елементите на разузнавателните структури следва да укрепват съществуващите аналитични практики и стандарти, като анализаторите трябва да се стремят да структурират запитванията или другите условия и техники на търсене с цел идентифициране на разузнавателна информация, която е релевантна за валидна задача в областта на разузнаването или правоприлагането; да фокусират търсенията за лица върху категориите разузнавателна информация, които съответстват на дадено изискване в областта на разузнаването или правоприлагането; и сведат до минимум прегледа на лична информация, която няма отношение към изискванията в областта на разузнаването или правоприлагането“. Вж. напр. ЦРУ, Дейности на радиоелектронното разузнаване, стр. 5; ФБР, Президентска изпълнителна директива 28, политики и процедури, стр. 3. Съгласно доклада за напредъка от 2016 г. относно реформата на радиоелектронното разузнаване, разузнавателните структури (включително ФБР, ЦРУ и АНС) са предприели мерки да повишат осведомеността на своя персонал относно изискванията на ПИД-28, като са въвели нови или са модифицирали съществуващи политики за обучение.

([91]) Съгласно писмените изявления на ODNI тези ограничения се прилагат независимо от това, дали информацията е събрана като масиви от данни, чрез целенасочено събиране и с оглед на националността на физическите лица.

(85) Правителството на САЩ поясни, че това изискване за разумност означава, че не е необходимо разузнавателните структури да предприемат „всички теоретично възможни мерки“, а трябва да „установяват баланс между усилията си за защита на легитимните интереси, касаещи неприкосновеността на личния живот и гражданските свободи, и практическите потребности при дейностите на радиоелектронното разузнаване“ ([92]). В това отношение физическите лица, които не са граждани на САЩ, ще бъдат третирани по същия начин както американските граждани, въз основа на процедури, одобрени от министъра на правосъдието ([93]).

(86) Съгласно тези правила запазването обикновено е ограничено до максимален срок от пет години, освен ако в закон се посочва конкретно, че удължаването на срока на запазване е в интерес на националната сигурност или когато директорът на националното разузнаване е приел изрично решение в същия смисъл след внимателна преценка на съображенията за неприкосновеността на личния живот и след отчитане на становищата на служителя по защита на гражданските свободи към ODNI и на служителите на агенцията, отговарящи за неприкосновеността на личния живот и гражданските свободи ([94]). Разпространението се ограничава до случаите, когато информацията е релевантна за основната цел, за която е събрана, и поради това отговаря на условие за извършване на разрешено разузнаване или правоприлагане ([95]).

(87) Съгласно уверенията, дадени от правителството на САЩ, личната информация не може да бъде разпространявана просто защото съответното лице не е гражданин на САЩ и „радиоелектронните разузнавателни данни относно рутинни дейности на чуждестранно лице не могат да се считат за разузнавателни данни, които могат да се разпространяват или запазват трайно само по силата на този факт, освен ако по друг начин отговарят на изискване за разрешено разузнаване“ ([96]).

(88) Поради това Комисията стига до заключението, че в Съединените американски щати има установени правила, предназначени да ограничат всяка намеса за целите на националната сигурност в основните права на физическите лица, чиито лични данни се предават от Съюза към Съединените американски щати съгласно Щита за личните данни в отношенията между ЕС и САЩ, като тази намеса се ограничава до строго необходимото за постигането на посочената легитимна цел.

(89) Както е видно от горепосочения анализ показа, законодателството на САЩ гарантира, че мерки за наблюдение ще се използват само за получаване на външноразузнавателна информация — което представлява легитимна цел на политиката ([97]), като бъдат съобразени във възможно най-голяма степен. По-конкретно, събиране на масиви от

([92]) Вж. писмените изявления на ODNI (приложение VI).

([93]) Вж. раздел 4, буква а), подточка i) от ПИД-28, заедно с раздел 2.3 от Изпълнителен декрет 12333. 12333.

([94]) Вж. раздел 4, буква а, подточка i) от ПИД-28. Писмени изявления на ODNI (приложение VI), стр. 7. Например за лична информация, събирана съгласно раздел 702 от ЗУНВР, в процедурите на АНС за свеждане до минимум, одобрени от Съда по надзора върху външното разузнаване, е предвидено по правило метаданните и информацията с неанализирано съдържание за програмата PRISM да бъдат съхранявани не по-дълго от пет години, докато данни за програма UPSTREAM се съхраняват не по-дълго от две години. АНС осигурява спазването на тези ограничения за съхранението посредством автоматизиран процес, чрез който събраните данни се изтриват в края на съответния срок на съхранение. Виж АНС, раздел 702 от ЗУНВР, Процедури за свеждане до минимум, раздел 7 във връзка с раздел 6, буква а), подточка 1); Изпълнение от страна на АНС на раздел 702 от ЗУНВР от 16.4.2014 г. на Службата за гражданските свободи и неприкосновеността на личния живот към АНС. По същия начин запазването съгласно раздел 501 от ЗУНВР (предишен раздел 215 от Закона за обединяване и укрепване на САЩ (U.S. PATRIOT ACT) е ограничено за срок от пет години, освен когато личните данни са част от одобрено по надлежния ред разпространение на външноразузнавателна информация или ако Министерството на правосъдието е уведомило писмено АНС, че по отношение на данните има задължение за съхраняване за решаването на висящ или предстоящ съдебен спор. Вж. АНС, Службата за гражданските свободи и неприкосновеността на личния живот, Доклад за прозрачността: Закон за свободата в САЩ, търговски регистър, в изпълнение на ЗУНВР, 15 януари 2016 г.

([95]) По-специално в случая на раздел 501 от ЗУНВР (предишен раздел 215 от Закона за обединяване и укрепване на САЩ (U.S. PATRIOT ACT) разпространяването на лична информация може да става само за целите на противодействие на тероризма или като доказателство при престъпление; в случая на раздел 702 от FISA само когато валидна цел във връзка с външното разузнаване или правоприлагането. Вж. Изпълнение от страна на АНС на раздел 702 от ЗУНВР от 16 април 2014 г. на Службата за гражданските свободи и неприкосновеността на личния живот към АНС. Доклад за прозрачността: Закон за свободата в САЩ, търговски регистър, в изпълнение на ЗУНВР, 15 януари 2016 г. Вж. също така АНС, Защита на гражданските свободи и неприкосновеността на личния живот за целеви дейности на радиоелектронното разузнаване (SIGINT) съгласно Изпълнителен декрет 12333, 7 октомври 2014 г.

([96]) Писмени изявления на ODNI (приложение VI), стр. 7 (във връзка с Указа за разузнавателните структури (Intelligence Community Directive (ICD)) 203).

([97]) Съдът на Европейските общности е пояснил, че националната сигурност представлява законосъобразна цел на политиката. Вж. *делото Schrems*, точка 88. Вж. също решение *Digital Rights Ireland и др.*, точки 42—44 и 51), в което Съдът установява, че борбата срещу тежката престъпност, и по-специално организираната престъпност и тероризма, могат да зависят в голяма степен от използването на модерни техники на разследване. Освен това за разлика от наказателните разследвания, които обикновено се отнасят до определяне на отговорността и вината за минало поведение със задна дата, разузнавателните дейности често са съсредоточени върху предотвратяването на заплахи за националната сигурност, преди да е нанесена вреда. Поради това обхватът на подобни разследвания често може да включва повече възможни участници („обекти“) и по-широк географски район. Вж. Решение на ЕСПЧ по делото *Weber и Saravia с/у Германия*, жалба № 54934/00, точки 105—118 (относно т.нар. „стратегически мониторинг“).

данни ще се разрешава само по изключение, когато не е осъществимо целенасочено събиране, и то ще бъде придружено от допълнителни гаранции за свеждане до минимум на количеството на събираните данни и последващия достъп (които трябва да бъдат целеви и да бъдат разрешени само за конкретни цели).

(90) Според оценката на Комисията това е в съответствие със стандарта, определен от Съда в решението по делото *Schrems* — в законодателство, при което има намеса спрямо основните права, гарантирани от членове 7 и 8 от Хартата, задължително се налагат „минимални защити“ ([98]) и „не се ограничава до строго необходимото правна уредба, която общо разрешава съхраняването на всички лични данни на всички лица, чиито данни са били прехвърлени от Съюза към Съединените щати, без да въвежда никакво разграничаване, ограничаване или изключение с оглед на преследваната цел и без да предвижда обективен критерий, позволяващ да се ограничи достъпът на публичните органи до данните и тяхното последващо използване за конкретни цели, които са строго ограничени и могат да обосноват намесата, каквато съдържат достъпът и използването на тези данни.“ ([99]). Няма да има също така неограничено събиране и съхранение на данни за всички лица без ограничение, нито неограничен достъп. Освен това предоставените на Комисията писмени изявления, включително уверението, че радиоелектронните разузнавателни дейности на Съединените американски щати обхващат само много малка част от комуникациите, преминаващи по интернет, изключват вероятността, че ще има „общ“ достъп до съдържанието на електронните съобщения ([100]).

3.2.1. Ефективна правна защита

(91) Комисията направи оценка на съществуващите механизми за надзор в Съединените американски щати по отношение на евентуална намеса на разузнавателните органи на САЩ в личните данни, които се предават на Съединените американски щати, и на наличните възможности за субектите на данни от ЕС да търсят индивидуална правна защита.

Надзор

(92) Разузнавателните структури на САЩ подлежат на различни механизми за преглед и надзор, които попадат в три държавни подразделения. Това включва вътрешни и външни органи в рамките на изпълнителната власт, редица комисии на Конгреса, както и съдебен надзор, по-специално във връзка с дейности по Закона за упражняване на надзор върху външното разузнаване.

(93) На първо място разузнавателните дейности на органите на САЩ са под строгия надзор на изпълнителната власт.

(94) Съгласно ПИД-28, раздел 4, буква а), подточка iv), политиките и процедурите на разузнавателните структури „следва да включват подходящи мерки за улесняване на надзора върху прилагането на гаранциите, предвидени за защита на личната информация“; за тези мерки трябва да е предвидено периодично одитиране ([101]).

([98]) Делото *Schrems*, точка 91 с допълнителните препратки.
([99]) Делото *Schrems*, точка 93.
([100]) Вж. *делото Schrems*, точка 94.
([101]) СДНР, Гаранции за личната информация на всички лица: Доклад за актуалното състояние относно изготвянето и прилагането на процедурите съгласно Президентска изпълнителна директива 28, стр. 7. Вж. напр. ЦРУ, Дейности на радиоелектронното разузнаване, стр. 6 (Спазване); ФБР, Президентска изпълнителна директива 28, „Политики и процедури“, раздел III (A)(4), (B)(4); АНС, ПИД-28, раздел 4, „Процедури“, 12 януари 2015 г., раздел 8.1, 8.6, буква c).

(95) За тази цел са установени множество нива на надзор, включително служители по въпросите на гражданските свободи или неприкосновеността на личния живот, главни инспектори, Службата за гражданските свободи и неприкосновеността на личния живот към ODNI, Надзорният съвет по въпросите на неприкосновеността на личния живот и гражданските свободи (PCLOB) и Надзорният съвет по въпросите на разузнаването към Президента. Тези надзорни органи се подпомагат от служители, отговарящи за спазването на нормативната уредба, във всички служби ([102]).

(96) Както беше пояснено от правителството на САЩ ([103]), *служители по въпросите на гражданските свободи или неприкосновеността на личния живот* с надзорни функции работят в различни министерства с отговорности в областта на разузнаването и в разузнавателните агенции ([104]). Въпреки че конкретните правомощия на тези служители може да се различават в известна степен в зависимост от законното основание за оправомощаването им, обикновено в тях се включва надзорът на процедурите с цел да се гарантира, че съответното министерство/агенция спазва по адекватен начин изискванията за неприкосновеност на личния живот и гражданските свободи и е въвело подходящи процедури за разглеждане на жалби от лица, които са счели, че неприкосновеността на личния им живот или гражданските им свободи са били нарушени (а в някои случаи, като например ODNI, могат да имат правомощия сами да провеждат разследвания по жалби ([105])). От своя страна ръководителят на министерството/агенцията трябва да осигури възможност служителят да получава цялата информация и да има осигурен достъп до всички материали, необходими за изпълнението на функциите му. Служителите по въпросите на гражданските свободи и неприкосновеността на личния живот периодично докладват пред Конгреса и Надзорния съвет по въпросите на неприкосновеността на личния живот и гражданските свободи, включително за броя и характера на получените в министерството/агенцията жалби и обобщение на разпорежданията по тези жалби, проведените проверки и разследвания и последиците от дейностите, извършени от служителя ([106]). Според оценката от страна на националните органи за защита на данните, вътрешният надзор, упражняван от граждански свободи или служителите, отговарящи за личните данни, могат да се считат за „достатъчно надеждни“, въпреки че според тях те не отговарят на необходимото ниво на независимост ([107]).

(97) В допълнение към това всяка разузнавателна структура има свой *главен инспектор*, в чиито отговорности се включва наред с останалото и упражняването на надзор върху разузнавателните дейности ([108]). В рамките на ODNI това е Службата на главния инспектор, която разполага с всеобхватна компетентност, обхващаща всички разузнавателни структури, и с правомощия да провежда разследвания въз основа на жалби или на информация относно обвинения в незаконни действия или злоупотреба с власт във връзка с програми и дейности на ODNI и/или на разузнавателните структури ([109]). По закон главните инспектори са структури с независим ([110]) статут, които отговарят за провеждането на одити и разследвания във връзка с програмите и операциите, изпълнявани от съответната агенция за целите на националното разузнаване, включително за злоупотреби или закононарушения ([111]). Те имат правомощия за достъп до всички записи, доклади, одити, прегледи, документи, писмени

([102]) Например в Дирекция „Спазване на нормативната уредба“ на АНС работят повече от 300 служители по спазването. Вж. писмените изявления на ODNI (приложение VI), стр. 7.

([103]) Вж. Механизъм на омбудсмана (приложение III), точка 6, буква б), подточки i) до iii).

([104]) Вж. 42 U.S.C.,§ 2000ee-1. Тук се включват например Държавният департамент, Министерството на правосъдието (вкл. ФБР), Министерството на вътрешната сигурност, Министерството на отбраната, АНС, ЦРУ и ODNI.

([105]) Според правителството на САЩ, ако в Службата по въпросите на гражданските свободи и неприкосновеността на личния живот на ODNI се получи жалба, този орган работи също така в координация с другите разузнавателни структури относно това как да продължи разглеждането на жалбата в рамките на разузнавателните структури. Вж. Механизъм на омбудсмана (приложение III), точка 6, буква б), подточка ii).

([106]) Вж. 42 U.S.C. § 2000ee-1 (f)(1),(2).

([107]) Становище 01/2016 на работната група по защита на данните по член 29 относно проекта на решение за адекватността на Щита за личните данни в отношенията между ЕС и САЩ (прието на 13 април 2016 г.), стр. 41.

([108]) Писмени изявления на ODNI (приложение VI), стр. 7. Вж. напр. АНС, ПИД-28, раздел 4 „Процедури“, 12 януари 2015 г., раздел 8.1.; ЦРУ, Дейности на радиоелектронното разузнаване, стр. 7 (Отговорности).

([109]) Този главен инспектор (длъжността е създадена през октомври 2010 г.) се назначава от Президента с утвърждаване от Сената и може да бъде отстранен от длъжност само от Президента, но не и от директора на националното разузнаване.

([110]) Тези главни инспектори са с постоянно назначение и могат да бъдат отстранени от длъжност само от Президента, който трябва да информира Конгреса писмено относно причините за отстраняването. Това не означава задължително, че те не получават никакви указания. В някои случаи ръководителят на министерството може да забрани на главния инспектор да инициира, извърши или завърши даден одит или разследване, когато счете това за необходимо за опазването на важни национални интереси (в областта на сигурността). Конгресът обаче трябва да е уведомен за упражняването на това правомощие и на тази основа може да потърси отговорност от съответния директор. Вж. напр. Закон за главния инспектор (Inspector General Act) от 1978 г., § 8 (Главен инспектор на Министерството на отбраната); § 8E (Главен инспектор на Министерството на правосъдието), § 8G (d)(2)(A),(B) (Главен инспектор на АНС); 50. U.S.C. § 403q (b) (Главен инспектор на ЦРУ); Закон за разрешаване на разузнавателни дейности за финансова година 2010 (Intelligence Authorization Act For Fiscal Year 2010), Sec 405(f) (Главен инспектор на структурите на разузнаването). Според оценката на националните органи за защита на данните главните инспектори „*по всяка вероятност отговарят на критерия за организационна независимост, определен от Съда на Европейския съюз и от Европейския съд по правата на човека, най-малкото от момента, в който новият процес на номиниране се прилага за всички*.“ Вж. становище 01/2016 на работната група по защита на данните по член 29 относно проекта на решение за адекватността на Щита за личните данни в отношенията между ЕС и САЩ (прието на 13 април 2016 г.), стр. 40.

([111]) Вж. писмените изявления на ODNI (приложение VI), стр. 7. Вж. също Закон за главния инспектор от 1978 г. с изменение, публ. L. 113-126 от 7 юли 2014 г.

материали, препоръки или други съответни материали, ако е необходимо чрез призоваване, и могат да събират показания ([112]). Докато главните инспектори могат да издават само препоръки за корективни мерки с необвързващ характер, техните доклади, включително относно последващите действия (или липсата на такива), се оповестяват публично и освен това се изпращат на Конгреса, който на тази основа може да упражни надзорните си функции ([113]).

(98) Освен това на *Надзорния съвет по въпросите на неприкосновеността на личния живот и гражданските свободи* (НСВНЛЖГС), който е независима агенция ([114]) в рамките на изпълнителната власт, в чийто състав влизат членове, назначени от Президента с одобрението на Сената ([115]), са поверени отговорности в сферата на политиките в областта на противодействието срещу тероризма и тяхното прилагане, с цел защита на неприкосновеността на личния живот и гражданските свободи. За тези цели той има достъп до всички съответни записи, доклади, одити, прегледи, документи, писмени материали и препоръки на агенциите, включително до класифицирана информация, може да провежда изслушвания и да събира устни свидетелски показания. Той получава докладите на служителите по въпросите на гражданските свободи и неприкосновеността на личния живот в няколко федерални министерства/агенции ([116]), може да издава препоръки за тях и докладва редовно пред комисиите в Конгреса и пред президента ([117]). PCLOB е натоварен също със задачата да изготвя в рамките на мандата си доклад за оценка на изпълнението на ПИД-28.

(99) И накрая, разгледаните по-горе надзорни механизми се допълват от Надзорния съвет по въпросите на разузнаването (*Intelligence Oversight Board*), създаден в рамките на Консултативния съвет по въпросите на разузнаването към Президента (President's Intelligence Advisory Board), който следи за спазването на конституцията и всички приложими правила от страна на органите на САЩ, работещи в областта на разузнаването.

(100) За улесняване на надзора разузнавателните структури се насърчават да проектират информационни системи, които да позволяват наблюдение, запис и преглед на запитванията или другите видове търсене на лична информация ([118]). Надзорните органи и органите по спазването на нормативната уредба извършват периодични проверки на практиките на разузнавателните структури в областта на защитата на личната информация, съдържаща се в радиоелектронните разузнавателни данни, и за спазването на процедурите ([119]).

(101) В допълнение тези надзорни функции са подсилени от изискванията за изготвяне на подробни доклади при случаи на неспазване на задълженията. По-специално процедурите на агенциите трябва да гарантират, че при възникване на значим проблем със спазването във връзка със събрана чрез радиоелектронно разузнаване лична информация на някое физическо лице, независимо от неговото гражданство, този проблем ще бъде своевременно докладван на ръководителя на разузнавателната структура, който от своя страна ще уведоми за това директора на Националното разузнаване, който съгласно ПИД-28 определя дали са необходими корективни мерки ([120]). Освен това съгласно Изпълнителен декрет 12333 е определено изискване всички разузнавателни структури да докладват на Надзорния съвет по въпросите на разузнаването относно случаите на неспазване ([121]). С тези механизми се гарантира, че проблемите ще бъдат решавани на най-високо равнище в разузнавателните структури. Когато се касае за лице, което не е американски гражданин, директорът на националното разузнаване, в консултация с държавния секретар

([112]) Вж. Закон за главния инспектор от 1978 г., § 6.

([113]) Вж. писмените изявления на ODNI (приложение VI), стр. 7. Вж. също Закон за главния инспектор от 1978 г., §§ 4(5), 5. Съгласно раздел 405(b)(3),(4) от Закона за разрешаване на разузнавателни дейности за финансова година 2010, публ. L. 111-259 от 7 октомври 2010 г., главният инспектор на структурите на разузнаването уведомява директора на Националното разузнаване и Конгреса относно необходимостта от корективни мерки и хода на изпълнението им.

([114]) Според оценката на националните органи за защита на данните, PCLOB е „доказал своите независими правомощия" в миналото. Вж. становище 01/2016 на работната група по защита на данните по член 29 относно проекта на решение за адекватността на Щита за личните данни в отношенията между ЕС и САЩ (прието на 13 април 2016 г.), стр. 42.

([115]) В допълнение към това в PCLOB са назначени около 20 души редовен персонал. Вж. https://www.pclob.gov/about-us/staff.html.

([116]) Тук се включват най-малкото Министерството на правосъдието, Министерството на отбраната, Министерството на вътрешната сигурност, директорът на националното разузнаване и Централното разузнавателно управление, както и други министерства, агенции или структури на изпълнителната власт, определени от PCLOB като подходящи да бъдат обхванати от правомощията му.

([117]) Вж. 42 U.S.C.,§ 2000ee. Вж. също Механизъм на омбудсмана (приложение III), точка 6, буква б), подточка iv). Наред с другото, PCLOB трябва да докладва, когато изпълнителна агенция отказва да я подкрепя.

([118]) ODNI, Гаранции за личната информация на всички лица: Доклад за актуалното състояние относно изготвянето и прилагането на процедурите съгласно Президентска изпълнителна директива 28, стр. 7-8.

([119]) Пак там на стр. 8. Вж. също писмените изявления на ODNI (приложение VI), стр. 9.

([120]) ODNI, Гаранции за личната информация на всички лица: Доклад за актуалното състояние относно изготвянето и прилагането на процедурите съгласно Президентска изпълнителна директива 28, стр. 7. Вж. напр. АНС, ПИД-28, раздел 4 Процедури, 12 януари 2015 г., раздел 7.3, 8.7(c),(d); ФБР, Президентска изпълнителна директива 28, Политики и процедури, раздел III.(A)(4), (B)(4); ЦРУ, Дейности на радиоелектронното разузнаване, стр. 6 (Спазване) и стр. 8 (Отговорности).

([121]) Вж. Изпълнителен декрет 12333, раздел 1.6(c).

и с ръководителя на министерството, департамента или агенцията, които са уведомили за случая, определя дали трябва да бъдат предприети стъпки за уведомяване на съответното чуждо правителство, като се спазват изискванията относно защитата на източниците и методите и защитата на служителите на САЩ ([122]).

(102) На второ място, в допълнение към тези надзорни механизми в рамките на изпълнителната власт, Конгресът на САЩ, и по-специално комисията по въпросите на разузнаването и правната комисия към Камарата на представителите и Сената (*House and Senate Intelligence and Judiciary Committees*), имат надзорни отговорности по отношение на всички дейности на САЩ в областта на разузнаването, включително радиоелектронното разузнаване на САЩ. Съгласно Закона за националната сигурност (National Security Act) „Президентът осигурява комисиите по въпросите на разузнаването в Конгреса да бъдат напълно и текущо информирани относно разузнавателните дейности на Съединените американски щати, включително за предвиждани значими разузнавателни дейности, както това се изисква съгласно настоящата подглава." ([123]). Също така „Президентът осигурява на комисиите по въпросите на разузнаването в Конгреса да бъде докладвано незабавно за всяка незаконна разузнавателна дейност, както и за всички корективни мерки, които са били взети или се планират във връзка с такава незаконна дейност." ([124]). Членовете на тези комисии имат достъп до класифицирана информация, както и до разузнавателните методи и програми ([125]).

(103) В по-новите закони се разширяват и прецизират изискванията за докладване към разузнавателните структури, съответните главни инспектори и Министъра на правосъдието. Например в ЗУНВР се съдържа изискване към Министъра на правосъдието да „информира в пълна степен" комисията по въпросите на разузнаването и правната комисия към Сената и Камарата на представителите относно дейностите на правителството съгласно определени раздели от ЗУНВР ([126]). Също така от правителството се изисква да предоставя на комисиите в Конгреса копия на „всички решения, разпореждания или становища на Съда по надзора върху външното разузнаване или документи, които включват значими конструкции или тълкувания" на разпоредбите на ЗУНВР. По-специално във връзка с наблюдението съгласно раздел 702 от ЗУНВР надзорът се осъществява посредством изисквани по закон доклади до комисията по въпросите на разузнаването и правната комисия, както и чести брифинги и изслушвания. Към тях се включват шестмесечният доклад на Министъра на правосъдието, в който описва как е бил използван раздел 702 от ЗУНВР, с придружаващите го документи, включително по-специално докладите на Министерството на правосъдието и на ODNI за спазването на нормативната уредба, с описание на евентуални случаи на неспазване ([127]), както и отделна шестмесечна оценка от Министъра на правосъдието и директора на Националното разузнаване, в която се описва спазването на процедурите за целево събиране и свеждане до минимум, включително спазването на процедурите, с които се цели да се гарантира, че събирането се извършва със законосъобразна разузнавателна цел ([128]). Също така в Конгреса се получават докладите от главните инспектори, които имат правомощия да извършват оценка на спазването от страна на агенциите на процедурите за целево събиране и свеждане до минимум и на насоките на Министъра на правосъдието.

(104) Съгласно Закона за свободата в САЩ (USA FREEDOM Act) от 2015 г. правителството е задължено всяка година да оповестява пред Конгреса (и обществеността) наред с останалото и броя на поисканите и получените разпореждания и указания съгласно ЗНЧРС, както и изчисления за броя на лицата — граждани на САЩ, и лицата, които не са американски граждани, които са били цел на наблюдение ([129]). Също така в закона се предвижда изискване за допълнително докладване пред обществеността относно броя на издадените писма във връзка с националната сигурност (ПНС), отново по отношение на лица — граждани на САЩ, и лица, които не са

([122]) ПИД-28, раздел 4(a)(iv).
([123]) Вж. раздел 501, буква a), точка 1) (50 U.S.C. § 413(a)(1)). В тази разпоредба се съдържат общите изисквания относно надзора, упражняван от Конгреса в областта на националната сигурност.
([124]) Вж. раздел 501, буква b) (50 U.S.C. § 413(b)).
([125]) Вж. раздел 501, буква d) (50 U.S.C. § 413(d)).
([126]) Вж. 50 U.S.C. §§ 1808, 1846, 1862, 1871, 1881f.
([127]) Вж. 50 U.S.C. § 1881f.
([128]) Вж. 50 U.S.C. § 1881a(l)(1).
([129]) Вж. Закон за свободата в САЩ (USA FREEDOM Act) от 2015 г., публ. L. № 114-23, раздел 602, буква a). В допълнение към това, съгласно раздел 402 „директорът на Националното разузнаване, в консултация с Министъра на правосъдието, извършва преглед за разсекретяване на всяко решение, разпореждане или становище на Съда по надзора върху външното разузнаване или на Апелативния съд по надзора върху външното разузнаване, (както това е предвидено в раздел 601, буква e)), в което се съдържат значими конструкции или тълкувания на някоя законова разпоредба, включително нови или значими конструкции или тълкувания на понятието „конкретен критерий за подбор", и съгласно този преглед обявява публично, доколкото това е практически възможно, всяко такова решение, разпореждане или становище."

американски граждани (като същевременно се предвижда получателите на разпореждания и сертифицирания съгласно ЗНЧРС, както и на искания за ПНС, да публикуват доклади за прозрачност при определени условия) ([130]).

(105) На трето място за разузнавателните дейности на публичните органи на САЩ на основание ЗНЧРС се предвижда разглеждане, а в някои случаи предварително разрешение на мерките от *Съда за наблюдение на чуждите разузнавателни служби (СНЧРС)* ([131]), от независим правораздавателен орган ([132]). чиито решения подлежат на обжалване пред Апелативния съд за наблюдение на чуждите разузнавателни служби (АСНЧРС) ([133]). и накрая от Върховния съд на Съединените щати ([134]). За целите на предварителното разрешение органите, които отправят искането (ФБР, АНС, ЦРУ и др.), трябва да представят проектно заявление пред юристите на Департамента по национална сигурност към Министерството на правосъдието, които го разглеждат подробно и ако е необходимо, изискват допълнителна информация ([135]). След като заявлението бъде финализирано, то трябва да бъде одобрено от Министъра на правосъдието, Заместник министъра на правосъдието или Заместник министъра на правосъдието по въпросите на националната сигурност ([136]). След това Министерството на правосъдието подава заявлението в Съда за наблюдение на чуждите разузнавателни служби, който го разглежда и се произнася с предварително определение относно това как да се процедира ([137]). Когато се провежда изслушване, Съдът за наблюдение на чуждите разузнавателни служби има правомощия да взема показания, което може да включва и експертно мнение ([138]).

(106) Дейността на Съда за наблюдение на чуждите разузнавателни служби и на Апелативния съд за наблюдение на чуждите разузнавателни служби се подпомага от постоянна работна група от пет лица с експертни знания и опит в областта на националната сигурност и в областта на гражданските свободи ([139]). От тази група съдът определя едно лице, което изпълнява функциите на *amicus curiae* и съдейства за разглеждането на всички заявления за разпореждане или разглеждане, които според становището на съда представляват ново или съществено тълкуване на закон, освен ако съдът счете, че е уместно да не определя такова лице ([140]). По-специално с това се гарантира, че съображенията за неприкосновеността на личния живот се отразяват по подходящ начин при преценката на съда. Също така съдът може да определи функциите на *amicus curiae* да изпълнява лице или организация, включително като предоставя техническа експертиза, когато бъде счетено за необходимо, или по предложение, да даде разрешение на дадено лице или организация да подаде подготвени от приятел на съда заключения (*amicus curiae*) ([141]).

([130]) Закон за свободата в САЩ (USA FREEDOM Act), раздел 602, буква а) и раздел 603, буква а).

([131]) За някои видове наблюдения като алтернативно решение може да са дадени правомощия на магистрат към окръжен съд (U.S. Magistrate Judge), определен официално от Председателя на Върховния съд на САЩ (Chief Justice of the United States), да изслушва тези молби и да издава разпореждания.

([132]) В състава на Съда по надзора върху външното разузнаване влизат единадесет съдии, назначени от Председателя на Върховния съд на САЩ измежду действащи окръжни съдии, които преди това са назначени от президента с утвърждението на Сената. Съдиите, които са с пожизнено назначение и могат да бъдат отстранявани от длъжност само с основателна причина, изпълняват задълженията си в Съда по надзора върху външното разузнаване с разпределен седемгодишен мандат. Съгласно Закона за упражняване на надзор върху външното разузнаване съдиите трябва да са подбрани от най-малко седем различни съдебни окръга на САЩ. Вж. раздел 103 от ЗУНВР (50 U.S.C. 1803 (a)); НСВНЛЖГС, раздел 215 доклад, стр. 174—187. Работата на съдиите се подпомага от опитни помощник-съдии, които са назначен юридически персонал в съда и подготвят правни анализи по колективни искания. Виж доклад на Надзорния съвет по въпросите на неприкосновеността на личния живот и гражданските свободи, раздел 215, стр. 178; Писмо от уважаемия Reggie B. Walton, съдията — председател на Съда по надзора върху външното разузнаване на САЩ, до уважаемия Patrick J. Leahy, председател на правната комисия в Сената на САЩ (29 юли 2013 г.) („писмо Walton“), стр. 2—3.

([133]) В състава на Апелативния съд за наблюдение на чуждите разузнавателни служби влизат трима съдии, назначени от Главния съдия на САЩ и избрани измежду съдиите в окръжните и апелативните съдилища на САЩ, които изпълняват задълженията си с разпределен седемгодишен мандат. Вж. раздел 103 FISA (50 U.S.C. § 1803 (b)).

([134]) Вж. 50 U.S.C. §§ 1803 (b), 1861 a (f), 1881 a (h), 1881 a (i)(4).

([135]) Например допълнителни фактически подробности относно целта на наблюдението, техническа информация за методологията на наблюдението, или уверения за това как придобитата информация ще бъде използвана и разпространявана. Виж доклад на Надзорния съвет по въпросите на неприкосновеността на личния живот и гражданските свободи, раздел 215, стр. 177;

([136]) 50 U.S.C. §§ 1804 (a), 1801 (g).

([137]) Съдът по надзора върху външното разузнаване може да приеме молбата, да изиска допълнителна информация, да определи, че е необходимо изслушване, или да посочи, че е възможно да отхвърли молбата. Въз основа на това предварително определение правителството подава окончателна молба. Тя може да включва съществени изменения на първоначалната молба въз основа на предварителните коментари на съдията. Въпреки че голям процент от окончателните заявления биват одобрявани от Съда за наблюдение на чуждите разузнавателни служби, значителна част от тях съдържат съществени изменения спрямо първоначалните, напр. 24 % от заявленията, одобрени в периода юли—септември 2013 г. Виж доклад на Надзорния съвет по въпросите на неприкосновеността на личния живот и гражданските свободи, раздел 215, стр. 179; писмо Walton, стр. 3.

([138]) Доклад на PCLOB, раздел 215, стр. 179, бел. под линия 619.

([139]) 50 U.S.C. § 1803 (i)(1),(3)(A). Това ново законодателство изпълнява препоръките на Надзорния съвет по въпросите на неприкосновеността на личния живот и гражданските свободи за създаване на група от експерти по въпросите на неприкосновеността на личния живот и гражданските свободи, които да могат да изпълняват функциите на *amicus curiae* с цел да предоставят на съда правни аргументи за развитието в сферата на неприкосновеността на личния живот и гражданските свободи. Виж доклад на НСВНЛЖГС, раздел 215, стр. 183—187.

([140]) 50 U.S.C. § 1803 (i)(2)(A). По информация на ODNI вече има определени такива. Вж. Реформа на радиоелектронното разузнаване, доклад за напредъка за 2016 г.

([141]) 50 U.S.C. § 1803 (i)(2)(B).

(107) По отношение на двете правни основания за осъществяване на наблюдение съгласно ЗУНВР, които са най-важни за предаването на данни съгласно Щита за личните данни в отношенията между ЕС и САЩ, надзорът, упражняван от Съда по надзора върху външното разузнаване, е по-различен.

(108) Съгласно раздел 501 от ЗУНВР ([142]), с който се разрешава събиране на „всякакви материални вещи (вкл. книги, записи, хартиени носители, документи и други вещи)“, молбата до Съда по надзора върху външното разузнаване трябва да включва изложение на фактите, от което да личи, че са налице разумни основания да се счита, че материалните вещи, за които се иска разрешението, са релевантни за разрешено разследване (различно от оценката на заплаха), провеждано с цел да бъде получена външноразузнавателна информация, която не се отнася за лице— гражданин на САЩ, или с цел защита срещу международния тероризъм или секретни разузнавателни дейности. Също така в молбата трябва да бъдат изброени процедурите за свеждане до минимум, предвидени от Министъра на правосъдието за запазването и разпространението на събраните разузнавателни данни ([143]).

(109) И обратно, съгласно раздел 702 от ЗУНВР ([144]) Съдът по надзора върху външното разузнаване не дава разрешение за отделни мерки за наблюдение, а за програми за наблюдение (като PRISM, UPSTREAM) въз основа на годишни сертифицирания, изготвени от Министъра на правосъдието и от директора на Националното разузнаване. Раздел 702 от ЗУНВР позволява за обект на разследване да се определят лица, за които има разумни основания да се счита, че се намират извън територията на Съединените американски щати, с цел събиране на външноразузнавателна информация ([145]). Определянето на такива обекти се извършва от АНС на два етапа: първо анализаторите на АНС идентифицират лица, които не са граждани на САЩ и се намират извън територията на САЩ, и чието наблюдаване по преценка на анализаторите ще осигури съответните разузнавателни данни, посочени при сертифицирането. Второ, след като са идентифицирани тези отделни лица и определянето им като цели бъде одобрено чрез механизъм за подробно разглеждане в рамките на АНС ([146]), се възлага задача за определянето на критерии за подбор (т.е. тяхното разработване и прилагане), чрез които да се набележат съобщителните средства (напр. адреси на ел. поща), използвани от обектите на разследването ([147]). Както е посочено, в сертифицираниятa, подлежащи на одобрение от Съда по надзора върху външното разузнаване, не се съдържа информация относно отделните лица, които ще бъдат обект на разследване, а се посочват категориите външноразузнавателна информация ([148]). Съдът по надзора върху външното разузнаване не прави преценка дали — по определена вероятна причина или според някакво друго изискване — лицата са определени правилно за обект на разследване с цел придобиване на разузнавателни данни ([149]), а неговите контролни функции се простират до проверка на условието, че„значима цел на придобиването е получаването на външноразузнавателна информация“ ([150]). На практика, съгласно раздел 702 от ЗУНВР АНС може да събира информация за съобщенията на лица, които не са граждани на САЩ и се намират извън територията на САЩ, само ако има разумни основания да се счита, че дадено съобщително средство се използва за предаване на данни, представляващи разузнавателен интерес (напр. свързани с международния тероризъм, с разпространението на ядрени оръжия или вражески кибернетични дейности). При определянето за тези цели се упражнява съдебен контрол ([151]). При сертифицираниятa е необходимо също така да се предвидят процедури за определяне на обекта на разузнаване и за свеждане до минимум ([152]). Министърът на правосъдието и директорът на Националното разузнаване проверяват дали разрешението се спазва и агенциите имат задължението

([142]) 50 U.S.C. § 1861
([143]) 50 U.S.C. § 1861 (b).
([144]) (50 U.S.C., § 1881).
([145]) 50 U.S.C. § 1881a (a).
([146]) Доклад на Надзорния съвет по въпросите на неприкосновеността на личния живот и гражданските свободи, раздел 702, стр. 46.
([147]) 50 U.S.C. § 1881a (h).
([148]) 50 U.S.C. § 1881a (g). Според НСВНЛЖГС тези категории досега са се отнасяли главно за международния тероризъм и теми като придобиването на оръжия за масово унищожение. Виж доклад на Надзорния съвет по въпросите на неприкосновеността на личния живот и гражданските свободи, раздел 702, стр. 25;
([149]) Доклад на Надзорния съвет по въпросите на неприкосновеността на личния живот и гражданските свободи, раздел 702, стр. 27.
([150]) 50 U.S.C. § 1881a.
([151]) „Свобода и сигурност в един променящ се свят“, доклад и препоръки на консултативната група към Президента по въпросите на разузнаването и далекосъобщителните технологии, 12 декември 2013 г., стр. 152.
([152]) 50 U.S.C.1881a (i).

да докладват за всички случаи на неспазване пред Съда по надзора върху външното разузнаване ([153]) (както и пред Конгреса и Надзорния съвет по въпросите на разузнаването към Президента), който може на това основание да промени разрешението ([154]).

(110) Освен това, с цел да се повиши ефективността на надзора от страна на Съда по надзора върху външното разузнаване, администрацията на САЩ се съгласи да изпълни препоръка на Надзорния съвет по въпросите на неприкосновеността на личния живот и гражданските свободи за предоставяне на Съда на документацията за решенията за определяне на обекта по раздел 702, включително случайна извадка от листовете за определяне на задачата, за да се предостави възможност на съда да направи преценка как на практика се спазва изискването за целта на разузнаването ([155]). Същевременно администрацията на САЩ прие идеята и взе мерки за преразглеждане на процедурите на АНС за определяне на обектите на разследване, с цел по-добро документиране на основанията на разузнавателните служби при вземането на решение за определяне на обект ([156]).

Индивидуална защита

(111) В законодателството на САЩ са предвидени редица възможности, от които могат да се ползват субектите на данни от ЕС, когато са обезпокоени дали техни лични данни се обработват (събират се, предоставя се достъп до тях и др.) от разузнавателните структури на САЩ, и когато това е така — дали са спазени ограниченията, приложими съгласно правото на САЩ. Те се отнасят основно до три области: намеса съгласно ЗУНВР; незаконен, умишлен достъп до лични данни от страна на правителствени длъжностни лица; и достъп до информация съгласно Закона за свобода на информацията (Freedom of Information Act (FOIA) ([157]).

(112) Първо, в Закона за упражняване на надзор върху външното разузнаване са предвидени редица средства за правна защита, с които разполагат също и лицата, които не са граждани на САЩ, за оспорване на неправомерно електронно наблюдение ([158]). Това включва възможността физическите лица да предявят срещу Съединените американски щати граждански иск за обезщетяване на финансови вреди, когато информацията за тях е била неправомерно и умишлено използвана или разкрита ([159]); да заведат дело срещу длъжностни лица от правителството на САЩ в лично качество („престъпление при изпълнение на служебните задължения“ — under colour of law) за финансови вреди ([160])); и да оспорват законността на наблюдението (и да искат заличаване на събраната информация), в случай че правителството на САЩ възнамерява да използва или разкрива информация, получена или производна от електронно наблюдение срещу лицето, в съдебни или административни производства в Съединените американски щати ([161]).

(113) Второ, правителството на САЩ насочи вниманието на Комисията към редица допълнителни възможности, които субектите на данни от ЕС могат да използват, за да търсят правна защита срещу длъжностни лица при

([153]) С правило 13(b) от процедурния правилник на Съда по надзора върху външното разузнаване се изисква от правителството да подаде писмено уведомление до Съда незабавно след като се установи, че дадено от съда разрешение или одобрение е изпълнено по начин, който не съответства на разрешението или одобрението или на приложим закон. Също така в него се изисква от правителството да уведоми писмено Съда относно фактите и обстоятелствата, свързани с това неспазване. Обикновено правителството подава окончателно уведомление съгласно правило 13(a), когато станат известни съответните факти и бъде унищожена всяка информация, събрана без разрешение. Вж. писмо Walton, стр. 10.

([154]) 50 U.S.C. § 1881 (l). Виж също доклад на Надзорния съвет по въпросите на неприкосновеността на личния живот и гражданските свободи, раздел 702, стр. 66—76; Изпълнение от страна на АНС на раздел 702 от ЗУНВР от 16.4.2014 г. на Службата за гражданските свободи и неприкосновеността на личния живот към АНС. Събирането на лични данни за целите на разузнаването съгласно раздел 702 от ЗУНВР подлежи на вътрешен и външен надзор в рамките на изпълнителните органи. Вътрешният надзор включва наред с останалото и вътрешни програми с цел оценка и надзор на спазването на процедурите за целево събиране и свеждане до минимум; докладване на случаите на неспазване както в рамките на организацията, така и извън нея, пред ODNI, Министерството на правосъдието, Конгреса и Съда по надзора върху външното разузнаване; и годишни прегледи, които се изпращат на същите органи. Външният надзор се изразява главно в прегледи на процедурите за целево събиране и свеждане до минимум, извършвани от ODNI, Министерството на правосъдието и главните инспектори, които от своя страна докладват пред Конгреса и Съда по надзора върху външното разузнаване, включително относно случаите на неспазване. Значимите случаи на неспазване трябва да бъдат докладвани незабавно на Съда по надзора върху външното разузнаване, а останалите — в тримесечни доклади. Виж доклад на НСВНЛЖГС, раздел 702, стр. 66—77.

([155]) PCLOB, Препоръки от доклада за оценка от 29 януари 2015 г., стр. 20.

([156]) PCLOB, Препоръки от доклада за оценка от 29 януари 2015 г., стр. 16.

([157]) В допълнение към това в раздел 10 от Закона за процедурите във връзка с класифицираната информация (Classified Information Procedures Act) е предвидено, че при всяко наказателно преследване, в което Съединените американски щати трябва да докажат, че даден материал представлява класифицирана информация (напр. защото се изисква защита срещу неразрешено разкриване по съображения, свързани с националната сигурност), Съединените щати следва да уведомят ответника за частите от материала, за които има разумни основания да се очаква да са основание за установяване на елемента на нарушението, който се отнася за класифицираната информация.

([158]) Вж. също писмените изявления на ODNI (приложение VI), стр. 16.

([159]) 18 U.S.C. § 2712.

([160]) 50 U.S.C., § 1810.

([161]) 50 U.S.C., § 1806.

неправомерен достъп или използване на лични данни от страна на правителството, включително за възнамеряваните цели на националната сигурност (т.е. Закона за компютърните измами и злоупотреби ([162]) (Computer Fraud Abuse Act); Закона за неприкосновеност на електронните съобщения ([163]) (Electronic Communications Privacy Act); и Закона за правото на неприкосновеност на личните финанси ([164]) (Right to Financial Privacy Act). Всички тези основания за подаване на иск се отнасят за конкретни данни, цели и/или видове достъп (напр. достъп от разстояние до един компютър чрез интернет) и могат да се ползват при определени условия (напр. преднамерено/умишлено поведение, поведение, излизащо извън служебните задължения, наличие на претърпени вреди) ([165]). В Закона за административното производство (U.S.C.5 § 702) се дава възможност за по-обща правна защита — „всяко лице, което е претърпяло правно нарушение поради действие на агенцията или е неблагоприятно засегнато или ощетено от действия на агенцията“, има право да поиска съдебен контрол. Това включва възможността да се поиска от Съда да „обяви за незаконно и да отмени действие, констатации и заключения на агенцията, за които е установено, че представляват […] произвол, каприз, злоупотреба с правото на преценка, или по друг начин не са в съответствие със закона“ ([166]).

(114) И накрая, правителството на САЩ посочи Закона за свобода на информацията като средство, чрез което лица, които не са граждани на САЩ могат да поискат достъп до съществуващи записи на федерални агенции, включително когато в тях се съдържат лични данни на лицето ([167]). Предвид насочеността му, този закон не осигурява възможност за индивидуална правна защита срещу намесата в лични данни като такава, въпреки че по принцип би могъл да позволява на физически лица да получат достъп до съответна информация, с която разполагат агенциите на националното разузнаване. Дори в това отношение възможностите изглеждат ограничени, тъй като агенциите могат да откажат достъп до информация, която попада в обхвата на определени изброени изключения, включително достъп до класифицирана информация в областта на националната сигурност и информация относно разследвания в областта на правоприлагането ([168]). Предвид казаното, използването на посочените изключения от агенциите на националното разузнаване може да бъде оспорено от лицата, както по административен, така и по съдебен ред.

(115) Макар от това да следва, че лицата, включително субектите на данни от ЕС, имат редица възможности за правна защита, когато са станали обект на неправомерно (електронно) наблюдение за целите на националната сигурност, също така е ясно, че не са обхванати най-малкото някои от правните основания, които могат да се използват от разузнавателните органи на САЩ (напр. Изпълнителен декрет 12333). Освен това, дори когато по принцип са налице възможности за съдебна правна защита за лицата, които не са граждани на САЩ, например при наблюдение съгласно ЗУНВР, възможните начини на действие са ограничени ([169]) и предявените от лицата (включително граждани на САЩ) искове ще бъдат обявени за недопустими, ако не може да се докаже тяхната „основателност“ ([170]), а това ограничава достъпа до обикновените съдилища ([171]).

(116) С цел да осигури за всички субекти на данни от ЕС достъп до допълнителни възможности, правителството на САЩ реши да създаде нов механизъм, омбудсмана към Щита за личните данни, както това е изложено в писмото на държавния секретар на САЩ до Комисията, съдържащо се в приложение III към настоящото решение. Механизмът е изграден, като се изхожда от определянето съгласно ПИД-28 на старши координатор (на ниво заместник-министър) в Държавния департамент за лице за контакт, пред което чуждите правителства могат да изразяват загриженост във връзка с дейности на радиоелектронното разузнаване на САЩ, но далеч надхвърля тази първоначална идея.

([162]) 18 U.S.C., § 1030.
([163]) 18 U.S.C. §§ 2701-2712.
([164]) (12 U.S.C., § 3417).
([165]) Писмени изявления на ODNI (приложение VI), стр. 17.
([166]) 5 U.S.C. § 706(2)(A).
([167]) (5 U.S.C., § 552). Подобни закони съществуват и в отделните щати.
([168]) Ако случаят е такъв, лицето обикновено получава само стандартен отговор, с който агенцията отказва да потвърди или да отрече наличието на някакви записи. Вж. *ACLU c/y CIA*, 710 F.3d 422 (D.C. Cir. 2014 г.).
([169]) Вж. писмените изявления на ODNI (приложение VI), стр. 16. Съгласно направените пояснения възможните начини на действие налагат да е налице *вреда* (18 U.S.C. § 2712; 50 U.S.C. § 1810) или да се докаже, че *правителството възнамерява да използва или разкрие информацията*, получена или производна от електронно наблюдение на съответното лице, срещу това лице *в съдебни или административни производства* в Съединените щати (50 U.S.C. § 1806). При все това, Съдът на Европейския съюз е подчертал неколкократно, за да се установи наличието на намеса в основното право на неприкосновеност на личния живот, няма значение дали в резултат от тази намеса е имало неблагоприятни последици за съответното лице. Вж. решение по делото *Schrems*, точка 89 с допълнителните препратки.
([170]) Този критерий за допустимост произтича от изискването„case or controversy“ („дело или противоречие“) съгласно Конституцията на САЩ, чл. III.
([171]) Вж. *Clapper c/y Amnesty Int'l USA*, 133 S.Ct. 1138, 1144 (2013 г.). По отношение на използването на ПНС, в Закона за свободата в САЩ (USA FREEDOM Act), (раздел 502(f)-503) е предвидено периодично да се преразглежда изискването за неразкриване и *получателите* на ПНС да бъдат уведомявани, когато фактите вече не са в подкрепа на изискването за неразкриване (вж. писмените изявления на ODNI (приложение VI), стр. 13). Това обаче не гарантира, че субектът на данните от ЕС ще бъде уведомен(а), че е обект на разследване.

(117) По-специално, съгласно обвързващите ангажименти на правителството на САЩ омбудсманът към Щита за личните данни ще гарантира, че ще бъдат проведени разследвания по отделните жалби и лицата ще получат потвърждение от независима инстанция, че законодателството на САЩ е спазено или, когато това законодателство е нарушено, че нарушението е отстранено ([172]). Механизмът включва „омбудсман към Щита за личните данни“, т.е. заместник-секретар и допълнителен персонал, както и други надзорни органи, компетентни за надзора на различните елементи на разузнавателните структури, на чието сътрудничество ще разчита омбудсманът към Щита за личните данни в хода на работата си с жалбите. По-специално, когато искането на дадено лице се отнася до съвместимостта на надзора със законодателството на САЩ омбудсманът към Щита за личните данни ще може да разчита на независими надзорни органи с правомощия за разследване (като например главни инспектори или PCLOB). Във всеки случай държавният секретар гарантира, че омбудсманът ще разполага с необходимите средства, за да се гарантира, че неговият отговор на индивидуални молби се основава на цялата необходима информация.

(118) Посредством тази „композитна структура“ механизмът на омбудсмана гарантира независим надзор и индивидуална защита. Освен това сътрудничеството с други надзорни органи осигурява достъп до необходимите експертни познания. Накрая, с налагането на задължение спрямо омбудсмана към Щита за личните данни да потвърждава спазването или отстраняването на несъответствие механизмът отразява ангажимента на правителството на САЩ като цяло за разглеждане и разрешаване на жалби от граждани на ЕС.

(119) На първо място за разлика от механизъма, в който участват само правителствени инстанции, омбудсманът към Щита за личните данни ще получава и ще отговаря на индивидуални жалби. Подобни жалби могат да се подават на надзорните органи в държавите членки, които са компетентни за надзора на националните служби за сигурност и/или обработката на лични данни от страна на публични органи, които ще ги представят на централизиран орган на ЕС, от който те ще бъдат пренасочени към омбудсмана към Щита за личните данни ([173]). Това всъщност ще бъде от полза за субектите на данни от ЕС, които ще могат да се обръщат към национален (както и към европейски) орган „близо до дома“ и на собствения си език. Задачата на този орган ще бъде да оказва подкрепа на лицата при изготвянето на искане до омбудсмана към Щита за личните данни, в което се съдържа основната информация и по този начин може да бъде считано за „пълно“. Лицето не се налага да доказва, че е осъществен фактически достъп до личните му/ѝ данни от правителството на САЩ чрез дейности на радиоелектронното разузнаване.

(120) На второ място, правителството на САЩ се ангажира да гарантира, че при изпълнението на функциите си, омбудсманът към Щита за личните данни ще може да разчита на надзора и сътрудничеството на други съществуващи механизми за разглеждане на спазването на законите на САЩ. В някои случаи това ще изисква участието на националните разузнавателни служби, по-специално когато искането следва да се тълкува като искане за достъп до документи съгласно Закона за свобода на информацията. В други случаи, когато исканията се отнасят до съвместимостта на надзора със законодателството на САЩ, това сътрудничество ще включва независими надзорни органи (напр. главни инспектори) с отговорност и правомощия да провеждат задълбочено разследване (по-специално чрез достъп до всички съответни документи и правомощие да изискват информация и отчети) и да разрешат несъответствието ([174]). Също така омбудсманът към Щита за личните данни ще може да отнася казусите за разглеждане от Надзорния съвет по въпросите на неприкосновеността на личния живот и гражданските свободи ([175]). Когато някой от тези надзорни органи установи несъответствие, съответната разузнавателна структура (напр. разузнавателна агенция) ще трябва да отстрани несъответствието, тъй като само въз основа на това омбудсманът ще може да даде „положителен“ отговор на физическото лице (т.е. че установеното нарушение е

([172]) В случай че жалбоподателят е поискал достъп до документи, държани от публичните органи на САЩ, се прилагат правилата и процедурите, определени в Закона за свобода на информацията (Freedom of Information Act). Това включва възможността да се търси защита по съдебен ред (вместо независим надзор), в случай че искането бъде отхвърлено, при условията, определени във FOIA.

([173]) Съгласно механизма за омбудсмана (приложение III), точка 4, буква е), омбудсманът към Щита за личните данни ще бъде в пряка връзка с органа на ЕС за разглеждане на жалби на физическите лица, който от своя страна ще има задължението да осъществява връзката с лицето, подало искането. Ако преките връзки са част от„основните процеси“, чрез които може да се удовлетвори искането (напр. при искане за достъп по FOIA, вж. раздел 5), тези връзки ще се осъществяват съобразно с приложимите процедури.

([174]) Вж. Механизъм за омбудсмана (приложение III), точка 2, буква а). Вж. също съображения 0—0.

([175]) Вж. Механизъм за омбудсмана (приложение III), точка 2, буква в). Съгласно поясненията, направени от правителството на САЩ, Надзорният съвет по въпросите на неприкосновеността на личния живот и гражданските свободи ще прави постоянен преглед на политиките и процедурите, както и на тяхното изпълнение, на онези органи на САЩ, които отговарят за противодействието на тероризма, за да определи дали техните действия„защитават по подходящ начин неприкосновеността на личния живот и гражданските свободи и са в съответствие с приложимите закони, подзаконови актове и политики в областта на неприкосновеността на личния живот и гражданските свободи“. Също така този съвет ще„приема и разглежда доклади и друга информация от служителите по въпросите на неприкосновеността на личния живот и служителите по въпросите на гражданските свободи, и когато е уместно, ще им дава препоръки за тяхната дейност.“

отстранено), за което правителството на САЩ е поело ангажимент. Също така в рамките на сътрудничеството омбудсманът към Щита за личните данни ще бъде информиран за резултата от разследването и ще разполага с необходимите средства, за да се получи цялата необходима информация, за да подготви отговора си.

(121) И накрая, омбудсманът към Щита за личните данни ще бъде независим и по този начин няма да получава указания от разузнавателните структури на САЩ ([176]). Това е от съществено значение, като се има предвид, че омбудсманът ще трябва да „потвърди“, че е проведено необходимото разследване по жалбата и че правото на САЩ, включително ограниченията и гаранциите, разгледани в писмените изявления на ODNI, са спазени, а в случай на неспазване, че нарушението е отстранено. За да бъдат в състояние да осигуряват тази защита на неприкосновеността на личния живот, независимо потвърждение омбудсманът към Щита за личните данни ще трябва да получи информацията, необходима за разследването, за да оцени точността на отговор на жалбата. Освен това държавният секретар се е ангажирала да гарантира, че помощник-държавен секретар ще изпълнява функцията на неприкосновеността на екран омбудсманът към Щита за личните данни обективен и независим от всякакво неправомерно влияние, което би могло да има отражение върху отговорите, които следва да се предоставят.

(122) Като цяло този механизъм гарантира, че индивидуалните жалби бъде щателно разследван и разрешен, и че поне в областта на наблюдението, това ще включва независими надзорни органи с необходимите експертни знания и правомощия за разследване и омбудсман, които ще могат да изпълняват функциите си свободно от неправилно, по-специално от политическо влияние. Освен това физическите лица ще могат да отнасят жалби, без да е необходимо да доказват (или само да дадат индикации) че са били обект на наблюдение ([177]). С оглед на тези характеристики Комисията е удовлетворена, че съществуват адекватни и достатъчни гаранции срещу злоупотреби.

(123) Въз основа на всичко посочено по-горе Комисията стига до заключението, че Съединените американски щати осигуряват ефективна правна защита срещу намеса на разузнавателните им органи в основните права на физическите лица, чиито данни се предават от Съюза към Съединените американски щати съгласно Щита за личните данни в отношенията между ЕС и САЩ.

(124) В тази връзка Комисията отбелязва решението на Съда по делото *Schrems*, според което „правна уредба, в която не се предвижда никаква възможност правният субект да използва правни средства за защита, за да получи достъп до засягащи го лични данни или да поправи или заличи такива данни, не зачита съществения съдържание на основното право на ефективна съдебна защита, признато в член 47 от Хартата.“ ([178]). Оценката на Комисията потвърди, че в САЩ е предвидена такава правна защита, в това число чрез въвеждането на механизма на омбудсмана. Механизмът на омбудсмана осигурява независим надзор с правомощия за провеждане на разследвания. Ефективността на този механизъм ще бъде подложена на повторна оценка в рамките на извършваното от Комисията непрекъснато наблюдение на Щита за личните данни, включително чрез годишния съвместен преглед, който също включва омбудсмана.

3.2. *Достъп и използване от органи на публичната власт на САЩ за целите на правоприлагането и за цели от обществен интерес*

(125) По отношение на намесата в личните данни, които се предават съгласно Щита за личните данни в отношенията между ЕС и САЩ за целите на правоприлагането, правителството на САЩ (чрез Министерството на правосъдието) даде уверения относно приложимите ограничения и гаранции, които по преценка на Комисията доказват адекватната степен на защита.

([176]) Вж. *Roman Zakharov c/y. Russia*, решение от 4 декември 2015 г. (голям състав), жалба № 47143/06, точка 275 („въпреки че по принцип е желателно контролът да се повери на съдия, надзорът от несъдебни органи може да се счита за съвместим с Конвенцията, при условие че въпросният надзорен орган е независим от органите, които извършват наблюдението, и има достатъчни и ефективни контролни правомощия“).

([177]) Вж. решението по дело *Kennedy c/y Обединено кралство*, решение от 18 май 2010 г., жалба № 26839/05, точка 167.

([178]) Делото *Schrems*, точка 95. Както е видно от точки 91—96 от решението, параграф 95 се отнася до степента на защита, гарантирана в правния ред на Съюза, за която степента на защита в третата държава трябва да бъде„равностойна по същество“. Съгласно точки 73 и 74 от решението, това не означава, че степента на защита или средствата, до които третата страна прибягва в това отношение, трябва да бъдат идентични, а че използваните средства е необходимо на практика да се окажат ефективни.

(126) Според тази информация, съгласно четвъртата поправка в Конституцията на САЩ ([179]) за претърсвания и изземвания от правоприлагащите органи по принцип ([180]) се изисква съдебна заповед, издадена след като бъде демонстрирано наличието на „вероятна причина“. В малкото изрично установени и изключителни случаи, когато не се прилага ([181]) изискването за съдебна заповед, при правоприлагането се извършва тест за „основателност“ ([182]). Дали едно претърсване или изземване е основателно се „определя чрез преценка, от една страна за степента, в която се извършва намеса в неприкосновеността на личния живот на лицето, и от друга за степента, в която това е необходимо за законни правителствени интереси“ ([183]). В по-общ аспект с четвъртата поправка се гарантират неприкосновеността на личния живот и достойнството и се осигурява защита срещу произволни действия и действия на вмешателство от страна на държавни длъжностни лица ([184]). Тези концепции отразяват идеята за необходимост и пропорционалност в правото на Съюза. След като вещите, иззети като доказателства вече не са необходими в рамките на правоприлагането, те следва да бъдат върнати ([185]).

(127) Въпреки че правата съгласно четвъртата поправка не се прилагат за лица, които не са американски граждани и не пребивават в САЩ, те все пак се ползват непряко от тази защита, като се има предвид, че личните данни се пазят от дружества в САЩ, т.е. правоприлагащите органи при всички случаи трябва да поискат разрешение от съдебен орган (или най-малкото да спазват изискването за разумно основание) ([186]). Допълнителна защита се осигурява и от специални законови разпоредби, както и от насоките на Министерството на правосъдието, с които достъпът на правоприлагащите органи до данни се ограничава чрез изискване за основания, които са еквивалентни на принципите на необходимост и пропорционалност (напр. като се поставя изискване към ФБР да използва методи на разследване, които са с най-ниската практически възможна степен на вмешателство, отчитайки последствията за неприкосновеността на личния живот и гражданските свободи) ([187]). Съгласно писмените изявления на правителството на САЩ, за разследванията за целите на правоприлагането на държавно равнище (по отношение на разследванията, които се извършват в съответствие с федералните закони) се прилага същата или по-висока степен на защита ([188]).

(128) Въпреки че не във всички случаи ([189]) се изисква предварително съдебно разрешение от съда или от „голямото жури“ (grand jury) (разследващо поделение на съда, което се конституира от съдия или магистрат), административните разпореждания се ограничават до отделни случаи и подлежат на независим съдебен контрол, най-малкото когато правителството иска от съда налагане на мерки по принудително изпълнение ([190]).

([179]) Съгласно четвъртата поправка„[п]равото на хората да се чувстват в безопасност, по отношение на себе си, къщите, документите и вещите си, срещу неразумни претърсвания и изземвания, не трябва да бъде нарушавано и няма да се издават актове на прокурора освен при основателни причини, подкрепени от клетва или потвърждение и при специално описание на мястото, което да се претърси или на лицата и на нещата, които трябва да бъдат иззети“. Само (магистрати) съдии могат да издават такива заповеди. Федерални заповеди за копиране на електронно съхранена информация подлежат също така на правило 41 от Федералните правила относно наказателното производство.

([180]) Върховният съд многократно определя претърсвания без заповет като„извънредни“. Вж. напр. *Johnson c/y United States*, 333 U.S. 10, 14 (1948); *McDonald c/y United States*, 335 U.S. 451, 453 (1948); *Camara c/y Municipal Court*, 387 U.S. 523, 528-29 (1967); *G.M. Leasing Corp. c/y United States*, 429 U.S. 338, 352-53, 355 (1977). По същия начин Върховният съд редовно подчертава, че „основното конституционно правило в тази област е, че претърсвания извън съдебен процес без предварително одобрение от съдия или магистрат са сами по себе си неоснователни съгласно четвъртата поправка и в това отношение се прилагат *сато* — няколко строго и изрично определени изключения.“ Вж. напр. *Coolidge c/y New Hampshire*, 403 U.S. 443, 454-55 (1971); *G.M. Leasing Corp. c/y United States*, 429 U.S. 338, 352-53, 358 (1977).

([181]) *City of Ontario, Cal. c/y Quon*, 130 S. Ct. 2619, 2630 (2010).

([182]) Доклад на Надзорния съвет по въпросите на неприкосновеността на личния живот и гражданските свободи, раздел 215, стр. 107, позоваване на решение по дело Maryland c/y. King, 133 S. Ct. 1958, 1970 (2013).

([183]) Доклад на Надзорния съвет по въпросите на неприкосновеността на личния живот и гражданските свободи, раздел 215, стр. 107, позоваване на решението по дело *Samson c/y California*, 547 U.S. 843, 848 (2006).

([184]) *City of Ontario, Cal. c/y Quon*, 130 S. Ct. 2619, 2630 (2010), 2627.

([185]) Вж. напр. *United Sates c/y Wilson*, 540 F.2d 1100 (D.C. Cir. 1976).

([186]) Вж. *Roman Zakharov c/y Russia*, решение от 4.12.2015 г. (голям състав), жалба № 47143/06, точка 269, съгласно което „изискването на доставчика на комуникационни услуги да се покаже разрешение за прихващане, преди да се получи достъп до съобщенията, е една от най-важните гаранции срещу злоупотреба от страна на правоприлагащите органи, като по този начин се гарантира, че във всички случаи на прихващане е получено съответното разрешение.“

([187]) Писмени изявления на Министерството на правосъдието (приложение VII), стр. 4 с допълнителните препратки.

([188]) Писмени изявления на Министерството на правосъдието (приложение VII), № 2.

([189]) Според получената от Комисията информация и като не се вземат предвид специфичните области, които вероятно не се отнасят за предаването на данни в рамките на Щита за личните данни в отношенията между ЕС и САЩ (напр. разследвания на измами в сферата на здравни грижи, малтретиране на деца или контролирани вещества), това се отнася най-вече до определени органи съгласно Закона за неприкосновеността на електронните съобщения Electronic Communications Privacy Act (ECPA), а именно исканията за основна информация за абонатите, сесията и фактурирането (18 U.S.C. § 2703(c)(1), (2), т.е. адрес, тип/продължителност на услугата) и за съдържанието на електронната поща на възраст над 180 дни (18 U.S.C. § 2703(a), (b)). Във втория случай обаче съответното лице трябва да бъде уведомено и по този начин да му се даде възможност да оспори искането в съда. Вж. също общия преглед на Министерство на правосъдието, Търсене и конфискация на компютри и получаване на електронни доказателства в наказателни разследвания (Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations), глава 3: Закон за съхранените съобщения (Stored Communications Act), стр. 115—138.

([190]) Съгласно писмените изявления на правителството на САЩ получателите на административните разпореждания могат да ги оспорят в съда на основание тяхната неоснователност, т.е. че са прекалени, репресивни или обременяващи. Вж. писмените изявления на Министерството на правосъдието (приложение VII), стр. 2.

(129) Същото се прилага и при използването на административни разпореждания за цели от обществен интерес. Освен това, съгласно писмените изявления на правителството на САЩ в тези случаи се прилагат сходни по същество ограничения, тъй като агенциите могат да искат достъп само до данни, които са релевантни по въпроси, попадащи в обхвата на правомощията им и трябва да спазват изискването за основателност.

(130) Освен това в законодателството на САЩ са предвидени редица възможности за съдебна защита на физическите лица срещу публичен орган или негово длъжностно лице, когато тези органи обработват лични данни. Тези възможности, които включват по-специално Закона за административното производство (APA), Закона за свобода на информацията (FOIA) и Закона за неприкосновеността на електронните съобщения (Electronic Communications Privacy Act (ECPA) са достъпни за всички лица, независимо от тяхната националност, при спазване на всички приложими условия.

(131) Като цяло съгласно разпоредбите за съдебния контрол на Закона за административното производство ([191]), „всяко лице, което е претърпяло правно нарушение поради действие на агенцията или е неблагоприятно засегнато или ощетено от действия на агенцията“, има право да поиска съдебен контрол. ([192]) Това включва възможността да се поиска от Съда да „обяви за незаконно и да отмени действие, констатации и заключения на агенцията, за които е установено, че представляват […] произвол, каприз, злоупотреба с правото на преценка, или по друг начин не са в съответствие със закона“ ([193]).

(132) По-конкретно, в дял II на Закона за неприкосновеността на електронните съобщения (Electronic Communications Privacy Act) се предвижда система на законоустановените права на ([194]) неприкосновеност на личния живот и по този начин се урежда достъпът за целите на правоприлагането до съдържанието на кабелни, устни или електронни съобщения, съхранявани от доставчици на услуги от трети страни ([195]). Със закона достъпът до такива съобщения се обявява за незаконен (т.е. без разрешение от съда или допустим другояче) и се дава възможност засегнатото физическо лице да предяви граждански иск в американски федерален съд за действителни и наказателни щети, както и за компенсация или установително решение срещу държавен служител, който произволно е извършил такива незаконни действия, или срещу Съединените американски щати.

(133) Също така съгласно Закона за свобода на информацията (FOIA, 5 U.S.C., § 552) всяко лице има право да поиска достъп до документите на федерални агенции и след изчерпване на административните средства за защита да предяви това право по съдебен ред, освен доколкото тези данни са защитени от публично оповестяване по силата на освобождаване или специално изключение във връзка с правоприлагането. ([196])

([191]) 5 U.S.C., § 702.

([192]) Като цяло само „окончателно“ действие на агенцията, вместо „предварително, процедурно или междинно“ действие на дадена агенция подлежи на съдебен контрол. Вж. 5 U.S.C. § 704.

([193]) 5 U.S.C. § 706(2)(A).

([194]) 18 U.S.C. §§ 2701-2712.

([195]) Законът за неприкосновеността на електронните съобщения (ECPA) осигурява защита на съобщенията, държани от две определени категории доставчици на мрежови услуги, а именно доставчици на: i) електронни съобщителни услуги, като например телефонията или електронната поща; ii) отдалечени изчислителни услуги, като например услуги по компютърно съхранение или обработване.

([196]) Тези изключения обаче са формулирани. Например съгласно 5 U.S.C. § 552 (b)(7) правата по FOIA не се прилагат за „документи или информация, изготвени за целите на правоприлагането, но само доколкото съставянето на такива документи или информация (A) може разумно да се очаква да възпрепятства процеса на правоприлагането, (Б) би лишило лицето от правото на справедлив процес или безпристрастна присъда, (В) може разумно да се очаква да представлява необосновано нарушение на неприкосновеността на личния живот, (Г) може разумно да се очаква да разкрие самоличността на поверителен източник, в това число държавна, местна или чуждестранна агенция или орган или частна институция, които са предоставили информация на поверителна основа, и — за документ или информация, изготвени от съдебен правоприлагащ орган в хода на наказателно разследване, или от агенция, провеждаща законно разузнавателно разследване във връзка с националната сигурност — информация, предоставена от поверителен източник, (Д) би разкрило техники и процедури за разследвания или наказателни преследвания за целите на правоприлагането или насоки за тях, ако може разумно да се очаква разкриването да предизвика риск от заобикаляне на закона, или (Е) може разумно да се очаква да застраши живота или физическата безопасност на дадено физическо лице.“ Също така „при искане, което предполага достъп по документи [чието съставяне може разумно да се очаква да възпрепятства процеса на правоприлагането] и — (A) разследването или производството предполага евентуално нарушение на наказателното право; и Б) има причина да смята, че i) обектът на разследването или производството не е запознат с висящото производство и ii) разкриването на наличието на документи може разумно да се очаква да възпрепятства процеса на правоприлагането, агенцията може да разглежда тези документи като документи, за които не се отнасят изискванията от настоящия раздел, само за толкова време, за колкото продължава съответното обстоятелство.“ (5 U.S.C. § 552 (c)(1)).

(134) Освен това няколко други закона дават на физическите лица право да заведат дело срещу публичен орган или длъжностно лице в САЩ във връзка с обработката на личните им данни, като например Закона за телефонното подслушване (Wiretap Act) ([197]), Закона за компютърните измами и злоупотреби (Computer Fraud and Abuse Act) ([198]), the Federal Torts Claim Act ([199]), Закона за правото на неприкосновеност на личните финанси (Right to Financial Privacy Act) ([200]), и Закон за оповестяване на информация за кредити (Fair Credit Reporting Act) ([201]).

(135) Поради това Комисията стига до заключението, че в Съединените американски щати са установени правила, предвидени да бъде ограничена всяка намеса за целите на правоприлагането ([202]) или за други цели от обществен интерес в основните права на физическите лица, чиито лични данни се предават от Съюза към Съединените американски щати съгласно Щита за личните данни в отношенията между ЕС и САЩ, като тази намеса се ограничава до строго необходимото за постигането на въпросната легитимна цел като посочените правила гарантират ефективна правна защита срещу подобна намеса.

4. АДЕКВАТНА СТЕПЕН НА ЗАЩИТА СЪГЛАСНО ЩИТА ЗА ЛИЧНИТЕ ДАННИ В ОТНОШЕНИЯТА МЕЖДУ ЕС И САЩ

(136) С оглед на тези констатации Комисията счита, че Съединените американски щати гарантират адекватна степен на защита за личните данни, които се предават от Съюза към самосертифицирани дружества в Съединените американски щати съгласно Щита за личните данни в отношенията между ЕС и САЩ.

(137) По-специално Комисията счита, че Принципите, публикувани от Министерството на търговията на САЩ, като цяло осигуряват ниво на защита на личните данни, което по същество е равностойно на гарантираното от основните принципи, установени в Директива 95/46/ЕО.

(138) В допълнение към това ефективното прилагане на Принципите е гарантирано от задълженията за прозрачност и управлението на Щита за личните данни от страна на Министерството на търговията.

(139) Освен това Комисията счита, че взети заедно механизмите за надзор и защита, предвидени съгласно Щита за личните данни, позволяват нарушенията на Принципите от организациите — участници в Щита за личните данни, да бъдат установявани и наказвани на практика и осигуряват средства за правна защита на субектите на данни, с възможност за достъп до свързаните с тях лични данни и евентуалното коригиране или заличаване на тези данни.

(140) И накрая, въз основа на наличната информация за правния ред на САЩ, включително съгласно писмените изявления и ангажименти на правителството на САЩ, Комисията счита, че всяка намеса на публичните органи на Съединените американски щати за целите на националната сигурност, правоприлагането или за други цели от обществен интерес в основните права на физическите лица, чиито данни се предават от Съюза към Съединените щати съгласно Щита за личните данни, и произтичащите от това ограничения, налагани на самосертифицираните организации във връзка със спазването от тяхна страна на Принципите, ще бъде ограничена до строго необходимото за постигането на набелязаната легитимна цел, и че е налице ефективна правна защита срещу подобна намеса.

([197]) 18 U.S.C. §§ 2510 и следв. Съгласно Закона за телефонното подслушване (Wiretap Act) (18 U.S.C. § 2520) лице, чиито кабелни, устни или електронни съобщения се прихващат, разкриват или умишлено се използват, може да заведе гражданско дело за нарушение на Закона за телефонното подслушване, в това число при определени обстоятелства — срещу конкретен държавен служител или Съединените американски щати. За събиране на информация, свързана с адреси, и друга информация без съществено съдържание (напр. IP адрес, имейл адрес до/от), вж. също глава „Pen Registers and Trap and Trace Devices“ в дял 18 (18 U.S.C. §§ 3121-3127 и — за граждански искове, § 2707).

([198]) 18 U.S.C., § 1030. Съгласно Закона за компютърните измами и злоупотреби (Computer Fraud and Abuse Act) дадено лице може да заведе иск срещу друго лице във връзка с преднамерен неразрешен достъп (или над разрешения достъп) с цел получаване на информация от финансова институция, компютърна система на правителството на САЩ или друг конкретен компютър, включително при определени обстоятелства срещу конкретен държавен служител.

([199]) 28 U.S.C. §§ 2671 и следв. Съгласно Закона за федералните претенции при непозволени действия (Federal Tort Claims Act) дадено лице може да заведе иск, при определени обстоятелства, срещу Съединените американски щати във връзка с „небрежност или неправомерно действие или бездействие на държавен служител, който е действал в рамките на служебните си задължения.“

([200]) 12 U.S.C. §§ 3401 и следв. Съгласно Закона за правото на неприкосновеност на личните финанси (Right to Financial Privacy Act), дадено лице може да заведе иск, при определени обстоятелства, срещу Съединените американски щати във връзка с получаването или разкриването на защитени финансови документи в нарушение на закона. Достъпът на държавата до защитени финансови документи като цяло е забранен, освен ако правителството не поиска това по силата на законна призовка или заповед за обиск или, при спазване на ограниченията, с официално писмено искане, а лицето, чиято информация се иска, бъде уведомено за подаденото искане.

([201]) 15 U.S.C. §§ 1681-1681x. Съгласно Закона за оповестяване на информация за кредити (Fair Credit Reporting Act) дадено лице може да предяви иск срещу всяко лице, което не спазва изискванията (по-специално необходимостта от законно разрешение) по отношение на събирането, разпространението и използването на информация за кредитите на потребителите, или, при определени обстоятелства, срещу държавна агенция.

([202]) Съдът на Европейските общности призна, че правоприлагането е законосъобразна цел на политиката. Вж. съединени дела C-293/12 и C-594/12, *Digital Rights Ireland и други*, EU:C:2014:238, точка 42. Вж. също член 8, параграф 2 от (ЕКПЧ) и решението на Европейския съд по правата на човека по делото *Weber и Saravia с/у Германия*, жалба № 54934/00, точка 104.

(141) Комисията стига до заключението, че това съответства на изискванията, установени в член 25 от Директива 95/46/ЕО, тълкувани в светлината на Хартата на основните права на Европейския съюз, както това е разяснено от Съда, по-специално в решението по делото *Schrems*.

5. ДЕЙСТВИЯ НА ОРГАНИТЕ ПО ЗАЩИТА НА ДАННИТЕ И ИНФОРМАЦИЯ ДО КОМИСИЯТА

(142) В решението по делото *Schrems* Съдът поясни, че Комисията няма компетенции да ограничава правомощията на ОЗД, които произтичат от член 28 от Директива 95/46/ЕО (включително правомощието да спрат предаването на данните), когато едно лице, предявило иск в съответствие с тази разпоредба, постави под въпрос съвместимостта на решение за адекватност на Комисията със защитата на основното право на неприкосновеност на личния живот и защитата на личните данни ([203]).

(143) За целите на ефективния мониторинг на функционирането на Щита за личните данни Комисията трябва да бъде информирана от държавите членки относно съответно предприетите действия от ОЗД.

(144) Освен това Съдът прие, че в съответствие с член 25, параграф 6, втора алинея от Директива 95/46/ЕО държавите членки и техните органи трябва да предприемат необходимите мерки за спазването на актовете на институциите на Съюза, тъй като последните по принцип се ползват с презумпция за законосъобразност и съответно произвеждат правно действие, докато не бъдат оттеглени, отменени в производство по жалба за отмяна или обявени за невалидни вследствие на преюдициално запитване или възражение за незаконосъобразност. Следователно решение за адекватност на Комисията, прието съгласно член 25, параграф 6 от Директива 95/46/ЕО, е обвързващо за всички органи на държавите членки адресати, включително за независимите им надзорни органи ([204]). Ако такъв орган получи жалба, в която се поставя под въпрос спазването от страна на решението за адекватност на Комисията на защитата на основното право на неприкосновеност на личния живот и защитата на личните данни, и този орган счете за основателни изложените твърдения, националното законодателство трябва да предвижда правни способи, позволяващи на съответния орган да изложи твърденията за нарушения пред национален съд, и ако последният споделя съмненията, той трябва да спре производството и да сезира Съда на ЕС с преюдициално запитване ([205]).

6. ПЕРИОДИЧНИ ПРЕГЛЕДИ НА КОНСТАТАЦИИТЕ ЗА АДЕКВАТНОСТ

(145) Предвид фактът, че степента на защита, осигурявана от правния ред на САЩ, може да претърпи промени, след приемането на настоящото решение Комисията ще извършва периодични проверки дали констатациите във връзка с адекватността на степента на защита, гарантирана от Щита за личните данни в отношенията между ЕС и САЩ остават фактически и правно обосновани. Такава проверка е наложителна във всички случаи, когато Комисията получи някаква информация, която поражда основателни съмнения в това отношение ([206]).

(146) Следователно Комисията ще извършва постоянно наблюдение над цялостната рамка за предаването на лични данни, създадена с Щита за личните данни в отношенията между ЕС и САЩ, както и над спазването от страна на органите на САЩ на писмените изявления и ангажиментите, съдържащи се в документите от приложенията към настоящото решение. За да се улесни този процес, САЩ се ангажира да информира Комисията за съществени промени в правото на САЩ, когато е целесъобразно, в областта на защитата на данните и на приложимите ограничения и гаранции по отношение на достъпа до лични данни от страна на публичните органи. Освен това настоящото решение подлежи на годишен съвместен преглед, който ще обхваща всички аспекти на функционирането на Щита за личните данни в отношенията между ЕС и САЩ, включително действието на изключенията от Принципите за целите на националната сигурност и правоприлагането. Освен това, тъй като констатацията за адекватността може да бъде повлияна и от развитието на правото в законодателството на Съюза, Комисията ще оцени степента на защита, предоставена от Щита за защита на личните данни, след влизането в сила на ОРЗД.

(147) За извършването на годишния съвместен преглед, както това е разгледано в приложения I, II и VI, Комисията ще се срещне с представители на Министерството на търговията и Федералната търговска комисия, ако е необходимо придружени от представители на други министерства и агенции, участващи в прилагането на договореностите съгласно Щита за личните данни, а по въпроси от областта на националната сигурност — и с представители на ODNI, на други разузнавателни структури и с омбудсмана. Срещата е отворена за участие на ОЗД от ЕС и представители на работната група по член 29.

([203]) Решение по делото *Schrems*, точки 40 и следв. и т.101—103.
([204]) Решение по делото *Schrems*, точки 51, 52 и 62.
([205]) Делото *Schrems*, точка 65.
([206]) Делото *Schrems*, точка 76.

(148) В рамките на годишния съвместен преглед Комисията ще изиска от Министерството на търговията да предостави изчерпателна информация относно всички съответни аспекти на функционирането на Щита за личните данни в отношенията между ЕС и САЩ, включително случаите, по които Министерството на търговията е било сезирано от ОЗД, и резултатите от *служебни* проверки за спазването. Също така Комисията ще се стреми да намери обяснение по евентуални въпроси или теми във връзка с Щита за личните данни в отношенията между ЕС и САЩ и неговото функциониране, които възникнат от налична информация, включително от докладите за прозрачност, предвидени съгласно Закона за свободата в САЩ (USA FREEDOM Act), публични доклади на националните разузнавателни органи на САЩ, на ОЗД, групи по въпросите на неприкосновеността на личния живот, медийна информация или други възможни източници. Освен това, за улесняване на работата на Комисията в тази връзка, държавите членки следва да уведомяват Комисията за случаи, когато действия на органите в Съединените американски щати, отговорни за гарантиране спазването на Принципите, не са успели да осигурят спазването и когато са налице признаци, че действията на публичните органи в САЩ, които отговарят за националната сигурност или за предотвратяването, разследването, разкриването или наказателното преследване на престъпления, не гарантират изискваното ниво на защита.

(149) Въз основа на годишния съвместен преглед Комисията ще изготви публичен доклад, който ще представи на Европейския парламент и на Съвета.

7. **СУСПЕНДИРАНЕ НА РЕШЕНИЕТО ЗА АДЕКВАТНОСТ**

(150) Когато въз основа на проверки или друга налична информация Комисията направи заключение, че са налице явни признаци, че ефективното спазване на Принципите на неприкосновеност на личния живот в Съединените щати вероятно повече не е гарантирано, или че действията на публичните органи в САЩ, които отговарят за националната сигурност или за предотвратяването, разследването, разкриването или наказателното преследване на престъпления, не гарантират изискваното ниво на защита, тя ще уведоми за това Министерството на търговията и ще изиска да бъдат предприети подходящи мерки, за да бъде бързо отстранена всяка потенциална възможност за неспазване на Принципите в рамките на определен в разумни граници срок. Ако след изтичането на определения срок органите на САЩ не докажат в задоволителна степен, че Щитът за личните данни в отношенията между ЕС и САЩ продължава да гарантира ефективното спазване и адекватна степен на защита, Комисията ще инициира процедурата, в резултат на която настоящото решение ще бъде частично или изцяло суспендирано или отменено ([207]). Алтернативна възможност е Комисията да направи предложение за изменение на настоящото решение, например като се ограничи обхватът на констатациите за адекватността само до предаване на данни при спазване на допълнителни изисквания.

(151) По-специално Комисията ще инициира процедурата за суспендиране или отмяна в случай на:

а) признаци, че органите на САЩ не спазват писмените изявления и ангажиментите, съдържащи се в документите от приложенията към настоящото решение, включително по отношение на условията и ограниченията за достъпа от страна на публичните органи на САЩ за целите на правоприлагането, националната сигурност или други цели от обществен интерес, до лични данни, предавани съгласно Щита за личните данни в отношенията между ЕС и САЩ;

б) неефективно предприемане на действия по жалби на субекти на данни от ЕС; в това отношение Комисията ще взема предвид всички обстоятелства, които оказват влияние върху възможността да бъдат приведени в изпълнение правата на субектите на данни от ЕС, включително по-специално доброволният ангажимент на самосертифицирани дружества в САЩ да си сътрудничат с ОЗД и да спазват техните препоръки; или

в) непредоставяне от страна на омбудсмана към Щита за личните данни на навременни и подходящи отговори на искания на субекти на данни от ЕС.

(152) Също така Комисията ще обмисли инициирането на процедура за изменение, суспендиране или отмяна на настоящото решение, ако в контекста на годишния съвместен преглед на функционирането на Щита за личните данни в отношенията между ЕС и САЩ или по друг начин Министерството на търговията или други министерства или агенции, участващи в прилагането на Щита за личните данни, а по въпроси от сферата на националната сигурност — представителите на разузнавателните структури на САЩ или омбудсманът, не предоставят информацията или разясненията, необходими за преценката за спазването на Принципите, за ефективността на процедурите за разглеждане на жалбите или за всяко понижаване на изискваната степен на защита вследствие от действия на националните разузнавателни органи на САЩ, и по-специално вследствие на събиране и/или достъп

([207]) Считано от датата на прилагане на Общия регламент относно защитата на данните, Комисията ще упражнява правомощията си да приеме по надлежно обосновани наложителни причини за спешност акт за изпълнение за суспендиране на настоящото решение, който ще се прилага незабавно, без предварително представяне пред съответния комитет в рамките на процедурата на комитология, и ще остане в сила за период не по-дълъг от шест месеца.

до лични данни, което не е било ограничено до строго необходимото и не е пропорционално. В тази връзка Комисията ще взема предвид степента, в която съответната информация може да бъде набавена от други източници, включително доклади на самосертифицирани дружества в САЩ, както това е предвидено в Закона за свободата в САЩ (USA FREEDOM Act).

(153) Работната група за защита на физическите лица по отношение на обработването на личните данни, създадена по силата на член 29 от Директива 95/46/ЕО, публикува своето становище за степента на защита, предоставяна от Щита за личните данни в отношенията между ЕС и САЩ ([208]), което е взето предвид при изготвянето на настоящото решение.

(154) Европейският парламент прие резолюция относно трансатлантическите потоци от данни ([209]).

(155) Мерките, предвидени в настоящото решение, са в съответствие със становището на комитета, създаден съгласно член 31, параграф 1 от Директива 95/46/ЕО,

ПРИЕ НАСТОЯЩОТО РЕШЕНИЕ:

Член 1

1. По смисъла на член 25, параграф 2 от Директива 95/46/ЕО Съединените американски щати гарантират адекватна степен на защита за личните данни, които се предават от Съюза към организации в Съединените щати съгласно Щита за личните данни в отношенията между ЕС и САЩ.

2. Щитът за личните данни в отношенията между ЕС и САЩ се състои от Принципите, публикувани от Министерството на търговията на САЩ на 7 юли 2016 г., както те са установени в приложение II, и официалните писмени изявления и ангажиментите, съдържащи се в документите, поместени в приложения I и III—VII.

3. За целите на параграф 1 личните данни се предават съгласно Щита за личните данни в отношенията между ЕС и САЩ, когато предаването се извършва от Съюза към организации в Съединените американски щати, които са включени в „списъка към Щита за личните данни“, който се поддържа и се предоставя за публичен достъп от Министерството на търговията на САЩ, в съответствие с точки I и III от Принципите, установени в приложение II.

Член 2

Настоящото решение не засяга прилагането на разпоредбите на Директива 95/46/ЕО, по-специално на член 4 от нея, с изключение на член 25, параграф 1, който се отнася за обработването на лични данни в рамките на територията на държавите членки.

Член 3

Когато компетентните органи в държавите членки упражняват правомощията си по член 28, параграф 3 от Директива 95/46/ЕО, което води до спиране или окончателна забрана за потоците от данни към дадена организация в Съединените американски щати, включена в списъка към Щита за личните данни съобразно с точки I и III от Принципите, установени в приложение II, за да защитят физическите лица във връзка с обработването на техните лични данни, съответната държава членка уведомява незабавно Комисията.

Член 4

1. Комисията извършва постоянен мониторинг на функционирането на Щита за личните данни в отношенията между ЕС и САЩ, с цел да преценява дали Съединените американски щати продължават да гарантират адекватна степен на защита на предаваните лични данни съгласно Щита за личните данни от Съюза към организации в Съединените американски щати.

([208]) Становище 01/2016 относно проект на решение за адекватността на Щита за личните данни в отношенията между ЕС и САЩ, публикувано на 13 април 2016 г.

([209]) Резолюция на Европейския парламент от 26 май 2016 г. относно трансатлантическите потоци от данни ((2016/2727 (RSP)).

2. Държавите членки и Комисията взаимно се уведомяват за случаите, когато изглежда, че правителствените органи в Съединените американски щати, които имат законоустановени правомощия да привеждат в изпълнение спазването на Принципите, установени в приложение II, не осигуряват ефективни механизми за откриване и надзор, които да позволяват идентифицирането на нарушения на Принципите и наказването им на практика.

3. Държавите членки и Комисията взаимно се уведомяват за евентуални признаци, че намесата от страна на публичните органи на САЩ, които отговарят за националната сигурност, правоприлагането или други обществени интереси, в правото на физическите лица на защита на личните им данни надхвърля строго необходимото, и/или че няма ефективна правна защита срещу подобна намеса.

4. В срок до една година от датата на нотифицирането на настоящото решение до държавите членки и ежегодно след това Комисията ще извършва оценка на констатацията, съдържаща се в член 1, параграф 1 въз основа на цялата налична информация, включително получената като част от годишния съвместен преглед, разгледан в приложения I, II и VI.

5. Комисията докладва всички съответни констатации на Комитета, създаден съгласно член 31 от Директива 95/46/ЕО.

6. Комисията ще представи проект на мерки в съответствие с процедурата по член 31, параграф 2 от Директива 95/46/ЕО с цел суспендиране, изменение или отмяна на настоящото решение или ограничаване на приложното му поле, когато наред с останалото са налице признаци:

— че публичните органи на САЩ не спазват писмените изявления и ангажиментите, съдържащи се в документите от приложенията към настоящото решение, включително по отношение на условията и ограниченията за достъпа от страна на публичните органи на САЩ за целите на правоприлагането, националната сигурност или други цели от обществен интерес, до лични данни, предавани съгласно Щита за личните данни в отношенията между ЕС и САЩ;

— за системно неефективно намиране на решение по жалби на субекти на данни от ЕС; или

— за системно непредоставяне от страна на омбудсмана към Щита за личните данни на навременни и подходящи отговори на искания на субекти на данни от ЕС съгласно изискването в раздел 4, буква д) от приложение III.

Комисията внася проекти на такива мерки и когато липсата на съдействие от страна на органите, които трябва да осигурят функционирането на Щита за личните данни в отношенията между ЕС и САЩ в Съединените щати не позволява на Комисията да определи дали е засегната констатацията в член 1, параграф 1.

Член 5

Държавите членки предприемат необходимите мерки, за да се съобразят с настоящото решение.

Член 6

Адресати на настоящото решение са държавите членки.

Съставено в Брюксел на 12 юли 2016 година.

За Комисията
Věra JOUROVÁ
Член на Комисията

ПРИЛОЖЕНИЕ I

Писмо от министъра на търговията на САЩ Penny Pritzker

7 юли 2016 г.

Г-жа Вера Йоурова
Комисар по въпросите на правосъдието, потребителите и равнопоставеността между половете
Европейска комисия
Rue de la Loi/Westraat 200
1049 Брюксел
Белгия

Уважаема комисар Йоурова,

От името на Съединените щати за мен е удоволствие да предам с настоящото писмо пакет от материали към Щита за личните данни в отношенията между ЕС и САЩ, резултат от двугодишните ползотворни обсъждания между нашите екипи. Наред с другите материали, които са на разположение на Комисията от публични източници, този пакет осигурява много здрава основа за нови констатации на Европейската комисия относно адекватността ([1]).

Ние заедно трябва да се гордеем с подобренията на рамката. Щитът за личните данни се основава на принципи, за които има силна консенсусна подкрепа от двете страни на Атлантика, и ние подсилихме тяхното действие. Чрез съвместната си работа имаме реалната възможност да подобрим защитата на неприкосновеността на личния живот в целия свят.

Пакетът към Щита за личните данни съдържа Принципите на Щита за личните данни заедно с включеното като приложение 1 писмо, в което Администрацията по международната търговия (АМТ) към управляващото програмата Министерство на търговията разглежда ангажиментите, поети от нашето министерство, за да гарантира ефективното функциониране на Щита за личните данни. Също така пакетът включва приложение 2, в което са разгледани други ангажименти на Министерството на търговията във връзка с новия арбитражен модел, който съществува съгласно Щита за личните данни.

Разпоредих на моите служители да бъдат вложени всички ресурси, необходими за експедитивното и цялостно прилагане на рамката на Щита за личните, както и за да се гарантира своевременното спазване на ангажиментите, посочени в приложения 1 и 2.

Пакетът към Щита за личните данни включва също така и други документи от други органи на Съединените щати, а именно:

— писмо от Федералната търговска комисия (ФТК), в което се разглеждат действията от нейна страна по прилагането на Щита за личните данни;

— писмо от Министерството на транспорта, в което се разглеждат действията от негова страна по прилагането на Щита за личните данни;

— две писма, изготвени от Службата на директора на Националното разузнаване (СДНР), относно гаранциите и ограниченията, които се прилагат за органите на националната сигурност на САЩ;

— писмо от Държавния департамент и съпътстващ го меморандум, в които се описва ангажиментът на Държавния департамент да създаде нов омбудсман към Щита за личните данни за отправяне на запитвания относно практиките в радиоелектронното разузнаване на Съединените щати; и

— писмо, изготвено от Министерството на правосъдието относно гаранциите и ограниченията по отношение на достъпа от страна на правителството на САЩ за целите на правоприлагането и за цели от обществен интерес.

Можете да бъдете уверена, че Съединените щати гледат сериозно на тези ангажименти.

([1]) Предвид това че решението на Комисията относно адекватността на защитата, осигурена от Щита за личните данни в отношенията между ЕС и САЩ, се прилага в Исландия, Лихтенщайн и Норвегия, пакетът към Щита за личните данни ще обхване както Европейския съюз, така и тези три държави.

В срок от 30 дни след окончателното одобрение на решението относно адекватността пълният пакет към Щита за личните данни ще бъде предоставен за публикуване във *Федералния регистър*.

Очакваме с нетърпение да работим с Вас в хода на прилагането на Щита за личните данни и заедно да се заемем със следващия етап от този процес.

С уважение,

Penny Pritzker

Приложение 1

Писмо от изпълняващия длъжността заместник-министъра на международната търговия Ken Hyatt

До уважаемата Вера Йоурова
Комисар по въпросите на правосъдието, потребителите и равнопоставеността между половете
Европейска комисия
Rue de la Loi/Westraat 200
1049 Брюксел
Белгия

Уважаема комисар Йоурова,

От името на Администрацията по международната търговия за мен е удоволствие да опиша повишената степен на защита на личните данни, която осигурява рамката за Щита за личните данни в отношенията между ЕС и САЩ („Щитът за личните данни“ или „рамката“), и ангажиментите, които пое Министерството на търговията („Министерството“), за да гарантира ефективното функциониране на Щита за личните данни. Финализирането на това историческо споразумение е значимо постижение за неприкосновеността на личния живот и за дружествата от двете страни на Атлантическия океан. То дава увереност на физическите лица от ЕС, че техните данни ще бъдат защитени и че разполагат със средства за правна защита за намирането на решения на евентуални проблеми. Дава сигурност, която ще спомогне за растежа на трансатлантическата икономика, като гарантира на хиляди европейски и американски дружества възможност да продължат да инвестират и да извършват стопанска дейност през границите ни. Щитът за личните данни е резултат от повече от две години усилена работа и сътрудничество с вас, нашите колеги в Европейската комисия („Комисията“). Очакваме с нетърпение да продължим да работим с Комисията, за да гарантираме, че Щитът за личните данни ще функционира според предвиденото.

Ние работихме съвместно с Комисията за разработването на Щита за личните данни, за да могат организациите, установени в Съединените щати, да изпълнят изискванията за адекватност по отношение на защитата на данните съгласно правото на ЕС. Новата рамка ще донесе няколко съществени ползи както за физическите лица, така и за дружествата. На първо място, тя осигурява важен набор от защити за неприкосновеността на личния живот по отношение на данните на физическите лица от ЕС. Тя изисква от организациите — участници от САЩ, да разработят съответна политика в областта на неприкосновеността на личния живот, да се ангажират публично да спазват Принципите на Щита за личните данни, така че ангажиментите им да подлежат на прилагане съгласно правото на САЩ, ежегодно да пресертифицират спазването пред министерството, да осигурят възможност за физическите лица от ЕС за безплатно, независимо разрешаване на спорове, и по отношение на тях Федералната търговска комисия на САЩ („ФТК“), Министерство на транспорта („МТ“) или друг правоприлагащ орган да упражнява правомощията си. На второ място, Щитът за личните данни ще позволи на хиляди дружества в Съединените щати и дъщерни на европейски дружества в САЩ да получават лични данни от Европейския съюз в улеснение на потоците от данни, които са в основата на трансатлантическата търговия. Трансатлантическите икономически отношения вече са най-мащабните в света, като на тях се дължи половината от световното икономическо производство и търговия на стоки и услуги на стойност близо един трилион долара, което осигурява милиони работни места от двете страни на Атлантика. Дружествата, които разчитат на трансатлантически потоци от данни, са представители на всички промишлени сектори и включват както големи дружества — сред първите 500 според класацията на Fortune, така и много малки и средни предприятия (МСП). Трансатлантическите потоци от данни позволяват на организации в САЩ да обработват данни, необходими за предлагането на стоки, услуги и възможности за трудова заетост на лица от Европа. Щитът за личните данни е в подкрепа на споделените принципи за неприкосновеност на личния живот, като изгражда мост между различията в нашите правни подходи и същевременно способства за постигането на целите в областта на търговията и икономиката както на Европа, така и на Съединените щати.

Въпреки че решението на едно дружество да се самосертифицира съгласно тази нова рамка ще бъде доброволно, след като то се ангажира публично с Щита за личните данни неговият ангажимент подлежи на прилагане съгласно правото на САЩ от Федералната търговска комисия или Министерството на транспорта, в зависимост от това кой орган е компетентен по отношение на организацията — участник в Щита за личните данни.

Подобрения съгласно Принципите на Щита за личните данни

Така създаденият Щит за личните данни повишава защитата на личните данни посредством:

— изискването за предоставяне на допълнителна информация на лицата съгласно принципа за уведомяване, включително за деклариране на участието на организацията в Щита за личните данни, декларация за правото на физическото лице на достъп до личните данни, и определянето на съответната независима организация за разрешаване на спорове;

— увеличаване на защитата на личните данни, които се предават от организация — участник в Щита за личните данни, към администратор на трета страна, като се поставя изискване към страните да сключат договор, в който е предвидено, че тези данни ще бъдат обработвани само с ограничени и конкретно определени цели в съответствие със съгласието, дадено от лицето, както и че получателят ще осигури същата степен на защита, която се осигурява от Принципите;

— увеличаване на защитата на личните данни, които се предават от организация — участник в Щита за личните данни, към трета страна представител, включително като се поставя изискване към организацията — участник в Щита за личните данни: да предприема обосновани и съответни мерки, за да гарантира, че представителят ефективно обработва предадената лична информация по начин, който съответства на задълженията на организацията съгласно Принципите; при уведомяване да предприема обосновани и съответни мерки, за да преустанови и отстрани последиците от неразрешено обработване; и при поискване да предоставя на министерство обобщение или представително копие на съответните разпоредби във връзка с личните данни от договора с третата страна;

— предвиждане, че организацията — участник в Щита за личните данни, носи отговорност за обработването на личната информация, която получава съгласно Щита за личните данни и впоследствие предава на трета страна, която изпълнява функциите на представител от нейно име, както и че организацията — участник в Щита за личните данни, ще продължи да носи отговорност съгласно Принципите, ако нейният представител обработва тази лична информация по начин, който не съответства на Принципите, освен ако организацията докаже, че не носи отговорност за събитието, породило вредата;

— поясняване, че организацията — участник в Щита за личните данни, трябва да ограничава личната информация до необходимото за целите на обработването;

— поставяне на изискване към организациите да удостоверяват ежегодно пред министерството своя ангажимент да прилагат Принципите по отношение на информацията, която са получили, докато са участвали в Щита за личните данни, в случай че напуснат Щита за личните данни и изберат да запазят тези данни;

— изискване да бъдат осигурени независими механизми за защита, безплатно за физическите лица;

— поставяне на изискване към организациите и избраните от тях независими механизми за защита да отговарят в кратки срокове на запитвания и искания за информация от страна на министерство във връзка с Щита за личните данни;

— поставяне на изискване към организациите да отговарят експедитивно на жалби във връзка със спазването на Принципите, насочени към тях от органи на държавите — членки на ЕС, чрез министерството; и

— поставяне на изискване към организациите — участници в Щита за личните данни, да обявяват публично всички съответно свързани с Щита за личните данни части от евентуални доклади за спазването или доклади за оценка, представени на ФТК, ако по отношение на организацията е издадена заповед от ФТК или съдебно разпореждане във връзка с неспазване.

Управление и надзор на Програмата на Щита за личните данни от Министерство на търговията

Министерство потвърждава ангажимента си да поддържа и предоставя за публичен достъп официален списък на организациите от САЩ, които са се самосертифицирали пред министерството и са декларирали ангажимента си да спазват Принципите („Списък към Щита за личните данни“). Министерството ще актуализира Списъка към Щита за личните данни, като ще заличава от него организациите, които са се оттеглили доброволно, не са изпълнили изискването за ежегодно пресертифициране съгласно процедурите на министерството или е установено, че трайно не спазват Принципите. Също така министерството ще поддържа и предоставя за публичен достъп официален регистър на организациите в САЩ, които по-рано са били самосертифицирани в министерството, но са заличени от Списъка към Щита за личните данни, включително заличените поради трайно неспазване на Принципите. Министерството ще посочи причините, поради които всяка организация е била отстранена от списъка.

В допълнение към това министерството се ангажира да засили управлението и надзора на Щита за личните данни. По-специално министерството ще:

Предоставя допълнителна информация на уебсайта на Щита за личните данни:

— поддържа Списъка към Щита за личните данни, както и справка за организациите, които по-рано са се самосертифицирали, че ще спазват принципите, но повече не се ползват с предимствата на Щита за личните данни;

— постави на видно място пояснение, с което да става ясно, че всички организации, които са били заличени от Списъка към Щита за личните данни, повече не се ползват с предимствата на Щита за личните данни, но въпреки това трябва да продължат да прилагат Принципите за личната информация, която са получили, докато са участвали в Щита за личните данни, за времето през което продължават да съхраняват тази информация; и

— предостави електронна връзка към списъка на регистрираните във Федералната търговска комисия случаи във връзка с Щита за личните данни, който се поддържа на уебсайта на ФТК.

Проверява изискванията за самосертифициране:

— преди окончателното самосертифициране на дадена организация (или ежегодното ѝ пресертифициране) и включването ѝ в Списъка към Щита за личните данни проверява дали организацията:

  — е посочила необходимата информация за връзка с нея;

  — е описала дейностите, които извършва във връзка с получената от ЕС лична информация;

  — е посочила каква е личната информация, за която се отнася самосертифицирането;

  — ако организацията има публичен уебсайт, е предоставила хипервръзка към адреса, където е предоставила на разположение политиката си в областта на неприкосновеността на личния живот и тази политика е достъпна на адреса на предоставената хипервръзка, а ако организацията няма публичен уебсайт, е посочила къде е предоставила на разположение за публичен достъп политиката си в областта на неприкосновеността на личния живот;

  — е включила в съответната си политика в областта на неприкосновеността на личния живот декларация, че спазва Принципите, и когато политиката ѝ в областта на неприкосновеността на личния живот е на разположение онлайн, е предоставила хипервръзка към страницата на Щита за личните данни на уебсайта на министерството;

  — е определила конкретния законоустановен орган, който е компетентен да разглежда жалби срещу организацията във връзка с евентуални нелоялни или измамни практики или нарушения на законите или разпоредбите, уреждащи неприкосновеността на личния живот (и който е посочен в Принципите или в бъдещо приложение към Принципите);

  — ако организацията е избрала да изпълни изискванията, посочени в буква а), подточки i) и iii) от принципа „Защита, прилагане и отговорност за причинени вреди“, като се е ангажирала да сътрудничи със съответните органи по защита на данните („ОЗД“) в ЕС, е посочила намерението си да сътрудничи с ОЗД при разследването и разрешаването на жалбите, подадени съгласно Щита за личните данни, и по-специално да отговаря на техни запитвания, когато субекти на данни от ЕС са подали жалба директно в националния си ОЗД;

  — е определила програма за неприкосновеността на личния живот, на която организацията е член;

  — е определила метод за проверка, с цел осигуряване на спазването на Принципите (напр. вътрешна или от трета страна);

  — е определила при подаване на самосертификацията си и в своята политика в областта на неприкосновеността на личния живот независимия механизъм за защита, който е на разположение за разследване и разрешаване на жалби;

  — е включила в съответната си политика в областта на неприкосновеността на личния живот, когато тази политиката е на разположение онлайн, хипервръзка към уебсайт или към формуляр за подаване на жалба на независимия механизъм за защита, който е на разположение за разследване на нерешени жалби; и

  — ако организацията е посочила, че възнамерява да получава информация във връзка с човешки ресурси, предавана от ЕС, за използване в контекста на трудови правоотношения, е декларирала ангажимента си да си сътрудничи с ОЗД и да спазва препоръките им за разрешаването на жалби относно нейни дейности във връзка с такива данни, е предоставила на министерството копие от политиката си в областта на неприкосновеността на личния живот на човешките ресурси и е посочила къде е предоставила на разположение на засегнатите служители тази политика, за да могат да я разгледат.

— работи с независими механизми за защита за удостоверяване, че организациите действително са се регистрирали в съответните механизми, които са посочили при самосертифицирането си, когато е поставено изискване за такава регистрация.

Разширява усилията за последващи действия спрямо организациите, които са били заличени от Списъка към Щита за личните данни:

— уведомява организациите, които са заличени от Списъка към Щита за личните данни поради „трайно неспазване“, че нямат право да задържат информацията, събрана съгласно Щита за личните данни; и

— изпраща въпросници до организациите, чието самосертифициране е изтекло или които доброволно са се оттеглили от Щита за личните данни, за да се провери дали организацията ще започне отново да участва, или ще се отпише, или ще продължи да прилага Принципите за личната информация, която е получила, докато е участвала в Щита за личните данни, и ако възнамерява да задържи личната информация, да удостовери кой в рамките на организацията ще служи за лице за постоянен контакт по въпросите във връзка с Щита за личните данни.

Търси неверни твърдения за участие и намира решения:

— прави преглед на политиката в областта на неприкосновеността на личния живот на организации, които са участвали в програма съгласно Щита за личните данни, но са били заличени от Списъка към Щита за личните данни, за да се следи за неверни твърдения за участие в Щита за личните данни;

— текущо, когато една организация: а) се оттегли от участие в Щита за личните данни, б) не се пресертифицира за спазването на Принципите или в) бъде отстранена от участие в Щита за личните данни, по-специално поради „трайно неспазване“, предприема по служебен път проверка за установяване дали организацията е изтрила от съответните публикации относно политиката си в областта на неприкосновеността на личния живот всички упоменавания на Щита за личните данни, които водят до заключението, че продължава да участва активно и се ползва с предимствата от участието си в Щита за личните данни. Когато министерството констатира, че тези упоменавания не са премахнати, той ще предупреди организацията, че ще отнесе въпроса според случая до съответната инстанция за евентуално предприемане на действия по правоприлагане, ако организацията продължава да твърди, че е сертифицирана съгласно Щита за личните данни. Ако организацията нито премахва упоменаванията, нито самосертифицира своето съответствие по отношение на Щита за личните данни, министерството ще отнесе въпроса по служебен път до ФТК, МТ или друг съответен правоприлагащ орган, или в случаите, когато това е уместно, ще предприеме действия по прилагане във връзка със сертификационния знак съгласно Щита за личните данни;

— полага други усилия да следи за неверни твърдения за участие в Щита за личните данни и за неправилно използване на сертификационния знак съгласно Щита за личните данни, включително като провежда търсене в интернет, за да установи появата на изображения на сертификационния знак съгласно Щита за личните данни и на упоменавания на Щита за личните данни в политиките на организациите в областта на неприкосновеността на личния живот;

— своевременно ще се намират решения на евентуални проблеми, които сме установили при служебните проверки за неверни твърдения за участие и неправилно използване на сертификационния знак, включително като се отправят предупреждения към организациите, които неправилно представят информация за участието си в програма съгласно Щита за личните данни, както това е описано по-горе;

— предприема други подходящи коригиращи мерки, включително чрез средства за правна защита, които министерството е компетентно да предприеме, и отнасяне на въпроса до ФТК, МТ или друг съответен правоприлагащ орган; и

— своевременно разглежда и намира решения на получаваните от нас жалби относно неверни твърдения за участие.

Министерството ще извършва преглед на политиките на организациите в областта на неприкосновеността на личния живот с цел по-ефективното установяване на неверни твърдения за участие в Щита за личните данни и намиране на решения. По-специално министерството ще извършва преглед на политиките в областта на неприкосновеността на личния живот на организации, чието самосертифициране е изтекло поради това, че не са се пресертифицирали за спазването на Принципите. Министерството ще извършва тези прегледи, за да проверява дали такива организации са премахнали от съответните публикации относно политиката си в областта на неприкосновеността на личния живот всички упоменавания, които водят до заключението, че продължават да участват активно в Щита за личните данни. В резултат от този вид прегледи ще идентифицираме организациите, които не са премахнали тези упоменавания и ще им бъдат изпращани писма от службата на главния юрисконсулт на министерството с предупреждение за предприемане на възможни действия по прилагане, ако упоменаванията не бъдат премахнати. Министерството ще предприема последващи мерки с цел да гарантира, че организациите са премахнали неуместните упоменавания или са се пресертифицирали за спазването на Принципите. Освен това министерството ще полага усилия за установяването на неверни твърдения за участие в Щита за личните данни от страна на организации, които никога не са участвали в програма съгласно Щита за личните данни, и ще предприема по отношение на тези организации коригиращи мерки.

Извършва периодични служебни прегледи и оценки на спазването на програмата:

— текущо следи за ефективното спазване, включително чрез изпращане на подробни въпросници на участващите организации, за да установи проблеми, които могат да налагат допълнителни последващи действия. По-специално тези прегледи на спазването ще се извършват, когато: а) министерството получи конкретна основателна жалба относно спазването от дадена организация на Принципите, б) дадена организация не предостави задоволителни отговори на запитванията на министерството за информация във връзка с Щита за личните данни, или в) има достоверни доказателства, че дадена организация не спазва ангажиментите си съгласно Щита за личните данни. Когато е уместно, министерството ще се консултира с компетентните органи по защита на данните относно тези проверки за спазването; и

— периодично прави оценка на управлението и надзора на програмата за Щита за личните данни с цел да гарантира, че мониторинговите усилия са уместни за намирането на решения на новите проблеми, които възникват.

Министерството увеличи ресурсите, които ще бъдат вложени за управлението и надзора на програмата за Щита за личните данни, включително увеличи два пъти броя на служителите, които ще отговарят за управлението и надзора на програмата. Ние ще продължим да заделяме съответните ресурси за тези усилия, за да гарантираме ефективния мониторинг и управление на програмата.

Адаптира уебсайта на Щита за личните данни според целевите: групи

Министерството ще адаптира уебсайта на Щита за личните данни с насоченост върху три целеви групи: физически лица от ЕС, дружества от ЕС и дружества от САЩ. Включването на материал, насочен пряко към физическите лица от ЕС и дружествата от ЕС, ще съдейства за прозрачността по няколко начина. По отношение на физическите лица от ЕС ще бъдат ясно пояснени: 1) правата, които Щитът за личните данни дава на физическите лица от ЕС; 2) механизмите за защита, с които разполагат физическите лица от ЕС, когато считат, че дадена организация нарушава ангажиментите си да спазва Принципите; и 3) как да намерят информация, отнасяща се до самосертифицирането на дадена организация съгласно Щита за личните данни. По отношение на дружествата от ЕС ще се улесни проверката: 1) дали дадена организация се ползва от предимствата на Щита за личните данни; 2) за вида на информацията, която е включена в самосертифицирането на дадена организация съгласно Щита за личните данни; 3) за политиката в областта на неприкосновеността на личния живот, която се прилага за включената информация; и 4) за метода, който организацията използва за проверка на спазването на Принципите.

Засилване на сътрудничеството с ОЗД

За увеличаване на възможностите за сътрудничество с ОЗД министерството ще определи конкретно лице за контакт в министерството, което да изпълнява функциите на връзка с ОЗД. В случаите, когато даден ОЗД счита, че организация не спазва Принципите, включително след подадена жалба от физическо лице от ЕС, ОЗД може да се свърже с определеното лице за връзка в министерството, за да посочи организацията за допълнителна проверка. Също така лицето за връзка ще получава сезирания за организации, които неправомерно твърдят, че участват в Щита за личните данни, въпреки че никога не са се самосертифицирали за спазването на Принципите. Лицето за връзка ще съдейства на ОЗД, търсещи информация, свързана със самосертифицирането на конкретна организация или предишно участие в програмата, и ще отговаря на запитвания от ОЗД във връзка с изпълнението на конкретни изисквания съгласно Щита за личните данни. На второ място, министерството ще предоставя на ОЗД материали във връзка с Щита за личните данни, които те да включват на уебсайтовете си за повишаване на прозрачността за физическите лица от ЕС и дружествата от ЕС. Повишаването на информираността относно Щита за личните данни и правата и отговорностите, които произтичат от него, трябва да улесни установяването на проблемите при тяхното възникване, така че да могат да бъдат решавани по подходящ начин.

Съдейства за разрешаването на жалби за неспазване

Чрез определеното лице за връзка министерството ще бъде сезирано от ОЗД относно жалби във връзка с неспазването на Принципите от страна на организация — участник в Щита за личните данни. Министерството ще полага всички възможни усилия да съдейства за разрешаването на жалбата съвместно с организацията — участник в Щита за личните данни. В срок до 90 дни от получаването на жалбата министерството ще информира ОЗД за актуалното състояние. За улесняване на подаването на такива жалби министерството ще създаде стандартен формуляр, който ОЗД да подават до определеното лице за връзка в министерството. Това лице ще проследява всички сезирания на министерството от ОЗД относно жалби и министерството ще предоставя доклад с обобщен анализ на жалбите, които са получени през годината, в разгледания по-долу годишен преглед.

Приема арбитражни процедури и избира арбитри в консултация с Комисията

Министерството ще изпълни ангажиментите си, разгледани в приложение I, и ще публикува процедурите след постигане на съгласие.

Механизъм за съвместен преглед на функционирането на Щита за личните данни

Министерството на търговията, ФТК и други агенции, според случая, ще провеждат ежегодни срещи с Комисията, заинтересовани ОЗД и съответни представители на работната група по член 29, на които министерството ще предоставя актуална информация относно програмата за Щита за личните данни. На годишните срещи ще се провеждат дискусии по текущи въпроси, свързани с функционирането, изпълнението, надзора и прилагането на Щита за личните данни, включително относно сезиранията на министерството от ОЗД във връзка с жалби, резултатите от служебните прегледи на спазването и също така могат да бъдат обсъждани съответни изменения в законодателството. Първият годишен преглед и съответно последващите прегледи ще включват и диалог по други въпроси, като например в областта на автоматизираното вземане на решения, включително що се отнася до приликите и разликите в подходите на ЕС и САЩ.

Актуализиране на законодателството

Министерството ще положи усилия в рамките на разумното, за да информира Комисията за съществени промени в законодателството на САЩ, доколкото те са от значение за Щита за личните данни в областта на защитата на личните данни и ограниченията и гаранциите, приложими към достъпа до лични данни от органите на САЩ и последващото им използване.

Изключение за целите на националната сигурност

Във връзка с ограниченията по отношение спазването на Принципите на Щита за личните данни за целите на националната сигурност главният юрисконсулт на Службата на директора на Националното разузнаване Robert Litt също изпрати две писма, адресирани до Justin Antonipillai и Ted Dean от Министерството на търговия, които ви бяха препратени. Наред с останалото в писмата се обсъждат нашироко политиките, гаранциите и ограниченията, които се прилагат за дейностите на радиоелектронното разузнаване, провеждани от САЩ. В допълнение към това в писмата са разгледани мерките за прозрачност, които се осигуряват от разузнавателната общност на САЩ по тези въпроси. Тъй като Комисията понастоящем прави преценка за рамката на Щита за личните данни, информацията в тези писма дава уверения да се направи заключението, че Щитът за личните данни ще функционира по съответен начин съгласно посочените в него принципи. Според нашето разбиране вие можете да набирате информация от публично обявената от разузнавателната общност, наред с друга информация, за целите на бъдещите годишни прегледи на рамката на Щита за личните данни.

Въз основа на Принципите на Щита за личните данни и придружаващите писма и материали, включително ангажиментите на министерството във връзка с управлението и надзора на рамката на Щита за личните данни, очакваме Комисията да констатира, че рамката на Щита за личните данни в отношенията между ЕС и САЩ осигурява адекватна защита за целите на правото на ЕС, и предаванията на данни от Европейския съюз за организациите — участници в Щита за личните данни, ще продължат.

С уважение,

Ken Hyatt

Приложение 2

Арбитражен модел

ПРИЛОЖЕНИЕ I

В настоящото приложение I се определят условията, при които организациите — участници в Щита за личните данни, са задължени да решават жалбите чрез арбитраж съгласно принципа за защита, прилагане и отговорност за причинени вреди. Възможността за правно обвързващ арбитраж, описана по-долу, се прилага за някои жалби относно данни, предавани съгласно Щита за личните данни в отношенията между ЕС и САЩ, по които няма определено решение. С тази възможност се цели да се предостави бърз, независим и справедлив механизъм, който по избор на физическите лица може да бъде прилаган за решаване на жалби за нарушаване на Принципите, по които няма определено решение чрез някой от другите механизми съгласно Щита за личните данни, ако съществуват такива.

А. **Обхват**

Тази възможност за арбитраж е на разположение на физическите лица за нерешените жалби, за да може да се определи дали организация — участник в Щита за личните данни, е нарушила задълженията си съгласно Принципите по отношение на това физическо лице и дали това нарушение е останало изцяло и частично неотстранено. Тази възможност е предвидена само за тези цели. Например по отношение на изключенията от Принципите ([1]) или на твърдения относно адекватността на Щита за личните данни не се предвижда такава възможност.

Б. **Налични средства за правна защита**

Съгласно тази процедура за арбитраж специалната група по Щита за личните данни (в чийто състав влизат един или трима арбитри по споразумение между страните) е компетентна да предписва специфични за конкретния случай непарични безпристрастни мерки (например предоставяне на достъп, коригиране, заличаване или връщане на въпросните данни на физическото лице), необходими като коригиращо действие срещу нарушаването на Принципите единствено по отношение на физическото лице. Специалната група по арбитража разполага единствено с тези правомощия във връзка със средствата за правна защита. Когато определя коригиращите мерки, от специалната група по арбитража се изисква да взема предвид и другите средства за правна защита, които са били определени преди това от други механизми съгласно Щита за личните данни. Не се предоставя правна защита по отношение на претърпени вреди, направени разходи, заплатени такси и други. Всяка страна по спора сама поема разноските по хонорарите на адвокати.

В. **Изисквания преди арбитраж**

Когато физическо лице реши да използва тази възможност за арбитраж, то трябва да предприеме следните стъпки, преди да инициира арбитражно производство: 1) да подаде жалбата срещу нарушението направо пред организацията и да предостави възможност на тази организация да намери решение на въпроса в рамките на срока, определен в раздел III, точка 11, буква г), подточка i) от Принципите; 2) да използва независимия механизъм за защита съгласно Принципите, който е безплатен за лицето; и 3) да отнесе въпроса до Министерството на търговията чрез съответния орган по защита на данните и да предостави възможност на министерството да положи максимални усилия да разреши въпроса в рамките на срока, определен в писмото на Администрацията по международна търговия към Министерството на търговията, безплатно за лицето.

Тази възможност за арбитраж не може да се използва, когато преди това по жалба на това физическо лице срещу същото нарушение на Принципите: 1) е прилаган правно обвързващ арбитраж; 2) е определено окончателно решение след съдебен процес, по който физическото лице е било страна; или 3) вече е постигнато споразумение между страните. Освен това тази възможност за арбитраж не може да се използва, когато орган по защита на данните от ЕС: 1) е компетентен съгласно раздел III, точки 5 или 9 от Принципите; или 2) е компетентен да определи решение по жалбата срещу нарушение директно с организацията. Компетентността на ОЗД да определи решение по същата жалба срещу администратор на данни от ЕС сама по себе си не изключва възможността да бъде използвана тази възможност за арбитраж срещу друго юридическо лице, спрямо което този ОЗД няма правомощия.

Г. **Правно обвързващ характер на решенията**

Решението на дадено физическо лице да използва тази възможност за правно обвързващ арбитраж е напълно доброволно. Арбитражните решения ще бъдат задължителни за всички страни по арбитражното производство. Инициирането на арбитраж означава, че физическото лице се отказва от възможността да търси решение по жалбата срещу същото нарушение пред друга инстанция, освен когато определените непарични безпристрастни мерки не компенсират напълно извършеното нарушение и инициирането на арбитражно дело не изключва възможността за физическото лице да поиска обезщетение за вреди в обикновените съдилища.

([1]) Раздел I.5 от Принципите.

Д. **Контрол и привеждане в изпълнение**

Физическите лица и организациите — участници в Щита за личните данни, могат да отнесат арбитражните решения за съдебен контрол и принудително изпълнение по силата на правото на САЩ съгласно Федералния арбитражен закон (Federal Arbitration Act) ([1]). В тези случаи отнасянето става във федерален окръжен съд, в чийто район на действие попада основното място на установяване на дейността на организацията— участник в Щита за личните данни.

Тази възможност за арбитраж е предназначена за разрешаване на индивидуални спорове и арбитражните решения нямат действието на убедителен или обвързващ прецедент по въпроси, в които участват други страни, включително за бъдещи арбитражни производства или за съдилищата в ЕС или в САЩ, както и за производства на ФТК.

Е. **Специална група по арбитража**

Страните ще избират арбитри от списъка, разгледан по-нататък.

В съответствие с приложимото законодателство Министерството на търговията на САЩ и Европейската комисия ще съставят списък с най-малко 20 арбитри, подбрани въз основа на техните независимост, почтеност и опит. Във връзка с този процес ще се прилага следното:

Арбитрите:

1) ще остават включени в списъка за срок от 3 години освен в изключителни случаи или по основателни причини, като този срок може да бъде еднократно удължаван за нови 3 години;

2) не трябва да действат под указания на която и да е от страните, на организация — участник в Щита за личните данни, на правителствена институция, публичен орган или правоприлагащ орган на САЩ, ЕС, държава — членка на ЕС, или друг такъв орган, както и не трябва да са обвързани с такива; и

3) трябва да имат разрешение да практикуват право в САЩ, да бъдат специалисти в законодателството на САЩ в областта на неприкосновеността на личния живот и да имат експертен опит и познания относно законодателството на ЕС в областта на защитата на данните.

Ж. **Арбитражни процедури**

Съобразно приложимото законодателство и в срок до 6 месеца, считано от приемането на решението за адекватност, Министерството на търговията и Европейската комисия ще се договорят относно приемането на набор от действащи и утвърдени арбитражни процедури в САЩ (като AAA или JAMS), които да уреждат производствата пред специалната група по Щита за личните данни, под условието на всяко от следните съображения:

1. Всяко физическо лице може да инициира правно обвързващ арбитраж при спазване на изискванията за действията преди арбитраж, разгледани по-горе, като изпрати „Уведомление“ на организацията. В уведомлението трябва да се съдържат обобщение на стъпките, предприети съгласно точка В за намиране на решение по жалбата, описание на твърдяното нарушение и, по избор на лицето, евентуални придружаващи документи и материали и/или правно изложение във връзка с твърдяното нарушение.

([1]) Съгласно глава 2 от Федералния арбитражен закон (Federal Arbitration Act) („ФАЗ“) „арбитражно споразумение или арбитражно решение, произтичащо от правни взаимоотношения, включително договорни, които могат да бъдат считани за търговски по характер, включително сделка, договор или споразумение от вида на описаните [в раздел 2 от ФАЗ], се включва в обхвата на Конвенцията [относно признаването и изпълнението на чуждестранни арбитражни решения от 10 юни 1958 г., 21 U.S.T. 2519, T.I.A.S. № 6997 („Конвенцията от Ню Йорк“)].“ 9 U.S.C. § 202. По-нататък във ФАЗ е предвидено, че „споразумение или решение, произтичащо от такива взаимоотношения, в които участват само граждани на Съединените щати, не се включва в обхвата на Конвенцията [от Ню Йорк], освен когато в тези взаимоотношения участва недвижимо имущество с местонахождение в чужбина, когато се предвижда изпълнение на дейност или прилагане в чужбина или по друг начин е налице някаква основателна връзка с една или повече чужди държави“. Съгласно глава 2 „всяка от страните по арбитражното дело може да се отнесе до съд с юрисдикция съгласно разпоредбите в настоящата глава, за да поиска разпореждане в потвърждение на арбитражното решение, постановено срещу някоя от другите страни по арбитражното дело. Съдът потвърждава решението, освен когато констатира, че е налице едно от основанията за отказ или отсрочване на признаването или изпълнението на решението, както това е определено в посочената Конвенция [от Ню Йорк].“, пак там § 207. По-нататък в глава 2 е предвидено, че „окръжните съдилища в Съединените щати.. са компетентни в първоначалния иск. … или първоначалното производство [съгласно Конвенцията от Ню Йорк], независимо от размерите на спора.“, пак там § 203.
Също така в глава 2 е предвидено, че „Разпоредбите съгласно глава 1 се прилагат за искове и производства, инициирани съгласно разпоредбите в настоящата глава, доколкото разпоредбите в глава 1 не влизат в противоречие с тези в настоящата глава или в Конвенцията [от Ню Йорк], както тя е ратифицирана от Съединените щати.“, пак там § 208. От друга страна в глава 1 е предвидено, че „писмени разпоредби в. .. договор за търговска сделка, отнасящи се до решаване чрез арбитраж на спорове, произтичащи от такъв договор, или сделка или от отказ да бъде изпълнен договорът изцяло или частично, както и писмено споразумение да бъде инициирано арбитражно дело по съществуващ спор, възникнал въз основа на такъв договор, сделка или отказ, се считат за валидни, неотменими и подлежащи на принудително изпълнение, освен когато са налице съществуващи по закон основания или справедливи основания за отмяна на договора.“, пак там § 2. По-нататък в глава 1 е предвидено, че „всяка страна по арбитражния спор може да изиска от посочения съд разпореждане за потвърждаване на решението, след което съдът е задължен да издаде такова разпореждане, освен когато решението е било отменено, изменено или поправено, както това е предвидено в раздели 10 и 11 [от ФАЗ].“, пак там § 9.

2. Ще бъдат създадени процедури, за да се гарантира, че няма да има дублиране на средствата или процедурите за правна защита по жалбата на това физическо лице срещу същото нарушение.

3. Действията на ФТК могат да се предприемат успоредно с арбитражното производство.

4. В тези арбитражни производства не може да участва представител на правителствена институция, публичен орган или правоприлагащ орган на САЩ, ЕС, държава — членка на ЕС, или друг такъв орган, като по искане на физическото лице от ЕС ОЗД могат да оказват съдействие само за изготвянето на уведомлението, но те не могат да имат достъп до разкрития или каквито и да е други материали във връзка с арбитражното дело.

5. Мястото на провеждане на арбитража ще е в Съединените щати, а физическото лице може да избере да участва чрез видео- или телефонна връзка, която се осигурява безплатно за него. Не е наложително да участва лично.

6. Езикът, на който ще се води арбитражното дело ще бъде английски, освен когато страните са се споразумели за друго. При мотивирано искане и като се взема предвид дали физическото лице се представлява от адвокат, ще се осигурява безплатно устен превод по време на изслушването и писмен превод на материалите по арбитражното дело, освен когато по преценка на специалната група поради обстоятелствата на конкретния арбитраж това би довело до необосновани или непропорционални разходи.

7. Предоставените на арбитрите материали ще се третират като поверителна информация и ще бъдат използвани само във връзка с арбитражното дело.

8. Ако е необходимо, може да се допусне да бъдат представени специални разкрития на физическото лице, които ще бъдат третирани от страните като поверителна информация и ще бъдат използвани само във връзка с арбитражното дело.

9. Арбитражните дела трябва да приключат в срок до 90 дни, считано от изпращането на уведомлението до въпросната организация, освен когато страните са се договорили за друго.

3. **Разходи**

Арбитрите следва да предприемат подходящи мерки за свеждане до минимум на разноските или хонорарите по арбитражните дела.

В съответствие с приложимото законодателство Министерството на търговията ще съдейства за създаването на фонд, в който ще се изисква от организациите — участници в Щита за личните данни, да внасят годишни вноски, въз основа отчасти на глобата на организацията, и от който ще бъдат покривани разходите по арбитражната процедура, включително хонорарите за арбитрите, до определени максимални размери („таван“), което ще се извърши в консултация с Европейската комисия. Фондът ще се управлява от трета страна, която редовно ще докладва за работата му. При годишния преглед Министерството на търговията и Европейската комисия ще извършват преглед на работата на фонда, включително необходимостта от промяна на размера на вноските или тавана, като наред с останалото ще вземат предвид и броя на арбитражните дела и разноските и времетраенето им, като общото разбиране е да не се създава прекомерна финансова тежест за организациите — участници в Щита за личните данни. Адвокатските хонорари не са обхванати от настоящата разпоредба, нито от фонда съгласно нея.

ПРИЛОЖЕНИЕ II

ПРИНЦИПИ НА РАМКАТА НА ЩИТА ЗА ЛИЧНИТЕ ДАННИ В ОТНОШЕНИЯТА МЕЖДУ ЕС И САЩ, ПУБЛИКУВАНИ ОТ МИНИСТЕРСТВОТО НА ТЪРГОВИЯТА НА САЩ

I. ОБЩ ПРЕГЛЕД

1. При все че Съединените щати и Европейският съюз споделят целта за повишаване на защитата на неприкосновеността на личния живот, подходът на Съединените щати към неприкосновеността на личния живот е различен от този на Европейския съюз. Съединените щати прилагат секторен подход, който се основава на законови и подзаконови разпоредби, както и кодекси за саморегулиране. Предвид тези различия и с цел да бъде предоставен на организациите в Съединените щати надежден механизъм за предаване на лични данни към САЩ от Европейския съюз, като същевременно се гарантира, че субектите на данни от ЕС ще продължат да се ползват с ефективни гаранции и защита, както това се изисква съгласно европейското законодателство по отношение на обработването на личните им данни, когато те се предават на държави извън ЕС, Министерството на търговията публикува тези Принципи на Щита за личните данни, включително допълнителните принципи (наричани общо „Принципите“), в съответствие със законоустановените си правомощия да засилва, насърчава и развива международната търговия (15 U.S.C. § 1512). Принципите бяха разработени в консултация с Европейската комисия и с представители на промишлеността и други заинтересовани страни с цел насърчаване на търговията между Съединените щати и Европейския съюз. Те са предназначени единствено за организациите в Съединените щати, които получават лични данни от Европейския съюз, с цел тези организации да изпълнят условията съгласно Щита за личните данни и по този начин да се ползват от решението за адекватност на Европейската комисия. ([1]) Принципите не засягат прилагането на националните разпоредби за прилагане на Директива 95/46/ЕО („Директивата“), които се прилагат за обработването на личните данни в държавите членки. По същия начин Принципите не ограничават задълженията по отношение на неприкосновеността на личния живот, които по принцип се прилагат съгласно правото на САЩ.

2. За да се основава на Щита за личните данни при извършването на предавания на лични данни с произход от ЕС, една организация трябва да се самосертифицира, че ще спазва Принципите пред Министерството на търговията (или определено от него орган) („министерството“). Независимо че решенията на организациите да се присъединят по този начин към Щита за личните данни са напълно доброволни, ефективното спазване на Принципите е задължително: организациите, които са се самосертифицирали пред министерството и са обявили публично своя ангажимент да спазват Принципите, трябва да ги спазват в пълна степен. За да се присъедини към Щита за личните данни, една организация трябва: а) да подлежи на правомощията по разследване и прилагане на Федералната търговска комисия („ФТК“), Министерството на транспорта или друг законоустановен орган, който гарантира за ефективното спазване на Принципите (*в бъдеще могат да бъдат добавени в приложение и други законоустановени органи на САЩ, признати от ЕС*); б) да обяви публично ангажимента си да спазва Принципите; в) да предостави за публичен достъп политиките си в областта на неприкосновеността на личния живот в съответствие с тези Принципи; и г) да ги прилага в пълна степен. Организация, която не спазва Принципите, подлежи на принудително изпълнение съгласно раздел 5 от Закона за Федералната търговска комисия, който забранява нелоялните и измамни практики в търговията или засягащи търговията, (15 U.S.C. § 45(a)) или съгласно друг законов или подзаконов акт, с който се забраняват тези практики.

3. Министерството на търговията ще поддържа и предоставя за публичен достъп официален списък на организациите в САЩ, които са се самосертифицирали пред министерството и са декларирали ангажимента си да спазват Принципите („Списък към Щита за личните данни“). Организацията се ползва с предимствата на Щита за личните данни, считано от датата, на която министерството включи организацията в Списъка към Щита за личните данни. Министерството ще заличи от Списъка към Щита за личните данни организацията, която се е оттеглила доброволно от Щита за личните данни или не е изпълнила изискването за ежегодно пресертифициране пред министерството. Заличаването на една организация от Списъка към Щита за личните данни означава, че тя повече не се ползва с предимствата на решението за адекватност на Европейската комисия при получаването на лична информация от ЕС. Организацията трябва да продължи да прилага Принципите по отношение на личната информация, която е получила, докато е участвала в Щита за личните данни, и ежегодно да потвърждава пред министерството ангажимента си за това, докато продължава да съхранява тази информация; в противен случай организацията трябва да върне или заличи информацията или да осигури „адекватна“ защита чрез други разрешени средства. Също така министерството ще заличава от Списъка към Щита за личните данни организациите, които трайно не спазват Принципите; тези организации не отговарят на условията да се ползват с предимствата на Щита за личните данни и трябва да върнат или заличат личната информация, която са получили съгласно Щита за личните данни.

4. Също така министерството ще поддържа и предоставя за публичен достъп официален регистър на организациите в САЩ, които по-рано са били самосертифицирани в министерството, но са заличени от Списъка към Щита за личните данни. Министерството ще отправя ясно предупреждение, че тези организации не участват в Щита за личните данни; че заличаването от Списъка към Щита за личните данни означава, че тези организации не могат да твърдят, че спазват изискванията съгласно Щита за личните данни и трябва да избягват да правят всякакви изявления или

([1]) Предвид това че решението на Комисията относно адекватността на защитата, осигурена от Щита за личните данни в отношенията между ЕС и САЩ, се прилага в Исландия, Лихтенщайн и Норвегия, пакетът към Щита за личните данни ще обхване както Европейския съюз, така и тези три държави. Следователно позоваването на Договора за ЕС и неговите държави членки да се чете като включващо Исландия, Лихтенщайн и Норвегия.

подвеждащи действия, които водят до заключението, че участват в Щита за личните данни; и че тези организации повече не се ползват с предимствата на решението за адекватност на Европейската комисия, което би им позволило да получават лична информация от ЕС. Спрямо организация, която продължава да твърди, че участва в Щита за личните данни, или по друг начин прави погрешно представяне на информация във връзка с Щита за личните данни, след като е била заличена от Списъка към Щита за личните данни, могат да бъдат предприети действия по правоприлагане от страна на ФТК, Министерството на транспорта или други правоприлагащи органи.

5. Придържането към тези Принципи може да бъде ограничено: а) до необходимата степен, с оглед спазване изискванията за националната сигурност, обществения интерес или изискванията на правоприлагането; б) със закон, правителствено регулиране или съдебна практика, които пораждат взаимнопротиворечиви задължения или предвиждат изрични разрешителни, при положение че дадена организация, която е поискала подобно разрешително, може да докаже, че неспазването на принципите е ограничено до необходимата степен за гарантиране на първостепенните законово предвидени интереси, за които е поискано разрешителното; или в) ако действието на Директивата или на законодателството на държавата членка предвижда изключения или дерогации, при условие че тези изключения или дерогации се прилагат в сравними контексти. Съгласно целта за по-голяма защита на неприкосновеността на личния живот, организациите трябва да се стремят да прилагат тези принципи изцяло и прозрачно, включително като посочват в своите политики за защита на неприкосновеността на личния живот — в кои области изключенията по отношение на принципите, предвидени в буква б) по-горе, ще се прилагат редовно. По същата причина, когато Принципите и/или законодателството на САЩ позволяват на организациите да направят избор, от тях се изисква да изберат, когато е възможно, по-високата степен на защита.

6. Организациите са задължени да прилагат Принципите за всички лични данни, предавани съгласно Щита за личните данни, след като се присъединят към Щита за личните данни. Организация, която е избрала да се ползва от предимствата на Щита за личните данни за лична информация за човешки ресурси, която се предава от ЕС, за да бъде използвана в контекста на трудови правоотношения, трябва да посочи това, когато се самосертифицира пред министерството, и трябва да спази изискванията, изложени в допълнителния принцип за самосертифицирането.

7. За въпроси, свързани с тълкуването и спазването на Принципите и на съответните политики в областта на неприкосновеността на личния живот от организациите — участници в Щита за личните данни, се прилага правото на САЩ, с изключение на случаите, когато тези организации са поели ангажимент да си сътрудничат с европейските органи по защита на данните („ОЗД“). Освен ако е посочено друго, всички разпоредби на Принципите се прилагат, когато са релевантни.

8. Определения:

   а) „Лични данни“ и „лична информация“ означават данни относно идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано, които са в обхвата на Директивата, предадени са от Европейския съюз на организация в Съединените щати и са записани под каквато и да е форма.

   б) „Обработване“ на лични данни означава всяка операция или съвкупност от операции, извършвана с лични данни чрез автоматични или други средства, като събиране, записване, организиране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване или разпространяване и изтриване или унищожаване.

   в) „Администратор“ означава физическо лице или организация, която сама или съвместно с други определя целите и средствата за обработването на лични данни.

9. Датата, от която Принципите ще се прилагат ефективно, е датата на окончателното одобрение на решението за адекватност на Европейската комисия.

II. ПРИНЦИПИ

1. **Уведомяване**

   а) Всяка организация трябва да уведомява физическите лица за:

      i. участието си в Щита за личните данни и да предоставя електронна връзка към Списъка към Щита за личните данни или адреса на уебстраницата,

      ii. видовете лични данни, които се събират, и правните субекти или дъщерните дружества на организацията, които също се придържат към Принципите, когато това е приложимо,

iii. ангажимента си да прилага Принципите за всички лични данни, които получава от ЕС съгласно Щита за личните данни,

iv. целите, с които събира и използва лична информация за тях,

v. как да се свържат с организацията, ако имат запитвания или оплаквания, включително съответни организации в ЕС, които могат да отговорят на тези запитвания или оплаквания,

vi. видовете или самоличността на трети страни, на които личната информация ще бъде разкрита и целите, с които се извършва това,

vii. правото на физическите лица на достъп до личните им данни,

viii. възможностите за избор и средствата, които предлага организацията на физическите лица с оглед ограничаване използването и разкриването на личните им данни,

ix. определения независим орган за разрешаване на спорове, към който да се адресират жалби и който следва да предоставя подходящи средства за правна защита, безплатно за физическото лице, и дали това е: 1) панелът, създаден от ОЗД, 2) организация за алтернативно разрешаване на спорове, установена в ЕС, или 3) организация за алтернативно разрешаване на спорове, установена в Съединените щати,

x. това, че за нея се прилагат правомощията за разследване и правоприлагане на ФТК, Министерството на транспорта или друг оправомощен законоустановен орган на САЩ,

xi. възможността при определени условия физическото лице да използва правно обвързващ арбитраж,

xii. изискването да бъде разкривана лична информация в отговор на законни искания на публични органи, включително в отговор на изисквания на националната сигурност или правоприлагането, и

xiii. отговорността на организацията в случаите на последващи предавания към трети страни.

б) Уведомяването трябва да бъде направено на ясен и разбираем език, когато физическите лица бъдат поканени за първи път да предоставят личната информация на организацията или веднага след като стане възможно, но във всеки случай преди тези данни да бъдат използвани от организацията за цел, различна от тази, за която са били първоначално събрани или обработени от организацията, която извършва предаването или разкриването им за първи път на трета страна.

2. **Избор**

а) Всяка организация трябва да предлага на физическите лица възможността да изберат (клауза за неучастие — „opt out“) дали личната информация за тях: а) може да бъде разкрита на трета страна, или б) може да бъде използвана за несъвместими по същество цели с предназначението или предназначенията, за които е била първоначално събрана или за които по-късно е дадено разрешение от физическите лица. Физическите лица трябва да разполагат с ясни, разбираеми и леснодостъпни механизми, за да направят своя избор.

б) Чрез дерогация от предходната буква, не е необходимо да се предоставя избор, когато разкриването се извършва пред трета страна, която изпълнява функциите на представител за изпълнение на задача(и) от името и под указанията на организацията. Организацията обаче трябва винаги да сключва договор с представителя.

в) Що се отнася до чувствителна информация (например лична информация, свързана с медицинското или здравословното състояние, с произход — раса или етнически произход, политически възгледи, вероизповедание или философски убеждения, членство в синдикат или сексуални предпочитания), организациите трябва да получат от лицата утвърждаващо изрично съгласие („opt in“), при условие че информацията трябва да бъде: i) разкрита на трета страна или ii) използвана с цел, различна от тази, за която е била първоначално събрана или за която по-късно е дадено разрешение от физическите лица посредством упражняването на правото им на изрично съгласие. Освен това организацията следва да разглежда всяка лична информация, получена от трета страна, като чувствителна информация, ако последната определя и третира тази информация като такава.

3. **Отчетност за последващото предаване**

а) За да предават лична информация на трета страна, която изпълнява функциите на администратор, организациите трябва да спазват принципите на уведомяването и на избора. Организациите трябва също така да сключат договор с третата страна администратор, в който да бъде предвидено, че тези данни могат да бъдат обработвани само с ограничена и конкретна цел в съответствие с даденото съгласие от физическото лице, както и че получателят ще осигури същата степен на защита, която се осигурява от Принципите, и ще уведоми организацията, ако констатира, че вече не е в състояние да изпълнява това задължение. Договорът предвижда, че когато тази констатация е направена, третата страна администратор прекратява обработката или предприема други за отстраняване на последиците.

б) За да предават лични данни на трета страна, която изпълнява функциите на представител, организациите трябва: i) да предават тези данни само с ограничена и конкретна цел; ii) да определят, че представителят е задължен да осигури най-малко същата степен на защита на неприкосновеността на личния живот, която се изисква съгласно Принципите; iii) да предприемат обосновани и съответни мерки, за да гарантират, че представителят ефективно обработва предадената лична информация по начин, който съответства на задълженията на организацията съгласно Принципите; iv) да изискват от представителя да уведоми организацията, ако констатира, че вече не е в състояние да изпълнява своето задължение да осигурява същата степен на защита на неприкосновеността на личния живот, която се изисква съгласно Принципите;; v) при уведомяване, включително съгласно подточка iv), да предприемат обосновани и съответни мерки да преустановят и отстранят последиците от неразрешено обработване; и vi) при поискване да предоставят на министерството обобщение или представително копие на съответните разпоредби във връзка с неприкосновеността на личния живот от договора с представителя.

4. **Сигурност**

а) Организациите, които създават, поддържат, използват или разпространяват лична информация, трябва да вземат обосновани и подходящи мерки, за да предотвратят загубата, злоупотребата, непозволения достъп, разкриването, изменението и унищожаването на тези данни, като надлежно вземат под внимание рисковете, свързани с обработването и характера на личните данни.

5. **Цялост на данните и ограничаване в рамките на целта**

а) Съгласно Принципите личната информация трябва да бъде ограничена до необходимата за целите на обработването ([1]). Никоя организация не може да обработва лична информация по начин, несъвместим с целите, за които тя е била събрана или за които по-късно е дадено разрешение от физическото лице. Доколкото е необходимо за тези цели, всяка организация трябва да вземе подходящи мерки, за да гарантира надеждността на личните данните по отношение на предвиденото им използване, както и тяхната точност, пълнота и актуалност. Организацията трябва да се придържа към Принципите през цялото време, докато запазва тази информация.

б) Информация може да бъде запазвана във форма, която идентифицира или позволява да се идентифицира ([2]) физическото лице, само за толкова дълго, колкото служи за целта на обработването по смисъла на точка 5, буква а). Това задължение не възпира организациите да обработват лични данни за по-дълги периоди, т.е. докогато и дотолкова, колкото това обработване е от определена полза за целите на архивирането в интерес на обществото, журналистиката, литературата и изкуството, научни или исторически изследвания и статистически анализ. В тези случаи обработването е подчинена на другите принципи и разпоредби на рамката. Организациите следва да предприемат разумни и подходящи мерки за спазване на тази разпоредба.

6. **Достъп**

а) Физическите лица трябва да имат достъп до личната информация за тях, с която разполага дадена организация, и да имат възможността да я коригират, променят или заличават, когато е неточна или се обработва в нарушение на Принципите, освен когато затрудненията или разходите по предоставяне на достъп биха били несъразмерни спрямо рисковете за неприкосновеността на личния живот на физическото лице във въпросния случай или когато биха били нарушени правата на лица, различни от заинтересованото.

([1]) В зависимост от обстоятелствата примерите за съвместими цели на обработването може да включват тези, които са от определена полза по отношение на връзките с клиенти, съображения относно спазването и правни съображения, одит, сигурност и предотвратяване на измами, опазване или защита на законните права на организацията или други цели, съответстващи на разумни очаквания в контекста на събирането на данни.

([2]) В този контекст, ако предвид средствата за идентификация, които е определено вероятно да бъдат използвани (като се имат предвид, наред с останалото, разходите и количеството време, необходими за идентифицирането, както и наличните технологии към момента на обработването), и формата, в който данните се запазват, физическо лице би могло да бъде идентифицирано от организацията или от трета страна, при условие че има достъп до данните, тогава лицето е „лице, което може да бъде идентифицирано“.

7. **Защита, прилагане и отговорност за причинени вреди**

а) Ефективната защита на неприкосновеността на личния живот трябва да включва сигурни механизми, които да гарантират спазването на Принципите, право на защита за физическите лица, засегнати от неспазването на принципите, както и санкциониране на организациите, когато не спазват принципите. Тези механизми трябва да включват най-малкото:

i. леснодостъпни независими механизми за защита, които да позволят експедитивно да се разгледат и решат жалбите или споровете на всяко физическо лице, безплатно за лицето и при позоваване на Принципите, както и предоставяне на обезщетения, когато приложимото законодателство или инициативите в частния сектор предвиждат това;

ii. процедури за последващ контрол, за да се провери дали уверенията и твърденията, предоставени от организациите за техните практики в областта на неприкосновеността на личния живот, са верни и дали тези практики се прилагат действително, както се твърди, и по-специално по отношение на случаите на неспазване на Принципите; и

iii. задължения за решаване на проблемите, произтичащи от неспазването на Принципите от организациите, обявяващи своето придържане към тях, и последствия за тези организации. Санкциите трябва да са достатъчно строги, за да гарантират спазването на Принципите от организациите.

б) Организациите и избраните от тях независими механизми за защита отговарят в кратки срокове на запитвания и искания за информация от страна на министерството във връзка с Щита за личните данни. Всички организации трябва да отговарят експедитивно на жалби във връзка със спазването на Принципите, насочени към тях от органи на държавите — членки на ЕС, чрез министерството. Организациите, които са избрали да си сътрудничат с ОЗД, включително обработващите данни за човешки ресурси, трябва да отговарят директно на тези органи във връзка с разследването и разрешаването на жалби.

в) Организациите са задължени да участват в арбитраж по отношение на жалбите и да спазват условията, посочени в приложение I, при условие че дадено физическо лице е отнесло въпроса за решаване чрез правно обвързващ арбитраж, като е уведомило въпросната организация и е спазило процедурите и условията, посочени в приложение I.

г) В контекста на последващото предаване всяка организация — участник в Щита за личните данни, носи отговорност за обработването на личната информация, която получава съгласно Щита за личните данни и впоследствие предава на трета страна, която изпълнява функциите на представител от нейно име. Организацията — участник в Щита за личните данни, продължава да носи отговорност съгласно Принципите, ако нейният представител обработва тази лична информация по начин, който не съответства на Принципите, освен ако организацията докаже, че не носи отговорност за събитието, породило вредата.

д) Когато по отношение на организацията е издадена заповед от ФТК или съдебно разпореждане във връзка с неспазване, организацията обявява публично всички съответно свързани с Щита за личните данни части от евентуален доклад за спазването или оценка, представени на ФТК, доколкото позволяват изискванията за поверителност. Министерството създаде специализирано звено за контакт с ОЗД относно проблеми на спазването от организации — участници в Щита за личните данни. ФТК ще разглежда случаите на неспазване на Принципите, за които е сезирана от министерството и органите на държавите — членки на ЕС, и ще обменя информация относно случаи, за които е сезирана с органите на съответната държава своевременно, при условията на съществуващите ограничения за поверителност.

III. ДОПЪЛНИТЕЛНИ ПРИНЦИПИ

1. **Чувствителни данни**

а) От организациите не се изисква да получат утвърдително изрично съгласие („opt in“) по отношение на чувствителни данни, когато обработването:

i. е от жизнено важен интерес за субекта на данните или за друго лице;

ii. е необходимо, за да се установи право на иск или право на защита;

iii. е необходимо, за да се окажат медицински грижи или за определяне на диагноза;

iv. се извършва в хода на законни дейности от фондация, асоциация или друга организация с нестопанска цел и с политическа, философска, религиозна или профсъюзна цел, както и при условие че обработването се отнася единствено до членовете на организацията или до лицата, които поддържат с нея редовни контакти във връзка с предназначението ѝ, и че тези данни не се разкриват на трета страна без съгласието на субектите на данните;

v. е необходимо, за да бъдат изпълнени задълженията на организацията по отношение на трудовото право; или

vi. е свързано с данни, които ясно са били оповестени публично от физическото лице.

2. **Изключения за журналистически цели**

а) С оглед предвидените съгласно Конституцията на САЩ защити за свободата на пресата и изключенията за журналистически материали съгласно Директивата, когато правата на свободната преса, заложени в първата поправка на Конституцията на САЩ, са несъвместими със защитата на неприкосновеността на личния живот, първата поправка се прилага с предимство за дейностите, които имат за предмет американски лица или организации.

б) Личната информация, събрана с цел публикуване, разпространение или други форми на обществена комуникация под формата на журналистически материали, независимо дали ще се използва, или не, както и информацията, която е била публикувана преди това, след което е била архивирана, не е предмет на изискванията съгласно Принципите на Щита за личните данни.

3. **Вторична отговорност**

а) Доставчиците на Интернет, далекосъобщителните дружества и другите организации не носят отговорност съгласно Принципите на Щита за личните данни, когато само предават, направляват, заместват или кешират информация от името на друга организация. Нито самата Директива, нито Щитът за личните данни могат да породят вторична отговорност. Не може да се търси отговорност на дадена организация, когато тя служи само за носител на данни, предавани от трети страни, и не определя нито целите, нито средствата за обработване на тези лични данни.

4. **Извършване на комплексни проверки и провеждане на одити**

а) В дейностите на одиторите и на инвестиционните банки може да се наложи обработване на лични данни без съгласието или без знанието на заинтересованото лице. Това се допуска съгласно принципите на уведомяването, на избора и на достъпа при описаните по-нататък обстоятелства.

б) Публичните акционерни дружества и предприятията с ограничен брой акционери, включително организациите — участници в Щита за личните данни, подлежат на редовно одитиране. Ако информацията за такива одити бъде разкрита преждевременно, това може да застраши целта им, особено когато се отнася до потенциални нарушения. По същия начин за организациите — участници в Щита за личните данни, които се включват в планирани сливания или поглъщания, е необходимо да се проведе или те подлежат на комплексна проверка. Това често налага събиране и обработване на лични данни, като например информация за служители на висши ръководни постове и други важни длъжности. Ако информацията бъде разкрита преждевременно, това може да попречи на сделката или дори да бъде в нарушение на приложимата правна уредба за ценните книжа. Инвестиционните банкери и адвокатите, работещи по комплексната проверка, или одиторите, когато провеждат одита, могат да обработват информация без знанието на физическото лице само в необходимите рамки и период от време за целите на спазването на законовите изисквания или изискванията от публичен интерес, както и в други обстоятелства, където прилагането на тези Принципи би засегнало легитимните интереси на организацията. Сред тези легитимни интереси са контролът на спазването от страна на организациите на техните законови задължения и законни счетоводни дейности, както и необходимостта от поверителност, свързана с евентуални поглъщания, сливания, съвместни предприятия или други сделки със сходен характер, извършвани от инвестиционните банкери или одиторите.

5. **Ролята на органите по защита на данните**

а) Организациите ще изпълняват ангажимента си да си сътрудничат с органите по защита на данните (ОЗД) в Европейския съюз, както е описано по-нататък. Съгласно Щита за личните данни организациите в САЩ, които получават лични данни от ЕС, трябва да поемат ангажимента да използват ефективни механизми, за да гарантират спазването на Принципите на Щита за личните данни. По-специално, както е определено в принципа за защита, прилагане и отговорност за причинени вреди, организациите участници трябва да предвидят: а) (i) средства за правна защита за физическите лица, за които се отнасят данните; а) (ii) процедури за последващ контрол, за да се провери дали уверенията и твърденията, предоставени от организациите за техните практики в областта на неприкосновеността на личния живот, са верни; и а) (iii) задължения за решаване на проблемите, произтичащи от неспазването на Принципите, и последствия за тези организации. Организация, която е поела задължението да си сътрудничи с ОЗД, предвидено в настоящата точка, може да изпълнява условията по буква а), подточки i) и iii) от принципа за защита, прилагане и отговорност за причинени вреди.

б) Всяка организация може да поеме ангажимент да си сътрудничи с ОЗД, като декларира при самосертифицирането си съгласно Щита за личните данни пред Министерството на търговията (вж. допълнителния принцип относно самосертифицирането), че:

i. избира да спазва изискванията по буква а), подточки i) и iii) от принципа за защита, прилагане и отговорност за причинени вреди съгласно Щита за личните данни, като поема ангажимента да сътрудничи с ОЗД;

ii. ще сътрудничи с ОЗД във връзка с разглеждането и решаването на депозираните жалби съгласно Щита за личните данни; и

iii. ще се съобрази с всяка препоръка, дадена от ОЗД, според която организацията трябва да вземе специални мерки, за да спази Принципите на Щита за личните данни, включително всякакви мерки, свързани със средства за правна защита или обезщетение в полза на физически лица, които са засегнати от неспазването на Принципите, и ще уведоми писмено ОЗД за взетите мерки по този повод.

в) Функциониране на панелите на ОЗД

i. Сътрудничеството на ОЗД ще се изразява в предоставяне на информация и препоръки, както следва:

1. Препоръките на ОЗД ще бъдат предоставяни чрез неформален панел на ОЗД, създаден на равнището на Европейския съюз, който ще помогне, наред с останалото, и за осигуряването на хармонизиран и съгласуван подход.

2. Панелът ще дава препоръки на съответните организации в САЩ по повод на жалби от физически лица, по които няма приети решения и които се отнасят до обработването на лична информация, която е била предадена от ЕС съгласно Щита за личните данни. Препоръките ще предвиждат гарантирането на правилното прилагане на Принципите на Щита за личните данни и ще включват средствата за правна защита за съответното/ите физическо/и лице/а, които ОЗД считат за подходящи.

3. Панелът ще дава тези препоръки в отговор на сезиране от заинтересованите организации и/или на жалби, получени директно от физически лица срещу организации, които са поели ангажимента да си сътрудничат с ОЗД с оглед спазването на Щита за личните данни, като ще насърчава и, при необходимост, подпомага тези физически лица да използват първо вътрешните механизми за разглеждане на жалбите, с които организацията разполага.

4. Препоръките ще се дават едва след като двете страни по спора са имали възможността да представят своите забележки и евентуално своите доказателства. Панелът ще се стреми да предостави препоръките си в най-кратки срокове, като спазва принципите на справедливия процес. По принцип панелът ще се произнася най-късно в срок от 60 дни, считано от получаването на жалбата или сезирането.

5. Ако сметне за необходимо, панелът ще направи публично достояние резултатите от разглеждането на жалбите, по които е бил сезиран.

6. Препоръката, предоставена от панела, няма да ангажира нито панела, нито ОЗД, които го съставляват.

ii. Както беше отбелязано по-рано, организациите, които изберат този начин за решаване на споровете, трябва да поемат задължението да спазват и прилагат препоръките, дадени от ОЗД. Ако някоя организация не изпълни препоръката в срок от двадесет и пет дни от получаването ѝ, без да посочи убедително обяснение за закъснението, панелът ще оповести намерението си да отнесе въпроса до Федералната търговска комисия, Министерството на транспорта или друг федерален или държавен орган на САЩ, който има законови правомощия да предприема действия по правоприлагане в случаи на измама или погрешно представяне, или да заключи, че е допуснато сериозно нарушение по отношение на споразумението за сътрудничество, което в такъв случай ще се счита за недействително. В последния случай панелът ще информира Министерството на търговията, за да може Списъкът към Щита за личните данни да бъде надлежно изменен. Всяко неспазване на задължението за сътрудничество с ОЗД, както и всяко неспазване на Принципите на Щита за личните данни, подлежи на санкциониране като измамна практика съгласно раздел 5 от закона за Федералната търговска комисия или на други сравними закони.

г) Всяка организация, която желае да се ползва с предимствата на Щита за личните данни за данните относно човешки ресурси, предавани от ЕС в контекста на трудовите правоотношения, трябва задължително да поеме ангажимента за тази цел да сътрудничи с ОЗД (вж. допълнителния принцип за данни относно човешки ресурси).

д) Организациите, които са избрали този вариант, ще плащат годишна такса за покриване на текущите разходите за панела и може допълнително да бъде поискано да поемат евентуално налагащи се разходи за превод, произтичащи от разглеждането от страна на панела на случаите на сезиране или жалбите срещу тях. Годишната такса не може да превишава 500 USD и ще бъде намалена за малките дружества.

6. **Самосертифициране**

а) Предимствата на участието в Щита за личните данни се ползват от датата, на която министерството включи самосертифицираната организация в Списъка към Щита за личните данни, след като преди това е преценил, че подадената информация за самосертифицирането е пълна.

б) За да се самосертифицира за участие в Щита за личните данни, една организация трябва да подаде в министерството заявление, подписано от корпоративен служител от името на организацията, която се присъединява към Щита за личните данни, което съдържа най-малко следната информация:

i. името на организацията, пощенския адрес, адрес на електронна поща, телефонен номер и номер на факс;

ii. описание на дейностите на организацията по отношение на личната информация, получавана от ЕС; и

iii. описание на политиката на организацията в областта на неприкосновеността на личния живот по отношение на тази лична информация, включително:

1. ако организацията има публичен уебсайт, тя трябва да предостави съответната хипервръзка към адреса, където е предоставила на разположение политиката си в областта на неприкосновеността на личния живот, а ако организацията няма публичен уебсайт, тя трябва да посочи къде е предоставила на разположение за публичен достъп политиката си в областта на неприкосновеността на личния живот;

2. датата, от която тази политика се прилага ефективно;

3. службата, която разглежда жалби, искания за достъп и други въпроси, произтичащи съгласно Щита за личните данни;

4. конкретния законоустановен орган, който е компетентен да разглежда жалби срещу организацията във връзка с евентуални нелоялни или измамни практики и нарушения на законите или разпоредбите, уреждащи неприкосновеността на личния живот (и който е посочен в Принципите или в бъдещо приложение към Принципите);

5. наименованието на всяка програма относно неприкосновеността на личния живот, в която членува организацията;

6. метода за проверка (напр. вътрешна, от трета страна) (вж. допълнителния принцип „проверка“; и

7. независимия механизъм за защита, който е на разположение за разследване на жалби, по които няма решение.

в) Когато организацията иска да се ползва от Щита за личните данни по отношение на информацията за човешки ресурси, която се предава от ЕС, за да бъде използвана в контекста на трудовите правоотношения, тя може да направи това, когато съществува законоустановен орган, компетентен да разглежда жалби срещу организацията, произтичащи от обработването на информация за човешки ресурси, и посочен в Принципите или в бъдещо приложение към Принципите. В допълнение организацията трябва да посочи това при самосертифицирането си и да заяви ангажимента си да си сътрудничи със съответния орган или органи на ЕС съгласно допълнителните принципи за данни относно човешки ресурси и за ролята на органите по защита на данните, според случая, както и че ще се съобразява с препоръките, давани от тези органи. Също така организацията трябва да предостави на министерството копие от политиката си в областта на неприкосновеността на личния живот относно човешките ресурси и да посочи къде е предоставила на разположение на засегнатите служители тази политика, за да могат да я разгледат.

г) Министерството ще поддържа Списъка към Щита за личните данни с организациите, които са подали пълна информация за самосертифициране, като по този начин ще гарантира те да се ползват с предимствата на Щита за личните данни и ще актуализира този списък въз основа на пресамосертифицирането им и уведомленията, получавани всяка година съгласно допълнителния принцип за разрешаване на спорове и принудително изпълнение. Тази информация за самосертифициране трябва да се подава ежегодно; в противен случай организацията ще бъде заличена от Списъка към Щита за личните данни и няма да продължи да се ползва с предимствата, които той осигурява. Списъкът към Щита за личните данни и подадената от организациите информация за самосертифициране ще бъдат предоставени за публичен достъп. Всички организации, които са включени в Списъка към Щита за личните данни от министерството, трябва също така да заявят в съответните си публични декларации относно политиката си в областта на неприкосновеността на личния живот, че спазват Принципите на Щита за личните данни. Когато политиката на една организация в областта на неприкосновеността на личния живот е на разположение онлайн, в нея трябва да се предостави хипервръзка към страницата

на Щита за личните данни на уебсайта на министерството, както и хипервръзка към уебсайт или към формуляр за подаване на жалба на независимия механизъм за защита, който е на разположение за разглеждане на нерешени жалби.

д) Принципите на неприкосновеност на личния живот се прилагат незабавно след сертифицирането. Предвид факта, че Принципите ще окажат влияние върху търговските взаимоотношения с трети страни, организациите, които се сертифицират съгласно рамката на Щита за личните данни през първите два месеца след датата, от която рамката се прилага ефективно, следва да приведат съществуващите си търговски взаимоотношения с трети страни в съответствие с принципа за отчетност за последващото предаване във възможно най-кратък срок и във всички случаи не по-късно от девет месеца, след като са се сертифицирали съгласно Щита за личните данни. Когато организациите предават данни на трета страна в този междинен период, те трябва: i) да прилагат принципите на уведомяването и на избора и ii) когато личните данни се предават на трета страна, която изпълнява функцията на представител, да определят, че представителят е задължен да осигури най-малко същата степен на защита, която се изисква съгласно Принципите.

е) Всяка организация трябва да прилага Принципите на неприкосновеност на личния живот за всички лични данни, които получава от ЕС съгласно Щита за личните данни. Задължението за спазване на Принципите на Щита за личните данни не е ограничено във времето по отношение на личните данни, получени през периода, когато организацията се ползва от предимствата на Щита за личните данни. Това задължение означава, че организацията ще продължи да прилага Принципите за тези данни, докато ги съхранява, използва или разкрива, дори ако по някаква причина впоследствие се напусне Щита за личните данни. Организация, която се оттегли от Щита за личните данни, но желае да запази тези данни, трябва ежегодно да потвърждава пред министерството ангажимента си, че ще продължи да прилага Принципите или ще осигури „адекватна“ защита за информацията чрез други разрешени средства (например като използва договор, в който изцяло са включени изискванията по съответните одобрени от Европейската комисия стандартни договорни клаузи); в противен случай организацията трябва да върне или заличи информацията. Организация, която се оттегли от Щита за личните данни, трябва да премахне от съответната си политиката в областта на неприкосновеността на личния живот всички упоменавания на Щита за личните данни, които могат да водят до заключението, че продължава да участва активно и се ползва с предимствата от участието си в Щита за личните данни.

ж) Организация, която престане да съществува като самостоятелно юридическо лице поради сливане или придобиване от друга организация, трябва предварително да уведоми за това министерството. В уведомлението трябва също така да бъде посочено дали организацията, която я е придобила или която се образува след сливането: i) ще продължи да бъде обвързана от Принципите на Щита за личните данни при действието на правото, уреждащо сливането или придобиването, или ii) ще избере да се самосертифицира за спазването на Принципите на Щита за личните данни или ще предвиди други гаранции, като писмено споразумение, гарантиращо спазването на тези принципи. Ако не е приложимо нито i), нито ii), всички лични данни, придобити съгласно Щита за личните данни, трябва да бъдат незабавно заличени.

з) Когато по някаква причина организация напусне Щита за личните данни, тя трябва да премахне всички твърдения, които могат да водят до заключението, че продължава да участва или се ползва с предимствата от участието си в Щита за личните данни. Също така трябва да премахне и сертификационния знак на Щита за личните данни в отношенията между ЕС и САЩ, ако го използва. Всяко погрешно представяне пред широката общественост относно придържането на организацията към Принципите на Щита за личните данни може да подлежи на санкциониране от ФТК или друг съответен държавен орган. Погрешно представяне пред министерството може да бъде санкционирано по силата на Закона за неверните твърдения (False Statements Act) (18 U.S.C. § 1001).

7. **Проверка**

а) Организациите трябва да предвидят процедури за последващ контрол, за да се провери дали уверенията и твърденията им относно техните практики в областта на неприкосновеността на личния живот съгласно Щита за личните данни са верни и дали тези практики се прилагат както са представени и съгласно Принципите на Щита за личните данни.

б) За да се отговори на изискванията за проверка съгласно принципа за защита, прилагане и отговорност за причинени вреди, организацията трябва да удостовери верността на тези уверения и твърдения чрез самооценка или външни прегледи на спазването.

в) Съгласно подхода за самооценка проверката трябва да установи, че обявената публично политика на организацията в областта на неприкосновеността на личния живот относно личната информация, получавана от ЕС, е точна, пълна, поставена на видно място, прилага се изцяло и е достъпна. Също така тя трябва да покаже, че политиката на тази организация в областта на неприкосновеността на личния живот съответства на Принципите на Щита за личните данни; че физическите лица са информирани за съществуването на вътрешни процедури за разглеждане на жалбите и независими механизми, до които те могат да отнесат жалбите си; че има процедури за подготовка на служителите за прилагането на тази политика и за дисциплинарна отговорност при неспазване; и че има вътрешни процедури с цел периодичното провеждане на обективен преглед на спазването на горното.

Поне веднъж годишно корпоративен служител или друг упълномощен представител на организацията трябва да подписва декларация за заверка на самооценката и тя трябва да бъде предоставяна на физическите лица при поискване или в рамките на дадено разследване или жалба за неспазване.

г) Ако организацията е избрала външен преглед на спазването, последният трябва да докаже, че политиката на организацията в областта на неприкосновеността на личния живот относно личната информация, получавана от ЕС, съответства на Принципите на Щита за личните данни, че тази политика се спазва и че физическите лица са информирани за механизмите, които им позволяват да подават жалби. Методите за преглед могат да включват без ограничение одит, случайни проверки, използването на разобличаващи средства или на подходящи технологични инструменти. Поне веднъж годишно от контролиращото лице, от корпоративен служител или от друг упълномощен представител на организацията трябва да бъде подписвана декларация, потвърждаваща, че е успешно извършен външен преглед на спазването и той трябва да бъде предоставен на физическите лица при поискване или в рамките на дадено разследване или жалба за неспазване.

д) Организациите трябва да съхраняват документацията си за прилагането на техните практики в областта на неприкосновеността на личния живот съгласно Щита за личните данни и да представят тази документация при поискване, в рамките на разследване или жалба за неспазване, на независимия орган, отговорен за разглеждане на жалбите, или на институцията, която е компетентна в областта на нелоялните и измамни практики. Организациите трябва също така да предоставят своевременно отговори на запитвания и други искания за информация на министерството във връзка със спазването от тяхна страна на Принципите.

8. **Достъп**

а) Принципът на достъпа на практика

i. Съгласно Принципите на Щита за личните данни правото на достъп е основен елемент от защитата на неприкосновеността на личния живот. По-конкретно то позволява на физическите лица да проверяват точността на наличната информация относно тях. Принципът на достъпа означава, че физическите лица имат право:

1. да получат от дадена организация потвърждение дали тя обработва лични данни, свързани с тях ([1]);

2. да им бъдат съобщени тези данни, за да могат да проверят дали са точни и дали обработването се извършва законосъобразно; и

3. да бъдат коригирани, изменени или заличени данните, когато са неточни или се обработват в нарушение на Принципите.

ii. От физическите лица не се изисква да обосновават исканията си за достъп до личните си данни. Когато отговарят на искания за достъп от страна на физическите лица, организациите следва да се ръководят преди всичко от мотивите на лицата. Например, ако искането за достъп е неясно или много общо по съдържание, организацията може да обсъди това с физическото лице, за да разбере по-точно мотивите му във връзка с искането и да потърси подходящата информация. Организацията може да поиска да разбере с коя(и) служба(и) физическото лице е имало контакти или какво е естеството или употребата на информацията, която е предмет на искането за достъп.

iii. В съответствие с фундаменталния характер на правото на достъп организациите следва винаги да полагат усилия, за да предоставят достъп. Например, ако трябва да се защити някаква информация и тя може лесно да бъде отделена от останалата лична информация, която е предмет на искането за достъп, организацията следва да отдели защитената информация, като направи достъпна останалата. Ако организацията реши да ограничи достъпа в конкретен случай, тя следва да предостави на физическото лице, изискващо достъп, обяснение за това свое решение и да посочи лице за контакт за повече информация.

б) Затруднения или разходи по предоставянето на достъп

i. Правото на достъп до лични данни може да бъде ограничавано при изключителни обстоятелства, когато биха били нарушени законните права на лица, различни от заинтересованото, или когато затрудненията или разходите по предоставяне на достъп биха били несъразмерни спрямо рисковете за неприкосновеността на личния живот на физическото лице във въпросния случай. Разходите и необходимите усилия са важни фактори и следва да бъдат взети предвид, но те не са решаващи при определяне основателността на предоставянето на достъп.

([1]) Организацията следва да отговаря на искания на физическите лица относно целите на обработването, категориите лични данни, за които се отнася, и получателите или категориите получатели, на които се разкриват личните данни.

ii. Така например, ако личната информация се използва, за да се вземат решения, които ще имат сериозни последици за физическото лице (например отказ или предоставяне на важни предимства, като застраховка, ипотека или работа), организацията е длъжна съобразно останалите разпоредби на тези допълнителни принципи да разкрие тази информация, дори ако това се окаже относително трудно или скъпо. Ако исканата лична информация не е с чувствителен характер и не се използва, за да се вземат решения, които ще имат сериозни последици за физическото лице, а е лесно достъпна и разходите за предоставянето ѝ не са високи, организацията трябва да предостави достъп до нея.

в) Поверителната търговска информация

i. Поверителната търговска информация е информация, която организацията полага усилия да пази от разкриване, защото нейното разкриване би улеснило конкуренти на пазара. Организациите могат да откажат или да ограничат достъпа, доколкото предоставянето на пълен достъп би разкрило тяхна собствена поверителна търговска информация, като например маркетингови концепции или класификации, изготвени от тази организация, или поверителна търговска информация, принадлежаща на други организации, когато тази информация е предмет на договорни задължения за поверителност.

ii. Ако поверителната търговска информация може лесно да се отдели от другата лична информация, която е предмет на искането за достъп, организацията следва да отдели поверителната търговска информация и да предостави неповерителната информация.

г) Организиране на бази данни

i. Достъпът може да се предостави като разкриване на съответната лична информация от организацията на физическото лице, без да се налага достъп от страна на физическото лице до базата данни на организацията.

ii. Достъпът се осигурява само в рамките на личната информация, която организацията съхранява. Принципът на достъпа сам по себе си не поражда никакво задължение за запазване, поддържане, реорганизация или преструктуриране на файловете с лична информация.

д) Кога достъпът може да бъде ограничаван

i. Тъй като организациите трябва винаги да полагат усилия, за да предоставят достъп на физическите лица до техните лични данни, обстоятелствата, при които те могат да ограничават този достъп, са ограничени и всички мотиви за това трябва да бъдат конкретни. Както това е установено в Директивата, организацията може да ограничава достъпа до информация, доколкото нейното разкриване има вероятност да засегне опазването на важни обществени интереси като националната сигурност, отбраната или обществената сигурност. Достъпът може също така да бъде отказан, когато личната информация се обработва единствено за целите на изследвания или статистически цели. Други мотиви за отказ или ограничаване на достъпа са:

1. накърняване на изпълнението или прилагането на законодателството или на частно-правен иск, включително предотвратяването, разследването или разкриването на престъпления или упражняване правото на справедлив съдебен процес;

2. разкриване, което би нарушило законните права или важни интереси на други лица;

3. нарушаване на правно или друго професионално задължение или привилегия;

4. нарушаване на разследвания на служители по отношение на сигурността или относно оплаквания, или във връзка с планиране на нови назначения и реорганизации на дружествата; или

5. нарушаване на поверителността, необходима при извършване на мониторинг, инспекции или изпълнение на регулаторни функции във връзка с доброто управление, или при бъдещи или текущи преговори, в които организацията участва.

ii. Задължение на организацията е, когато се позовава на изключение, да докаже неговата наложителност, както и да представи на физическите лица мотивите си за ограничаване на достъпа и да посочи лице за контакт за повече информация.

е) Право на получаване на потвърждение и определяне на такса за покриване на разходите по предоставяне на достъп

i. Всяко физическо лице има право да получи потвърждение дали дадена организация разполага с лични данни, свързани с него. Също така всяко физическо лице има право да му бъдат съобщени личните данни, свързани с него. Организацията може да определи такса, която не е прекалено висока.

ii. Определянето на такса може да е основателно, когато например исканията за достъп са явно прекомерни, и по-специално поради техния повтарящ се характер.

iii. Достъпът не може да бъде отказан по финансови причини, ако физическото лице предложи да поеме разноските.

ж) Искания за достъп с повтарящ се или злонамерен характер

Всяка организация може да определи допустимо ограничение на броя на исканията за достъп, подавани от конкретно физическо лице за определен период. Когато определя тези ограничения, организацията следва да отчита фактори като честота на актуализиране на информацията, целта, с която се използват данните, и естеството на информацията.

з) Искания за достъп с измамен характер

Организацията не е длъжна да предоставя достъп, ако не получи необходимата информация за потвърждаване на самоличността на лицето, отправило искането.

и) Срок за отговор

Организациите следва да отговарят на искания за достъп в рамките на разумни срокове, по допустим начин и във форма, която е лесноразбираема за физическото лице. Организация, която предоставя информация на субектите на данни през редовни интервали от време, може да отговори на искане за достъп от физическо лице с редовното предоставяне на информация, ако това няма да доведе до прекомерно забавяне.

9. **Данни за човешки ресурси**

а) Обхват на Щита за личните данни

i. Когато лична информация относно наети лица (настоящи или бивши), събирана в рамките на трудовите правоотношения, се предава от организация в ЕС на участващо в Щита за личните данни предприятие майка, дъщерно предприятие или доставчик на услуги, който не е свързано дружество, в Съединените щати, това предаване се ползва от предимствата на Щита за личните данни. В този случай събирането на информацията, както и обработването ѝ преди предаването ще се уреждат от националното законодателство на държавата от ЕС, където е било извършено събирането, и ще трябва да се спазват всички условия или ограничения по предаването ѝ в съответствие с това законодателство.

ii. Принципите на Щита за личните данни са релевантни само в случай на предаване или на достъп до конкретна информация за отделни лица. Статистическата информация, основаваща се на общи данни за заетостта, без да съдържа лични данни, или използването на анонимизирни данни, не поражда загриженост за неприкосновеността на личния живот.

б) Прилагане на принципите на уведомяването и на избора

i. Организация в САЩ, която е получила от ЕС информация за наети лица съгласно Щита за личните данни, може да я разкрива на трети страни или да я използва за други цели само ако са спазени принципите на уведомяването и на избора. Например, ако организация в САЩ възнамерява да използва личната информация, събрана в рамките на трудови правоотношения, за цели, които не са свързани с трудовите правоотношения — например маркетингови съобщения — тя трябва преди това да даде възможност за избор на засегнатите физически лица, освен ако последните не са дали вече своето разрешение информацията да бъде използвана за тази цел. Това използване не трябва да бъде несъвместимо с целите, за които личната информация е била събрана или впоследствие е дадено разрешение от физическото лице. От друга страна, такъв избор не трябва да бъде използван, за да бъдат ограничавани възможностите, произтичащи от трудовите правоотношения, или за предприемане на наказателни действия срещу тези наети лица

ii. Следва да се отбележи, че някои общоприложими условия за предаването на данни от страна на някои държави — членки на ЕС, може да изключват други употреби на такава информация, дори след предаването ѝ извън територията на ЕС, и такива условия трябва да бъдат спазени.

iii. В допълнение към това работодателите следва да се стремят да вземат предвид предпочитанията на наетите лица в областта на неприкосновеността на личния живот. Това може да включва например ограничаване на достъпа до личните данни, анонимизиране на някои данни или кодиране, или псевдонимизиране, когато за целите на управлението не се изисква използване на истинските имена.

iv. В рамките на необходимото и за срока, необходим, за да се избегне накърняването на законните права на организацията да извършва повишаване в длъжност, назначения или вземането на други подобни решения в областта на трудовите правоотношения, не е необходимо организацията да спазва принципите на уведомяването и на избора.

в) Прилагане на принципа на достъпа

В допълнителния принцип на достъпа се предоставят насоки относно причините, на които може да се основава отказът или ограничаването на поискан достъп в контекста на човешките ресурси. В Европейския съюз, разбира се, работодателите трябва да спазват правните разпоредби, приложими в тяхната държава, и да гарантират, че наетите лица в Европейския съюз имат достъп до информацията съгласно законодателствата на техните държави, независимо от мястото, където се извършва обработването и съхраняването на данните. Съгласно Щита за личните данни организация, която обработва такива данни в Съединените щати, трябва да сътрудничи при предоставянето на такъв достъп или пряко, или чрез работодателя от ЕС.

г) Прилагане

i. Доколкото личната информация се използва само в рамките на трудовите правоотношения, основната отговорност за данните по отношение на наетото лице носи организацията в ЕС. От това следва, че ако европейски наети лица възразят срещу нарушаване на правата им за защита на данните и не са удовлетворени от резултатите от вътрешните процедури за преглед, разглеждане на жалбите и обжалване (или от всяка друга вътрешна процедура, приложима по силата на сключен договор с профсъюз), те следва да бъдат насочвани към щатския или националния орган по защита на данните или към орган трудово-правни отношения, в чийто района на компетентност работи наетото лице. Тук се включват и случаите, когато за твърдяното нарушение на правата при обработването на лична информация е отговорна организацията в САЩ, която е получила информацията от работодателя, и следователно е налице твърдяно нарушение на Принципите на Щита за личните данни. Това ще бъде най-ефикасният начин за разрешаване на проблемите, които се проявяват често между застъпващите се права и задължения, определени от националните законодателства в областта на трудовото право и от колективните трудови договори, както и от законодателството в областта на защитата на данните.

ii. Следователно организация в САЩ — участник в Щита за личните данни, която използва данни от ЕС относно човешки ресурси, предадени от Европейския съюз в рамките на трудовите правоотношения, и която желае това предаване да бъде обхванато от Щита за личните данни, трябва да поеме ангажимента за тази цел да сътрудничи при разследвания от страна на компетентните органи на ЕС и да спазва препоръките им.

д) Прилагане на принципа на отчетност за последващото предаване

За свързани с трудово-правните отношения оперативни нужди със случаен характер на организация — участник в Щита за личните данни, които касаят лични данни, предавани съгласно Щита за личните данни, като например резервация на полет, стая в хотел или застраховка, предаванията на лични данни на малко на брой наети лица към администратори може да се извършват, без да се прилага принципът на достъпа или да се сключва договор с третата страна администратор, както иначе се изисква по силата на принципа на отчетност за последващото предаване, при условие че организацията — участник в Щита за личните данни, е спазила принципите на уведомяването и на избора.

10. **Задължителни договори за последващите предавания**

а) Договори за обработване на данни

i. Когато предаването на лични данни от ЕС към Съединените щати се извършва само за целите на обработването, се изисква договор независимо дали обработващият е организация — участник в Щита за личните данни.

ii. От администраторите на данни в Европейския съюз се изисква винаги да подписват договор, когато се извършва предаване за целите само на обработване на данните, независимо дали това обработване се извършва във или извън ЕС и дали обработващият е организация — участник в Щита за личните данни. Предназначението на договора е да се осигури, че обработващият данните:

1. действа единствено по указания на администратора;

2. осигурява подходящи технически и организационни мерки за защита на личните данни от случайно или неправомерно унищожаване, случайна загуба, промяна, неразрешено разкриване или достъп, и е наясно дали е разрешено последващото предаване; и

3. като взема предвид естеството на обработването, подпомага администратора да отговори на искания на физически лица за упражняване на предвидените в Принципите права.

iii. Имайки предвид, че организациите — участници в Щита за личните данни, гарантират адекватна защита, договорите само за целите на обработването, сключени с такива участници, не изискват предварително разрешение (или такова разрешение се дава автоматично от държавите — членки на ЕС), за разлика от договорите с получателите на данни, които не са участници в Щита за личните данни или които не гарантират адекватна защита.

б) Предавания в рамките на група дружества или група субекти под общ контрол

Когато личната информация се предава между двама администратори в рамките на група дружества или група субекти под общ контрол, невинаги се изисква договор в съответствие с принципа на отчетност за последващото предаване. Администраторите на данни в рамките на група дружества или група субекти под общ контрол могат да се основават при тези предавания на данни на други инструменти, като например задължителни фирмени правила на ЕС или други вътрешно-групови инструменти (напр. програми за спазване и контрол), които гарантират непрекъснатост на защитата на личната информация съгласно Принципите на Щита за личните данни. В случаи на такива предавания организацията — участник в Щита за личните данни, остава отговорна за спазването на Принципите на Щита за личните данни.

в) Предавания на данни между администратори

При предавания на данни между администратори не е необходимо получателят да бъде организация — участник в Щита за личните данни, или да разполага с независим механизъм за защита. Организацията — участник в Щита за личните данни, трябва да сключи договор с администратора — получател на третата страна, в който да се предвижда същата степен на защита, която осигурява Щитът за личните данни, без да се включва изискването към администратора на третата страна да е организация — участник в Щита за личните данни, или да разполага с независим механизъм за защита, при условие че той осигурява еквивалентен механизъм.

11. **Разрешаване на спорове и прилагане**

а) В принципа на защита, прилагане и отговорност за причинени вреди се определят изискванията за прилагане съгласно Щита за личните данни. В допълнителния принцип на проверка е определен начинът да се удовлетворят изискванията, формулирани в буква а), подточка ii) от принципа. В посочения допълнителен принцип се определят решения съгласно формулираните условия в буква а), подточки i) и iii), в които се поставя изискване за независим механизъм за защита. Тези механизми могат да имат различна форма, но трябва да отговарят на изискванията на принципа на защита, прилагане и отговорност за причинени вреди. Организациите отговарят на изискванията чрез следното: i) като се съобразяват с разработени от частния сектор програми за неприкосновеността на личния живот, в чиито правила са залегнали Принципите на Щита за личните данни и в които са предвидени ефективни механизми за прилагане от същото естество като описаните в принципа на защита, прилагане и отговорност за причинени вреди; ii) като се съобразяват с указанията на законоустановените или регулаторните органи за надзор, които осигуряват разглеждането на жалби на физическите лица и решаването на споровете; или iii) като се ангажират да сътрудничат с органите по защита на данните в рамките на Европейския съюз или с техните упълномощени представители.

б) Настоящият списък е примерен и не е ограничаващ. Частният сектор може да предвиди други механизми за прилагане, при условие че отговарят на изискванията на принципа на защита, прилагане и отговорност за причинени вреди и на допълнителните принципи. Моля, имайте предвид, че изискванията съгласно принципа на защита, прилагане и отговорност за причинени вреди допълват изискването, че мерките за саморегулиране трябва

да подлежат на принудително изпълнение съгласно раздел 5 от Закона за Федералната търговска комисия, който забранява нелоялните и измамни практики, или съгласно друг законов или подзаконов акт, с който се забраняват тези практики.

в) С цел да спомогнат за гарантиране спазването на ангажиментите си съгласно Щита за личните данни и да подпомагат управлението на програмата, организациите и техните независими механизми за защита трябва да предоставят информация във връзка с Щита за личните данни при поискване от министерството. Допълнително организациите трябва да отговарят експедитивно на жалби във връзка със спазването от тяхна страна на Принципите, за които са сезирани от ОЗД чрез министерството. В отговора трябва да се дава преценка по същество на жалбата и информация как организацията ще разреши проблема, ако случаят е такъв. Министерството ще осигури защита на поверителността на информацията, която получава, в съответствие с изискванията на правото на САЩ.

г) Механизъм за защита

i. Потребителите следва да бъдат насърчавани да подават жалбите, които евентуално биха повдигнали, до съответната организация, преди да се обърнат към независими механизми за защита. Организациите трябва да отговорят на потребителя в срок от 45 дни, считано от получаването на жалбата. Независимостта на механизма за защита се преценява на фактическа основа, като се доказва чрез критерии като безпристрастност, прозрачност по отношение на неговия състав и на неговото финансиране и доказан професионален опит. Както се предвижда съгласно принципа на защита, прилагане и отговорност за причинени вреди, подаването на жалби, което е право на физическите лица, трябва да е лесно осъществимо и безплатно за тях. Органите за разрешаване на спорове следва да разглеждат всички получени жалби от физическите лица, освен в случаите, когато са явно необосновани или нямат сериозен характер. Това условие не възпрепятства установяването от страна на организацията, която разглежда жалбите в рамките на механизма за защита, на критерии за допустимост, но те трябва да бъдат прозрачни и обосновани (примерно да се изключват жалби, които не са в обхвата на програмата или които са от компетенциите на други инстанции) и не би следвало да засягат ангажимента да се разглеждат законосъобразните жалби. Освен това механизмите за защита следва да дават на физическите лица пълна и лесно достъпна информация за функционирането на процедурата по разрешаване на спорове, когато подават жалба. Тази информация следва да включва уведомяване относно практиките на механизма в областта на неприкосновеността на личния живот съгласно Принципите на Щита за личните данни. Също така механизмите следва да си сътрудничат за разработването на инструменти за улесняване на процеса по разрешаване на споровете, като например стандартни формуляри за жалби.

ii. Независимите механизми за защита трябва да включват на своите публични уебсайтове информация относно Принципите на Щита за личните данни и услугите, които извършват съгласно Щита за личните данни. Тази информация трябва да включва: 1) информация или електронна връзка към изискванията относно независимите механизми за защита съгласно Принципите на Щита за личните данни; 2) електронна връзка към страницата на Щита за личните данни на уебсайта на министерството; 3) пояснение, че техните услуги по разрешаване на споровете съгласно Щита за личните данни са безплатни за физическите лица; 4) описание на това как може да бъде подадена жалба във връзка с Щита за личните данни; 5) сроковете, в които се разглеждат жалбите във връзка с Щита за личните данни; и 6) описание на набора от възможни средства за правна защита.

iii. Независимите механизми за защита трябва да публикуват годишен доклад с обобщена статистическа информация относно своите услуги по разрешаване на спорове. В годишния доклад трябва да бъдат включени: 1) общият брой на получените през отчетната година жалби във връзка с Щита за личните данни в отношенията между ЕС и САЩ; 2) видът на получените жалби; 3) качествени показатели за решаването на спора, напр. времето за обработването на жалбите; и 4) резултатите от получените жалби, а именно броят и видовете средства за правна защита или санкции, които са били наложени.

iv. Както е разгледано в приложение I, на разположение на физическите лица е възможност за арбитраж за неразрешените жалби, чрез която може да се определи дали организация — участник в Щита за личните данни, е нарушила задълженията си съгласно Принципите по отношение на това физическо лице и дали това нарушение е останало изцяло и частично неотстранено. Тази възможност е предвидена само за тези цели. Например по отношение на изключенията от Принципите ([1]) или на твърдения относно адекватността на Щита за личните данни не се предвижда такава възможност. Съгласно тази процедура за арбитраж специалната група по Щита за личните данни (в чийто състав влизат един или трима арбитри по споразумение между страните) е компетентна да предписва специфични за конкретния случай непарични безпристрастни мерки (например предоставяне на достъп, коригиране, заличаване или връщане на въпросните данни на физическото лице), необходими като коригиращо действие срещу нарушаването на Принципите единствено по отношение на физическото лице. Физическите лица и организациите — участници в Щита за личните данни, могат да отнасят арбитражните решения за съдебен контрол и принудително изпълнение по силата на правото на САЩ съгласно Федералния арбитражен закон (Federal Arbitration Act).

([1]) Раздел I.5 от Принципите.

д) Средства за правна защита и санкции

Средствата за правна защита, предоставени от органа, който решава споровете, би следвало да доведат до анулиране или коригиране от страна на организацията, в рамките на възможното, на последиците от неспазването на Принципите и до спазване на Принципите при по-нататъшното обработване на личните данни от същата организация или, когато случаят е такъв, до преустановяване на обработването на личните данни на физическото лице, подало жалбата. Санкциите трябва да са достатъчно строги, за да гарантират спазването на Принципите от страна на организацията. Набор от санкции с различна степен на строгост ще позволи на органите по разрешаване на споровете да предприемат подходящи ответни мерки спрямо различните степени на неспазване. Санкциите следва да включват даване на публичност в случаите на установяване на неспазване и изискване да се заличат данните при определени обстоятелства ([1]). Други санкции биха могли да включват спиране и отнемане на разрешителното, обезщетение за физическите лица за загубите, претърпени в резултат на неспазването, и разпореждания за прекратяване. Органите по разрешаване на споровете и саморегулиращите се организации от частния сектор трябва да уведомят съдилищата или държавните органи със съответна юрисдикция, според случая, относно организациите — участници в Щита за личните данни, които не спазват техните решения, и да уведомят министерството.

е) Действия на ФТК

ФТК се ангажира да разглежда с предимство случаи на неспазване на Принципите, за които е била сезирана от: i) саморегулиращи се организации в областта на неприкосновеността на личния живот и други независими инстанции за разрешаване на спорове; ii) държавите — членки на ЕС; и iii) министерството, за да определи дали са нарушени изискванията на раздел 5 от закона за Федералната търговска комисия за забраната на нелоялни или измамни действия или практики в търговията. Ако ФТК заключи, че има основание да счете, че раздел 5 е бил нарушен, тя може да реши въпроса, като изиска административна заповед за преустановяване и прекратяване, забраняваща оспорваните практики, или като внесе жалба пред федерален областен съд, който, ако признае жалбата, може да се произнесе с разпореждане със същото действие. Тук се включват и неверни твърдения за спазване на Принципите на Щита за личните данни или за участие в Щита за личните данни от страна на организации, които повече не са в Списъка към Щита за личните данни или никога не са се самосертифицирали пред министерството. ФТК може да поиска граждански санкции при неизпълнение на административна заповед за преустановяване и прекратяване и да преследва нарушителя за незачитане на съда — по реда на гражданското или наказателното право — ако не изпълни разпореждането на федералния съд. ФТК уведомява министерството за всички такива действия, които предприема. Министерството насърчава другите държавни органи да го уведомяват за изхода на всички подобни случаи на сезиране или други решения, определящи спазването на Принципите на Щита за личните данни.

ж) Трайно неспазване

i. Ако дадена организация трайно не се съобразява с Принципите, тя повече няма право да се ползва от предимствата на Щита за личните данни. Организации, които трайно не се съобразяват с Принципите, се заличават от Списъка към Щита за личните данни от министерството и трябва да върнат или заличат личната информация, която са получили съгласно Щита за личните данни.

ii. Трайно неспазване е налице, когато организацията, която се е самосертифицирала пред министерството, отказва да изпълнява окончателното решение на саморегулираща се организация в областта на неприкосновеността на личния живот, на независим орган по решаване на спорове или на държавен орган, или когато даден орган констатира, че организация често нарушава Принципите, дотолкова че нейното твърдение за спазване вече не е достоверно. В такива случаи организацията трябва незабавно да уведоми за това министерството. В противен случай тя може да бъде санкционирана по силата на Закона за неверните твърдения (False Statements Act) (18 U.S.C. § 1001). Оттеглянето на дадена организация от програма на частния сектор за саморегулиране в областта на неприкосновеността на личния живот или от независим механизъм за разрешаване на спорове не я освобождава от задължението да спазва Принципите и може да се счита за трайно неспазване.

iii. Министерството ще заличава организации от Списъка към Щита за личните данни в отговор на постъпило уведомление за трайно неспазване, независимо дали то е получено от самата организация, от саморегулираща се организация в областта на неприкосновеността на личния живот, от друг независим орган за разрешаване на спорове или от държавен орган, но едва след като е изпратило на организацията нарушител тридесет

([1]) Органите по разрешаване на споровете решават по собствено усмотрение относно обстоятелствата, при които да прилагат тези санкции. Един от факторите, които трябва да се отчитат, когато се взема решение дали ще се наложи данните да бъдат заличени, е дали това са чувствителни данни, както и дали организацията е събрала, използвала или разкрила информацията при явно неспазване на Принципите на Щита за личните данни.

дневно предизвестие и е дало възможност за отговор. В Списъка към Щита за личните данни, поддържан от министерството, съответно ще се посочва кои организации се ползват от предимствата на Щита за личните данни и кои вече не могат да се ползват от тях.

iv. Всяка организация, която заяви, че иска да участва в саморегулираща се организация, за да може отново да изпълни изискванията съгласно Щита за личните данни, трябва да предостави на тази организация пълна информация относно предишното си участие в Щита за личните данни.

12. **Избор — момент на прилагане на клаузата за неучастие („opt out“)**

а) Като цяло принципът на избора има за цел да гарантира, че личната информация се използва и разкрива съгласно очакванията и избора на физическото лице. Следователно, когато лична информация се използва в рамките на директния маркетинг, всяко физическо лице трябва да има възможност да упражни правото си на неучастие („opt out“) във всеки един момент и в определени допустими граници, установени от организацията, като например в срок, в който да може организацията да направи неучастието ефективно. Организацията може също така да изиска достатъчно информация, за да потвърди самоличността на физическото лице, което иска упражняването на „opt out“. В Съединените щати това право може да се упражнява от физическите лица чрез централна „opt out“ програма като Mail preference service на Direct Marketing Association. Организациите, които участват в Mail preference service на Direct Marketing Association, следва да насърчават предоставянето на тази програма на разположение на потребителите, които не искат да получават търговска информация. Във всеки случай за упражняването на тази възможност физическото лице следва да разполага с лесно достъпен механизъм на приемлива цена.

б) По същия начин организацията може да използва информацията за някои цели на директния маркетинг, когато условията не позволяват да се осигури възможност на физическото лице за „opt out“ преди използването на данните, при условие че след това в кратки срокове (и във всеки един момент при поискване) осигури такава възможност на лицето да откаже да получава други съобщения на директния маркетинг, без разноски за него, и уважи желанието на физическото лице.

13. **Информация, свързана с пътуване**

а) Резервационни данни на пътниците във въздушния транспорт и друга информация, свързана с пътуване, например информация за редовни клиенти или за резервации за хотел, както и за специфични нужди, като например предпочитания за храната в зависимост от изискванията на религията или необходимостта от физическа помощ при пътуването, може да се предава на организации извън ЕС при няколко различни обстоятелства. Съгласно член 26 от Директивата личните данни могат да се предават на „трета страна(, която) не осигурява достатъчна степен на защита по смисъла на (член 25,) параграф 2“, при условие че: i) е необходимо за предоставяне на исканите от потребителя услуги или за изпълнение на условията на даден договор, например споразумение за „редовни пътници“; или ii) потребителят е дал категоричното си съгласие. Организациите в САЩ, които участват в Щита за личните данни, осигуряват адекватна защита на личните данни и следователно могат да получават такива данни, предавани от ЕС, без да отговарят на тези условия или на другите условия, установени в член 26 от Директивата. След като в Щита за личните данни се съдържат специфични правила относно чувствителната информация, такава информация (която може да е необходимо да бъде събирана например във връзка с нуждата на клиенти от физическа помощ) може да бъде включена в данните, предавани на организациите — участници в Щита за личните данни. Във всички случаи обаче организацията, която предава информацията, трябва да спазва законодателството на държавата — членка на ЕС, в която осъществява дейността си, като в това законодателство може, наред с останалото, да са определени и специални условия за обработването на чувствителни данни.

14. **Фармацевтични и медицински продукти**

а) Прилагане на правото на държавите — членки на ЕС, или на Принципите на Щита за личните данни

Законодателството на държавите — членки на ЕС, се прилага за събирането на личните данни и за всяко обработване, което се извършва преди предаването в Съединените щати. Принципите на Щита за личните данни се прилагат за данните, след като те са били предадени в Съединените щати. За да бъдат използвани за фармацевтични изследвания и други цели, данните трябва да бъдат анонимизирани, когато това е уместно.

б) Бъдещи научни изследвания

i. Личните данни, събрани при конкретни медицински или фармацевтични изследвания, често имат важна роля за бъдещите научни изследвания. Когато личните данни, събрани за едно изследване, се предават на организация в САЩ съгласно Щита за личните данни, тази организация може да ги използва за нови научни изследвания, ако преди това съответно е уведомила за това и е предоставила възможност за избор. С това уведомяване трябва да се предостави информация за всяка бъдеща специфична употреба на данните, като например за периодичен последващ контрол, свързани изследвания или търговски цели.

ii. Разбираемо е, че не могат да бъдат уточнени всички бъдещи употреби на данните, тъй като ново приложение за целите на научните изследвания може да е налице и когато се прави нов анализ на първоначалните данни, нови медицински открития и разработки, както и при развитието в областта на общественото здраве и нормативната уредба. Следователно уведомяването трябва да включва по целесъобразност и пояснение, че личните данни могат да бъдат използвани в бъдещи медицински и фармацевтични изследвания, които не е възможно да бъдат предвидени. Ако тази употреба не е съвместима с общите изследователски цели, за които личните данни са били събрани първоначално или за които физическото лице е дало одобрението си впоследствие, трябва да бъде получено ново съгласие.

в) Оттегляне от клинично изпитание

Участниците в клинично изпитание могат във всеки един момент да решат да се оттеглят от него или да бъдат помолени за това. Всички лични данни, събрани преди оттеглянето, могат да бъдат обработвани заедно с другите данни, събрани в рамките на клиничното изпитание, но при условие че това е било ясно посочено на участника при уведомяването в момента, когато той е дал съгласието си за участие.

г) Предавания на данни за регулаторни и надзорни цели

На дружествата за фармацевтична и медицинска апаратура се позволява да предоставят личните данни, извлечени от клинични изпитания, осъществени в ЕС, на органи в Съединените щати за регулаторни и надзорни цели. По същия начин се позволява предаване на данни на други страни освен регулаторните органи, като например обекти на дружеството на друго място или други изследователи, съгласно принципите на уведомяването и на избора.

д) „Кодирани“ изследвания

i. За да се гарантира обективността, при много клинични изпитания достъпът до информацията, отнасяща се до лечението, проведено на всеки от участниците, е забранен за самите тях, а често пъти и за изследователите. Противното би поставило под въпрос валидността на изследването и на резултатите. За участниците в такива клинични изпитания (наричани „кодирани“ изследвания) не е необходимо да се осигурява достъп до информацията, отнасяща се до лечението им по време на изпитанието, ако това ограничение е било обяснено, когато е започнало изпитанието, и ако разкриването на тази информация може да навреди на почтеността на изследователската работа.

ii. Съгласието да се участва в изпитанията при тези условия предполага и отказ от правото на достъп. След приключването на изпитанията и анализа на резултатите, на участниците трябва да се предостави достъп до техните данни, ако поискат това. Те следва да се обърнат първо към лекаря или другите медицински обслужващи кадри, които са провеждали лечението им по време на клиничните изпитания, или на второ място — към организацията възложител.

е) Контрол на безопасността и ефикасността на продуктите

Не е необходимо дружествата за фармацевтична или медицинска апаратура да прилагат за своите дейности по контрол на безопасността и ефикасността на продуктите Принципите на Щита за личните данни по отношение на принципите на уведомяването, избора, отчетността за последващите предавания и достъпа, включително за докладите за неблагоприятни събития и за проследяването на пациенти/субекти, използващи определени лекарствени продукти или медицински изделия, доколкото придържането към Принципите е в противоречие със спазването на нормативните изисквания. Това се отнася както за докладите, изготвени например от лица, предоставящи здравни услуги, за фармацевтичните дружества и дружествата за медицински изделия, така и за

докладите на фармацевтичните дружества и дружествата за медицински изделия, изготвяни за държавни институции, като например Администрацията по храните и лекарствата (Food and Drug Administration).

ж) Данни, кодирани с ключ

Данните в изследването обикновено са кодирани с уникален ключ още в мястото им на произход от главния изследовател, за да не бъде разкрита самоличността на отделните субекти на данните. Фармацевтичните дружества, които възлагат подобни изследвания, не получават ключа на кода. Единствено изследователят съхранява уникалния ключ на кода, за да може да идентифицира субекта на изследването при извънредни обстоятелства (например, ако след това се налага медицинска помощ). Предаването от ЕС към Съединените щати на данни, които са били кодирани по този начин, не би представлявало предаване на лични данни, което се извършва съгласно Принципите на Щита за личните данни.

15. **Публични регистри и информация, достъпна за широката общественост**

а) Всяка организация трябва да прилага Принципите на Щита за личните данни за сигурността, цялостта на данните и ограничаване в рамките на целта, както и за защитата, прилагането и отговорността за причинени вреди спрямо личните данни от източници с публичен достъп. Тези Принципи трябва да се прилагат и за всички лични данни, събрани от публични регистри, т.е. от регистрите, водени от държавните агенции или организации на всяко равнище, които са на разположение на широката общественост за справки.

б) Не е необходимо принципите на уведомяването, на избора или на отчетността за последващото предаване да се прилагат за информацията в публичните регистри, ако тя не е съчетана с непублична информация от регистъра и ако са спазени всички условия за ползването ѝ за справки, установени от компетентните органи. Също така обикновено не е необходимо да се прилагат принципите на уведомяването, на избора или на отчетността за последващото предаване за информацията, предоставена за публичен достъп, освен когато предаващата организация от ЕС е указала, че тази информация подлежи на ограничения, които налагат организацията получател да прилага тези принципи при използването ѝ по предназначение. Организациите не носят отговорност обаче за това как се използва тази информация от лица, които са я придобили от публикувани материали.

в) Ако се окаже, че дадена организация умишлено е публикувала лична информация в нарушение на принципите, по такъв начин, че тя или други лица да могат да се ползват от тези изключения, тогава тя ще бъде изключена от участие в Щита за личните данни.

г) Не е необходимо принципът на достъпа да се прилага за информация в публичните регистри, ако тя не е съчетана с друга лична информация (освен малко количество данни, използвани за индексиране или организиране на информацията в публичните регистри), но трябва да се спазят всички условия за ползването ѝ за справки, установени от компетентните органи. За разлика от това, когато информацията в публичните регистри е съчетана с друга информация от непублични регистри (с изключение на случая, изрично посочен по-горе), организацията е длъжна да предостави достъп до цялата такава информация, при положение че за нея не се прилагат други разрешени изключения.

д) Както при информацията от публичните регистри, не е необходимо да се предоставя достъп до информация, която вече е предоставена на разположение на широката общественост, освен ако тази информация не е съчетана с такава, която не е за публичен достъп. Организациите, които участват в дейности по продажба на достъпна за обществеността информация, могат да удовлетворяват исканията за достъп срещу заплащане на обичайната такса, която са определили за това. По избор физическите лица могат да поискат достъп до информацията, която ги засяга, като се обръщат направо към организацията, която първоначално е събрала данните.

16. **Искания за достъп от публични органи**

а) За да се осигури прозрачност във връзка със законни искания на публични органи за достъп до лична информация, организациите — участници в Щита за личните данни, могат при желание да издават периодични доклади за прозрачност с броя на исканията за лична информация, които са получили от публични органи за целите на правоприлагането или националната сигурност, доколкото това разкриване е разрешено съгласно приложимото право.

б) Предоставената информация в тези доклади от организациите — участници в Щита за личните данни, наред с публикуваната информация от разузнавателната общност и друга информация, може да се използва за целите на годишния съвместен преглед на функционирането на Щита за личните данни, както това е предвидено в Принципите.

в) Ако не е направено уведомяване съгласно изискванията на буква а), подточка xii) от принципа на уведомяването, това не пречи и не намалява възможността за организацията да отговаря на всички законни искания.

Приложение I

Арбитражен модел

В настоящото приложение I се определят условията, при които организациите — участници в Щита за личните данни, са задължени да решават жалбите чрез арбитраж съгласно принципа за защита, прилагане и отговорност за причинени вреди. Възможността за правно обвързващ арбитраж, описана по-долу, се прилага за някои жалби относно данни, предавани съгласно Щита за личните данни в отношенията между ЕС и САЩ, по които няма определено решение. С тази възможност се цели да се предостави бърз, независим и справедлив механизъм, който по избор на физическите лица може да бъде прилаган за решаване на жалби за нарушаване на Принципите, по които няма определено решение чрез някой от другите механизми съгласно Щита за личните данни, ако съществуват такива.

А. **Обхват**

Тази възможност за арбитраж е на разположение на физическите лица за нерешените жалби, за да може да се определи дали организация — участник в Щита за личните данни, е нарушила задълженията си съгласно Принципите по отношение на това физическо лице и дали това нарушение е останало изцяло и частично неотстранено. Тази възможност е предвидена само за тези цели. Например по отношение на изключенията от Принципите ([1]) или на твърдения относно адекватността на Щита за личните данни не се предвижда такава възможност.

Б. **Налични средства за правна защита**

Съгласно тази процедура за арбитраж специалната група по Щита за личните данни (в чийто състав влизат един или трима арбитри, по споразумение между страните) е компетентна да предписва специфични за конкретния случай непарични безпристрастни мерки (например предоставяне на достъп, коригиране, заличаване или връщане на въпросните данни на физическото лице), необходими като корективно действие срещу нарушаването на Принципите единствено по отношение на физическото лице. Специалната група по арбитража разполага единствено с тези правомощия във връзка със средствата за правна защита. Когато определя корективните мерки, от специалната група по арбитража се изисква да взема предвид и другите средства за правна защита, които са били определени преди това от други механизми съгласно Щита за личните данни. Не се предоставя правна защита по отношение на претърпени вреди, направени разходи, заплатени такси и други. Всяка страна по спора сама поема разноските по хонорарите на адвокати.

В. **Изисквания преди арбитраж**

Когато едно физическо лице реши да използва тази възможност за арбитраж, то трябва да предприеме следните стъпки, преди да инициира арбитражно производство: 1) да подаде жалбата срещу нарушението направо пред организацията и да предостави възможност на тази организация да намери решение на въпроса в рамките на срока, определен в раздел III, точка 11, буква г), подточка i) от Принципите; 2) да използва независимия механизъм за защита съгласно Принципите, който е безплатен за физическите лица; и 3) да отнесе въпроса до Министерството на търговията чрез съответния орган по защита на данните и да предостави възможност на министерството да положи максимални усилия да разреши въпроса в рамките на срока, определен в писмото на Администрацията по международна търговия към Министерството на търговията, безплатно за лицето.

Тази възможност за арбитраж не може да се използва, когато преди това по жалба на това физическо лице срещу същото нарушение на Принципите: 1) е прилаган правно обвързващ арбитраж; 2) е определено окончателно решение след съдебен процес, по който физическото лице е било страна; или 3) вече е постигнато споразумение между страните. Освен това тази възможност за арбитраж не може да се използва, когато орган по защита на данните от ЕС: 1) има правомощия съгласно раздел III, точки 5 или 9 от Принципите; или 2) има правомощия да определи решение по жалбата срещу нарушение директно с организацията. Компетентността на ОЗД да определи решение по същата жалба срещу администратор на данни от ЕС сама по себе си не изключва възможността да бъде използвана тази възможност за арбитраж срещу друго юридическо лице, спрямо което този ОЗД няма правомощия.

Г. **Обвързващ характер на решенията**

Решението на дадено физическо лице да използва тази възможност за правно обвързващ арбитраж е напълно доброволно. Арбитражните решения ще бъдат задължителни за всички страни по арбитражното производство. Инициирането на арбитраж означава, че физическото лице се отказва от възможността да търси решение по жалбата срещу същото нарушение пред друга инстанция, освен когато определените непарични безпристрастни мерки не компенсират напълно извършеното нарушение и инициирането на арбитражно дело не изключва възможността за физическото лице да поиска обезщетение за вреди в обикновените съдилища.

([1]) Раздел I.5 от Принципите.

Д. **Контрол и принудително изпълнение**

Физическите лица и организациите — участници в Щита за личните данни, могат да отнесат арбитражните решения за съдебен контрол и принудително изпълнение по силата на правото на САЩ съгласно Федералния арбитражен закон (Federal Arbitration Act) ([1]). В тези случаи отнасянето става във федерален окръжен съд, в чиято териториална компетентност се намира основното място на установяване на дейността на организацията— участник в Щита за личните данни.

Тази възможност за арбитраж е предназначена за разрешаване на индивидуални спорове и арбитражните решения нямат действието на убедителен или обвързващ прецедент по въпроси, в които участват други страни, включително за бъдещи арбитражни производства или за съдилищата в ЕС или в САЩ, както и за производства на ФТК.

Е. **Специална група по арбитража**

Страните ще избират арбитри от списъка, разгледан по-нататък.

В съответствие с приложимото законодателство Министерството на търговията на САЩ и Европейската комисия ще съставят списък с най-малко 20 арбитри, подбрани въз основа на техните независимост, почтеност и опит. Във връзка с този процес ще се прилага следното:

Арбитрите:

1) ще остават включени в списъка за срок от 3 години освен в изключителни случаи или по основателни причини, като този срок може да бъде еднократно удължаван за нови 3 години;

2) не трябва да действат под указания на която и да е от страните, на организация — участник в Щита за личните данни, на правителствена институция, публичен орган или правоприлагащ орган на САЩ, ЕС, държава — членка на ЕС, или друг такъв орган, както и не трябва да са обвързани с такива; и

3) трябва да имат разрешение да практикуват юридическа професия в САЩ, да бъдат специалисти в законодателството на САЩ в областта на неприкосновеността на личния живот и да имат експертен опит и познания относно законодателството на ЕС в областта на защитата на данните.

Ж. **Арбитражни процедури**

Съобразно приложимото законодателство и в срок до 6 месеца, считано от приемането на решението за адекватност, Министерството на търговията и Европейската комисия ще се договорят относно приемането на набор от действащи и утвърдени арбитражни процедури в САЩ (като AAA или JAMS), които да уреждат производствата пред специалната група по Щита за личните данни, под условието на всяко от следните съображения:

1. Всяко физическо лице може да инициира правно обвързващ арбитраж при спазване на изискванията за действията преди арбитраж, разгледани по-горе, като изпрати „Уведомление“ на организацията. В уведомлението трябва да се съдържа обобщение на стъпките, предприети съгласно точка B за намиране на решение по жалбата, описание на твърдяното нарушение и, по избор на лицето, евентуални приложени документи и материали и/или правно изложение във връзка с твърдението за нарушение.

([1]) Съгласно глава 2 от Федералния арбитражен закон (Federal Arbitration Act) („ФАЗ“) „арбитражно споразумение или арбитражно решение, произтичащо от правни взаимоотношения, включително договорни, които могат да бъдат считани за търговски по характер, включително сделка, договор или споразумение от вида на описаните [в раздел 2 от ФАЗ], се включва в обхвата на Конвенцията [относно признаването и изпълнението на чуждестранни арбитражни решения от 10 юни 1958 г., 21 U.S.T. 2519, T.I.A.S. № 6997 („Конвенцията от Ню Йорк“)].“ 9 U.S.C. § 202. По-нататък във ФАЗ е предвидено, че „споразумение или решение, произтичащо от такива взаимоотношения, в които участват само граждани на Съединените щати, не се включва в обхвата на Конвенцията [от Ню Йорк], освен когато в тези взаимоотношения участва недвижимо имущество с местонахождение извън САЩ, когато се предвижда изпълнение на дейност или прилагане извън САЩ или по друг начин е налице някаква основателна връзка с една или повече чужди държави.“ Съгласно глава 2 „всяка от страните по арбитражното дело може да се отнесе до съд с юрисдикция съгласно разпоредбите в настоящата глава, за да поиска разпореждане в потвърждение на арбитражното решение, постановено срещу някоя от другите страни по арбитражното дело. Съдът потвърждава решението, освен когато констатира, че е налице едно от основанията за отказ или отсрочване на признаването или изпълнението на решението, както това е определено в посочената Конвенция [от Ню Йорк].“, пак там § 207. По-нататък в глава 2 е предвидено, че „окръжните съдилища в Съединените щати … са компетентни в първоначалния иск … или първоначалното производство [съгласно Конвенцията от Ню Йорк], независимо от размерите на спора.“, пак там § 203.
Също така в глава 2 е предвидено, че „Разпоредбите съгласно глава 1 се прилагат за искове и производства, инициирани съгласно разпоредбите в настоящата глава, доколкото разпоредбите в глава 1 не влизат в противоречие с тези в настоящата глава или в Конвенцията [от Ню Йорк], както тя е ратифицирана от Съединените щати.“, пак там § 208. От друга страна в глава 1 е предвидено, че „писмени разпоредби в … договор за търговска сделка, отнасящи се до решаване чрез арбитраж на спорове, произтичащи от такъв договор, или сделка или от отказ да бъде изпълнен договорът изцяло или частично, както и писмено споразумение да бъде инициирано арбитражно дело по съществуващ спор, възникнал въз основа на такъв договор, сделка или отказ, се считат за валидни, неотменими и подлежащи на принудително изпълнение, освен когато са налице съществуващи по закон основания или справедливи основания за отмяна на договора.“, пак там § 2. По-нататък в глава 1 е предвидено, че „всяка страна по арбитражния спор може да изиска от посочения съд разпореждане за потвърждаване на решението, след което съдът е задължен да издаде такова разпореждане, освен когато решението е било отменено, изменено или поправено, както това е предвидено в раздели 10 и 11 [от ФАЗ].“, пак там § 9.

2. Процедурите трябва да бъдат изпълнени, за да се гарантира, че няма да има дублиране на средствата или процедурите за правна защита по жалбата на това физическо лице срещу същото нарушение.

3. Действията на ФТК могат да се предприемат успоредно с арбитражното производство.

4. В тези арбитражни производства не може да участва представител на правителствена институция, публичен орган или правоприлагащ орган на САЩ, ЕС, държава — членка на ЕС, или друг такъв орган, като по искане на физическото лице от ЕС ОЗД могат да оказват съдействие само за изготвянето на уведомлението, но те не могат да имат достъп до разкрития или каквито и да е други материали във връзка с арбитражното дело.

5. Мястото на провеждане на арбитража ще е в Съединените щати, а физическото лице може да избере да участва чрез видео- или телефонна връзка, която се осигурява безплатно за него. Не е наложително да участва лично.

6. Езикът, на който ще се води арбитражното дело ще бъде английски, освен когато страните са се споразумели за друго. При мотивирано искане и като се взема предвид дали физическото лице се представлява от адвокат, ще се осигурява безплатно устен превод по време на изслушването и писмен превод на материалите по арбитражното дело, освен когато по преценка на специалната група при конкретните обстоятелства по арбитража това би довело до необосновани или непропорционални разходи.

7. Предоставените на арбитрите материали ще се третират като поверителна информация и ще бъдат използвани само във връзка с арбитражното дело.

8. Ако е необходимо, може да се допусне да бъдат представени специални разкрития на физическото лице, които ще бъдат третирани от страните като поверителна информация и ще бъдат използвани само във връзка с арбитражното дело.

9. Арбитражните дела трябва да приключат в срок до 90 дни, считано от изпращането на уведомлението до въпросната организация, освен когато страните са се договорили за друго.

3. **Разходи**

Арбитрите следва да предприемат подходящи мерки за свеждане до минимум на разноските или таксите по арбитражните дела.

В съответствие с приложимото законодателство Министерството на търговията ще съдейства за създаването на фонд, в който ще се изисква от организациите — участници в Щита за личните данни, да внасят годишни вноски, въз основа отчасти на глобата на организацията, и от който ще бъдат покривани разходите по арбитражната процедура, включително хонорарите за арбитрите, до определени максимални размери („таван“), което ще се извърши в консултация с Европейската комисия. Фондът ще се управлява от трета страна, която редовно ще докладва за работата му. При годишния преглед Министерството на търговията и Европейската комисия ще извършват преглед на работата на фонда, включително необходимостта от промяна на размера на вноските или тавана, като наред с останалото ще вземат предвид и броя на арбитражните дела и разноските и времетраенето им, като общото разбиране е да не се създава прекомерна финансова тежест за организациите — участници в Щита за личните данни. Таксите за хонорари на адвокати няма да се поемат съобразно с настоящата разпоредба, нито от фонда, създаден както това е предвидено в нея.

ПРИЛОЖЕНИЕ III

Писмо от Държавния секретар на САЩ Джон Кери

7 юли 2016 г.

Уважаема комисар Йоурова,

Радвам се, че постигнахме разбиране относно Щита за личните данни в отношенията между Европейския съюз и Съединените щати с включен Механизъм на омбудсмана, чрез който органите в ЕС ще могат да подават искания от името на физически лица от ЕС във връзка с практиките в радиоелектронното разузнаване на САЩ.

На 17 януари 2014 г. президентът Барак Обама обяви важни реформи в областта на разузнаването, включени в Президентски изпълнителен указ 28 (ПИУ-28). Съгласно ПИУ-28 определих заместник-държавния секретар Catherine A. Novelli, която също така изпълнява функциите на старши координатор на международната дипломация в областта на информационните технологии, да бъде нашето лице за връзка с чуждите правителства, които желаят да изразят безпокойство във връзка с дейностите на радиоелектронното разузнаване на САЩ. Въз основата на тази функция създадох Механизъм на омбудсмана към Щита за личните данни съобразно с условията, разгледани в приложение А, което бе актуализирано след моето писмо от 22 февруари 2016 г. Определих заместник-държавния секретар NovelliI да изпълнява тази функция. Заместник-държавният секретар NovelliI е независима от разузнавателните структури на САЩ и е пряко подчинена на мен.

Разпоредих на моите служители да бъдат вложени всички необходими ресурси за прилагането на този нов механизъм на омбудсмана и съм уверен, че той ще бъде ефективно средство за решаване на проблемните въпроси на физическите лица от ЕС.

С уважение,

Джон Ф. Кери

ПРИЛОЖЕНИЕ А

Механизъм на омбусмана на щита за личните данни в отношенията между ЕС и САЩ по отношение на радиоелектронното разузнаване

Като признава значението на рамката на Щита за личните данни в отношенията между ЕС и САЩ, настоящият меморандум определя процеса за прилагането на нов механизъм във връзка с радиоелектронното разузнаване в съответствие с Президентски изпълнителен указ 28 (ПИУ-28) ([1]).

На 17 януари 2014 г. президентът Обама обяви в своя реч важни реформи в областта на разузнаването. В тази реч той отбеляза, че „нашите усилия спомагат да защитим не само нашата нация, но също и нашите приятели и съюзници. Усилията ни ще бъдат ефективни само ако обикновените граждани в нашите държави имат увереността, че Съединените щати уважават неприкосновеността и на техния личен живот“. Президентът Обама обяви издаването на нов президентски указ — ПИУ-28 — „за определяне по ясен начин какво правим и какво не правим, когато се отнася за нашите наблюдения зад граница“.

В раздел 4, буква d) от ПИУ-28 се дават указания на държавния секретар да определи „старши координатор на международната дипломация в областта на информационните технологии“ (старши координатор), „който ... да изпълнява функциите на лице за връзка с чуждите правителства, които желаят да изразят безпокойство във връзка с дейностите на радиоелектронното разузнаване, провеждани от Съединените щати“. От януари 2015 г. функциите на старши координатор изпълнява заместник-държавният секретар C. Novelli.

В настоящия меморандум е разгледан един нов механизъм, който ще бъде прилаган от старшия координатор за улесняване обработването на искания във връзка с достъпа за целите на националната сигурност до данни, предавани от ЕС към Съединените щати съгласно Щита за личните данни, стандартни договорни клаузи (СДК), задължителни фирмени правила (ЗФП), „дерогации“ ([2]) или „възможни бъдещи дерогации“ ([3]), по установения ред съгласно приложимото законодателство и политиката на Съединените щати, както и предоставянето на отговор на такива искания.

1. **Омбудсманът към Щита за личните данни.** Старшият координатор ще изпълнява функциите на омбудсман към Щита за личните данни и ще определи допълнително длъжностни лица от Държавния департамент да я подпомагат, когато е необходимо за изпълняването на нейните задължения, разгледани подробно в настоящия меморандум. (Понататък в текста координаторът и длъжностните лица, които изпълняват тези задължения, ще бъдат наричани „Омбудсман към Щита за личните данни.“) Омбудсманът към Щита за личните данни ще работи в тясно сътрудничество със съответните длъжностни лица от други министерства и агенции, които отговарят за обработването на искания съгласно приложимото законодателство и политиката на Съединените щати. Омбудсманът е независим от разузнавателната общност. Омбудсманът е пряко подчинен на държавния секретар, който ще гарантира, че Омбудсманът изпълнява функциите си обективно и без неправомерно влияние, което може да има отражение върху отговорите, които следва да се предоставят.

2. **Ефективна координация.** Омбудсманът към Щита за личните данни ще може ефективно да използва описаните по-долу надзорни органи, както и да се координира с тях, с цел да се гарантира, че отговорът на Омбудсмана на органа на ЕС за разглеждане на индивидуални жалби, се основава на необходимата информация. Когато искането се отнася до

([1]) Предвид това че решението на Комисията относно адекватността на защитата, осигурена от Щита за личните данни в отношенията между ЕС и САЩ, се прилага в Исландия, Лихтенщайн и Норвегия, пакетът към Щита за личните данни ще обхване както Европейския съюз, така и тези три държави. Следователно позоваването на Договора за ЕС и неговите държави членки да се чете като включващо Исландия, Лихтенщайн и Норвегия.

([2]) В този контекст „дерогации“ означава предаване или предавания за търговски цели, които се извършват, при условие че: а) съответният субект на данните недвусмислено е дал съгласието си за предлаганото предаване на данни; или б) предаването е необходимо за изпълнението на договор между субекта на данните и администратора или за изпълнението на преддоговорни мерки, взети по искане на субекта на данните; или в) предаването е необходимо за сключването или изпълнението на договор, сключен в интерес на субекта на данните между администратора и трета страна; или г) предаването е необходимо или изисквано от закона поради важни причини от обществен интерес или за установяването, упражняването или защитата на правни претенции; или д) обработването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните; или е) предаването се извършва от регистър, който съгласно законите или подзаконовите актове е предназначен да предоставя информация на обществеността и е достъпен за справка от обществеността по принцип или от всяко лице, което може да докаже, че има законен интерес за това, доколкото условията, установени в правото, уреждащо извършването на справката, са изпълнени в конкретния случай.

([3]) В този контекст „Възможни бъдещи дерогации“ означава предаване или предавания за търговски цели, които се извършват при едно от следните условия, доколкото това условие представлява законно основание за извършване на предавания на лични данни от ЕС на САЩ: а) субектът на данните изрично е дал съгласието си за предлаганото предаване на данни, след като е бил информиран за свързаните с предаването възможни рискове за него поради липсата на решение относно адекватното ниво на защита и на подходящи гаранции; или б) предаването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на други лица, когато субектът на данните е физически или юридически неспособен да даде своето съгласие; или в) в случай на предаване на данни на трета държава или международна организация само ако предаването не е повторяемо, засяга само ограничен брой субекти на данни, необходимо е за целите на неоспоримите законни интереси, преследвани от администратора, над които не стоят интересите или правата и свободите на субекта на данни и администраторът е оценил всички обстоятелства, свързани с предаването на данните, и въз основа на тази оценка е предоставил подходящи гаранции във връзка със защитата на личните данни.

съвместимостта на наблюдението с правото на САЩ, Омбудсманът към Щита за личните данни ще може да си сътрудничи с един от независимите надзорни органи с правомощия за провеждане на разследвания.

а) Омбудсманът към Щита за личните данни ще работи в тясно сътрудничество с други длъжностни лица от правителството на Съединените щати, включително със съответните независими надзорни органи, с цел да се гарантира, че изготвените искания са разглеждани и решени в съответствие с приложимото законодателство и политиките. По-специално омбудсманът към Щита за личните данни ще може, според случая, да работи в тясна координация със Службата на директора на Националното разузнаване, Министерството на правосъдието и други министерства и агенции, свързани с националната сигурност на Съединените щати, както и с главните инспектори, служителите по Закона за свобода на информацията и служителите по въпросите на гражданските свободи и неприкосновеността на личния живот.

б) Правителството на Съединените щати ще разчита на механизмите за координиране и надзор по въпросите на националната сигурност между министерствата и агенциите, за да съдейства да се гарантира, че омбудсманът към Щита за личните данни ще може да отговаря по смисъла на раздел 4, буква д) на искания, изготвени съгласно раздел 3, буква б).

в) Омбудсманът към Щита за личните данни може да отнася въпроси, свързани с исканията, за разглеждане от Надзорния съвет по въпросите на неприкосновеността на личния живот и гражданските свободи.

3. **Подаване на исканията.**

а) Първоначално искането ще се подава до компетентните органи на държавите членки в областта на надзора на дейностите в националната сигурност и/или обработването на лични данни от публични органи. Искането се подава до Омбудсмана от централизиран орган на ЕС (наричан по-долу „централизираният орган на ЕС за разглеждане на индивидуални жалби“).

б) Органът на ЕС за разглеждане на жалби на физическите лица ще осигурява искането да бъде пълно, като се съобразява със следните действия:

i) проверка за самоличността на физическото лице и дали то действа от собствено име, а не като представител на правителствена или международна организация;

ii) осигуряване искането да бъде оформено писмено и да съдържа следната основна информация:

— информацията, която съставлява основанието за искането,

— естеството на исканата информация или исканото решение,

— правителствените институции на Съединените щати, за които се смята, че се отнася искането, ако има такива, и

— други мерки, които са били приложени, за да бъде получена исканата информация или исканото решение и получения резултат чрез тях;

iii) проверка дали искането се отнася за данни, за които има основания да се счита, че са предадени от ЕС на Съединените щати съгласно Щита за личните данни, стандартни договорни клаузи, задължителни фирмени правила, дерогации или възможни бъдещи дерогации;

iv) първоначално определяне дали искането не е несериозно, злонамерено или недобросъвестно.

в) За да бъде пълно за целите на по-нататъшното му разглеждане от Омбудсмана към Щита за личните данни съгласно настоящия меморандум, не е необходимо искането да доказва, че действително е осъществен достъп до данните на подаващия го при дейности на радиоелектронното разузнаване, провеждани от правителството на Съединените щати.

4. **Ангажименти за поддържане на връзка с подаващия орган на ЕС за разглеждане на жалби на физическите лица.**

а) Омбудсманът към Щита за личните данни ще изпраща потвърждение за получаването на искането до изпращащия го орган на ЕС за разглеждане на жалби на физическите лица.

б) Омбудсманът към Щита за личните данни ще извършва първоначална проверка, за да удостовери дали искането е изготвено съобразно с изискванията в раздел 3, буква б). Ако Омбудсманът към Щита за личните данни забележи непълноти или има въпроси относно изготвянето на искането, той ще се стреми да обсъди и намери решение на тези въпроси съвместно с подаващия орган на ЕС за разглеждане на жалби на физическите лица.

в) Ако за улесняване на правилното разглеждане на искането Омбудсманът към Щита за личните данни се нуждае от допълнителна информация за него или се налага физическото лице, което първоначално е подало искането, да предприеме определени действия, Омбудсманът към Щита за личните данни ще информира за това подаващия орган на ЕС за разглеждане на жалби на физическите лица.

г) Омбудсманът към Щита за личните данни ще следи етапите на разглеждане на исканията и ще предоставя съответна актуална информация на подаващия орган на ЕС за разглеждане на жалби на физическите лица.

д) След като искането бъде изготвено, както това е описано в раздел 3 от настоящия меморандум, Омбудсманът към Щита за личните данни ще изпрати своевременно съответен отговор на подаващия орган на ЕС за разглеждане на жалби на физическите лица, като при това прилага постоянното си задължение да осигурява защита на информацията съгласно приложимото право и политиките. Омбудсманът към Щита за личните данни ще предостави отговор на подаващия орган на ЕС за разглеждане на жалби на физическите лица в потвърждение на това, че: i) оплакването е надлежно разгледано и ii) са спазени правото на САЩ, законите, декретите, президентските укази и политиките на институциите, които предвиждат ограничения и гаранции, както това е разгледано в писмото на Службата на директора на Националното разузнаване, или ако не са спазени, че това неспазване е било отстранено. Омбудсманът към Щита за личните данни нито потвърждава, нито отрича, че се извършва целево наблюдение на физическото лице, както и не потвърждава конкретната корективна мярка, която е приложена. Както е пояснено допълнително в точка 5, исканията съгласно Закона за свобода на информацията ще бъдат разглеждани както това е предвидено в закона и приложимите подзаконови актове.

е) Омбудсманът към Щита за личните данни ще бъде в пряка връзка с органа на ЕС за разглеждане на жалби на физическите лица, който от своя страна ще има задължението да осъществява връзката с физическото лице, което подава искането. Ако пряката връзка е част от един от основните процеси, описани по-нататък, тази връзка ще се осъществява съгласно съществуващите процедури.

ж) Ангажиментите в настоящия меморандум не се прилагат за жалби от общ характер относно несъответствие на Щита за личните данни в отношенията между ЕС и САЩ с изискванията на Европейския съюз в областта на защитата на данните. Ангажиментите в настоящия меморандум са поети въз основа на общото разбиране на Европейската комисия и правителството на САЩ, че предвид обхвата на ангажиментите съгласно настоящия механизъм е възможно да възникнат ресурсни ограничения, включително по отношение на исканията съгласно Закона за свобода на информацията (ЗСИ). В случай че изпълнението на функциите на Омбудсмана към Щита за личните данни надхвърли допустимите ресурсни ограничения и пречи на изпълнението на тези ангажименти, правителството на САЩ ще обсъди с Европейската комисия евентуални промени, които може да са необходими за справяне с положението.

5. **Искания за информация.** Искания за достъп до регистрите на правителството на Съединените щати могат да се подават и разглеждат съгласно Закона за свобода на информацията (*Freedom of Information Act* (FOIA)).

а. В него са предвидени възможности за което и да било лице да поиска достъп до съществуващите регистри на федерални институции, независимо от неговото гражданство. Този закон е кодифициран в Кодекса на Съединените щати, 5 U.S.C. § 552. Законът, както и допълнителна информация за него са на разположение на адрес www.FOIA.gov и http://www.justice.gov/oip/foia-resources. Всяка институция има главен служител по FOIA и предоставя информация на своя публичен уебсайт как може да бъде подадено искане съгласно FOIA до институцията. Институциите имат процедура за консултации помежду си относно исканията съгласно FOIA, които се отнасят до регистри на друга институция.

б) Пример:

i) Службата на директора на Националното разузнаване (*Office of the Director of National Intelligence* (ODNI)) е създала специален портал за FOIA и искания към ODNI: http://www.dni.gov/index.php/about-this-site/foia. На портала е посочена информация как може да се подаде искане, да се провери етапът на разглеждане на подадено искане и се предоставя достъп до издадена и публикувана от ODNI информация съгласно FOIA. Освен това порталът за FOIA на ODNI предоставя електронна връзка към уебсайтовете за искания съгласно FOIA на други разузнавателни структури: http://www.dni.gov/index.php/about-this-site/foia/other-ic-foia-sites.

ii) Службата по информационна политика на Министерството на правосъдието предоставя обстойна информация относно FOIA: http://www.justice.gov/oip. Това се отнася не само за информация относно подаването на искания съгласно FOIA до Министерството на правосъдието, но са дадени също и насоки към правителството на Съединените щати относно тълкуването и прилагането на изискванията, предвидени в FOIA.

в) Съгласно FOIA, за достъпа до правителствените регистри се прилагат някои изключения, изброени в закона. Към тях спадат ограниченията за достъпа до класифицирана информация във връзка с националната сигурност, до лична информация на трети страни и информация относно разследвания на правоприлагащите органи, като тези ограничения са сходни на налаганите от всяка от държавите — членки на ЕС, съгласно националното им право в областта на достъпа до информация. Те се прилагат еднакво за американски граждани и за лица, които не са граждани на САЩ.

г) Споровете във връзка с предоставяне на регистри по искане съгласно FOIA могат да се обжалват по административен ред, след което и пред федерален съд. От съда се изисква да се произнесе отново с решение дали регистрите правомерно не са били предоставени, 5 U.S.C. § 552(a)(4)(B), и той може да задължи правителството да предостави достъп до регистрите. В някои случаи съдът е отхвърлил доводите на правителството, че информацията не трябва да се предоставя, тъй като е класифицирана. Въпреки че не се предоставят обезщетения за финансови вреди, съдът може да разпореди да бъдат изплатени разноските за адвокатски хонорари.

6. **Искания за последващи действия.** Исканията във връзка с предполагаемо нарушение на законодателството или друго неправомерно действие ще бъдат насочвани към съответните органи на правителството на Съединените щати, включително независими надзорни органи, които имат правомощия да провеждат разследвания по съответното искане и да отстранят неспазването, както това е разгледано по-нататък.

а) Главните инспектори са с независим статут, имат широки правомощия да провеждат разследвания, одити и проверки на програмите, включително за измами и злоупотреби или нарушаване на закона, и могат да правят препоръки за корективни мерки.

i) Със Закона за главния инспектор от 1978 г. (*Inspector General Act*) и последващите изменения беше създадена със закон длъжността на федералния главен инспектор като независимо и обективно звено в рамките на повечето агенции, чиито задължения са борбата с разхищението, измамите и злоупотребите по програмите и в работата на съответните агенции. За тази цел всеки главен инспектор отговаря за провеждането на одити и разследвания във връзка с програмите и работата на съответната агенция. Освен това главните инспектори ръководят, координират и дават препоръки за политики във връзка с дейности, насочени към повишаване на икономиите, ефективността и ефикасността, както и превенция и разкриване на измами и злоупотреби по програмите и в работата на съответните агенции.

ii) Всяка от разузнавателните структури има своя служба на главния инспектор, в чиито отговорности се включва наред с останалите въпроси и упражняването на надзор върху дейностите за външно разузнаване. До редица доклади на главни инспектори във връзка с разузнавателни програми беше предоставен публичен достъп.

iii) Пример:

— Службата на главния инспектор на Разузнавателната общност (*Office of the Inspector General of the Intelligence Community* (IC IG)) беше създадена по силата на раздел 405 от Закона за разрешаване на разузнавателни дейности за финансовата година 2010 (*Intelligence Authorization Act of Fiscal Year 2010* — http://www.gpo.gov/fdsys/pkg/PLAW-111publ259/pdf/PLAW-111publ259.pdf). IC IG отговаря за провеждането във всички разузнавателни структури на одити, разследвания, инспектиране и проверки за идентифициране и отстраняване на системни рискове, слаби места и недостатъци, които засягат мисиите на разузнавателните агенции, за да има положителен ефект върху икономиите и ефективността на всички разузнавателни структури. IC IG има правомощия да провежда разследвания по жалби или информация във връзка с предполагаеми нарушения на закони, правила, подзаконови актове или по обвинения за разхищение, измами, злоупотреби с власт или за значими или специфични рискове за общественото здраве и обществената безопасност във връзка с разузнавателни програми и дейности на ODNI и/или разузнавателните структури. IC IG предоставя информация как да се осъществи пряка връзка с него за подаването на сигнал: http://www.dni.gov/index.php/about-this-site/contact-the-ig.

— Службата на главния инспектор (*Office of the Inspector General* (OIG — https://www.oig.justice.gov)) на Министерството на правосъдието на САЩ е създадена със закон независима структура, чиято мисия е откриването и възпирането на разхищения, измами, злоупотреби и неправомерни действия в програмите и сред служителите на Министерството на правосъдието, както и повишаването на икономиите и ефективността по тези програми. OIG провежда разследвания по предполагаеми нарушения на наказателното и гражданското право от страна на служители на министерството и също така извършва одити и проверки по неговите програми. OIG има компетентност по всички жалби срещу неправомерни действия на служители на Министерството на правосъдието, включително на Федералното бюро за разследвания, Администрацията за борба с наркотиците, Федералното бюро за местата за лишаване от свобода, Маршалската служба на САЩ, Бюрото по въпросите на алкохола, тютюна, огнестрелните оръжия и експлозивите, Адвокатските колегии в Съединените щати, както и на служителите, които работят в други подразделения или служби на Министерството на правосъдието. (Единствено изключение са обвиненията в неправомерни действия срещу юристи или правоприлагащи служители на министерството, когато обвиненията са свързани с упражняването на правомощията на юриста на министерството по разследване, водене на дела или предоставяне на юридическа консултация, по които отговорност за разглеждането носи Службата за професионална

отговорност към министерството). Освен това в раздел 1001 от Закона за обединяване и укрепване на САЩ (*USA Patriot Act*), промулгиран на 26 октомври 2001 г., се дават указания на главния инспектор да разглежда информация и приема жалби срещу злоупотреби с граждански права и граждански свободи от страна на служители на Министерството на правосъдието. OIG поддържа публичен уебсайт — https://www.oig.justice.gov — на който има и „гореща линия“ за подаване на жалби — https://www.oig.justice.gov/hotline/index.htm.

б) Службите и структурите по въпросите на неприкосновеността на личния живот и гражданските свободи в правителството на Съединените щати също имат релевантни отговорности. Пример:

i) С раздел 803 от Закона за изпълнение на препоръките на комисията по атентатите от 11 септември от 2007 г. (*Implementing Recommendations of the 9/11 Commission Act*), кодифициран в Кодекса на Съединените щати, 42 U.S.C. § 2000-ee1, се въвеждат служители по въпросите на неприкосновеността на личния живот и гражданските свободи в някои министерства и агенции (включително Държавния департамент, Министерството на правосъдието и ODNI). В раздел 803 се определя, че тези служители по въпросите на неприкосновеността на личния живот и гражданските свободи ще имат функцията на главен съветник, който наред с останалото осигурява в съответното министерство, агенция или структура наличието на адекватни процедури за разглеждане на жалби на физически лица по обвинения за нарушаване на неприкосновеността на личния им живот или гражданските им свободи от страна на това министерство, агенция или структура.

ii) Службата за гражданските свободи и неприкосновеността на личния живот към ODNI (*Civil Liberties and Privacy Office* (ODNI CLPO) се ръководи от служителя на ODNI по въпросите на защитата на гражданските свободи — длъжност, създадена със Закона за националната сигурност от 1948 г. (*National Security Act*), с последващите му изменения. Сред задълженията на ODNI CLPO е да осигури наличието на адекватна защита на неприкосновеността на личния живот и гражданските свободи в политиките и процедурите на разузнавателните структури, както и да разглежда и разследва жалби по обвинения за злоупотреби или нарушаване на гражданските свободи и неприкосновеността на личния живот в програми и дейности на ODNI. На своя уебсайт ODNI CLPO предоставя информация на обществеността, включително указания как може да бъде подадена жалба: www.dni.gov/clpo. Когато в ODNI CLPO се получи жалба във връзка с неприкосновеността на личния живот или гражданските свободи по отношение на програми и дейности на разузнавателните структури, службата работи координирано с други разузнавателни структури за по-нататъшното разглеждане на жалбата в рамките на тези структури. Трябва да се има предвид, че Агенцията за национална сигурност (*National Security Agency* (NSA)) също разполага със служба за гражданските свободи и неприкосновеността на личния живот, която предоставя информация относно своите отговорности на уебсайта си — https://www.nsa.gov/civil_liberties/. Ако има информация, че дадена агенция не спазва изискванията в областта на неприкосновеността на личния живот (напр. такова изискване е предвидено в раздел 4 от ПИД-28), тогава агенциите разполагат с механизми за гарантиране на спазването, с които да направят проверка и да отстранят нарушението. Съгласно ПИД-28 от агенциите се изисква да докладват пред ODNI за случаите на неспазване.

iii) Службата за неприкосновеността на личния живот и гражданските свободи (*Office of Privacy and Civil Liberties* (OPCL)) към Министерството на правосъдието подпомага изпълнението на задълженията и отговорностите на главния служител по въпросите на неприкосновеността на личния живот и гражданските свободи (*Chief Privacy and Civil Liberties Officer* (CPCLO)) на министерството. Основната мисия на OPCL е защитата на неприкосновеността на личния живот и гражданските свободи на американците чрез проверки, надзор и координация на работата на министерството по отношение на неприкосновеността на личния живот. OPCL предоставя правни консултации и насоки за структурите на министерството; осигурява спазването от страна на министерството на изискванията в областта на неприкосновеността на личния живот, включително съгласно Закона за неприкосновеността на личния живот от 1974 г. (*Privacy Act*), разпоредбите в областта на неприкосновеността на личния живот от Закона за електронното правителство от 2002 г. (*E-Government Act*) и от Закона за федералното управление на информационната сигурност (*Federal Information Security Management Act*), както и директивите за административната политика, издадени в изпълнение на тези закони; разработва и провежда обучение в областта на неприкосновеността на личния живот за работещите в министерството; подпомага CPCLO за разработването на политиката на министерството в областта на неприкосновеността на личния живот; изготвя доклади във връзка с неприкосновеността на личния живот до президента и Конгреса; и прави преглед на практиките за обработване на информация в министерството, за да гарантира, че те са съобразени с изискванията за защита на неприкосновеността на личния живот и гражданските свободи. OPCL предоставя информация на обществеността относно своите отговорности на адрес http://www.justice.gov/opcl.

iv) Съгласно 42 U.S.C. § 2000ee *et seq*. Надзорният съвет по въпросите на неприкосновеността на личния живот и гражданските свободи (*Privacy and Civil Liberties Oversight Board*) извършва постоянен преглед на i) политиките и процедурите на министерствата, агенциите и подразделенията на изпълнителната власт във връзка с усилията да бъде защитена нацията от тероризма, както и на тяхното прилагане, за да гарантира, че са защитени неприкосновеността на личния живот и гражданските свободи, и ii) други действия на изпълнителната власт във връзка с тези усилия, за да определи дали тези действия осигуряват адекватна защита на неприкосновеността на личния живот и гражданските свободи и дали те са съобразени с уреждащите ги закони, подзаконови актове и политиките в областта на неприкосновеността на личния живот и гражданските свободи. Този съвет приема и разглежда доклади и друга информация от служителите по въпросите на неприкосновеността на личния живот и служителите по въпросите на гражданските свободи и когато е уместно им дава препоръки за тяхната дейност. В раздел 803 от Закона за изпълнение на препоръките на комисията по атентатите от 11 септември от

2007 г., кодифициран в Кодекса на Съединените щати, 42 U.S.C. § 2000-ee1, е указано служителите по въпросите на неприкосновеността на личния живот и гражданските свободи в осем федерални агенции (включително Министърът на отбраната, Министърът на вътрешната сигурност, директорът на националното разузнаване и директорът на Централното разузнавателно управление), както и евентуално други агенции, определени от Съвета, да представят периодични доклади пред Надзорния съвет по въпросите на неприкосновеността на личния живот и гражданските свободи, в които да бъде включена информация за броя, характера и разпореждането по жалбите, получени в съответната агенция по обвинения за нарушения. В закона за правомощията на Надзорния съвет по въпросите на неприкосновеността на личния живот и гражданските свободи са дадени указания той да приема тези доклади и когато е необходимо, да дава препоръки на служителите по въпросите на неприкосновеността на личния живот и гражданските свободи във връзка с тяхната дейност.

ПРИЛОЖЕНИЕ IV

Писмо от Председателя на Федералната търговска комисия, г-жа Edith Ramirez

7 юли 2016 г.

По елекронна поща

Вера Йоурова
Комисар по въпросите на правосъдието, потребителите и равнопоставеността между половете
Европейска комисия
Rue de la Loi/Wetstraat 200
1049 Брюксел
Белгия

Уважаема комисар Йоурова,

Федералната търговска комисия на Съединените американски щати (ФТК) (*United States Federal Trade Commission*) благодари за възможността да даде описание на своите действия по прилагане на новата Рамка на Щита за личните данни в отношенията между ЕС и САЩ („Рамка на Щита за личните данни“ или „Рамката“). Считаме, че Рамката ще има решаваща роля за улесняване осигуряването на защита за неприкосновеността на личния живот при търговските сделки в един все по-взаимообвързан свят. Тя ще позволи на дружествата да осъществяват важни операции в глобалната икономика, като същевременно ще гарантира, че потребителите от ЕС ще продължат да се ползват от съществена защита на неприкосновеността на личния живот. ФТК е поела траен ангажимент за защитата на неприкосновеността на личния живот през граници и ще отдаде приоритетно място на прилагането на новата рамка. По-долу описваме опита на ФТК за решително прилагане на договореностите в областта на неприкосновеността на личния живот като цяло, включително на първоначалната програма за сфера на неприкосновеност на личния живот, както и подхода на ФТК за прилагането на новата рамка.

За първи път ФТК пое публично ангажимент да прилага програмата за сфера на неприкосновеност на личния живот през 2000 г. Тогавашният председател на ФТК Robert Pitofsky изпрати на Европейската комисия писмо, в което беше очертан ангажиментът на ФТК да прилага активно принципите от схемата за сфера на неприкосновеност на личния живот. ФТК продължи да спазва този ангажимент чрез предприемането на близо 40 действия за правоприлагане и множество допълнителни разследвания и чрез сътрудничеството си с отделните органи по защита на данните от ЕС (ОЗД от ЕС) по въпроси от взаимен интерес.

След като през ноември 2013 г. Европейската комисия изрази загриженост относно управлението и прилагането на програмата за сфера на неприкосновеност на личния живот, заедно с Министерството на търговията на САЩ започнахме консултации със служители на Европейската комисия, за да проучим възможностите за укрепване на програмата. Докато тези консултации бяха в ход, на 6 октомври 2015 г. Съдът на Европейския съюз се произнесе с решение по делото *Schrems*, в което наред с останалото беше обявено за невалидно решението на Европейската комисия относно адекватността на програмата за сфера на неприкосновеност на личния живот. След това решение продължихме да работим в тясно взаимодействие с Министерството на търговията и Европейската комисия в стремеж да подсилим защитата за неприкосновеността на личния живот, която се осигурява за физическите лица от ЕС. Рамката на Щита за личните данни е резултат от тези текущи консултации. Както и по отношение на програмата за сфера на неприкосновеност на личния живот, с настоящето ФТК се ангажира да прилага активно новата рамка. Настоящото писмо ознаменува този ангажимент.

По-специално потвърждаваме своя ангажимент в четири основни направления: 1) отдаване на приоритет на сезирания и разследване; 2) предприемане на действия по неправомерни или измамни твърдения за участие в Щита за личните данни; 3) непрекъснат контрол по заповедите; и 4) засилена съвместна работа и сътрудничество по правоприлагане с ОЗД от ЕС. По-нататък представяме подробна информация за всеки от тези ангажименти и съответния минал опит на ФТК, както и ролята ѝ за защита на неприкосновеността на личния живот на потребителите и при прилагането на програмата за сфера на неприкосновеност на личния живот, а така също и по-общия контекст във връзка с неприкосновеността на личния живот в Съединените щати. ([1])

I. КОНТЕКСТ

A. **Работата на ФТК за изпълнение на изискванията за неприкосновеност на личния живот и съответната политика**

ФТК разполага с широки правомощия за правоприлагане с гражданскоправни средства за повишаване на защитата на потребителите и насърчаване на конкуренцията в сферата на търговията. Като част от мандата ѝ в областта на защитата на потребителите ФТК осигурява прилагането на широка гама от закони за защита на неприкосновеността на личния живот

([1]) В приложение А сме предоставили допълнителна информация относно федералните и щатските закони в областта на неприкосновеността на личния живот в САЩ. Освен това на уебсайта на ФТК е представено обобщение на неотдавнашните ни действия по прилагане на изискванията за неприкосновеност на личния живот и сигурността: https://www.ftc.gov/reports/privacy-data-security-update-2015.

и сигурността на данните на потребителите. Основният закон, който ФТК прилага — Законът за ФТК — забранява „нелоялни“ и „измамни“ действия или практики в търговията или засягащи търговията ([1]). Под „измамни“ действия или практики се разбира представяне, пропуск или практика, които са съществени и са в състояние да заблудят потребители, които действат по разумен начин в дадените обстоятелства ([2]). Под „нелоялни“ действия или практики се разбират действия или практики, които нанасят или са в състояние да нанесат на потребителите сериозни вреди, които при нормални обстоятелства не могат да бъдат избегнати или които не са компенсирани с предимства за потребителите или конкуренцията ([3]). Също така ФТК прилага специални закони за защита на информация относно здравословното състояние, заеми и други финансови въпроси, както и онлайн информация за деца, и издава разпоредби за прилагането на всеки един от тези закони.

Съгласно Закона за ФТК правомощията на ФТК обхващат въпроси „в търговията или засягащи търговията“. ФТК не е компетентна по отношение на прилагането на наказателното право или по въпроси на националната сигурност и няма правомощия по повечето от останалите действия на правителството. Освен това има изключения от компетентността на ФТК за търговските дейности, включително по отношение на банките, въздушните превозвачи, застрахователната дейност и дейностите на доставчиците на далекосъобщителни услуги в качеството им на общи преносители. Също така ФТК не е компетентна по отношение на повечето нестопански организации, но е компетентна за привидните благотворителни организации и за нестопански организации, които реално работят за печалба. Компетентността на ФТК обхваща и нестопански организации, които работят за печалба в полза на свои стопански членове, включително като им осигуряват значителни икономически ползи. ([4]) В някои случаи компетентността на ФТК съвпада с тази на други правоприлагащи агенции.

Изградили сме здрави работни взаимоотношения с федералните и щатските органи и работим в тясно взаимодействие с тях за координиране на разследванията или за сезиране, когато е необходимо.

Правоприлагането е ключов елемент на подхода на ФТК към защитата на неприкосновеността на личния живот. Към днешна дата ФТК е образувала над 500 дела за защита на неприкосновеността на личния живот и сигурността на информацията за потребителите. В този обем от дела се обхваща онлайн и офлайн информация и се включват действия по правоприлагане срещу малки и големи дружества по обвинения, че не са обработвали по подходящ начин чувствителни данни на потребители, не са осигурили защита на лична информация на потребители, проследявали са по измамен начин потребители онлайн, изпращали са нежелани съобщения, инсталирали са шпионски или друг злонамерен софтуер на компютрите на потребители, нарушили са правила на телемаркетинга като например правилото за необаждане („Do Not Call“) и други, и неправомерно са събирали и споделяли информация за потребители от мобилни устройства. Действията на ФТК по принудително изпълнение — както във физическия, така и в цифровия свят — са важно послание към дружествата относно необходимостта да бъде защитена неприкосновеността на личния живот на потребителите.

Също така ФТК предприе множество политически инициативи, насочени към повишаване на защитата на неприкосновеността на личния живот на потребителите, които формират работата ѝ по правоприлагане. ФТК беше домакин на работни срещи и изготви доклади с препоръки за добри практики, насочени към подобряване на защитата на неприкосновеността на личния живот в екосистемата на мобилните услуги; за повишаване на прозрачността в сектора на търговията с данни; за максимално увеличаване на ползите от големите данни при същевременно смекчаване на рисковете, които те носят, особено за потребители с ниски доходи и в райони с недостатъчно обслужване; и за изтъкване на значението на неприкосновеността на личния живот и последиците за сигурността при лицевото разпознаване и „интернет на нещата“, наред с другите области.

Също така ФТК се включва в обучения за потребителите и дружествата, за да увеличи ефекта от своята работа по правоприлагане и инициативите си за разработване на политики. ФТК използва различни средства — публикации, онлайн ресурси, работни срещи и социалните медии, за да осигурява учебни материали по широк диапазон от теми, включително мобилните приложения, неприкосновеността на личния живот на децата и сигурността на данните. Съвсем наскоро комисията стартира своята инициатива „Започни от сигурността“, с която се дават нови насоки на дружествата въз основа на опита от работата на агенцията по дела във връзка със сигурността на данните, както и поредица от работни срещи из цялата страна. Освен това ФТК е с дългогодишна водеща роля в огрмотяването на потребителите в областта на основите на компютърната сигурност. Миналата година нашият уебсайт OnGuardOnline и неговият испански езиков вариант Alerta en Línea имаха над 5 милиона посетители.

Б. **Правни инструменти за защита в САЩ, от които могат да се ползват потребителите от ЕС**

Рамката ще функционира в общия контекст на инструменти в САЩ в областта на неприкосновеността на личния живот, които осигуряват защита за потребителите от ЕС по редица начини.

([1]) 15 U.S.C. § 45(a).

([2]) Вж. Политическа декларация на ФТК относно измамите, допълнение към Cliffdale Assocs., Inc., 103 F.T.C. 110, 174 (1984), на адрес: https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception.

([3]) Вж. 15 U.S.C § 45(n); Политическа декларация на ФТК относно нелоялността, допълнение към Int'l Harvester Co., 104 F.T.C. 949, 1070 (1984), на адрес: https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.

([4]) Вж. *California Dental Ass'n c/y ФТК*, 526 U.S. 756 (1999).

Забраната за нелоялни и измамни действия или практики в Закона за ФТК не се ограничава до защитата на потребителите в САЩ срещу дружества от САЩ, тъй като се отнася за практики, които 1) нанасят или са в състояние да нанесат разумно предвидими вреди в Съединените щати, или 2) се отнасят за действия по същество, извършвани в Съединените щати. Освен това, когато защитава чуждестранни потребители ФТК може да използва всички средства за правна защита, включително възстановяване, с които разполага за защита на националните потребители.

Действително работата на ФТК по правоприлагане е от съществена полза за потребителите, както в САЩ, така и за тези от чужди държави. Например в нашите дела във връзка с прилагането на раздел 5 от Закона за ФТК бе защитена по еднакъв начин неприкосновеността на личния живот за потребителите в САЩ и за тези от чужди държави. В дело срещу търговец на информация, Accusearch, ФТК поддържаше становището, че продажбата от страна на дружеството на конфиденциални записи на телефонни разговори на трети страни без знанието или съгласието на потребителите е нелоялна практика в нарушение на раздел 5 от Закона за ФТК. Accusearch бяха продали информация във връзка с потребители от САЩ и от други държави ([1]). Съдът издаде разпореждане за прекратяване срещу Accusearch, с което наред с другото се забранява предлагането на пазара или продажбата на лична информация на потребители без писменото им съгласие, освен когато тя е законосъобразно придобита от публично достъпна информация, и определи обезщетение в размер на близо 200 000 щатски долара ([2]).

Друг пример е споразумението на ФТК с TRUSTe. В него се гарантира, че потребителите, включително тези от Европейския съюз, могат да имат доверие на представянията, които една световна саморегулираща се организация прави на своите проверки и сертификации на вътрешни и чуждестранни онлайн услуги ([3]). Освен това нашите действия срещу TRUSTe укрепват системата на саморегулиране в областта на неприкосновеността на личния живот в по-общ план, като осигуряват отчетността на субектите, които имат важна роля в схемите за саморегулиране, включително трансграничните рамки в областта на неприкосновеността на личния живот.

ФТК прилага и други специални закони, в които защитата се прилага и за потребители извън САЩ, като например Закона за защита на неприкосновеността на личния живот на децата онлайн. Наред с останалото в този закон се поставя изискване към операторите на уебсайтове и онлайн услуги, предназначени за деца, или общодостъпни сайтове, които съзнателно събират лична информация от деца на възраст под 13 години, да уведомяват за това родителите и да изискват родителско съгласие, което може да се провери. Уебсайтовете и услугите, базирани в САЩ, за които се прилага Законът за защита на неприкосновеността на личния живот на децата онлайн и които събират лична информация от деца извън САЩ, са задължени да спазват този закон. Чуждестранните уебсайтове и онлайн услуги също са задължени да спазват този закон, ако дейностите им са насочени към деца в Съединените щати или съзнателно събират лична информация от деца в Съединените щати. Освен федералните закони, които прилага ФТК, допълнителни ползи за потребителите от ЕС могат да предоставят и някои други федерални и щатски закони в областта на защитата на неприкосновеността на личния живот.

B. **Прилагане на схемата за сфера на неприкосновеност на личния живот**

Като част от своята програма по правоприлагане в областта на неприкосновеността на личния живот и сигурността, ФТК прие стъпки за защита на потребителите от ЕС и чрез предприемането на действия по правоприлагане във връзка с нарушения на схемата за сфера на неприкосновеност на личния живот. ФТК предприе 39 действия по принудително изпълнение във връзка с тази схема: 36 по обвинение за неправомерни твърдения за сертифициране и три дела — срещу Google, Facebook, и Myspace — по обвинения за нарушаване на принципите на сферата на неприкосновеност на личния живот ([4]). Тези случаи доказват изпълняемостта на сертифицирането и последиците от неспазването на принципите. Заповедите за съгласие с валидност 20 години задължават Google, Facebook и Myspace да прилагат всеобхватни програми за защита на неприкосновеността на личния живот, които да са подходящо проектирани, така че да се премахнат рисковете за неприкосновеността на личния живот при разработването и управлението на нови и съществуващи продукти и услуги и да се защити неприкосновеността на личния живот и поверителността на личната информация. Чрез всеобхватните програми в областта на неприкосновеността на личния живот, които се налагат като задължение съгласно тези заповеди, трябва да се идентифицират предвидими материални рискове и да се предвидят средства за контрол за отстраняването на тези рискове. Също така дружествата трябва да приемат текущи независими оценки на своите програми в областта на неприкосновеността на личния живот, които трябва да бъдат предоставяни на ФТК. Със заповедите се забранява на тези дружества също и да представят подвеждащо практиките си в областта на неприкосновеността на личния живот и евентуалното си участие в програма за неприкосновеността на личния живот или за сигурността. Тази забрана ще се прилага също и за действия и практики на дружествата съгласно новата рамка на Щита за личните данни. ФТК може да предприема принудително изпълнение по тези заповеди, като налага гражданскоправни санкции. През

([1]) *Вж.* Служба на комисаря на Канада по неприкосновеността на личния живот, жалба съгласно PIPEDA срещу Accusearch, Inc., осъществяващо дейност под името Abika.com, https://www.priv.gc.ca/cf-dc/2009/2009_009_0731_e.asp. Службата на комисаря на Канада по неприкосновеността на личния живот подаде кратко изложение в качеството на *amicus curiae* при обжалването на действието на ФТК и проведе собствено разследване, като констатира, че практиките на Accusearch са в нарушение и на правото на Канада.

([2]) Вж. *ФТК с/у Accusearch, Inc.*, № 06CV015D (D. Wyo. Dec. 20, 2007), *aff'd* 570 F.3d 1187 (10th Cir. 2009).

([3]) Вж. *Относно True Ultimate Standards Everywhere, Inc.*, No. C-4512 (F.T.C. Mar. 12, 2015) (решение и заповед), *на адрес* https://www ftc.gov/system/files/documents/cases/150318trust-edo.pdf.

([4]) Вж. *Относно Google, Inc.,* No. C-4336 (F.T.C. Oct. 13 2011) (решение и заповед), *на адрес*: https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz; *Относно Facebook, Inc.*, No. C-4365 (F.T.C. July 27, 2012) (решение и заповед), *на адрес* https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook; *Относно Myspace LLC*, No. C-4369 (F.T.C. Aug. 30, 2012) (решение и заповед), *на адрес*: https://www.ftc.gov/news-events/press-releases/2012/09/ftc-finalizes-privacy-settlement-myspace.

2012 г. Google платиха гражданска санкция в рекордния размер от 22,5 милиона щатски долара по обвинения за нарушаване на адресирана към дружеството заповед. По този начин тези заповеди на ФТК спомагат за защитата на над един милиард потребители по целия свят, стотици милиони от които живеят в Европа.

Делата на ФТК са насочени също и към неправомерни, измамни или подвеждащи твърдения за участие в рамката за сфера на неприкосновеност на личния живот. ФТК се отнася сериозно към тези твърдения. Например по делото ФТК с/у Karnani през 2011 г. ФТК предприе действия срещу лице, извършващо търговия по интернет в Съединените щати, по обвинения, че то и дружеството му са подвели британски потребители, като са ги накарали да смятат, че дружеството е базирано в Обединеното кралство, включително като са използвали разширение.uk на уебсайта и са посочвали цени в британски лири и пощенски услуги на Обединеното кралство ([1]). Когато потребителите получили продуктите обаче, те установили неочаквано за тях, че са наложени вносни мита, че гаранциите не са валидни за Обединеното кралство и че трябва да заплатят такса, за да им бъде възстановена платената сума. ФТК също отсъди, че ответниците са измамили потребителите във връзка с участието си в програмата за сфера на неприкосновеност на личния живот. Всички потребители, станали жертва на измамата, са били от Обединеното кралство.

Много от другите ни случаи на принудително изпълнение на рамката за сфера на неприкосновеност на личния живот бяха свързани с организации, които след първоначалното си присъединяване към тази програма не бяха подновили ежегодното си сертифициране, а продължаваха да се представят като настоящи участници. Както е разгледано по-нататък, ФТК се ангажира също така и с дейности срещу неправомерни твърдения за участие в Рамката на Щита за личните данни. Тази стратегическа дейност по правоприлагане ще допълва засилените мерки от страна на Министерството на търговията за проверка на спазването на изискванията на програмата за сертифициране и пресертифициране, неговия контрол върху ефективното спазване, включително с използване на въпросници към участниците в Рамката, както и увеличените усилия за идентифициране на неправомерни твърдения за членство и неправомерно използване на сертификационния знак за Рамката ([2]).

II. ОТДАВАНЕ НА ПРИОРИТЕТ НА СЕЗИРАНИЯ И РАЗСЛЕДВАНЕ

Както и по програмата за сфера на неприкосновеност на личния живот, ФТК се ангажира да разглежда с предимство случаите, по които е сезирана от държавите — членки на ЕС, съгласно Щита за личните данни. ФТК ще отдава предимство и на сезирания за неспазване на саморегулаторните насоки във връзка с Рамката на Щита за личните данни, изпратени от саморегулиращи се организации в областта на неприкосновеността на личния живот и други независими органи за решаване на спорове.

За улесняване на сезиранията съгласно Рамката от държавите — членки на ЕС, ФТК създава стандартизиран процес за сезиране и дава насоки на тези държави относно вида на информацията, която би подпомогнала най-много ФТК при събирането на доказателства по случая. Като част от тези усилия ФТК ще определи лице за връзка с институцията относно сезирания от държавите — членки на ЕС. Особено полезно е, когато сезиращият орган е събрал доказателства по твърдението за нарушение и може да сътрудничи на ФТК при разследването.

След като бъде сезирана от държава — членка на ЕС, или от саморегулираща се организация, ФТК може да предприеме редица действия за разглеждане на поставените проблеми. Например можем да направим преглед на политиките на дружеството в областта на неприкосновеността на личния живот, да получим допълнителна информация директно от дружеството или от трети страни, да осъществим последващ контрол съвместно със сезиращия субект, да направим оценка дали има модел на извършване на нарушенията или са засегнати значителен брой потребители, да определим дали сезирането засяга въпроси, които са от компетентността на Министерството на търговията, да направим преценка дали ще е от полза да се проведе обучение на потребителите и на дружествата, и ако е необходимо, да инициираме производство по принудително изпълнение.

Също така ФТК се ангажира с обмен на информация по случаите, за които е била сезирана, със сезиращите правоприлагащи органи, включително относно етапа на разглеждане на случаите, при спазване на законите и ограниченията относно поверителността. Доколкото позволяват условията и предвид броя и вида на случаите на сезиране, предоставената информация ще включва оценка на въпросите, повдигнати в сезирането, включително описание на значимите проблеми, които са повдигнати, и на евентуално предприетите действия за отстраняване на нарушенията на законите в рамките на компетентността на ФТК. Освен това ФТК ще предоставя информация на сезиращия орган относно вида на получените сезирания, за да бъде повишена ефективността на усилията за справяне с неправомерните действия. Когато сезиращ

([1]) Вж. *ФТК с/у Karnani*, № 2:09-cv-05276 (C.D. Cal. May 20, 2011) (посоченото окончателно разпореждане), *на адрес* https://www ftc.gov/sites/default/files/documents/cases/2011/06/110609karnanistip.pdf; *вж. също* Lesley Fair, FTC Business Center Blog, *Around the World in Shady Ways*, https://www.ftc.gov/blog/2011/06/around-world-shady-ways (June 9, 2011).

([2]) Писмо от Ken Hyatt, изпълняващ длъжността Заместник министър на търговията, отговарящ за международната търговия, Администрация по международната търговия, до Вера Йоурова, Комисар по въпросите на правосъдието, потребителите и равнопоставеността между половете.

правоприлагащ орган търси информация относно етапа на разглеждане на конкретен случай на сезиране за целите на собственото си производство по принудително изпълнение, ФТК ще предоставя отговор, като взема предвид броя на сезиранията, които са в процес на разглеждане, както и изискванията за поверителност и други законови условия.

ФТК ще работи в тясно взаимодействие и с ОЗД от ЕС, за да предоставя съдействие при правоприлагането. В случаите, когато е уместно, това може да се изразява във взаимен обмен на информация и съдействие при разследвания в съответствие със Закона за безопасен интернет на САЩ, с който се разрешава на ФТК да оказва съдействие на чужди правоприлагащи институции, когато предприемат действия по прилагането на закони, забраняващи практики, които по същество са еднакви с тези, които се забраняват със законите, които ФТК прилага ([1]). Като част от това съдействие ФТК може да споделя информация, получена във връзка с разследване на ФТК, да инициира задължителен процес от името на ОЗД от ЕС, провеждащ собствено разследване, да взема устни показания от свидетели или ответници във връзка с производството по принудително изпълнение на ОЗД, ако това съответства на изискванията на Закона за безопасен интернет на САЩ. ФТК редовно използва правомощията си да съдейства на други органи по света по случаи в областта на неприкосновеността на личния живот и защитата на потребителите ([2]).

Освен разглеждането с предимство на случаите, по които е сезирана съгласно Щита за личните данни от страна на държавите — членки на ЕС, и саморегулиращи се организации в областта на неприкосновеността на личния живот ([3]), ФТК се ангажира да провежда разследвания по собствена инициатива по предполагаеми нарушения на Рамката, когато това е необходимо и като използва набор от средства.

Вече над десетилетие ФТК поддържа стабилна програма за разследвания по въпроси от областта на неприкосновеността на личния живот и сигурността, свързани с търговски организации. Като част от тези разследвания ФТК редовно проверява дали въпросният субект прави изявления във връзка с рамката за сфера на неприкосновеност на личния живот. Когато това е така и разследването разкрие явни нарушения на принципите за сфера на неприкосновеност на личния живот, ФТК включва обвинението за нарушаване на тези принципи в своите действия по принудително изпълнение. Ще продължим да прилагаме този проактивен подход и съгласно новата рамка. Важно е да се отбележи, че ФТК провежда много по-голям брой разследвания от тези, които в крайна сметка водят до действия по публично правоприлагане. Много от разследванията на ФТК се приключват, защото служителите не констатират явно нарушение на законодателството. Тъй като разследванията на ФТК не са публични и са поверителни, приключването им често не се оповестява публично.

Близо 40-те действия по принудително изпълнение, които ФТК е предприела съгласно програмата за сфера на неприкосновеност на личния живот, са доказателство за ангажираността на агенцията с проактивното прилагане на трансгранични програми в областта на неприкосновеността на личния живот. ФТК ще следи редовно за евентуални нарушения на новата рамка като част от разследванията, които предприема в областта на неприкосновеността на личния живот и сигурността.

III. ПРЕДПРИЕМАНЕ НА ДЕЙСТВИЯ ПО НЕПРАВОМЕРНИ ИЛИ ИЗМАМНИ ТВЪРДЕНИЯ ЗА УЧАСТИЕ В ЩИТА ЗА ЛИЧНИТЕ ДАННИ

Както беше разгледано по-горе, ФТК ще предприема действия срещу субекти, които представят погрешно своето участие в Рамката. ФТК ще разглежда с предимство случаите, по които е сезирана от Министерството на търговията във връзка с организации, за които е определила, че погрешно твърдят, че участват понастоящем в Рамката, или използват сертификационен знак за Рамката без разрешение.

Освен това трябва да отбележим, че ако в политиката в областта на неприкосновеността на личния живот на една организация се твърди, че тя спазва принципите на Щита за личните данни и тя не се регистрира или не поддържа регистрацията си в Министерството на търговията, това само по себе си вероятно няма да е причина ФТК да не предприеме действия по принудителното изпълнение на тези ангажименти по Рамката по отношение на тази организация.

([1]) Когато определя дали да упражни правомощията си по силата на Закона за безопасен интернет на САЩ, ФТК взема предвид наред с останалото и следното: „А) дали отправилата искането институция се е съгласила да предостави или ще предостави реципрочно съдействие на комисията; Б) дали удовлетворяването на искането би засегнало обществен интерес на Съединените щати; и В) дали разследването или производството по принудително изпълнение на отправилата искането институция засяга действия или практики, които нанасят или са в състояние да нанесат вреда на значителен брой лица.“ 15 U.S.C. § 46(j)(3). Това правомощие не се прилага по отношение на правоприлагането на законите в областта на конкуренцията.

([2]) Например през финансовите години 2012—2015 ФТК използва правомощията си по силата на Закона за безопасен интернет на САЩ за обмен на информация в отговор на близо 60 искания от чуждестранни институции и издаде почти 60 призовки по граждански разследвания (еквивалент на административните разпореждания), за да съдейства на 25 чуждестранни разследвания.

([3]) Въпреки че ФТК не издава решения и не е медиатор по индивидуални жалби на потребители, комисията потвърждава ангажимента си да разглежда с предимство случаите, за които е сезирана от ОЗД на ЕС съгласно Щита за личните данни. Освен това ФТК използва жалбите, въведени в нейната база данни за потребители (до която имат достъп много други правоприлагащи агенции), за да определя тенденциите, приоритетите при прилагането и потенциалните обекти за разследване. Физическите лица от ЕС могат да използват същата система, с която разполагат гражданите на САЩ за подаването на жалби до ФТК, на адрес: www.ftc.gov/complaint. Въпреки това за предпочитане е физическите лица от ЕС да подават индивидуалните си жалби по Щита за личните данни до ОЗД в своята държава членка или до инстанция за алтернативно решаване на спорове.

IV. КОНТРОЛ ПО ЗАПОВЕДИТЕ

ФТК потвърждава също ангажимента си да упражнява контрол по заповедите за принудително изпълнение, за да гарантира спазването на Рамката на Щита за личните данни.

Ние ще изискваме Рамката да бъде спазвана посредством различни подходящи разпореждания за прекратяване, предвидени в бъдещите заповеди на ФТК съгласно Рамката. Тук се включва забраната за подвеждащо представяне във връзка с участието в Рамката и други програми в областта на неприкосновеността на личния живот, когато това е основанието за действията на ФТК.

Случаите на правоприлагане от страна на ФТК във връзка с първоначалната програмата за сфера на неприкосновеност на личния живот са показателни. Всяка от заповедите по 36-те дела за неправомерни или измамни твърдения за сертифициране съгласно сферата на неприкосновеност на личния живот забранява на ответника да представя подвеждащо участието си в тази или друга програма в областта на неприкосновеността на личния живот или сигурността и задължава дружествата да представят пред ФТК доклади за изпълнението на заповедта. В случаите на нарушаване на принципите на сферата на неприкосновеност на личния живот дружествата бяха задължавани да прилагат всеобхватни програми в областта на неприкосновеността на личния живот и на всеки две години в продължение на двадесет години да получават независима оценка от трета страна за тези програми, която да представят на ФТК.

Неизпълнението на административна заповед на ФТК може да води до налагане на гражданскоправни санкции в размер до 16 000 щатски долара за всяко нарушение или 16 000 щатски долара на ден за продължаващо нарушаване ([1]), като санкцията може да достигне милиони долари при практики, засягащи голям брой потребители. Всяка заповед за съгласие съдържа също разпоредби за докладване и спазване. Субектите, по отношение на които е издадена заповед, трябва да пазят документацията, доказваща изпълнението, за срок от определен брой години. Заповедите трябва също така да бъдат сведени до знанието на служителите, които отговарят за гарантиране на изпълнението им.

ФТК провежда системен контрол на изпълнението на заповедите съгласно сферата на неприкосновеност на личния живот, така както и за всички останали свои заповеди. ФТК се отнася сериозно към изпълнението на нейните заповеди в областта на неприкосновеността на личния живот и сигурността на данните и когато е необходимо, предприема действия по принудителното им изпълнение. Например, както беше отбелязано по-горе, Google платиха 22,5 милиона щатски долара гражданскоправни санкции по решение за обвинение в неспазване на заповед на ФТК. Важно е да се отбележи, че заповедите на ФТК ще продължат да осигуряват защита за всички потребители от целия свят, които имат взаимоотношения с дружества, не само за тези, които подават жалби.

В заключение, ФТК ще продължи да поддържа онлайн списък на дружествата, по отношение на които са издадени заповеди във връзка с прилагането на програмата за сфера на неприкосновеност на личния живот и на новата рамка на Щита за личните данни. ([2]) Освен това съгласно принципите на Щита за личните данни сега се изисква от дружествата, по отношение на които е издадена заповед на ФТК или съдебно разпореждане поради неспазване на принципите, да оповестяват публично всички съответни части от докладите си за спазването или за оценка, представени пред ФТК, доколкото това е съобразено със законите и правилата за поверителност.

V. СЪВМЕСТНА РАБОТА С ОЗД ОТ ЕС И СЪТРУДНИЧЕСТВО ПРИ ПРАВОПРИЛАГАНЕТО

ФТК признава важната роля на ОЗД от ЕС за спазването на Рамката и насърчава засилването на консултациите и сътрудничеството при правоприлагането. Освен с евентуалните консултации със сезиращите ОЗД по специфични за всеки случай въпроси, ФТК се ангажира да участва в периодични срещи с определени представители на Работната група по член 29 за обсъждане на възможности за подобряване на сътрудничеството по прилагане на Рамката като цяло. ФТК ще участва също, заедно с Министерството на търговията, Европейската комисия и представители на Работната група по член 29, в годишния преглед на Рамката за обсъждане на нейното прилагане.

ФТК насърчава също така и разработването на инструменти, чрез които да се подобри сътрудничеството при правоприлагането с ОЗД от ЕС, както и с други правоприлагащи органи в областта на неприкосновеността на личния живот от целия свят. По-специално ФТК, съвместно с партньорите по правоприлагането в Европейския съюз и от целия свят, стартира миналата година система за предупреждение в рамките на Световната мрежа по прилагане на изискванията за неприкосновеността на личния живот (*Global Privacy Enforcement Network* (GPEN)) с цел обмен на информация по разследвания и повишаване на координацията при правоприлагането. Този инструмент за предупреждение може да бъде особено полезен в контекста на рамката на Щита за личните данни. ФТК и ОЗД от ЕС могат да го използват в координацията във връзка с разследванията съгласно рамката и други разследвания в областта на неприкосновеността на личния живот, включително и като начална точка за обмен на информация, за да бъде осигурена координирана и по-ефективна защита на неприкосновеността на личния живот за потребителите. Очакваме с нетърпение да продължим да работим с органите — участници

([1]) 15 U.S.C. § 45(m); 16 C.F.R. § 1.98.

([2]) *Вж.* FTC, Business Center, Legal Resources, https://www.ftc.gov/tips-advice/business-center/legal-resources?type=case&field-consumer-protection-topics-tid=251.

от ЕС, за намиране на по-широко приложение на системата за предупреждение в GPEN и за разработване на други инструменти за подобряване на сътрудничеството при правоприлагането по случаи в областта на неприкосновеността на личния живот, включително съгласно Рамката.

ФТК с удоволствие потвърждава ангажимента си за прилагането на новата рамка на Щита за личните данни. Също така очакваме с нетърпение да продължим съвместната ни работа с колегите от ЕС по защитата на неприкосновеността на личния живот на потребителите от двете страни на Атлантическия океан.

Искрено Ваша,

Edith Ramirez

Председател

Притурка А

Рамката на Щита за личните данни в отношенията между ЕС и САЩ в контекст: преглед на средата в САЩ в областта на неприкосновеността на личния живот и сигурността

Защитата, осигурявана с Рамката на Щита за личните данни в отношенията между ЕС и САЩ („Рамката“), съществува в контекста на по-широката защита на неприкосновеността на личния живот, осигурявана от правната система на САЩ като цяло. На първо място Федералната търговска комисия на САЩ („ФТК“) разполага със солидна програма за защита на неприкосновеността на личния живот и сигурността на данните за търговските практики в САЩ, която защитава потребителите в целия свят. На второ място, средата в САЩ за защита на неприкосновеността на личния живот и сигурността значително еволюира след 2000 г., когато беше приета първоначалната програма за сфера на неприкосновеност на личния живот. Оттогава влязоха в сила голям брой федерални и щатски закони за защита на неприкосновеността на личния живот и сигурността и значително се увеличи броят на частноправните и публичноправните съдебни спорове за налагане на спазването на правата на неприкосновеност на личния живот. Широкият обхват на осигуряваната от САЩ правна защита на неприкосновеността на личния живот и сигурността на потребителите, приложима по отношение на данните при търговски практики, допълва защитата, която новата рамка осигурява на физическите лица от ЕС.

I. ОБЩА ПРОГРАМА НА ФТК ЗА ПРАВОПРИЛАГАНЕ В ОБЛАСТТА НА ЗАЩИТАТА НА НЕПРИКОСНОВЕНОСТТА НА ЛИЧНИЯ ЖИВОТ И СИГУРНОСТТА

ФТК е водещата агенция на САЩ за защита на потребителите, като нейната работа е съсредоточена върху защита на неприкосновеността на личния живот в търговския сектор. ФТК е компетентна да преследва нелоялни и измамни действия или практики, които нарушават неприкосновеността на личния живот на потребителите, както и да прилага по-специализирани закони за неприкосновеността на личния живот, които защитават определена информация от финансово и здравно естество, информация за деца и информация, използвана за определянето на някои решения за допустимост във връзка с потребителите.

ФТК има уникален опит в правоприлагането в областта на защитата на неприкосновеността на личния живот на потребителите. Действията по принудително изпълнение на ФТК бяха насочени към неправомерни практики в онлайн и офлайн среда. Така например ФТК предприе действия по принудително изпълнение срещу добре известни дружества като Google, Facebook, Twitter, Microsoft, Wyndham, Oracle, HTC и Snapchat, както и срещу по-малко известни дружества. ФТК заведе дела срещу дружества по обвинения, че са изпращали нежелани съобщения на потребители, инсталирали са шпионски софтуер на компютри, не са осигурили защита на лична информация на потребители, проследявали са по измамен начин потребители онлайн, нарушили са правото на неприкосновеност на личния живот на деца, неправомерно са събирали информация за потребители от мобилни устройства и не са осигурили защита на устройства, свързани с интернет, които се използват за съхраняване на лични данни. Постановените в резултат от това заповеди обикновено предвиждаха наблюдение от страна на ФТК в рамките на период от двадесет години, забраняваха по-нататъшни нарушения на закона и налагаха на дружествата значителни финансови санкции в случай на неизпълнение на заповедта ([1]). Важно е да се отбележи, че заповедите на ФТК защитават не само потребителите, които са се оплакали във връзка с даден проблем — те защитават всички потребители, които имат отношение към въпросното дружество. В международен контекст ФТК е компетентна да защитава потребителите в целия свят от практики, които се осъществяват в Съединените щати ([2]).

До момента ФТК е водила дела или е предприела действия във връзка с над 130 случая на изпращане на нежелани съобщения и инсталиране на шпионски софтуер, над 120 случая на нарушаване на правилото на телемаркетинга за необаждане („Do Not Call“), над 100 случая на нарушаване на Закона за оповестяване на информация за кредити, почти 60 случая във връзка със сигурността на данните, над 50 случая на общо нарушаване на неприкосновеността на личния живот, почти 30 случая на нарушаване на Закона Gramm-Leach-Bliley и над 20 случая за налагане на спазването на Закона за защита на неприкосновеността на личния живот на децата онлайн ([3]). Наред с това ФТК също така отправи предупредителни писма, които направи обществено достояние ([4]).

([1]) На всеки субект, който не изпълни заповед на ФТК, може да се наложи гражданскоправна санкция в размер до 16 000 щатски долара за всяко нарушение или 16 000 щатски долара на ден за продължаващо нарушаване. *Вж.* 15 U.S.C. § 45(l); 16 C.F.R. § 1.98(c).

([2]) Конгресът изрично потвърди правомощието на ФТК да използва средства за правна защита, включително възстановяване, във връзка действия или практики за международна търговия, които 1) нанасят или са в състояние да нанесат разумно предвидими вреди в Съединените щати, или 2) се отнасят за действия по същество, извършвани в Съединените щати. *Вж.* 15 U.S.C. § 45(a)(4).

([3]) В част от разглежданите от ФТК случаи във връзка с неприкосновеността на личния живот и сигурността на данни се твърди, че дружеството извършва както некоректни, така и измамни практики; понякога случаите включват твърдения за нарушения на няколко закона, като например Закона за оповестяване на информация за кредити, Закона Gramm-Leach-Bliley и Закона за защита на неприкосновеността на личния живот на децата онлайн.

([4]) *Вж. например* Съобщение за медиите на ФТК „ФТК предупреждава производителя на приложения за деца BabyBus за възмножни нарушения на Закона за защита на неприкосновеността на личния живот на децата онлайн“ (Dec. 22, 2014), https://www.ftc.gov/news-events/press-releases/2014/12/ftc-warns-childrens-app-maker-babybus-about-potential-coppa; Съобщение за медиите на ФТК „ФТК предупреждава за възможно нарушение на защитата на неприкосновеността на личния живот при операции на информационни брокери“ (May 7, 2013), https://www.ftc.gov/news-events/press-releases/2013/05/ftc-warns-data-broker-operations-possible-privacy-violations; Съобщение за медиите на ФТК „ФТК предупреждава информационните брокери, които предоставят информация за наематели във връзка с тяхното поведение като наематели в миналото, че за тях може да се прилага Законът за оповестяване на информация за кредити“ (Apr. 3, 2013), https://www.ftc.gov/news-events/press-releases/2013/04/ftc-warns-data-brokers-provide-tenant-rental-histories-they-may.

Като част от своя значителен опит за правоприлагане в областта на неприкосновеността на личния живот ФТК редовно следеше за възможни нарушения на програмата за сфера на неприкосновеност на личния живот. След приемането на тази програма ФТК предприе по собствена инициатива многобройни разследвания във връзка с нейното спазване и предприе действия срещу дружества на САЩ в 39 случая на нарушаване на сферата на неприкосновеност на личния живот. ФТК ще продължи да следва този проактивен подход, като отдаде приоритет на прилагането на новата рамка.

II. ЗАЩИТА НА ФЕДЕРАЛНО И ЩАТСКО РАВНИЩЕ ЗА НЕПРИКОСНОВЕНОСТТА НА ЛИЧНИЯ ЖИВОТ НА ПОТРЕБИТЕЛИТЕ

Обзорът на прилагането на сферата на неприкосновеност на личния живот, приложен към решението на Европейската комисия относно адекватността на програмата за сфера на неприкосновеност на личния живот, предлага обобщение на голям брой федерални и щатски закони за защита на неприкосновеността на личния живот, действащи към момента на приемането на програмата за сфера на неприкосновеност на личния живот през 2000 г. ([1]). Към онзи момент събирането и използването на лични данни при търговски операции бе уредено с редица федерални закони, в допълнение към раздел 5 от Закона за ФТК, в това число Закона за кабелните далекосъобщения, Закона за защита на неприкосновеността на личния живот на водачите на МПС, Закона за защита на неприкосновеността на личния живот при електронните комуникации, Закона за превод на средства по електронен път, Закона за оповестяване на информация за кредити, Закона Gramm-Leach-Bliley, Закона за правото на неприкосновеност на личните финанси, Закона за защита на неприкосновеността на личния живот на потребителите при телефонни комуникации и Закона за защита на неприкосновеността на личния живот във връзка с ползването на видео. Много от щатите също разполагат с аналогични закони в тези области.

От 2000 г. насам настъпиха редица промени както на федерално, така и на щатско равнище, благодарение на които се предоставя допълнителна защита на неприкосновеността на личния живот на потребителите ([2]). Така например на федерално равнище през 2013 г. ФТК въведе изменения в акта за изпълнение на Закона за защита на неприкосновеността на личния живот на децата онлайн, с което предвиди редица допълнителни защитни мерки във връзка с личната информация на деца. Освен това ФТК прие два акта за изпълнение на Закона Gramm- Leach-Bliley — единия за защита на неприкосновеността на личния живот, а другия за гаранции — с които задължи финансовите институции ([3]) да разкриват своите практики за споделяне на информация и да прилагат всеобхватна програма за гарантиране на сигурността на информация, за да защитават информацията за потребителите ([4]). По същия начин Законът за достоверни и точни сведения за кредитни трансакции (*Fair and Accurate Credit Transactions Act* (FACTA)), въведен в действие през 2003 г., допълва отдавна прилаганите кредитни закони на САЩ с изисквания по отношение на маскирането, споделянето и заличаването на някои видове чувствителна финансова информация. ФТК промулгира редица актове за изпълнение по FACTA във връзка, наред с другото, с правото на потребителите да получават безплатно годишна кредитна информация, изисквания за сигурно заличаване на кредитната информация на потребителите, правото на потребителите да откажат да получават определени кредитни и застрахователни оферти, правото на потребителите да откажат използването на информация, предоставена от свързано дружество за предлагане на неговите продукти и услуги, и изисквания за финансовите институции и кредиторите да приложат програми за откриване и предотвратяване на кражбата на самоличност ([5]). Освен това през 2013 г. бяха изменени актовете за изпълнение по Закона за преносимост и отчетност при здравното застраховане (*Health Insurance Portability and Accountability Act*), като бяха добавени гаранции за защитата на неприкосновеността на личния живот и сигурността на личната информация за здравословното състояние ([6]). В сила бяха приведени и актове във връзка със защитата на потребителите от нежелани обаждания, свързани с телемаркетинг, автоматизирани обаждания и изпращане на нежелани съобщения. Освен това Конгресът приведе в действие закони, с които се изисква от определени дружества, които събират информация за здравословното състояние, да уведомяват потребителите в случай на нарушение ([7]).

Отделните щати също бяха особено активни в приемането на закони във връзка с неприкосновеността на личния живот и сигурността. От 2000 г. насам четиридесет и седем щата, Окръг Колумбия, Гуам, Пуерто Рико и Вирджинските острови въведоха закони, които изискват от дружествата да уведомяват физическите лица в случай на нарушаване на сигурността

([1]) *Вж.* Министерство на търговията на САЩ, Обзор на прилагането на сферата на неприкосновеност на личния живот, https://build.export.gov/main/safeharbor/eu/eg_main_018476.

([2]) За по-подробна информация относно правната защита в САЩ вж. Daniel J. Solove & Paul Schwartz, *Information Privacy Law* (5th ed. 2015).

([3]) Определението за финансови институции по Закона Gramm-Leach-Bliley е особено широко, като обхваща всички дружества, които „се занимават в значителна степен“ с предоставянето на финансови продукти и услуги. Това включва, например, дружества за осребряване на чекове, дружества, предоставящи кредити до заплата, ипотечни брокери, небанкови кредитори, оценители, извършващи оценки на лично или на недвижимо имущество, и професионални съставители на данъчни документи.

([4]) Съгласно Закона за финансова защита на потребителите от 2010 г. („CFPA“), глава X от Pub. L. 111-203, 124 Stat. 1955 (21 юли 2010 г.) (наричан още „Dodd-Frank Wall Street Reform and Consumer Protection Act“), по-голямата част от правомощията на ФТК за изработване на актове за изпълнение по Закона Gramm-Leach-Bliley бяха прехвърлени на Бюрото за финансова защита на потребителите („CFPB“). ФТК продължава да има правомощия за правоприлагане по Закона Gramm-Leach-Bliley, както и правомощие за изпълнителни актове по отношение на акта за изпълнение във връзка с гаранциите и ограничени правомощия за изработване на изпълнителни актове във връзка с акта за изпълнение за защита на неприкосновеността на личния живот по отношение на търговците на автомобили.

([5]) Съгласно Закона за финансова защита на потребителите Комисията споделя своята роля за правоприлагане по Закона за оповестяване на информация за кредити с Бюрото за финансова защита на потребителите, но правомощието за изработване на изпълнителни актове е прехвърлено до голяма степен на Бюрото за финансова защита на потребителите (с изключение на изпълнителните актове за кражба на самоличност и за заличаване на лична информация).

([6]) *Вж.* 45 C.F.R. pts. 160, 162, 164.

([7]) *Вж. например* Закона за възстановяване и реинвестиране в Америка от 2009 г. (*American Recovery & Reinvestment Act*), Pub. L. № 111-5, 123 Stat. 115 (2009) и съответните изпълнителни актове, 45 C.F.R. §§ 164.404-164.414; 16 C.F.R. pt. 318.

на личната информация ([1]). Поне тридесет и два щата и Пуерто Рико разполагат със закони за заличаването на данни, които предвиждат изисквания за унищожаването или заличаването на лична информация ([2]). Редица щати въведоха в действие общи закони за сигурността на данните. В допълнение към това Калифорния въведе няколко закона за неприкосновеност на личния живот, в това число закон, който изисква от дружествата да разполагат с политики за защита на неприкосновеността на личния живот и да публикуват своите практики за гарантиране, че не следят потребителите (Do Not Track) ([3]), закона „Shine the Light“, който изисква по-голяма прозрачност във връзка с информационните брокери ([4]), и закон, който нарежда да се предвиди въвеждането на „копче за изтриване“, което дава възможност на непълнолетните потребители да искат заличаването на част от информацията в социалните медии ([5]). Използвайки тези закони и други правомощия федералното правителство и щатските правителства наложиха значителни глоби на дружества, които не са защитили правото на неприкосновеност на личния живот и сигурността на личната информация на потребителите ([6]).

Редица частни съдебни дела също доведоха до успешни съдебни решения и до споразумения, които осигуриха допълнителна защита във връзка с неприкосновеността на личния живот и сигурността за потребителите. Така например през 2015 г. Target се съгласи да изплати 10 милиона щатски долара като част от споразумение с потребители, които твърдяха, че отнасяща се до тях лична финансова информация е била компрометирана поради широкомащабно нарушение на сигурността на данните. През 2013 г. AOL се съгласи да изплати 5 милиона щатски долара като част от споразумение след колективен иск по твърдения за неподходящо заличаване на идентификационна информация във връзка с публикуването на заявките за търсения на стотици хиляди членове на AOL. Така също федерален съд одобри изплащането от страна на Netflix на 9 милиона щатски долара за това, че дружеството е съхранявало записи за наеманите продукти в нарушение на Закона от 1988 г. за защита на неприкосновеността на личния живот във връзка с ползването на видео. Федерални съдилища в Калифорния одобриха две отделни споразумения с Facebook, едното за 20 милиона щатски долара, а другото за 9,5 милиона щатски долара, във връзка с практиките на дружеството за събиране, използване и споделяне на лична информация на своите потребители. А през 2008 г. щатски съд в Калифорния одобри споразумение на стойност 20 милиона щатски долара с LensCrafters във връзка с неправомерното разкриване на медицинска информация на потребителите.

Накратко, както е видно от настоящото обобщение, Съединените американски щати осигуряват значителна правна защита на неприкосновеността на личния живот и сигурността на потребителите. Новата рамка на Щита за личните данни, която осигурява съдържателни гаранции за физическите лица от ЕС, ще действа в рамките на този по-широк контекст, в който продължава да заема важно място защитата на неприкосновеността на личния живот и сигурността на потребителите.

([1]) *Вж. например* National Conference of State Legislatures („NCSL“), *State Security Breach Notification Laws* (Jan. 4, 2016), *на адрес:* http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

([2]) NCSL, *Data Disposal Laws* (Jan. 12, 2016), *на адрес:* http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx.

([3]) Cal. Bus. & Professional Code §§ 22575-22579.

([4]) Cal. Civ. Code §§ 1798.80-1798.84.

([5]) Cal. Bus. & Professional Code § 22580-22582.

([6]) *Вж.* Jay Cline, *U.S. Takes the Gold in Doling Out Privacy Fines,* Computerworld (Feb. 17, 2014), *на адрес:* http://www.computerworld.com/s/article/9246393/Jay-Cline-U.S.-takes-the-gold-in-doling-out-privacy-fines?taxonomyId=17&pageNumber=1.

ПРИЛОЖЕНИЕ V

Писмо от Министъра на транспорта на САЩ, Anthony Foxx

19 февруари 2016 г.

Комисар Вера Йоурова
Европейска комисия
Rue de la Loi/Wetstraat 200
1 049 l 049 Брюксел
Белгия

Относно: Рамка на Щита за личните данни в отношенията между ЕС и САЩ

Уважаема комисар Йоурова,

Министерството на транспорта на Съединените щати („министерството“ или „МТ“) благодари за възможността да опише своята роля при прилагането на Рамката на Щита за личните данни в отношенията между ЕС и САЩ. Тази рамка има решаваща роля за защитата на личните данни, които се предоставят при извършването на търговски сделки в един все по-взаимосвързан свят. Тя позволява на дружествата да осъществяват важни операции в глобалната икономика, като същевременно ще гарантира, че потребителите от ЕС ще продължат да се ползват от съществена защита на неприкосновеността на личния живот.

Преди повече от 15 години МТ за първи път пое публично ангажимент да прилага Рамката за сфера на неприкосновеност на личния живот в писмо, изпратено до Европейската комисия. В това писмо МТ се ангажира да прилага активно принципите от схемата за сфера на неприкосновеност на личния живот. МТ поддържа този свой ангажимент и настоящото писмо ознаменува това.

По-специално МТ отново се ангажира да работи в следните основни области: 1) приоритетно разследване на обвинения за нарушаване на Щита за личните данни; 2) подходящи действия по принудително изпълнение срещу субекти, които правят неправомерни или измамни твърдения за сертифицирането си съгласно Щита за личните данни; и 3) контрол по изпълнението и публично оповестяване на заповеди по принудително изпълнение във връзка с нарушения на Щита за личните данни. Предоставяме информация относно всеки от тези ангажименти и в необходимия контекст — съответния минал опит във връзка с ролята на МТ за защита на неприкосновеността на личния живот на потребителите и прилагането на Рамката на Щита за личните данни.

I. КОНТЕКСТ

A. **Правомощия на МТ в областта на неприкосновеността на личния живот**

Министерството е силно ангажирано с гарантирането на неприкосновеността на личния живот при предоставянето на информация от потребителите на въздушните превозвачи и билетните агенции. МТ е упълномощено да предприема действия в тази област по силата на глава 49, раздел 41712 от U.S.C., който забранява на превозвач или билетна агенция „всяка некоректна или измамна практика или всеки акт на нелоялна конкуренция“ при продажбата на въздушни транспортни услуги, която води или би могла да доведе до вреда за потребителя. Раздел 41712 е изработен по модела на раздел 5 от Закона за Федералната търговска комисия (ФТК) (15 U.S.C. 45). Тълкуването, което даваме на законовото изискване по отношение на некоректна или измамна практика е, че се забранява на превозвачи или билетни агенции: 1) да нарушават условията на тяхната политика в областта на неприкосновеността на личния живот, или 2) да събират или разкриват лична информация по начин, който е в нарушение на обществения ред, е неморален или предизвиква за потребителите сериозни вреди, които не са компенсирани с евентуални предимства. Също така, според нашето тълкуване на раздел 41712, се забранява на превозвачи и билетни агенции: l) да нарушават някой от изпълнителните актове, издадени от министерството, с което конкретни практики в областта на неприкосновеността на личния живот се определят като некоректни или измамни; или 2) да нарушават Закона за защита на неприкосновеността на личния живот на децата онлайн (*Children's Online Privacy Protection Act* (COPPA)) или актовете на ФТК за изпълнение на този закон. Съгласно федералното право МТ има изключителни правомощия да регулира практиките на въздушните превозвачи в областта на неприкосновеността на личния живот и споделени правомощия с ФТК във връзка с практиките на билетните агенции в областта на неприкосновеността на личния живот при продажбата на въздушни транспортни услуги.

В тази си функция министерството може да използва законоустановените правомощия съгласно раздел 41712, за да гарантира спазването на принципите на неприкосновеност на личния живот съгласно рамката на Щита за личните данни, когато превозвач или продавач на въздушни транспортни услуги публично се е ангажирал да спазва тези принципи. Следователно, когато даден пътник съобщи информация на превозвач или билетна агенция, които са поели задължението да спазват принципите на неприкосновеност на личния живот съгласно рамката на Щита за личните данни, всяко едно нарушаване на това задължение от страна на превозвача или билетната агенция ще бъде нарушение на раздел 41712.

Б. **Практики по принудително изпълнение**

Службата по принудително изпълнение и производства в областта на авиацията към Министерството на транспорта (Службата по принудително изпълнение в авиацията) разглежда делата и придвижва производствата в случаи по силата на глава 49, раздел 41712 на U.S.C. Тя предприема принудително изпълнение по законовата забрана съгласно раздел 41712 срещу некоректни и измамни практики, предимно чрез преговори и изготвяне на заповеди за прекратяване и за оценка на размера на гражданскоправни санкции. Службата получава информация за предполагаеми нарушения главно от жалби, подадени от физически лица, пътнически агенции, въздушни превозвачи и американски и чуждестранни правителствени органи. Потребителите могат да използват уебсайта на МТ да подават жалби във връзка с неприкосновеността на личния живот срещу въздушни превозвачи и билетни агенции ([1]).

Ако по дадено дело не бъде постигнато разумно и подходящо решение, Службата по принудително изпълнение в авиацията има правомощия да започне производство по принудително изпълнение с изслушване за събиране на доказателства пред съдия по административно право на министерството. Този съдия има правомощия да издава заповеди за прекратяване и за налагане на гражданскоправни санкции. Неспазването на разпоредбите на раздел 41712 може да доведе до издаването на заповеди за прекратяване и налагането на гражданскоправни санкции в размер до 27 500 щатски долара за всяко нарушаване на разпоредбите на раздел 41712.

Министерството не е компетентно да отпуска обезщетения или парични репарации на физическите лица жалбоподатели. То обаче има правомощието да одобрява споразумения, постигнати в резултат на разследвания, проведени от Службата по принудително изпълнение в авиацията, които предвиждат предоставянето директно на обезщетения на потребителите (напр. средства в брой, ваучери) като компенсация вместо парична санкция, платима на правителството на САЩ. Има примери на такова уреждане в миналото, като то може да се използва и в контекста на принципите на неприкосновеност на личния живот съгласно рамката на Щита за личните данни, когато обстоятелствата го налагат. Повтарянето на нарушенията по раздел 41712 от страна на въздушен превозвач поставя под съмнение добрата воля на този превозвач по отношение на спазването на поетото задължение. В крайни случаи може да се реши, че той повече не отговаря на условията да извършва дейност и следователно, да загуби лиценза си за упражняване на икономическа дейност.

Към днешна дата министерството е получило сравнително малко на брой жалби по обвинения за нарушаване от страна на билетни агенции или въздушни превозвачи на принципите на неприкосновеност на личния живот. Когато се получат такива, те се разглеждат съгласно изложените по-горе принципи.

В. **Правни инструменти за защита, осигурявани от МТ, от които могат да се ползват потребителите от ЕС**

Забраната срещу некоректни или измамни практики при предоставянето или продажбата на въздушни транспортни услуги, предвидена съгласно раздел 41712, се прилага едновременно за американски и за чуждестранни въздушни превозвачи и билетни агенция. МТ често предприема действия срещу въздушни превозвачи от САЩ и от други държави за практики, които засягат едновременно чуждестранни и американски потребители, на основание на това, че практиките на този превозвач са се осъществили в процеса на предоставянето на въздушни транспортни услуги до или от Съединените щати. МТ прилага и ще продължи да прилага всички средства за правна защита, с които разполага, за да защитава едновременно чуждестранни и американски потребители от некоректни или измамни практики във въздушните транспортни услуги от страна на субектите, които подлежат на регулиране.

МТ прилага по отношение на въздушните превозвачи и други закони, които предвиждат защита за потребители извън САЩ, като например Закона за защита на неприкосновеността на личния живот на децата онлайн. Наред с останалото в този закон се поставя изискване към операторите на уебсайтове и онлайн услуги, предназначени за деца, или общодостъпни сайтове, които съзнателно събират лична информация от деца на възраст под 13 години, да уведомяват за това родителите и да изискват родителско съгласие, което може да се провери. Уебсайтовете и услугите, базирани в САЩ, за които се прилага Законът за защита на неприкосновеността на личния живот на децата онлайн и които събират лична информация от деца извън САЩ, са задължени да спазват този закон. Чуждестранните уебсайтове и онлайн услуги също са задължени да спазват този закон, ако дейностите им са насочени към деца в Съединените щати или съзнателно събират лична информация от деца в Съединените щати. МТ е компетентно да предприема действия по принудително изпълнение за нарушаване на Закона за защита на неприкосновеността на личния живот на децата онлайн от страна на американски и чужди въздушни превозвачи, доколкото те осъществяват дейността си в Съединените щати.

II. ПРАВОПРИЛАГАНЕ ВЪВ ВРЪЗКА С ЩИТА ЗА ЛИЧНИТЕ ДАННИ

Ако даден въздушен превозвач или билетна агенция са избрали да участват в рамката на Щита за личните данни и в министерството бъде получена жалба срещу такъв субект по обвинение за нейното нарушаване, министерството ще предприеме следните действия за стриктното прилагане на рамката.

([1]) http://www.transportation.gov/airconsumer/privacy-complaints.

А. **Отдаване на приоритет на разследвания на обвинения за нарушаване**

Службата по принудително изпълнение в авиацията ще разглежда всяка жалба по обвинение за нарушаване на Щита за личните данни (включително жалби, получени от органите по защита на данните от ЕС) и ще предприема действия по принудително изпълнение, когато са налице доказателства за нарушение. Освен това тя ще си сътрудничи с ФТК и с Министерството на търговията и ще разследва с предимство обвинения срещу подлежащите на регулиране субекти в неспазване на ангажиментите за защита на неприкосновеността на личния живот, които те са поели като част от рамката на Щита за личните данни.

Когато получи твърдения за нарушаване на рамката на Щита за личните данни, Службата по принудително изпълнение в авиацията може да предприеме редица действия като част от своето разследване. Например тя може да направи преглед на политиките в областта на неприкосновеността на личния живот на билетната агенция или въздушния превозвач, да получи допълнителна информация от тях или от трети страни, да осъществи последващ контрол съвместно със сезиращия субект и да направи оценка дали има модел на извършване на нарушенията или са засегнати значителен брой потребители. Освен това службата може да определи дали случаят засяга въпроси, които са от компетентността на Министерството на търговията или ФТК, да направи преценка дали ще е от полза да се проведе обучение на потребителите и на дружествата, и ако е необходимо, да инициира производство по принудително изпълнение.

Ако министерството получи информация за евентуални нарушения на Щита за личните данни от страна на билетни агенции, то ще работи по случая в координация с ФТК. Също така ще информира ФТК и Министерството на търговията за резултатите от действията по принудително прилагане съгласно Щита за личните данни.

Б. **Предприемане на действия по неправомерни или измамни твърдения за участие в Щита за личните данни**

Министерството остава ангажирано да провежда разследвания за нарушения на Щита за личните данни, включително за неправомерни или измамни твърдения за участие в тази програма. Ние ще разглеждаме с предимство случаите, по които сме сезирани от Министерството на търговията във връзка с организации, за които е определено, че погрешно твърдят, че участват понастоящем в Щита за личните данни, или използват сертификационен знак за рамката без разрешение.

Освен това трябва да отбележим, че ако в политиката в областта на неприкосновеността на личния живот на една организация се твърди, че тя спазва основните принципи на Щита за личните данни и тя не се регистрира или не поддържа регистрацията си в Министерството на търговията, това само по себе си вероятно няма да е причина Министерството на транспорта да не предприеме действия по принудителното изпълнение на тези ангажименти по отношение на тази организация.

В. **Контрол по изпълнението и публично оповестяване на заповеди по принудително изпълнение във връзка с нарушения на Щита за личните данни**

Службата по принудително изпълнение в авиацията към МТ ще продължава да спазва също и ангажимента за контрол по заповедите за принудително изпълнение, според необходимостта, за да гарантира спазването на програмата на Щита за личните данни. По-специално, когато службата издаде заповед, с която указва на въздушен превозвач или билетна агенция да прекрати и да се въздържа от бъдещи нарушения на Щита за личните данни и на раздел 41712, тя ще упражнява контрол върху спазването от страна на субекта на разпоредбите за прекратяване и въздържане от нарушения, включени в заповедта. Освен това службата ще следи за публикуването на своя уебсайт на заповедите, издадени по дела във връзка с Щита за личните данни.

Очакваме с нетърпение да продължим да работим съвместно с нашите федерални партньори и заинтересованите страни от ЕС по въпроси във връзка с Щита за личните данни.

Надявам се тази информация да е полезна. Ако имате въпроси или се нуждаете от допълнителна информация, моля не се колебайте да се свържете с мен.

Искрено Ваш,

Anthony R. Foxx

Министър на транспорта

ПРИЛОЖЕНИЕ VI

Писмо от главния юрисконсулт Robert Litt
Служба на директора на Националното разузнаване

22 февруари 2016 г.

Г-н Justin S. Antonipillai
Съветник
Министерство на търговията на САЩ
1401 Constitution Ave., NW
Вашингтон, DC 20230

Г-н Ted Dean
Заместник помощник-секретар
Администрация по международната търговия
1401 Constitution Ave., NW
Вашингтон, DC 20230

Уважаеми г-н Antonipillai и г-н Dean,

През изминалите две и половина години Съединените щати предоставиха в контекста на преговорите за Щита за личните данни в отношенията между ЕС и САЩ значителен обем информация относно дейностите по събиране на данни в радиоелектронното разузнаване, извършвани от разузнавателните структури на САЩ. Това включва информация за уреждащата правна рамка, многостепенния надзор и разширената прозрачност относно тези дейности, както и за защитата като цяло на неприкосновеността на личния живот и гражданските свободи, за да съдействаме на Европейската комисия за вземането на решение за адекватността на тази защита, що се отнася до изключението за целите на националната сигурност от принципите на Щита за личните данни. В настоящия документ е обобщена информацията, която беше предоставена.

I. ПИД-28 И ОСЪЩЕСТВЯВАНЕ НА ДЕЙНОСТИ ЗА РАДИОЕЛЕКТРОННО РАЗУЗНАВАНЕ НА САЩ

Разузнавателните структури на САЩ събират външноразузнавателни данни по внимателно контролиран начин, при строго спазване на законите на САЩ и в условията на множество нива на надзор, като се съсредоточават върху важни приоритети във връзка с външното разузнаване и националната сигурност. Събирането от страна на САЩ на радиоелектронни разузнавателни данни е уредено в редица закони и политики, включително Конституцията на САЩ, Закона за надзор върху външното разузнаване (*Foreign Intelligence Surveillance Act* (FISA)) (50 U.S.C. § 1801 et seq.), Изпълнителен декрет 12333 и процедурите за прилагането му, насоки на Президента и множество процедури и насоки, одобрени от Съда за надзор върху външното разузнаване и Министъра на правосъдието, с които се определят допълнителни правила за ограничаване на събирането, запазването, използването и разпространението на външноразузнавателна информация ([1]).

a) **Общ преглед на ПИД 28**

През януари 2014 г. Президентът Обама произнесе реч, в която очерта различни реформи в дейностите за радиоелектронно разузнаване на САЩ и издаде Президентска изпълнителна директива 28 (ПИД-28) относно тези дейности ([2]). Президентът изтъкна, че дейностите за радиоелектронно разузнаване на САЩ спомагат за сигурността не само на нашата страна и на нашите свободи, но и за тези на другите страни, включително държавите — членки на ЕС, които използват информацията, събрана от разузнавателните агенции на САЩ за защитата на своите граждани.

В ПИД-28 се определят поредица от принципи и изисквания, които се прилагат за всички дейности за радиоелектронно разузнаване на САЩ и за всички лица, независимо от тяхното гражданство или местонахождение. По-специално в директивата се определят някои изисквания за процедурите относно събирането, запазването и разпространението на лична информация, събрана чрез радиоелектронно разузнаване на САЩ, за лица, които не са граждани на САЩ. Тези изисквания са разгледани подробно по-нататък, но в резюме те включват следното:

— В ПИД-28 още веднъж се потвърждава, че Съединените щати събират радиоелектронни разузнавателни данни само съгласно правомощията, предоставени по закон, с изпълнителен декрет или друга президентска директива.

([1]) Допълнителна информация относно външноразузнавателните дейности на САЩ е предоставена онлайн за обществен достъп на уебсайта на СДНР IC on the Record (www.icontherecord.tumblr.com), който е публичен и е предназначен да повишава обществената информираност за разузнавателните дейности на правителството.

([2]) *На разположение на адрес:* https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

— В ПИД-28 се установяват процедури, с които да се гарантира, че дейностите за радиоелектронно разузнаване се осъществяват единствено в преследване на законни и разрешени цели в областта на националната сигурност.

— В ПИД-28 се поставят също така изисквания неприкосновеността на личния живот и гражданските свободи да бъдат неразделна част от съображенията при планирането на радиоелектронни разузнавателни дейности по събирането на информация. По-специално, Съединените щати не събират разузнавателна информация, за да потискат или затрудняват критиката или несъгласието; да поставят в неблагоприятно положение лица на основата на техния етнически или расов произход, пол, сексуална ориентация или религия; или да предоставят конкурентни търговски предимства за дружествата и икономическите сектори на САЩ.

— С ПИД-28 се дават указания събирането на радиоелектронни разузнавателни данни да бъде съобразено с конкретния случай, доколкото това е практически възможно, и събирането на масиви от данни да се прилага само за специфични посочени цели.

— В ПИД-28 са дадени указания към разузнавателните структури да приемат процедури, „които са разумно проектирани да свеждат до минимум разпространението и запазването на лична информация, събрана от дейностите за радиоелектронно разузнаване“, и по-специално се разширява обхватът на някои защити, осигурявани за личната информация на граждани на САЩ и за информацията на граждани на други държави.

— Агенциите приеха процедури в изпълнение на изискванията на ПИД-28 и ги предоставиха за публичен достъп.

Приложимостта на разгледаните тук процедури и защити за целите на Щита за личните данни е ясна. Когато се извършва предаване на данни към дружества в Съединените щати съгласно Щита за личните данни или по всякакъв друг начин, разузнавателните агенции на САЩ могат да отправят искания към дружествата по отношение на такива данни само ако това става съобразно с FISA или по силата на една от разгледаните по-нататък законови разпоредби за писма във връзка с националната сигурност ([1]). Освен това, без да потвърждава или отрича твърденията в медиите, че разузнавателните структури на САЩ събират данни при предаването им към Съединените щати по трансатлантическите кабелни връзки, дори ако разузнавателните структури на САЩ събираха данни по този начин, това би ставало под условията на ограниченията и гаранциите, разгледани в настоящия документ, включително в съответствие с изискванията на ПИД-28.

б) **Ограничения за събирането**

В ПИД-28 са определени редица важни общи принципи, от които се ръководи събирането на информация в радиоелектронното разузнаване:

— Събирането на радиоелектронна разузнавателна информация трябва да се основава на законови разпоредби или разрешение от Президента и трябва да се осъществява съобразно с Конституцията и правото.

— Неприкосновеността на личния живот и гражданските свободи следва да бъдат неразделна част от съображенията при планирането на дейностите за радиоелектронно разузнаване.

— Събирането на радиоелектронна разузнавателна информация може да става единствено когато е налице валидна цел по отношение на външното разузнаване или контраразузнаването.

— Съединените щати не събират радиоелектронна разузнавателна информация с цел да потискат или затрудняват критиката или несъгласието.

— Съединените щати не събират радиоелектронна разузнавателна информация с цел да поставят в неблагоприятно положение лица на основата на техния етнически или расов произход, пол, сексуална ориентация или религия.

— Съединените щати не събират радиоелектронна разузнавателна информация с цел да предоставят конкурентни търговски предимства за дружествата и икономическите сектори на САЩ.

— Дейностите за радиоелектронно разузнаване на САЩ трябва *винаги* да бъдат съобразени с конкретния случай, доколкото това е практически възможно, като се взема предвид наличността на други източници на информация. Това означава, че наред с останалото и доколкото е практически възможно, дейностите по събиране на радиоелектронна разузнавателна информация трябва за предпочитане да се извършват целево, вместо под формата на събиране на масиви от данни.

Изискването радиоелектронната разузнавателна дейност да бъде „съобразена с конкретния случай, доколкото това е практически възможно“ се прилага едновременно за начина, по който се събира радиоелектронна разузнавателна

([1]) Правоприлагащите или регулаторните агенции могат да отправят искания за информация от дружества за целите на разследвания в Съединените щати по силата на други наказателноправни, гражданскоправни и регулаторни нормативни актове, които са извън обхвата на настоящия документ, който се ограничава само до тези за националната сигурност.

информация, и за това, което реално се събира. Например, когато определят дали да събират радиоелектронна разузнавателна информация, разузнавателните структури трябва да вземат предвид наличието на друга информация, включително от дипломатически или публични източници, и да предпочетат събирането да става чрез такива средства, когато това е уместно и практически възможно. Освен това политиките на разузнавателните структури следва да изискват събирането да бъде съсредоточено върху конкретни обекти или теми на външното разузнаване, където това е практически възможно, като за целта се използват ограничителни параметри (напр. конкретни съоръжения, критерии за избор и идентификатори).

Важно е информацията, предоставена на Комисията, да се разглежда като цяло. Вземането на решенията относно това кое е „практически възможно“ не е оставено на отделни лица, а е предмет на политики, които агенциите са разработили съгласно ПИД-28 и са предоставили за публичен достъп, и също е съобразено с останалите процеси, описани в директивата ([1]). Както е предвидено в ПИД-28, събирането на масиви от радиоелектронна разузнавателна информация е събиране, което „по технически или оперативни съображения се извършва без да се използват разграничителни критерии, (напр. конкретни идентификатори, критерии за избор и др.)“. В този смисъл в ПИД-28 се признава, че се налага при определени обстоятелства разузнавателните структури да извършват събиране на масиви от радиоелектронни разузнавателни данни, за да бъдат идентифицирани нови или възникващи заплахи и друга информация, която е от критично значение за националната сигурност, които често остават скрити в голямата и сложна съобщителна система в съвременния свят. Също така се признава загрижеността, която поражда за неприкосновеността на личния живот и гражданските свободи събирането на масиви от радиоелектронни разузнавателни данни. Поради това в ПИД-28 се дават указания към разузнавателните структури да използват с предимство алтернативни възможности, които биха позволили провеждането на целево радиоелектронно разузнаване, вместо събиране на масиви от данни. Съответно разузнавателните структури следва да извършват дейности по целево събиране, вместо събиране на масиви от радиоелектронни разузнавателни данни, когато това е практически възможно ([2]). Тези принципи са гаранция, че изключението за събиране на масиви от данни няма да надделее над общото правило.

Относно понятието „разумност“ може да се каже, че е фундаментален принцип в законодателството на САЩ. То означава, че не е необходимо разузнавателните структури да предприемат всички теоретично възможни мерки, а да балансират усилията си с цел защита на законните интереси за неприкосновеност на личния живот и гражданските свободи с практическите потребности при дейностите за радиоелектронно разузнаване. Тук отново са предоставени на разположение политиките на агенциите и те дават сигурност, че концепцията „разумно проектирани да свеждат до минимум разпространението и запазването на лична информация“ няма да намали тежестта на общото правило.

В ПИД-28 е предвидено също, че събраните масиви от радиоелектронна разузнавателна информация могат да се използват само за шест конкретни цели: откриване и противодействие на конкретни дейности на чужди сили; противодействие на тероризма; неразпространение на оръжия; киберсигурност; откриване и противодействие на заплахи за въоръжените сили на САЩ или на съюзнически държави; и борба със заплахи, произтичащи от трансгранична престъпна дейност, включително заобикаляне на санкции. Съветникът на Президента по въпросите на националната сигурност, в консултация с директора на Националното разузнаване (ДНР) правят годишен преглед на тези допустими употреби на събраните масиви от радиоелектронна разузнавателна информация, за да преценят дали трябва да бъдат изменени. ДНР предоставя този списък за публичен достъп, доколкото това е максимално възможно съобразно с националната сигурност. Това е едно важно и прозрачно ограничение за използването на събраните масиви от радиоелектронна разузнавателна информация.

Освен това разузнавателните структури, които изпълняват ПИД-28, укрепиха съществуващите аналитични практики и стандарти за търсене в неанализирана радиоелектронна разузнавателна информация ([3]). Анализаторите трябва да структурират запитванията или другите условия и техники на търсене, за да гарантират че са подходящи за идентифицирането на разузнавателна информация, която е релевантна за валидна задача, свързана с външното разузнаване или правоприлагането. За тази цели разузнавателните структури трябва да фокусират търсенията за лица върху категориите разузнавателна информация, които съответстват на дадено изискване в областта на външното разузнаване или правоприлагането, за да предотвратят използването на лична информация, която няма отношение към изискванията в областта на външното разузнаване или правоприлагането.

Важно е да се подчертае, че всички дейности по събиране на масиви от данни по отношение на съобщения в интернет, които разузнавателните структури на САЩ извършват при радиоелектронното разузнаване, се осъществяват в малка част от интернет. Освен това използването на целеви запитвания, както това е разгледано по-горе, е гаранция, че за задълбочено проучване от анализаторите се предава само тази информация, за която може да се счита, че има потенциална разузнавателна стойност. Тези ограничения са предвидени да осигуряват защита за неприкосновеността на личния живот и гражданските свободи за всички лица, независимо от тяхното гражданство и местопребиваването им.

([1]) *На разположение на адрес* www.icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties#ppd-28. С тези процедури се прилага концепцията за целево и съобразено със случая събиране, която е разгледана в настоящото писмо, по специфичен начин за всяка отделна разузнавателна структура.

([2]) За да цитираме един пример, в процедурите на АНС за прилагане на ПИД-28 се посочва, че „когато е практически възможно, събирането става чрез използване на един или повече критерии за избор, за да бъде съсредоточено върху конкретни обекти на външното разузнаване (напр. конкретен и известен международен терорист или терористична група) или конкретни теми на външното разузнаване (напр. разпространение на оръжия за масово унищожение от чужда сила или нейни агенти).“

([3]) *На адрес:* http://www.dni.gov/files/documents/1017/PPD-28_Status_Report_Oct_2014.pdf.

Съединените щати разполагат с добре разработени процеси за осигуряване, че дейностите за радиоелектронно разузнаване се осъществяват в изпълнение само на съответни цели в областта на националната сигурност. Ежегодно Президентът определя най-приоритетните задачи за събирането на външноразузнавателна информация, което е резултат от разширен и официален междуведомствен процес. ДНР е отговорен за превръщането на тези приоритети за разузнаването в Рамка на приоритетите в националното разузнаване (*National Intelligence Priorities Framework* (NIPF). С ПИД-28 междуведомственият процес беше укрепен и подобрен, за да гарантира проверка и одобрение на всички разузнавателни приоритети на разузнавателните структури на високо политическо ниво. В Директивата за разузнавателните структури (ДРС) 204 са дадени допълнителни насоки относно NIPF, като тя беше актуализирана през януари 2015 г., за да бъдат включени изискванията съгласно ПИД-28 ([1]). Въпреки че информацията в NIPF е класифицирана, частта, свързана с конкретни външноразузнавателни приоритети на САЩ намира отражение в ежегодната Оценка на световните заплахи, която се изготвя от ДНР и не е класифицирана информация и също така се предоставя на разположение на уебсайта на ODNI.

Приоритетите в NIPF са с доста общ характер. В тях се включват теми, като преследване на ядрени възможности и възможности за балистични ракети на конкретни чужди противници, на влиянието на корупцията в наркокартелите и на нарушаването на човешките права в конкретни държави. Те се прилагат не само за радиоелектронното разузнаване, но и за всички разузнавателни дейности. Организацията, която е отговорна за превръщането на приоритетите в NIPF в реални дейности по събиране на радиоелектронна разузнавателна информация, е Националният комитет по радиоелектронно разузнаване или SIGCOM. Той работи под егидата на директора на Агенцията за национална сигурност (NSA), който е определен съгласно Изпълнителен декрет 12333 за „финансов ръководител на радиоелектронното разузнаване“ и отговаря за надзора и координацията на радиоелектронното разузнаване във всички разузнавателни структури под надзора на Министъра на отбраната и на ДНР. В SIGCOM има представители на всички разузнавателни структури и когато Съединените щати приложат изцяло ПИД-28, ще има представители и на други департаменти и агенции с политически интерес в областта на радиоелектронното разузнаване.

Всички министерства и агенции на САЩ, които са потребители на външноразузнавателна информация, подават искания за събиране до SIGCOM. SIGCOM разглежда тези искания, осигурява те да са в съответствие с NIPF и определя приоритетен ред, като прилага критерии, като:

— Може ли радиоелектронното разузнаване да предостави полезна информация в този случай или има по-добри или икономически по-ефективни източници на информация, за да се отговори на изискването, като обработка на изображения или открити източници?

— Доколко е важна тази потребност от информация? Ако е от голям приоритет в NIPF, тогава най-вероятно ще е от голям приоритет и за радиоелектронното разузнаване.

— Какъв вид радиоелектронно разузнаване може да се използва?

— Събирането съобразено ли е с конкретния случай, доколкото е практически възможно? Трябва ли да има срок, или географски или други ограничения?

Процесът за определяне на изискванията към радиоелектронното разузнаване на САЩ налага също изрично съобразяване и с други фактори, а именно:

— Дали обектът на събирането или методологията, която се използва за това, са особено чувствителни? Ако е така, ще се наложи да бъде направена проверка на високо политическо ниво.

— Дали събирането ще представлява неоправдан риск за неприкосновеността на личния живот и гражданските свободи, независимо от гражданството?

— Необходими ли са допълнителни гаранции за разпространението и запазването, за да бъде защитена неприкосновеността на личния живот или интересите на националната сигурност?

И накрая, в края на процеса обучени служители на NSA вземат приоритетите, които са потвърдени от SIGCOM, провеждат изследвания и определят конкретни критерии за избор, като например телефонни номера или адреси на електронна поща, с които се очаква да бъде събрана външноразузнавателна информация в съответствие с тези приоритети. Всеки критерий за избор трябва да бъде проверен и одобрен преди да се въведе в системите за събиране на информация на NSA. Дори тогава обаче това дали и кога ще се осъществи самото събиране ще зависи донякъде от допълнителни

([1]) *На адрес:* http://www.dni.gov/files/documents/ICD/ICD%20204%20National%20Intelligence%20Priorities%20Framework.pdf.

съображения, като например наличието на подходящи ресурси за събирането. Този процес гарантира, че обектите, за които САЩ събират радиоелектронна разузнавателна информация, отразяват валидни и важни потребности в областта на външното разузнаване. И разбира се, когато събирането се осъществява в съответствие с FISA, NSA и другите агенции трябва да спазват допълнителните ограничения, одобрени от Съда за надзор върху външното разузнаване. Накратко, нито NSA, нито друга разузнавателна агенция на САЩ вземат решения сами относно това каква информация да бъде събирана.

Като цяло този процес гарантира, че всички приоритети на САЩ в областта на разузнаването се определят от отговорни за политическите решения лица на високо ниво, които най-добре могат да определят изискванията във връзка с външноразузнавателните дейности на САЩ, и че тези лица вземат предвид не само потенциалната стойност на събраната разузнавателна информация, но и рисковете, свързани със събирането, за националните икономически интереси и външните отношения, включително рисковете за неприкосновеността на личния живот.

По отношение на данните, предавани на Съединените щати съгласно Щита за личните данни, въпреки че Съединените щати не могат да потвърдят, нито да отрекат, че се прилагат конкретни разузнавателни методи или операции, изискванията, предвидени в ПИД-28 се прилагат за всички операции за радиоелектронно разузнаване, които Съединените щати провеждат, независимо от вида или източника на събираните данни. Освен това ограниченията и гаранциите, които се прилагат за събирането на радиоелектронна разузнавателна информация, се прилагат и за събраната такава информация за всякакви разрешени цели, включително за целите на външните отношения и на националната сигурност.

Разгледаните по-горе процедури доказват ясния ангажимент да бъде предотвратено произволното и безразборно събиране на радиоелектронна разузнавателна информация и да бъде въведен принципът на разумността от най-високите нива на нашето правителство. В ПИД-28 и процедурите на агенциите за изпълнение на тази директива са пояснени новите и съществуващите ограничения и са описани по-конкретно целите, с които Съединените щати събират и използват радиоелектронна разузнавателна информация. Те трябва да дават увереност, че дейностите за радиоелектронно разузнаване са и ще продължат да бъдат осъществявани единствено в изпълнение на легитимни външноразузнавателни цели.

в) **Ограничение за запазването и разпространението**

В раздел 4 от ПИД-28 се поставя изискване всички разузнавателни структури да разполагат с изрично посочени ограничения за запазването и разпространението на личната информация, събрана чрез радиоелектронно разузнаване, на лица, които не са граждани на САЩ, сравними с ограниченията за такава информация за американски граждани. Тези правила са залегнали в процедурите на всяка агенция от разузнавателните структури, които бяха публикувани през февруари 2015 г. и са предоставени за публичен достъп. За да отговаря на условията за запазване или разпространение като външноразузнавателна информация, личната информация трябва да е свързана с разрешено изискване в разузнаването, определено съгласно разгледания по-горе процес във връзка с NIPF; да може основателно да се счита за доказателство за престъпление; или да отговаря на едно от останалите изисквания за запазване на лична информация на граждани на САЩ, определени в Изпълнителен декрет 12333, раздел 2.3.

Информацията, за която не е налице такова определение, не може да бъде запазвана в продължение на повече от пет години, освен с изрично решение на ДНР, че удължаването на срока на запазването е в интерес на националната сигурност на Съединените щати. Следователно разузнавателните структури са задължени да изтриват информация, събрана чрез радиоелектронно разузнаване, за лица, които не са граждани на САЩ, след като изминат пет години от събирането, освен ако е определено например, че информацията е свързана с разрешено изискване за външното разузнаване, или ако ДНР определи, след като се съобрази със становищата на служителя по защита на гражданските свободи към ODNI и на служителите на агенцията, отговарящи за неприкосновеността на личния живот и гражданските свободи, че удължаването на срока на запазването е в интерес на националната сигурност.

Освен това в политиките на всички агенции в изпълнение на ПИД-28 сега е предвидено изрично изискване, че информация за дадено лице не може да бъде разпространявана единствено защото физическото лице не е гражданин на САЩ и ODNI е издала директива, адресирана към всички разузнавателни структури ([1]), за отразяването на това изискване. От служителите в разузнавателните структури специално се изисква да отчитат интересите за неприкосновеност на личния живот на лицата, които не са граждани на САЩ, когато изготвят и разпространяват разузнавателни доклади. По-специално, радиоелектронна разузнавателна информация по отношение на рутинни дейности на чуждестранно лице не може да се счита за външноразузнавателна информация, която може да се разпространява или запазва трайно само по силата на този факт, освен ако по друг начин отговаря на разрешено изискване във връзка с външното разузнаване. С това се признава едно важно ограничение и е в отговор на загрижеността на Европейската комисия относно широкия обхват на определението за външноразузнавателна информация, установено с Изпълнителен декрет 12333.

([1]) Директива за разузнавателните структури 203, на разположение на адрес: http://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf.

г) **Спазване и надзор**

Системата на САЩ за надзор върху външното разузнаване осигурява строг контрол на няколко нива за гарантиране спазването на приложимите закони и процедури, включително на тези, които се отнасят за събирането, запазването и разпространението на информация за лица, които не са граждани на САЩ, придобита чрез радиоелектронно разузнаване, както това е посочено в ПИД-28. Това включва:

— В разузнавателните структури работят стотици служители по надзора. Само в NSAима над 300 души, чиято работа е свързана със спазването на нормите, а други структури също имат служби по надзора. Освен това Министерството на правосъдието осъществява задълбочен надзор над разузнавателните дейности и Министерството на отбраната също извършва надзор.

— Всяка от разузнавателните структури има своя служба на главния инспектор, в чиито отговорности се включва наред с останалите въпроси и упражняването на надзор върху дейностите за външно разузнаване. Главните инспектори са с независим статут, имат широки правомощия да провеждат разследвания, одити и проверки на програмите, включително за измами и злоупотреби или нарушаване на закона, и могат да правят препоръки за корективни мерки. Докато препоръките на главните инспектори са с необвързващ характер, техните доклади често се оповестяват публично и във всички случаи се изпращат на Конгреса; тук се включват и докладите относно последващи действия, когато препоръчаните в предходни доклади корективни мерки още не са изпълнени. По този начин Конгресът е информиран за всяко неспазване и може да упражни натиск за изпълнението на корективните действия, включително чрез бюджетни механизми. До редица доклади на главни инспектори във връзка с разузнавателни програми беше предоставен публичен достъп ([1]).

— Службата за гражданските свободи и неприкосновеността на личния живот към ODNI (*Civil Liberties and Privacy Office*) (CLPO) има задължението да гарантира, че разузнавателните структури работят по начин, който повишава националната сигурност, като същевременно защитава гражданските свободи и правата на неприкосновеност на личния живот ([2]). Други разузнавателни структури имат свои служители по въпросите на неприкосновеността на личния живот.

— Надзорният съвет по въпросите на неприкосновеността на личния живот и гражданските свободи (*Privacy and Civil Liberties Oversight Board*) (PCLOB) е независим орган, създаден със закон и натоварен със задачата да извършва анализ и преглед на програмите и политиките за противодействие на тероризма, включително използването на радиоелектронно разузнаване, с цел да гарантира, че се осигурява адекватна защита на неприкосновеността на личния живот и гражданските свободи. Той е публикувал няколко обществено достъпни доклада за дейността на разузнаването.

— Както ще бъде разгледано по-подробно по-нататък, Съдът за надзор върху външното разузнаване е със състав от независими федерални съдии и отговаря за спазването на изискванията и надзора по отношение на всички дейности по събиране на радиоелектронна разузнавателна информация, извършвани съгласно FISA.

— И накрая, Конгресът на САЩ, и по-специално комисията по въпросите на разузнаването и правната комисия към Камарата на представителите и Сената, имат важни надзорни отговорности по отношение на всички външноразузнавателни дейности на САЩ, включително радиоелектронното разузнаване.

Освен тези официални надзорни механизми, разузнавателните структури имат изградени множество механизми за осигуряване спазването от тяхна страна на ограниченията върху събирането на информация, разгледани по-горе. Например:

— От високопоставените правителствени служители се изисква ежегодно да потвърждават валидността на своите изисквания във връзка с външното разузнаване.

— NSAпроверява обектите на радиоелектронно разузнаване през целия процес на събиране на данни, за да определи дали наистина осигуряват ценна външноразузнавателна информация в съответствие с приоритетите, и преустановява събирането на данни във връзка с обекти, които не осигуряват такава информация. С допълнителни процедури се гарантира периодичното преразглеждане на критериите за избор.

([1]) Вж. напр. доклада на главния инспектор на Министерството на правосъдието на САЩ „Преглед на дейността на Федералното бюро за разследвания съгласно раздел 702 от Закона за надзор върху външното разузнаване от 2008 г.“ (A Review of the Federal Bureau of Investigation's Activities Under Section 702 of the Foreign Intelligence Surveillance Act of 2008) от септември 2012 г., на разположение на адрес: https://oig.justice.gov/reports/2016/o1601a.pdf.

([2]) Вж. www.dni.gov/clpo.

— Въз основа на препоръка от независима надзорна група, назначена от Президента Обама, ДНР създаде нов механизъм за контрол на събирането и разпространението на радиоелектронна разузнавателна информация, която е с особено чувствителен характер поради естеството на обекта или средствата за събирането, за да се гарантира, че това е съобразено с решенията на отговорните за политическите решения лица.

— И накрая, ODNI прави ежегоден преглед на разпределението на ресурсите в разузнавателните структури според приоритетите в NIPF и разузнавателната мисия като цяло. Този преглед включва оценки на стойността на всички видове събрана разузнавателна информация, включително радиоелектронна, както и преценка за това, доколко разузнавателните структури са успели да постигнат целите си и от какво ще се нуждаят за в бъдеще. Това е гаранция, че ресурсите за радиоелектронно разузнаване се използват за най-значимите национални приоритети.

Както се вижда от този обстоен общ преглед, разузнавателните структури не решават сами кои разговори да подслушват, не се опитват да събират всякаква информация и не работят без надзор. Дейностите им са съсредоточени върху приоритетите, определени от създателите на политики чрез процес, в който участва цялото правителство и върху който се осъществява надзор, както в рамките на NSA, така и от ODNI, Министерството на правосъдието и Министерството на отбраната.

В ПИД-28 се съдържат също така и множество други разпоредби за гарантиране, че събраната в хода на радиоелектронно разузнаване лична информация е защитена, независимо от националността. Например в ПИД-28 са предвидени процедури за сигурността на данните, достъпа и качеството, за да бъде защитена събраната в хода на радиоелектронно разузнаване лична информация, както и задължително обучение за гарантиране, че служителите разбират отговорността за защита на личната информация, независимо от националността на лицата. Също така в ПИД-28 са предвидени допълнителни механизми за надзор и спазване. Към тях спадат периодичният одит и прегледи от страна на съответните длъжностни лица по спазването и надзора на практиките за защита на личната информация, съдържаща се в радиоелектронната разузнавателна информация. Прегледите трябва също така да направят оценка на спазването от страна на агенциите на процедурите за защита на тази информация.

Освен това в ПИД-28 е предвидено значими проблеми със спазването във връзка с лица, които не са граждани на САЩ, да бъдат решавани на по-високи нива в правителството. Когато възникне значим проблем със спазването, в който се засяга лична информация на което и да е лице, събрана в резултат от радиоелектронни разузнавателни дейности, въпросът задължително се докладва освен по реда на съществуващите изисквания за докладване, и своевременно на ДНР. Ако проблемът засяга лична информация на лице, което не е гражданин на САЩ, ДНР, в консултация с Държавния секретар и с ръководителя на съответната разузнавателна структура, определят дали трябва да бъдат предприети стъпки за уведомяване на съответното чуждо правителство, като се спазват изискванията относно защитата на източниците и методите и на служителите на САЩ. Освен това, както е указано в ПИД-28, Държавният секретар е определил висш правителствен служител, Заместник държавния секретар Catherine A. Novelli, да изпълнява функциите на лице за връзка с чуждите правителства, които желаят да изразят безпокойство във връзка с дейностите за радиоелектронно разузнаване на Съединените щати. Този ангажимент на високо ниво е пример за усилията, които правителството на САЩ прави през изминалите няколко години да вдъхне доверие към многобройните и припокриващи се защити за неприкосновеността на личния живот, които са изградени за личната информация на американските граждани и на лицата, които не са граждани на САЩ.

д) **Обобщение**

Процесите в Съединените щати за събиране, запазване и разпространение на външноразузнавателна информация предвиждат важни защити за неприкосновеността на личния живот по отношение на личната информация на всички лица, независимо от тяхното гражданство. По-специално с тези процеси се гарантира, че нашите разузнавателни структури се съсредоточават върху своята мисия за национална сигурност, така както тя е определена в приложимите закони, изпълнителни декрети и президентските директиви; защитават информацията от неразрешен достъп, употреба и разкриване, и осъществяват дейността си под контрол и надзор на няколко равнища, включително на надзорните комисии в Конгреса. ПИД-28 и процедурите за нейното изпълнение са израз на нашите усилия да разширим свеждането до минимум и някои други съществени принципи на защитата на данни също и за личната информация на всички лица, независимо от тяхното гражданство. За личната информация, получена при осъществяваното от САЩ събиране на радиоелектронни разузнавателни данни, се прилагат принципите и изискванията съгласно правото на САЩ и президентските директиви, включително защитата, предвидена в ПИД-28. Тези принципи и изисквания са гаранция, че всички лица се третират по достоен начин и с уважение, независимо от тяхното гражданство или местопребиваването им, и са признание за това, че всички лица имат законни интереси за неприкосновеност на личния живот при обработването на тяхна лична информация.

II. ЗАКОН ЗА НАДЗОР ВЪРХУ ВЪНШНОТО РАЗУЗНАВАНЕ — РАЗДЕЛ 702

Съгласно раздел 702 от Закона за надзор върху външното разузнаване ([1]) събирането не е „масово и безразборно“, а тясно съсредоточено върху събирането на външноразузнавателна информация от индивидуално идентифицирани съгласно закона обекти; то е разрешено по ясен начин в изрични законови разпоредби; и подлежи едновременно на независим съдебен контрол и на задълбочен преглед и надзор в рамките на изпълнителните органи и Конгреса. Събирането съгласно раздел 702 се счита за радиоелектронно разузнаване, при условие че отговаря на изискванията на ПИД-28 ([2]).

Събирането съгласно раздел 702 е един от най-ценните източници на разузнавателна информация за защитата както на Съединените щати, така и на европейските ни партньори. Подробна информация относно функционирането и надзора съгласно раздел 702 е предоставена за публичен достъп. Множество разсекретени съдебни дела, съдебни решения и надзорни доклади във връзка с програмата са публикувани и предоставени на разположение на уебсайта на ODNI за публичен достъп на адрес: www.icontherecord.tumblr.com. Освен това Надзорният съвет по въпросите на неприкосновеността на личния живот и гражданските свободи (PCLOB) направи обстоен анализ на прилагането на раздел 702 в доклад, който е на разположение на адрес: https://www.pclob.gov/library/702-Report.pdf ([3]).

Раздел 702 беше приет като част от Закона за изменение на FISA от 2008 г. ([4]), след задълбочени публични обсъждания в Конгреса. С него се разрешава придобиването на външноразузнавателна информация чрез целево събиране от лица, които не са граждани на САЩ и с местонахождение извън САЩ, при задължително съдействие от страна на доставчиците на електронни далекосъобщителни услуги в САЩ. С раздел 702 се упълномощават Министърът на правосъдието и ДНР — служители на министерско равнище, определени от Президента с одобрението на Сената — да подават ежегодно заявление за сертифициране до Съда за надзор върху външното разузнаване ([5]). С това сертифициране се определят конкретни категории външноразузнавателна информация, която да бъде събирана, като например разузнавателна информация, свързана с противодействие на тероризма или оръжия за масово унищожение, която трябва да отговаря на изискванията за категориите външноразузнавателна информация, така както те са определени в FISA ([6]). Както отбелязва PCLOB, „тези ограничения не разрешават неограниченото събиране на информация за чужденци“ ([7]).

Също така се изисква в сертифицирането да бъдат включени процедури за целево събиране и за свеждане до минимум, които трябва да бъдат проверени и одобрени от Съда за надзор върху външното разузнаване ([8]). Процедурите за целево събиране са предназначени да гарантират, че събирането ще се извършва само както това е разрешено по закон и в обхвата на сертифицирането; процедурите за свеждане до минимум са предназначени да се ограничи придобиването, разпространението и запазването на информация за американски граждани, но съдържат и разпоредби, с които се осигурява значителна степен на защита на информацията също и за лица, които не са американски граждани, както това е разгледано по-нататък. Освен това, както е разгледано по-горе, в ПИД-28 Президентът даде указания разузнавателните структури да предоставят допълнителна защита за личната информация на лица, които не са американски граждани, и тази защита се прилага за информацията, събрана съгласно раздел 702.

След като съдът одобри процедурите за целево събиране и за свеждане до минимум, събирането съгласно раздел 702 не е общо или безразборно, а „се състои изцяло от целенасочено разследване на конкретни лица, за които е направено индивидуализирано определяне“, както е посочено от PCLOB ([9]). Събирането е целево, като се използват конкретни критерии за избор, като например адреси на електронна поща или телефонни номера, за които служителите на разузнаването на САЩ

([1]) 50 U.S.C. § 1881a.

([2]) Също така в Съединените щати могат да бъдат издадени съдебни разпореждания съгласно други разпоредби на FISA за получаването на данни, включително лични данни, предавани съгласно Щита за личните данни. Вж. 50 U.S.C. § 1801 *et seq*. В дялове I и III от FISA, в които се разрешават съответно електронното наблюдение и физическото претърсване, се изисква съдебно разпореждане (освен при спешни обстоятелства) и винаги се изисква правдоподобна причина в уверение на това, че обектът на разузнаване е чужда сила или агент на чужда сила. В дял IV от FISA се разрешава използването на електронни устройства за регистриране и проследяване в разрешени външноразузнавателни дейности, контраразузнавателни дейности или разследвания за противодействие на тероризма, съгласно издадено съдебно разпореждане (освен при спешни обстоятелства). В дял V от FISA се разрешава на ФБР да получават търговски справки, отнасящи се за разрешени външноразузнавателни дейности, контраразузнавателни дейности или разследвания за противодействие на тероризма, съгласно издадено съдебно разпореждане (освен при спешни обстоятелства). Както ще бъде разгледано по-нататък, със Закона за свободата в САЩ (*USA FREEDOM Act*) конкретно се забранява използването на разпорежданията съгласно FISA за електронни устройства за регистриране или за търговски справки за целите на събиране на масиви от данни и се поставя изискване за „конкретен критерий за избор“, за да се гарантира, че тези правомощия се прилагат целенасочено.

([3]) Доклад относно програмата за наблюдение, функционираща съгласно раздел 702 от Закона за надзор върху външното разузнаване („Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act“) от 2 юли 2014 г., („доклад на PCLOB“).

([4]) *Вж.* Pub. L. № 110-261, 122 Stat. 2436 (2008).

([5]) *Вж.* 50 U.S.C. § 1881a(a) и (b).

([6]) Вж. пак там § 1801(e).

([7]) Вж. доклада на PCLOB, стр. 99.

([8]) *Вж.* 50 U.S.C. § 1881a(d) и (e).

([9]) Вж. доклада на PCLOB, стр. 111.

са определили, че може да се счита, че се използват за предаване на външноразузнавателна информация от вида, определен при сертифицирането, за което е подадено заявление в съда ([1]). Основанието за избора на обект задължително се документира и впоследствие документите за всеки критерий за избор се проверяват от Министерството на правосъдието ([2]). Правителството на САЩ публикува в информация, че през 2014 г. се е осъществявало целево разследване съгласно раздел 702 на приблизително 90 000 физически лица, което е съвсем малка част от всичките над 3 милиарда потребители на интернет в света ([3]).

Събраната информация съгласно раздел 702 подлежи на одобрените от съда процедури за свеждане до минимум, с които се осигурява защита на информацията за лица, които не са американски граждани, така както и за американските граждани, и които са обявени публично ([4]). Например комуникационни данни, придобита съгласно раздел 702, независимо дали от американски граждани или от лица, които не са американски граждани, се съхранява в бази данни със строг контрол на достъпа. Такива данни могат да се разглеждат само от служителите на разузнаването, които са обучени за процедурите за свеждане до минимум с цел защита на неприкосновеността на личния живот и които са получили специално одобрение за този достъп, за да изпълняват функциите, за които са упълномощени ([5]). Използването на данните се ограничава до идентифицирането на външноразузнавателна информация или доказателство за престъпление ([6]). Съгласно ПИД-28 тази информация може да се разпространява само ако е налице валидна цел във връзка с външното разузнаване или правоприлагането; само фактът, че едната страна в комуникацията не е лице, гражданин на САЩ, не е достатъчен ([7]). С процедурите за свеждане до минимум, както и в ПИД-28, се определят също и ограничения за продължителността на запазване на данните, придобити съгласно раздел 702 ([8]).

Надзорът над изпълнението на раздел 702 е засилен и се осъществява от всяка от трите власти на нашето правителство. В агенциите, които прилагат закона, има няколко нива на вътрешен контрол, включително независими главни инспектори, както и технологичен контрол върху достъпа до данните. Министерството на правосъдието и ODNI строго следят и проверяват как се прилага раздел 702, за да контролират спазването на законовите правила; също така агенциите имат самостоятелното задължение да докладват за потенциални случаи на неспазване. Такива случаи се разследват и всички случаи на неспазване се докладват на Съда за надзор върху външното разузнаване, Надзорния съвет по въпросите на разузнаването към Президента и на Конгреса, като се вземат съответните мерки за отстраняване на нарушенията ([9]). Досега няма случаи на целенасочен опит за нарушаване на закона или за заобикаляне на законовите изисквания ([10]).

Съдът за надзор върху външното разузнаване има важна роля за прилагането на раздел 702. В състава му влизат независими федерални съдии със седемгодишен мандат в този съд, които обаче, както всички федерални съдии, са с пожизнено назначение като съдии. Както беше отбелязано, съдът задължително проверява дали са спазени законовите изисквания при годишните сертифицирания и процедурите за целево следене и за свеждане до минимум. Освен това, както също вече беше отбелязано, от правителството се изисква да уведомява съда незабавно при проблеми със спазването ([11]), а няколко решения на съда, които вече бяха разсекретени и обявени публично, показват изключително високия съдебен контрол и независимостта, която той упражнява при разглеждането на такива случаи.

Взискателните процеси на съда бяха описани от предишния съдия председател в писмо до Конгреса, което беше публикувано за широката общественост ([12]). А по силата на Закона за свободата в САЩ, разгледан по-нататък, сега съдът е изрично упълномощен да назначава външен юрист като независим защитник по въпроси на неприкосновеността на личния живот по дела, които представляват нови или значими юридически казуси ([13]). Тази степен на ангажираност от страна на независимата съдебна система на една държава с външноразузнавателни дейности, насочена към лица, които не са граждани на тази държава и са с местонахождение извън нея, е необичайна, и дори безпрецедентна и спомага за гарантирането, че събирането на информация съгласно раздел 702 се осъществява в рамките на съответните законови ограничения.

([1]) *пак там*

([2]) Пак там, стр. 8; 50 U.S.C. § 1881a(l); вж. също доклада на директора на Службата за гражданските свободи и неприкосновеността на личния живот към АНС: Изпълнение от страна на АНС на раздел 702 от Закона за надзор върху външното разузнаване (по-нататък наричан „доклад на АНС“) на стр. 4, на разположение на адрес: http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.

([3]) Директор на Националното разузнаване, Доклад за прозрачност за 2014, на разположение на адрес: http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014.

([4]) Процедурите за свеждане до минимум са на разположение на адрес: http://www.dni.gov/files/documents/ppd-28/2014%20NSA%20702%20Minimization%20Procedures.pdf („Процедури на АНС за свеждане до минимум“) (*NSA Minimization Procedures*); http://www.dni.gov/files/documents/ppd-28/2014%20FBI%20702%20Minimization%20Procedures.pdf; и http://www.dni.gov/files/documents/ppd-28/2014%20CIA%20702%20Minimization%20Procedures.pdf.

([5]) Вж.доклада на АНС на стр. 4.

([6]) Вж. например процедурите на АНС за свеждане до минимум, стр. 6.

([7]) Процедурите на разузнавателните агенции съгласно ПИД-28 са на разположение на адрес: http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.

([8]) Вж. процедурите на АНС за свеждане до минимум; раздел 4 от ПИД-28.

([9]) *Вж.* 50 U.S.C. § 1881(l); вж. също доклада на PCLOB на стр. 66—76.

([10]) Вж. Оценка за полугодието на въпросите във връзка със спазването на процедурите и насоките съгласно раздел 702 от Закона за надзор върху външното разузнаване, изготвена от Министъра на правосъдието и директора на Националното разузнаване, стр. 2—3, на разположение на адрес: http://www.dni.gov/files/documents/Semiannual%20Assessment%20of%20Compliance%20with%20procedures%20and%20guidelines%20issued%20pursuant%20to%20Sect%20702%20of%20FISA.pdf.

([11]) Правило 13 от процедурния правилник на Съда за надзор върху външното разузнаване, на разположение на адрес: http://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf.

([12]) 29 юли 2013 г., Писмо от уважаемия Reggie B. Walton до уважаемия Patrick J. Leahy, на разположение на адрес: http://fas.org/irp/news/2013/07/fisc-leahy.pdf.

([13]) Вж. раздел 401 от Закона за свободата в САЩ, P.L. 114-23.

Конгресът осъществява надзор посредством изисквани по закон доклади до комисията по въпросите на разузнаването и правната комисия, както и чести брифинги и изслушвания. Тук се включва докладът за полугодието на Министъра на правосъдието за документиране прилагането на раздел 702 и евентуални случаи на неспазване ([1]); отделна шестмесечна оценка на Министъра на правосъдието и ДНР за документиране спазването на процедурите за целево събиране и свеждане до минимум, включително спазването на процедурите, предвидени за гарантиране, че събирането се извършва за валидна цел на външното разузнаване ([2]); и годишен доклад на ръководителите на разузнавателните структури, в който се включва удостоверяване, че събирането на информация съгласно раздел 702 все още осигурява външноразузнавателна информация ([3]).

Накратко, събирането на информация съгласно раздел 702 е разрешено по закон; подлежи на проверка, съдебен контрол и надзор на няколко нива; и, както постанови Съдът за надзор върху външното разузнаване в едно наскоро разсекретено решение, не „се извършва общо или безразборно“, а „чрез … отделни решения за целево определяне на индивидуални [комуникационни] съоръжения“ ([4]).

III. ЗАКОН ЗА СВОБОДАТА В САЩ

Със Закона за свободата в САЩ, промулгиран през юни 2015 г., бяха внесени значителни промени в надзорните правомощия в САЩ и други правомощия в областта на националната сигурност, като беше повишена прозрачността за обществеността относно прилагането на тези правомощия и относно решенията на Съда за надзор върху външното разузнаване, както това е разгледано по-нататък ([5]). С този закон се гарантира, че нашите професионалисти в областта на разузнаването и правоприлагането ще разполагат с необходимите правомощия за защитата на нацията, като едновременно с това се гарантира подходяща защита за неприкосновеността на личния живот на физическите лица, когато се прилагат тези правомощия. С това се подобряват неприкосновеността на личния живот и гражданските свободи и се повишава прозрачността.

Със закона се забранява събиране на масиви от каквато и да било информация, включително за американски граждани и за лица, които не са граждани на САЩ, по силата на различни разпоредби на FISA или посредством писмо във връзка с националната сигурност, което е вид разрешено по закон административно разпореждане ([6]). Тази забрана включва по-специално метаданни за телефонни разговори, отнасящи се за обаждания между лица на територията на САЩ и лица извън САЩ, като тук се включва също събирането на информация съгласно Щита за личните данни по силата на тези законови правомощия. Със закона се поставя изискване към правителството да обосновава всяко заявление за информация съгласно тези правомощия чрез „специален критерий за избор“ — понятие, което определя по специфичен начин дадено лице, профил, адрес или персонално устройство, така че да бъде ограничен в максимално възможната разумна и допустима степен обхватът на исканата информация ([7]). С това освен това се гарантира, че събирането на информация за целите на разузнаването е прецизно насочено и целево.

Със закона бяха внесени също и съществени изменения в производствата пред Съда за надзор върху външното разузнаване, с които се повишава прозрачността и се дават допълнителни гаранции, че неприкосновеността на личния живот ще бъде защитена. Както беше отбелязано, с него беше разрешено създаването на постоянна група от юристи с разрешение за достъп до класифицирана информация, специализирали в областта на неприкосновеността на личния живот и гражданските свободи, събирането на разузнавателна информация, комуникационните технологии или други подходящи сфери, които могат да бъдат определени да се явят в съда в качеството на *amicus curiae* по дела, в които се дава ново или съществено тълкуване на закона. Тези юристи са с правомощия да привеждат правни аргументи в защита на неприкосновеността на личния живот и гражданските свободи и имат достъп до всякаква информация, за която съдът определи, че е необходима за изпълнение на задълженията им, включително класифицирана ([8]).

Също така със закона се доизгражда безпрецедентната прозрачност на действията на правителството на САЩ в областта на разузнавателните дейности, като се определя изискване към ДНР, в консултация с Министъра на правосъдието, да декласифицира или публикува обобщение, което не съдържа класифицирана информация, на всяко решение, разпореждане или становище, постановено от Съда за надзор върху външното разузнаване или апелативен съд за надзор на външното разузнаване, в което се съдържат значими конструкции или тълкувания на някоя законова разпоредба.

([1]) *Вж.* 50 U.S.C. § 1881f.
([2]) Вж. пак там § 1881a(l)(1).
([3]) Вж. пак там § 1881a(l)(3). Някои от тези доклади са класифицирана информация.
([4]) Запис на решението и разпореждането, стр. 26 (FISC 2014 г.), на разположение на адрес: http://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf.
([5]) *Вж.* Закон за свободата в САЩ от 2015 г., Pub. L. № 114-23, § 401, 129 Stat. 268.
([6]) Вж. пак там §§ 103, 201, 501. Писмата във връзка с националната сигурност са уредени в различни закони и позволяват на ФБР да събира информация, съдържаща се в справки за кредити, финансови справки и електронни регистри на абонати и на трансакции от определен вид дружества, единствено за защита срещу международния тероризъм или секретни разузнавателни дейности. *Вж.* 12 U.S.C. § 3414; 15 U.S. C. §§ 1681u-1681v; 18 U.S.C. § 2709. Писмата във връзка с националната сигурност обикновено се използват от ФБР за събиране на важна информация, която не се отнася за съдържание, на ранен етап от разследвания в сферата на противодействието на тероризма и контраразузнаването, например самоличност на абонат на профил, който може да е бил във връзка с членове на терористична група, като Даеш. Получателите на писма във връзка с националната сигурност имат право да ги обжалват в съда. *Вж.* 18 U.S.C. § 3511;
([7]) *Вж. пак там*,.
([8]) Вж. пак там § 401.

Освен това в закона се предвижда подробно разкриване на информация относно събиране на данни съгласно FISA и искания за писма във връзка с националната сигурност. Правителството на Съединените щати трябва да разкрива ежегодно пред Конгреса и обществеността броя на заповедите и поисканите и получени сертифицирания съгласно FISA, изчисления за броя на американските граждани и лицата, които не са граждани на САЩ, които са били обект и са били засегнати от наблюдение, както и броя на определените *amici curiae*, наред с други видове информация ([1]). Също така със закона се изисква от правителството допълнително да докладва пред обществеността относно броя на поисканите писма във връзка с националната сигурност по отношение на американски граждани и на лица, които не са граждани на САЩ ([2]).

По отношение на корпоративната прозрачност в закона се дават редица възможности на дружествата да докладват публично за общия брой заповеди и указания съгласно FISA или писма във връзка с националната сигурност, които са получили от правителството, както и броя на потребителските профили, които са били предмет на тези заповеди ([3]). Няколко дружества вече разкриха такава информация и тя показва, че броят на клиентите, чиято информация е била обект на търсене, е ограничен.

Тези доклади за корпоративната прозрачност доказват, че исканията за целите на разузнаването в САЩ засягат само малка част от информацията. Например един наскоро публикуван доклад за прозрачността на едно от големите дружества показва, че то е получило искания в областта на националната сигурност (съгласно FISA или писма във връзка с националната сигурност), с които са били засегнати по-малко от 20 000 от профилите в момент, когато дружеството е имало поне 400 милиона регистрирани абоната. С други думи всички искания във връзка с националната сигурност на САЩ, за които съобщава това дружество, са засегнали по-малко от 0,005 % от абонатите му. Дори ако всяко от тези искания засягаше данни съгласно Щита за личните данни, което разбира се не е така, очевидно е, че исканията са целеви и съобразени по мащаб, и не са нито за събиране на масиви от данни, нито за безразборно събиране.

И накрая, въпреки че със законовите разпоредби, с които се разрешава издаването на писма във връзка с националната сигурност, се ограничават обстоятелствата, при които се забранява на получател на такова писмо да го разкрива, в закона се предвижда допълнително тези изисквания за неразкриване да подлежат на задължителен периодичен преглед; получателите на писма във връзка с националната сигурност да бъдат уведомени кога фактите, на които се основава изискването за неразкриване повече не са налице; и се кодифицират процедурите за обжалване от получателите на изискването за неразкриване ([4]).

В обобщение, важните изменения в правомощията в областта на разузнаването в САЩ, внесени със Закона за свободата, са ясно доказателство за големите усилия, които полагат Съединените щати да поставят на преден план във всички практики в разузнаването на САЩ защитата на личната информация, неприкосновеността на личния живот, гражданските свободи и прозрачността.

IV. ПРОЗРАЧНОСТ

В допълнение към прозрачността, която се изисква съгласно Закона за свободата в САЩ, разузнавателните структури предоставят на обществеността много допълнителна информация, с което дават много добър пример във връзка с прозрачността за разузнавателната си дейност. Разузнавателните структури публикуват много от своите политики, процедури, решения на Съда за надзор върху външното разузнаване и други материали, които не са класифицирана информация, като осигуряват изключително висока степен на прозрачност. Освен това значително се увеличи разкриването на статистическа информация за използването от страна на правителството на правомощията за събиране на информация за целите на националната сигурност. На 22 април 2015 г. разузнавателните структури публикуваха втория си годишен доклад със статистически данни за това колко често правителството използва тези важни правомощия. ODNI също публикува на уебсайта си и на специалния уебсайт *IC On the Record* набор от конкретни принципи за прозрачност ([5]) и план за изпълнение, в който тези принципи са заложени в конкретни измерими инициативи ([6]). През октомври 2015 г. директорът на Националното разузнаване даде указания към всяка разузнавателна агенция да определи служител по прозрачността на разузнаването в рамките на ръководството, който да съдейства за повишаване на прозрачността и да ръководи инициативите за прозрачност ([7]). Служителят по прозрачността ще работи в тясно взаимодействие със служителите на всяка разузнавателна агенция, отговарящи за неприкосновеността на личния живот и гражданските свободи, за гарантиране запазването на първостепенното значение на прозрачността, неприкосновеността на личния живот и гражданските свободи.

([1]) Вж. пак там § 602.
([2]) *Вж. пак там.*
([3]) Вж. пак там § 603.
([4]) Вж. пак там §§ 502(f)–503.
([5]) *На разположение на адрес:* http://www.dni.gov/index.php/intelligence-community/intelligence-transparency-principles.
([6]) *На разположение на адрес:* http://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/Principles%20of%20Intelligence%20Transparency%20Implementation%20Plan.pdf.
([7]) Вж. пак там.

Като пример за тези усилия, през изминалите няколко години главният служител на NSAпо въпросите на неприкосновеността на личния живот и гражданските свободи публикува няколко доклада, които не съдържат класифицирана информация, включително докладите за дейностите съгласно раздел 702, Изпълнителен декрет 12333 и Закона за свободата в САЩ ([1]). Освен това разузнавателните структури работят в тясно взаимодействие с Надзорния съвет по въпросите на неприкосновеността на личния живот и гражданските свободи, Конгреса и защитниците на неприкосновеността на личния живот в САЩ, за да се осигури допълнителна прозрачност във връзка с разузнавателните дейности на САЩ, когато това е практически осъществимо и в съответствие с изискванията за защита на разузнавателните източници и методи с чувствителен характер. Като цяло прозрачността за разузнавателните дейности на САЩ е също толкова висока или по-висока от тази на всяка друга нация в света и в степента, която позволява да бъде съобразена с необходимостта за защита на източниците и методите с чувствителен характер.

В обобщение на високата прозрачност, която е налице за разузнавателните дейности на САЩ:

— Разузнавателните структури са публикували и предоставили на разположение онлайн хиляди страници със становища на съда и процедури на агенциите, в които са очертани специфичните процедури и изисквания за нашите разузнавателни дейности. Също така сме публикувани доклади за спазването на приложимите ограничения от страна на разузнавателните агенции.

— Висши служители в разузнаването редовно говорят пред обществеността за ролята и дейността на своите организации, включително с описание на режимите за спазване на изискванията и гаранциите, от които се ръководят в работата си.

— Разузнавателните структури са публикували и множество допълнителни документи относно разузнавателните дейности съгласно Закона за свобода на информацията.

— Президентът издаде ПИД-28, като определи пред обществеността допълнителни ограничения за нашите разузнавателни дейности, а ODNI е издала два доклада за публичен достъп относно изпълнението на тези ограничения.

— Сега от разузнавателните структури се изисква по закон да оповестяват значими правни становища на Съда за надзор върху външното разузнаване или обобщения на тези становища.

— От правителството се изисква да докладва ежегодно за степента, в която използва някои от своите правомощия в областта на националната сигурност и дружествата също имат такова право.

— Надзорният съвет по въпросите на неприкосновеността на личния живот и гражданските свободи публикува няколко подробни доклада относно разузнавателните дейности и ще продължи да прави това.

— Разузнавателните структури предоставят голям обем класифицирана информация на надзорните комисии в Конгреса.

— ДНР издаде принципи за прозрачност, от които да се ръководят дейностите на разузнавателните структури.

Тази висока прозрачност ще продължи да се прилага и в бъдеще. Всяка информация, която се публикува за обществен достъп, ще бъде предоставена, разбира се, и на Министерството на търговията и Европейската комисия. Годишният преглед, който Министерството на търговията и Европейската комисия ще извършват относно изпълнението на Щита за личните данни, ще даде възможност на Европейската комисия да обсъди всички въпроси, възникнали във връзка с публикувана нова информация, както и други такива във връзка с Щита за личните данни и неговото функциониране, и разбираме, че по своя преценка министерството може да покани за участие в този преглед и представители на други агенции, включително на разузнавателните структури. Това, разбира се, е в допълнение към механизма, предвиден в ПИД-28, според който държавите — членки на ЕС, могат да изразят загриженост във връзка с дейностите по надзор пред определения висш служител на Държавния департамент.

V. СРЕДСТВА ЗА ПРАВНА ЗАЩИТА

Правото на САЩ осигурява редица възможности за правна защита на физическите лица, когато са станали обект на неправомерно електронно наблюдение за целите на националната сигурност. Съгласно FISA правото да се търси решение по жалба в съда в САЩ не е ограничено само за американските граждани. Физическо лице, което може да обоснове иск да заведе дело се ползва със средства за правна защита срещу неправомерно електронно наблюдение съгласно FISA.

([1]) *На разположение на адрес:* https://www.nsa.gov/civil_liberties/_files/nsa_report_on_section_702_program.pdf; https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf; https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf.

Например в FISA се предвижда лицата, които са станали обект на неправомерно електронно наблюдение, да могат да заведат дело срещу длъжностни лица от правителството на САЩ, в качеството им на частни лица, за финансови щети, включително за наказателни обезщетения и компенсиране на разноските по адвокатски хонорари. *Вж.* 50 U.S.C. § 1810; Физическите лица, които имат основания да заведат дело, могат също така да предявят граждански иск за обезщетение за финансови щети срещу Съединените щати, включително за разходите, свързани с процеса, когато информацията за тях, придобита чрез електронно наблюдение съгласно FISA, е била неправомерно и умишлено използвана или разкрита. *Вж.* 18 U.S.C. § 2712; В случай, че правителството възнамерява да използва или разкрие информация, получена или производна от електронно наблюдение на засегнатото лице съгласно FISA, срещу това лице в съдебни или административни производства в Съединените щати, правителството трябва да уведоми предварително за това си намерение съда и лицето, което тогава може да предяви иск срещу законността на наблюдението и да иска забрана на информацията. *Вж.* 50 U.S.C. § 1806; И накрая, в FISA се предвиждат също така наказателни санкции за физическите лица, които умишлено извършват неправомерно електронно наблюдение под прикритието на закона или които умишлено използват или разкриват информация, получена от неправомерно наблюдение. *Вж.* 50 U.S.C. § 1809;

Гражданите на ЕС имат други възможности да търсят правна защита срещу длъжностни лица от правителството на САЩ за неправомерно използване или достъп от страна на правителството до данни, включително срещу длъжностни лица, които нарушават закона в хода на неправомерен достъп или използване на информация за претендирани цели на националната сигурност. Съгласно Закона за компютърните измами и злоупотреби (*Computer Fraud and Abuse Act*) се забранява умишленият неразрешен достъп (или превишаването на правомощията за достъп) с цел придобиване на информация от финансови институции, от компютърна система на правителството на САЩ или от компютър, до който има достъп през интернет, както и заплахите за увреждане на защитени компютри с цел изнудване или измама. *Вж.* 18 U.S.C. § 1030; Всяко лице, независимо от гражданството му, което понесе вреди или загуби поради нарушаване на този закон, може да заведе дело срещу нарушителя (включително срещу длъжностно лице от правителството) за обезщетение за вредите и за мерки за прекратяване или други равностойни мерки съгласно раздел 1030(g), независимо дали е предприето наказателно преследване, при условие че виновното действие е свързано с поне едно от няколко обстоятелства, определени в закона. Законът за неприкосновеност на електронните съобщения (*Electronic Communications Privacy Act* (ECPA)) урежда достъпът от страна на правителството до съхранени електронни съобщения и справки за трансакции, както и информация за абонатите, с които разполагат доставчици на електронни съобщителни услуги в качеството им на трета страна.*Вж.* 18 U.S.C. §§ 2701-2712. С този закон се дава право на засегнато физическо лице да заведе дело срещу длъжностно лице от правителството за умишлен неправомерен достъп до съхранени данни. Законът се прилага за всички лица, независимо от гражданството им, и засегнатите физически лица могат да получат обезщетение за вреди и за компенсиране на разноските за адвокатски хонорари. Законът за правото на неприкосновеност на личните финанси (*Right to Financial Privacy Act* (RFPA)) ограничава достъпа на правителството на САЩ до банкова и брокерско-дилърска информация за отделни клиенти. *Вж.* 12 U.S.C. §§ 3401-3422. Съгласно този закон клиент на банка, брокер или дилър, може да заведе дело срещу правителството на САЩ за законоустановени и наказателни обезщетения и за обезщетения за действително претърпени вреди поради виновно получаване на достъп до справки за клиента, а ако в съдебното решение се констатира, че това виновно поведение е било умишлено, автоматично се задейства разследване за налагане на евентуално дисциплинарно наказание на съответните правителствени служители. *Вж.* 12 U.S.C. § 3417;

И накрая, в Закона за свобода на информацията (FOIA) се предвиждат средства за всяко физическо лице да може да поиска достъп до налични регистри на федералните агенции по всякакви теми, освен ако не се прилагат някои категории изключения. *Вж.* 5 U.S.C. § 552(b). Към тях се включват ограниченията за достъпа до класифицирана информация относно националната сигурност, лична информация на други физически лица и информация със връзка с разследвания в правоприлагането, като тези ограничения са сравними с налаганите от държавите в техните закони за достъп до информацията. Те се прилагат еднакво за американски граждани и за лица, които не са граждани на САЩ. Споровете във връзка с предоставяне на регистри по искане съгласно FOIA могат да се обжалват по административен ред, след което и пред федерален съд. От съда се изисква да се произнесе отново с решение дали регистрите правомерно не са били предоставени, 5 U.S.C. § 552(a)(4)(B), и той може да задължи правителството да предостави достъп до регистрите. В някои случаи съдът е отхвърлил доводите на правителството, че информацията не трябва да се предоставя, тъй като е класифицирана ([1]). Въпреки че не се предоставят обезщетения за финансови вреди, съдът може да разпореди да бъдат изплатени разноските за адвокатски хонорари.

VI. ЗАКЛЮЧЕНИЕ

Съединените щати признават факта, че нашите дейности за радиоелектронно разузнаване и другите ни разузнавателни дейности трябва да отчитат, че всички лица следва да се третират по достоен начин и с уважение, независимо от тяхното гражданство или местопребиваването им, и че всички лица имат законни интереси за неприкосновеност на личния живот при обработването на личната им информация. Съединените щати използват радиоелектронно разузнаване единствено с цел повишаване на националната сигурност и в интерес на външната си политика, както и за защита на своите граждани и гражданите на съюзниците и партньорите си. Накратко, разузнавателните структури не извършват безразборно наблюдение на който и да било, включително на обикновени европейски граждани. Събирането на радиоелектронна разузнавателна информация се извършва само когато това е разрешено по надлежния ред и при строго спазване на тези ограничения; само след като е взето предвид наличието на алтернативни източници, включително дипломатически и

([1]) Вж. напр. дело *New York Times с/у Министерството на правосъдието*, 756 F.3d 100 (2d Cir. 2014); Американски съюз за граждански свободи с/у ЦРУ, 710 F.3d 422 (D.C. Cir. 2014).

публично достъпни; и при отдаване на предпочитание на уместни и практически възможни алтернативни варианти. Също така, където това е практически възможно, радиоелектронното разузнаване се извършва само чрез събиране, съсредоточено върху конкретни обекти или теми на външното разузнаване, като се използват ограничителни параметри.

Политиката на САЩ в тази връзка бе затвърдена с ПИД-28. В тези рамки разузнавателните агенции на САЩ нямат правомощията, ресурсите, техническия капацитет, нито желание да прихващат съобщенията на целия свят. Тези агенции не четат електронната поща на всеки в Съединените щати или на всеки в света. В съответствие с ПИД-28 Съединените щати осигуряват сигурна защита на личната информация, събрана при дейностите за радиоелектронно разузнаване за лица, които не са граждани на САЩ. Доколкото това е максимално възможно съобразно с националната сигурност, тази защита включва политики и процедури за свеждане до минимум на запазването и разпространението на лична информация за лица, които не са американски граждани, и е сравнима със защитата, осигурявана за американски граждани. Освен това, както беше разгледано, всеобхватният надзорен режим по отношение на прилагането на съответните правомощия съгласно раздел 702 от FISA е безпрецедентен. И накрая, съществените изменения в законодателството на САЩ, уреждащо разузнаването, внесени със Закона за свободата в САЩ, както и инициативите под ръководството на ODNI за повишаване на прозрачността в разузнавателните структури, в голяма степен повишават защитата на неприкосновеността на личния живот и гражданските свободи на всички физически лица, независимо от тяхното гражданство.

Искрено Ваш,

Robert S. Litt

21 юни 2016 г.

Г-н Justin S. Antonipillai
Съветник
Министерство на търговията на САЩ
1401 Constitution Avenue, N.W.
Вашингтон, DC 20230

Г-н Ted Dean
Заместник помощник-секретар
Администрация по международната търговия
1401 Constitution Avenue, N.W.
Вашингтон, DC 20230

Уважаеми г-н Antonipillai и г-н Dean,

С настоящото писмо искаме да предоставим допълнителна информация относно начина, по който Съединените американски щати извършват събирането на масиви от радиоелектронна разузнавателна информация. Както е обяснено в бележка под линия 5 от президентската изпълнителна директива 28 (ПИД-28), събирането на „масиви от данни“ се отнася по-скоро до придобиването на относително голям обем радиоелектронна разузнавателна информация или данни при обстоятелства, при които разузнавателните структури не могат да използват идентификатор, свързан с конкретния обект на разузнаване (като например негов електронен адрес или телефонен номер), за да концентрират събирането на данни. Това обаче не означава, че този вид събиране на данни е „масово“ или „неселективно“. ПИД-28 изисква „радиоелектронните разузнавателни дейности да бъдат възможно най-целенасочени“. В изпълнение на този мандат разузнавателните структури предприемат стъпки, за да гарантират, че дори когато не са в състояние да използват специфични идентификатори за целево събиране на информация, данните, които ще се събират, е вероятно да съдържат чужди разузнавателни сведения, които ще отговарят на изискванията, формулирани от създателите на политики на САЩ съгласно процеса, обяснен в предишното ми писмо, и така се свежда до минимум количеството на събираната нерелевантна информация.

Така например от разузнавателните структури може да бъде поискано да придобият радиоелектронна разузнавателна информация относно дейностите на терористична група, която действа в регион на държава от Близкия изток и за която се смята, че планира нападение срещу държави от Западна Европа, но те може да не разполагат с имената, телефонните номера, електронните адреси или други идентификатори на лицата, свързани с тази терористична група. Нашият избор за целенасочено събиране на данни за тази група би могъл да се изрази в събирането на данни за комуникациите от и към този регион за по-нататъшен преглед и анализ, за да се идентифицират онези комуникации, които се отнасят до групата. При такива действия разузнавателните структури се стремят да стеснят обхвата на събирането във възможно най-голяма степен. Този вид събиране се счита за събиране на масиви от данни, тъй като не е възможно използването на ограничителни параметри, но то не е нито масово, нито неселективно, а е по-скоро концентрирано възможно най-точно.

По този начин, дори когато не е възможно целенасочено събиране на данни чрез използването на избирателни критерии, Съединените щати не събират данни за всички комуникации от всички комуникационни съоръжения навсякъде по света, а прилагат филтри и други технически средства за съсредоточаване на събирането до онези съоръжения, за които има вероятност да съдържат комуникации със стойност за външното разузнаване. При тези действия радиоелектронните разузнавателни дейности на САЩ обхващат само много малка част от комуникациите, преминаващи по интернет.

Освен това, както е отбелязано в предишното ми писмо, тъй като събирането на масиви от данни води до повишен риск от събиране на нерелевантни комуникации, ПИД-28 ограничава целите, за които разузнавателните структури могат да използват събраните масиви от радиоелектронни разузнавателни данни, до шест конкретни цели. ПИД-28 и политиките на агенциите за изпълнение на ПИД-28 също така налагат ограничения по отношение на съхраняването и разпространението на лична информация, придобита чрез радиоелектронно разузнаване, независимо дали тази информация е събрана като част от събиране на масиви от данни или чрез целенасочено събиране и без оглед на гражданството на лицето.

По този начин събирането на масиви от данни от страна на разузнавателните структури не е нито масово, нито неселективно, а включва използването на методи и инструменти за филтриране на събирането, така че то да бъде концентрирано върху материал, който би могъл да отговаря на изискванията, формулирани от създателите на политики по

отношение на външното разузнаване, като същевременно се свежда до минимум събирането на нерелевантна информация, и предвижда строги правила за защита на събраната нерелевантна информация. Политиките и процедурите, описани в настоящото писмо, се прилагат за всяко събиране на масиви от данни в радиоелектронното разузнаване, включително събиране на масиви от данни за комуникации към и от Европа, без това да представлява потвърждение или отричане на извършването на такова събиране.

От Ваша страна беше поискана допълнителна информация относно Надзорния съвет по въпросите на неприкосновеността на личния живот и гражданските свободи (PCLOB) и главните инспектори, както и относно техните правомощия. Надзорният съвет по въпросите на неприкосновеността на личния живот и гражданските свободи е независим орган в изпълнителната власт. В състава на този съвет влизат петима членове, представители и на двете партии, които се назначават от президента и се потвърждават от Сената ([1]). Всеки член е с мандат от шест години. Членовете и служителите на PCLOB разполагат с подходящи разрешения за достъп до класифицирана информация, за да могат да изпълняват в пълна степен своите законови задължения и отговорности ([2]).

Мисията на PCLOB е да гарантира, че се постига равновесие между усилията на федералното правителство за борба с тероризма и необходимостта от защита на неприкосновеността на личния живот и гражданските свободи. Надзорният съвет има две основни отговорности — да упражнява надзор и да предоставя съвети. Той сам определя своя дневен ред и дейностите по упражняване на надзор или предоставяне на съвети, които желае да осъществи.

В своята *надзорна* роля, PCLOB прави преглед и анализ на действията, които изпълнителната власт предприема за защита на нацията от тероризъм, като следи за това необходимостта от такива действия да бъде балансирана с необходимостта от защита на неприкосновеността на личния живот и гражданските свободи ([3]). Последният завършен преглед за надзор на PCLOB бе съсредоточен върху програмите за наблюдение по раздел 702 от Закона за надзор върху външното разузнаване ([4]). Понастоящем Надзорният съвет провежда преглед на разузнавателните дейности, извършвани съгласно Изпълнителен декрет 12333 ([5]).

В *консултативната* си роля PCLOB следи за това съображенията, свързани със свободата, да се разглеждат по подходящ начин при разработването и прилагането на законите, подзаконовите актове и политиките, свързани с усилията за защита на нацията от тероризъм ([6]).

За да изпълнява своята мисия, PCLOB има законоустановено право на достъп до всички архиви, доклади, одити, прегледи, документи, работни документи, препоръки и други подходящи материали на агенциите, в това число до класифицирана информация в съответствие със закона ([7]). Освен това Надзорният съвет може да провежда събеседвания, да снема показания или публично да изслушва като свидетел всяко длъжностно лице или служител на изпълнителната власт ([8]). Надзорният съвет може също така да отправя писмено искане до главния прокурор за издаването, от името на Надзорния съвет, на разпореждания, които задължават страни извън изпълнителната власт да предоставят съответната информация ([9]).

Накрая, по отношение на PCLOB има законоустановени изисквания за публична прозрачност. Те включват информиране на обществеността за дейностите на PCLOB чрез организиране на обществени изслушвания и предоставяне на обществеността на неговите доклади във възможно най-голяма степен, доколкото това е в съответствие със защитата на класифицираната информация ([10]). Освен това от PCLOB се изисква да докладва в случай че агенция на изпълнителната власт отказва да последва неговите съвети.

Главните инспектори в рамките на разузнавателните структури извършват одити, инспекции и прегледи на програмите и дейностите на тези структури, за да установят системни рискове, слабости и недостатъци и да предприемат действия за тяхното отстраняване. Главните инспектори разследват също така жалби или информация по твърдения за нарушения на

([1]) 42 U.S.C. 2000ee(a), (h).
([2]) 42 U.S.C. 2000ee(k).
([3]) 42 U.S.C. 2000ee(d)(2).
([4]) *Вж.* https://www.pclob.gov/library.html#oversightreports.
([5]) *Вж.* https://www.pclob.gov/events/2015/may13.html.
([6]) 42 U.S.C. 2000ee(d)(1); *вж. също* Политика и процедура при консултативната роля на PCLOB, Политика 2015-004, *на адрес* https://www.pclob.gov/library/Policy-Advisory_Function_Policy_Procedure.pdf.
([7]) 42 U.S.C. 2000ee(g)(1)(A).
([8]) 42 U.S.C. 2000ee(g)(1)(B).
([9]) 42 U.S.C. 2000ee(g)(1)(D).
([10]) 42 U.S.C. 2000eee(f).

законите и подзаконовите актове или за лошо управление, сериозно разхищение на средства, злоупотреба с власт, или съществена и специфична опасност за общественото здраве и безопасност в програми и дейности на разузнавателните структури. Независимостта на главните инспектори е изключително важен елемент за обективността и достоверността на всеки един от техните доклади, констатации и препоръки. Сред някои от най-важните компоненти за поддържане на независимостта на главните инспектори са процедурите за тяхното назначаване и освобождаване, отделните правомощия във връзка с оперативното управление, бюджета и персонала, и изискването за двойно докладване пред ръководителите на агенциите на изпълнителната власт и пред Конгреса.

Конгресът създаде независима служба на главния инспектор във всяка една от агенциите на изпълнителната власт, в това число във всяка от разузнавателните структури ([1]). С приемането на Закона за разрешаване на разузнавателни дейности за финансова година 2015 президентът назначи, а Сенатът потвърди назначаването на почти всички главни инспектори с надзорна функция в разузнавателна структура, включително в Министерството на правосъдието, Централното разузнавателно управление, Агенцията за национална сигурност и групата на разузнавателните структури ([2]). Освен това главните инспектори са постоянно назначени, независими служители, които могат да бъдат отстранени само от президента. Въпреки че в Конституцията на САЩ се изисква президентът да разполага с правомощието да отстранява главните инспектори, това правомощие е упражнявано рядко, като от президента се изисква, 30 дни преди да отстрани главен инспектор, да представи на Конгреса писмена обоснова за това ([3]). Тази процедура за назначаване на главните инспектори гарантира отсъствието на неправомерно влияние на служители на изпълнителната власт при подбора, назначаването или отстраняването на главните инспектори.

Второ, главните инспектори разполагат със значителни законоустановени правомощия да извършват одити, разследвания и прегледи на програмите и действията на изпълнителната власт. Освен разследванията и прегледите за надзор, изисквани по закон, главните инспектори имат свобода на действие да упражняват надзорните си правомощия, като правят прегледи на програми и действия по свой избор ([4]). При упражняването на това правомощие законът гарантира, че главните инспектори разполагат с независими ресурси, за да изпълняват своите задължения, включително с правомощието да наемат свои служители и да документират отделно бюджетните си искания към Конгреса ([5]). Законът гарантира, че главните инспектори разполагат с информацията, необходима за изпълнение на техните задължения. Това включва правомощието им да имат пряк достъп до цялата документация на агенцията и до подробна информация за нейните програми и операции, независимо от нивото на поверителност, правомощието да изискват информация и документи и да приемат клетвени декларации ([6]). В ограничен брой случаи ръководителят на агенция на изпълнителната власт може да забрани дейността на главния инспектор, например ако одит или разследване на главен инспектор може значително да засегне интересите на националната сигурност на САЩ. Упражняването на това правомощие обаче е изключително необичайно и изисква от ръководителя на агенцията да уведоми Конгреса в срок от 30 дни за причините за такова действие ([7]). На практика директорът на националното разузнаване никога не е използвал това правомощие за ограничение на дейностите на главните инспектори.

Трето, главните инспектори имат задължението да предоставят цялостна и редовна информация на ръководителите на агенциите от изпълнителната власт и Конгреса под формата на доклади относно измами и други сериозни проблеми, злоупотреби и пропуски, свързани с програмите и дейностите на изпълнителната власт ([8]). Това двойно докладване укрепва независимостта на главните инспектори, като осигурява прозрачност в техния процес за надзор и дава възможност на ръководителите на агенциите да приложат препоръките на главните инспектори преди Конгресът да приеме законодателно действие. Така например законът изисква от главните инспектори да представят шестмесечни доклади, в които се описват установените проблеми и приетите до момента корективни действия ([9]). Агенциите на изпълнителната власт

([1]) Раздели 2 и 4 от Закона за главния инспектор от 1978 г., с измененията (по-нататък „Законът за ГИ“); раздел 103H(b) и (e) от Закона за националната сигурност от 1947 г., с измененията (по-нататък „Законът за НС“); раздел 17(a) от Закона за Централното разузнавателно управление (по-нататък „Законът за ЦРУ“).

([2]) *Вж.* Pub. L. № 113-293, 128 Stat. 3990, (Dec. 19, 2014). Единствено главните инспектори на Агенцията за военно разузнаване и на Националната агенция за геокосмическо разузнаване не се назначават от президента, но главните инспектори на Министерството на отбраната и на Разузнавателната общност имат паралелна компетентност над тези агенции.

([3]) Раздел 3 от Закона за ГИ от 1978 г., с измененията; раздел 103H(c) от Закона за НС; раздел 17(b) от Закона за ЦРУ.

([4]) *Вж.* раздели 4(a) и 6(a)(2) от Закона за ГИ от 1947 г.; раздел 103H(e) и (g)(2)(A) от Закона за НС; раздел 17(a) и (c) от Закона за ЦРУ.

([5]) Раздели 3(d), 6(a)(7) и 6(f) от Закона за ГИ; раздели 103H(d), (i), (j) и (m) от Закона за НС; раздели 17(e)(7) и (f) от Закона за ЦРУ.

([6]) Раздели 6(a)(1), (3), (4), (5), и (6) Закона за ГИ; раздели 103H(g)(2) от Закона за НС; раздели 17(e)(1), (2), (4), и (5) от Закона за ЦРУ.

([7]) *Вж. например* раздели 8(b) и 8E(a) от Закона за ГИ; раздел 103H(f) от Закона за НС; раздел 17(b) от Закона за ЦРУ.

([8]) Раздел 4(a)(5) от Закона за ГИ; раздел 103H(a)(b)(3) и (4) от Закона за НС; раздел 17(a)(2) и (4)от Закона за ЦРУ.

([9]) Раздел 2(3), 4(a), и 5 от Закона за ГИ; раздел 103H(k) от Закона за НС; раздел 17(d) от Закона за ЦРУ. Главният инспектор на Министерството на правосъдието публикува своите доклади, които са достъпни за обществеността, на следния адрес: http://oig.justice.gov/reports/all.htm. По същия начин главният инспектор на Разузнавателната общност публикува своите шестмесечни доклади на адрес: https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig.

подхождат сериозно към констатациите и препоръките на главните инспектори и често са в състояние да включат в тези и други доклади, представяни на Конгреса, а понякога и предоставяни на обществеността, своето съгласие с препоръките на главния инспектор и изпълнението на тези препоръки ([1]). В допълнение към тази двойна структура на докладва главните инспектори носят отговорност и да насочват служителите от изпълнителната власт, които подават сигнали за нарушения, към подходящите надзорни комисии в Конгреса, за да разкриват случаи на предполагаеми измами, разхищения или злоупотреби в рамките на програми или действия на изпълнителната власт. Самоличността на лицата, сигнализиращи за нередности, е защитена от разкриване пред изпълнителната власт, което ги предпазва от евентуални забранени кадрови действия или действия във връзка с разрешаването на достъп до класифицирана информация като репресивна мярка за това, че лицето е докладвало на главния инспектор ([2]). Тъй като често източник за разследванията на главните инспектори са именно лица, сигнализиращи за нередности, възможността да представят своите опасения пред Конгреса без влияние от страна на изпълнителната власт увеличава ефективността на надзора, упражняван от главните инспектори. Благодарение на тази независимост главните инспектори са в състояние да насърчават икономиите, ефективността и отчетността в агенциите на изпълнителната власт по обективен и етичен начин.

Накрая, Конгресът създаде Съвета на главните инспектори за етично поведение и ефикасност. Този съвет, наред с другото, разработва стандарти за одити, разследвания и прегледи, насърчава обучението и има правомощието да разглежда твърденията за неправомерни действия от страна на главните инспектори, като по този начин наблюдава дейността на главните инспектори, натоварени със задачата да наблюдават дейността на всички останали ([3]).

Надявам се тази информация да Ви бъде от полза.

С уважение,
Robert S. Litt
Главен съветник

([1]) Раздел 2(3), 4(a) и 5 от Закона за ГИ; раздел 103H(k) от Закона за НС; раздел 17(d) от Закона за ЦРУ. Главният инспектор на Министерството на правосъдието публикува своите доклади, които са достъпни за обществеността, на следния адрес: http://oig.justice.gov/reports/all.htm. По същия начин главният инспектор на Разузнавателната общност публикува своите шестмесечни доклади на адрес: https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig.

([2]) Раздел 7 от Закона за ГИ; раздел 103H(g)(3) от Закона за НС; раздел 17(e)(3) от Закона за ЦРУ.

([3]) Раздел 11 от Закона за ГИ.

ПРИЛОЖЕНИЕ VII

Писмо от Заместник министъра на правосъдието и съветник по международните въпроси, Bruce Swartz, Министерство на правосъдието на САЩ

19 февруари 2016 г.

Г-н Justin S. Antonipillai
Съветник
Министерство на търговията на САЩ
1401 Constitution Ave., NW
Вашингтон, DC 20230

Г-н Ted Dean
Заместник помощник-секретар
Администрация по международната търговия
1401 Constitution Ave., NW
Вашингтон, DC 20230

Уважаеми г-н Antonipillai и г-н Dean,

В настоящото писмо е направен кратък преглед на основните средства за разследване, използвани за получаването на търговска информация и други справочни данни от дружествата в Съединените щати за целите на правоприлагането в наказателната сфера или в сферата на обществените интереси (гражданскоправната и регулаторната сфера), включително ограниченията за достъпа, определени в тези законови разпоредби ([1]). Този процес на призоваване е недискриминационен, тъй като се прилага за получаване на информация от дружествата в Съединените щати, включително такива, които ще се самосертифицират съгласно рамката на Щита за личните данни в отношенията между ЕС и САЩ, независимо от гражданството на субекта на данните. Освен това дружествата, които са призовани по този начин в Съединените щати, могат да обжалват това в съда, както ще бъде разгледано по-нататък ([2]).

От специално значение за изземването на информация от страна на публичните органи е четвъртата поправка в Конституцията на Съединените щати, в която се предвижда, че „правото на хората на лична сигурност, сигурност на дома, документите и действията им, срещу извършване на неоснователни обиски и изземвания, не трябва да бъде нарушавано и не трябва да бъдат издавани заповеди за такива действия, освен когато е налице правдоподобна причина и издаването става под клетва или с официална декларация, с точно описание на мястото на обиска и лицата или вещите, които подлежат на изземване“, Конституция на САЩ, IVта поправка. Както постанови Върховният съд на Съединените щати по делото Berger с/у щата Ню Йорк, „основната цел на тази поправка, както това се признава в множество решения на този съд, е да бъдат защитени неприкосновеността на личния живот и сигурността на физическите лица срещу произволни посегателства на длъжностни лица на правителството“. 388 U.S. 41, 53 (1967) (*цитирано в Camara с/у Районен съд на Сан Франциско*, 387 U.S. 523, 528 (1967 г.)) За националните наказателни разследвания в четвъртата поправка се поставя общо изискване към длъжностните лица в правоприлагането да получат заповед по съдебно разпореждане преди да извършат обиск. Вж. *Katz с/у Съединените щати*, 389 U.S. 347, 357 (1967 г.). Когато това изискване за заповед не се прилага, за действията на правителството се прилага тест за „основателност“ съгласно четвъртата поправка. Следователно в самата Конституция е гарантирано, че правителството на САЩ няма неограничени или произволни права да изземва частна информация.

Правомощия в наказателното правоприлагане:

Федералните прокурори, които са служители на Министерството на правосъдието (МП), и федералните следователи, включително във Федералното бюро за разследвания (ФБР), което е правоприлагаща агенция в рамките на МП, могат да задължат дружества в Съединените щати да им предоставят документи и друга регистрирана информация за целите на

([1]) В този преглед не се разглеждат инструментите за разследвания в националната сигурност, които се използват при правоприлагането в областта на тероризма и други разследвания в националната сигурност, включително писмата във връзка с националната сигурност (ПНС) за някои видове справочна информация в справки за кредити, финансова информация и електронни регистри за абонати и трансакции, вж. 12 U.S.C. § 3414; 15 U.S.C. § 1681u; 15 U.S.C. § 1681v; 18 U.S.C. § 2709, и за електронно наблюдение, заповеди за обиск, търговски регистри и друг вид събиране на съобщителна информация съгласно Закона за надзор върху външното разузнаване, вж. 50 U.S.C. § 1801 *et seq*.

([2]) Настоящият документ се отнася за федералното правоприлагане и федералните регулаторни режими; нарушения на щатското право се разследват от щатите и делата по тях се водят в щатските съдилища. Щатските правоприлагащи органи използват заповеди и призовки, издадени съгласно щатското право, което по същество се извършва по същия ред, както това е разгледано в настоящия документ, но е възможно за процеса на призоваване в щатите да се прилагат защити, предвидени в щатските конституции, които са с по-висока степен от предвидените в Конституцията на САЩ. Защитите съгласно щатското право трябва да са най-малкото равни по степен на предвидените в Конституцията на САЩ, включително, но не само в четвъртата поправка.

наказателни разследвания чрез няколко вида процеси за задължително призоваване, включително призовки на „голямото жури“, административни разпореждания и заповеди за обиск, и могат да придобиват друг вид съобщителна информация съгласно правомощията си за подслушване и използване на устройства за регистриране за целите на федерални наказателни разследвания.

Призовки на „голямото жури“ или по конкретен съдебен процес: Призовките в наказателното правосъдие се използват за оказване на съдействие по конкретни разследвания в правоприлагането. Призовката на „голямото жури“ е официално искане, издадено от „голямото жури“ (обикновено по искане на федерален прокурор) за съдействие по разследване на „голямото жури“ по конкретно предполагаемо нарушение на наказателното право. „Голямото жури“ е разследващо поделение на съда, което се конституира от съдия или магистрат. С призовката може да се изиска от дадено лице да даде свидетелски показания по съдебен процес или да извлече или предостави на разположение търговска информация, данни, съхранени по електронен път, или други материали. Информацията трябва да е релевантна за целите на разследването и призовката не може да е неоснователна поради прекалено широко формулиране, или с репресивен или обременяващ характер. Получателят може да подаде предложение за оспорване в съда на призовка на тези основания. Вж. Федерален регистър наказ. дела 17. В ограничени случаи могат да бъдат издавани призовки за документи по конкретен процес, след като делото бъде указано от „голямото жури“.

Правомощия за административни разпореждания: Правомощията за издаване на административни разпореждания могат да бъдат упражнявани в наказателноправни или гражданскоправни разследвания. В контекста на наказателното правоприлагане няколко федерални закона дават правомощия за използването на административни разпореждания за извличане или предоставяне на разположение на търговска информация, данни, съхранявани в електронна форма, или други материали по разследвания за измами в здравеопазването, малтретиране на деца, защита на тайните служби, по дела за контролирани вещества и в разследвания на главни инспектори, в които са въвлечени правителствени институции. Ако правителството предприеме принудително изпълнение в съда на административно разпореждане, получателят на това разпореждане, както и получателят на призовка на „голямото жури“, може да оспори неговата основателност поради прекалено широко формулиране, или репресивен или обременяващ характер.

Съдебни разпореждания за устройства за регистриране или проследяване: Съгласно разпоредбите за устройствата за регистриране или проследяване в наказателни разследвания, правоприлагащите органи могат да получат съдебно разпореждане за придобиване в реално време на информация, която не се отнася за съдържание, във връзка с избиране, направление, адресиране и радиоелектронна информация относно даден телефонен номер или електронна поща, след като удостоверят, че предоставената информация е релевантна за провеждащо се наказателно разследване. *Вж.* 18 U.S.C. §§ 3121-3127. Неправомерното използване или монтиране на такива устройства е престъпление по федералните закони.

Закон за неприкосновеност на електронните съобщения (Electronic Communications Privacy Act) (ECPA): Достъпът на правителството до информация за абонати, данни за трафика и съхранено съдържание на разговори и съобщения, с които разполагат телефонните дружества — доставчици на интернет услуги, и други доставчици, в качеството им на трети страни, се урежда от допълнителни правила съгласно дял II от ECPA, който се нарича също Закон за съхраняваните съобщения (*Stored Communications Act* — SCA), 18 U.S.C. §§ 2701–2712. С този закон се определя система от законоустановени права на неприкосновеност на личния живот, с което се ограничава достъпът за целите на правоприлагането до данни за клиенти и абонати на доставчици на интернет услуги, който надхвърля изискванията съгласно конституционното право. Със SCA се предвижда повишаване на нивото на защита на неприкосновеността на личния живот, в зависимост от степента на намеса при събирането на информацията. За целите на наказателното правоприлагане органите са задължени да получат разпореждане, за да се сдобият с информация за регистрация на потребители, IP адреси и съответните удостоверения за време, както и информация за разплащането. За повечето други видове съхранена информация, която не се отнася за съдържание, като например заглавен ред на електронни съобщения, без реда „Относно“, правораздавателните органи задължително трябва да представят пред съдия конкретни факти в доказателство, че исканата информация е релевантна и се отнася по същество за провеждащо се наказателно разследване. За да се сдобият със съхраненото съдържание на електронни съобщения, обикновено органите в наказателното правоприлагане получават разпореждане от съдия на основание правдоподобна причина, поради която се счита, че въпросният профил съдържа доказателства за извършено престъпление. В SCA се предвиждат също така и гражданскоправни и наказателни санкции.

Съдебни разпореждания за наблюдение съгласно федералния закон за подслушванията: В допълнение към това правоприлагащите органи могат да подслушват в реално време кабелни, устни или електронни съобщения за целите на наказателни разследвания съгласно федералния закон за подслушванията. *Вж.* 18 U.S.C. §§ 2510-2522. Това право се дава само със съдебно разпореждане, в което наред с останалото се съдържат констатации на съдия, че е налице правдоподобна

причина да се счита, че подслушването или прихващането по електронен път ще дадат доказателства за престъпление срещу федералните закони или информация за местонахождението на лице, укриващо се с цел избягване на наказателна отговорност. Законът предвижда гражданскоправни и наказателни санкции за нарушения на разпоредбите за подслушване.

Заповед за обиск — правило 41: Правоприлагащите органи могат да извършват физическо претърсване на помещения в Съединените щати, когато им е дадено разрешение за това от съдия. Те трябва да докажат пред съдията въз основа на явна „правдоподобна причина“, че е било извършено или предстои да бъде извършено престъпление и че има вероятност на мястото, посочено в заповедта, да бъдат намерени вещи, свързани с престъплението. Това правомощие често се използва, когато е необходимо да се извърши физическо претърсване на помещения от полицията, поради опасност от унищожаване на доказателствата, ако на дружеството бъде връчена призовка или друго процесуално разпореждане. Вж. Конституция на САЩ, IVта поправка. (разгледано по-подробно по-горе), Федерален регистър на наказ. дела 41. Субект, по отношение на който е издадена заповед за претърсване, може да предприеме действия за отмяната ѝ на основание, че е прекалено широко формулирана, злонамерена или по друг начин е получена неправомерно, и засегнатите страни, които разполагат с аргументи, могат да предприемат действия за спиране разглеждането на доказателства, получени чрез неправомерен обиск. Вж. дело *Мapp с/у Охайо*, 367 U.S. 643 (1961 г.).

Насоки и политики на Министерството на правосъдието: В допълнение към тези базирани на Конституцията, законите и правилата ограничения за достъпа от страна на правителството до данни, Министърът на правосъдието издаде насоки, с които се определят допълнителни ограничения за достъпа до данни за целите на правоприлагането и в които се съдържат също и защити за неприкосновеността на личния живот и гражданските свободи. Например в насоките на Министъра на правосъдието за национални оперативни дейности на Федералното бюро за разследвания (ФБР) от септември 2008 г. (наричани по-нататък „насоки за ФБР от МП“), които са на разположение на адрес: http://www.justice.gov/archive/opa/docs/guidelines.pdf, се определят ограничения за използването на разузнавателни средства за набиране на информация във връзка с разследвания по престъпления срещу федералните закони. В тези насоки се поставя изискване към ФБР да използва методи на разследване, които са с най-ниската практически възможна степен на вмешателство, отчитайки последствията за неприкосновеността на личния живот и гражданските свободи и евентуалното накърняване на доброто име. Освен това в тях се отбелязва, че „е задължително ФБР да провежда разследванията и другите си дейности по законосъобразен и разумен начин, при уважаване на свободата и неприкосновеността на личния живот и избягване на ненужно вмешателство в живота на лица, които спазват законите“. Вж. насоките за ФБР от МП на стр. 5. ФБР е привело в изпълнение тези насоки чрез Ръководство за национални оперативни дейности и разследвания на ФБР (*FBI Domestic Investigations and Operations Guide* (DIOG)), което е на разположение на адрес: https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20(DIOG), един изчерпателен наръчник, в който са включени подробно разгледани ограничения за използването на средства за разследване и насоки за гарантиране защитата на гражданските свободи и неприкосновеността на личния живот във всяко разследване. Допълнителни правила и политики, с които се предвиждат ограничения за разследващите дейности на федералните прокурори, са определени в **Наръчника на прокурорите в Съединените щати**, (*United States Attorneys' Manual* (USAM)), който също е на разположение онлайн на адрес: http://www.justice.gov/usam/united-states-attorneys-manual.

Гражданскоправни и регулаторни правомощия (обществен интерес):

Съществуват и значителни ограничения за достъпа до данни, с които разполагат дружествата в САЩ, за целите на гражданскоправното и регулаторното правоприлагане (т.е. правоприлагане в обществен интерес). Институциите, които имат гражданскоправни и регулаторни отговорности, могат да издават разпореждания за дружествата във връзка с търговска информация, данни, съхранени в електронна форма, или други материали. Тези институции са ограничени при упражняването на правомощията им за издаване на административни или гражданскоправни разпореждания, не само съгласно законите, с които се урежда статутът им, но и чрез независимия съдебен контрол на разпорежданията преди евентуалното принудително изпълнение по съдебен ред. Вж. напр. Федерален регистър гражд. дела 45. Институциите могат да искат достъп само до данни, които са релевантни за въпросите в обхвата на техните регулаторни правомощия. Освен това получател на административно разпореждане може да оспори изпълнението му в съда, като представи доказателства, че институцията не е действала съобразно с основните изисквания за основателност, както това беше разгледано по-горе.

Съществуват и други правни основания за оспорване от страна на дружествата на искания за информация от административни институции, според конкретната стопанска дейност и вида на данните, с които разполагат. Например финансовите институции могат да оспорят административни разпореждания, с които се изисква конкретен вид информация в нарушение на Закона за банковата тайна (*Bank Secrecy Act*) и подзаконовите разпоредби за прилагането му. Вж. 31 U.S.C. § 5318, 31 C.F.R. част X. Други стопански субекти могат да се основат на Закона за оповестяване на информация за кредити (*Fair Credit Reporting Act*), вж. 15 U.S.C. § 1681b, или множество други закони, специфични за конкретния сектор. Злоупотребата с правото за издаване на разпореждане от страна на дадена институция може да доведе до подвеждане под отговорност на институцията или на нейни служители за причинени вреди. Вж. напр. Закона за правото на неприкосновеност на личните финанси (*Right to Financial Privacy Act*), 12 U.S.C. §§ 3401–3422. По този начин съдилищата в Съединените щати са в ролята на защитник срещу неправомерни регулаторни искания и осигуряват независим надзор на действията на федералните институции.

И накрая, всяко законоустановено правомощие на административните органи да извършват „физически“ изземване на информация от дружество в Съединените щати по силата на административно разпореждане за обиск трябва да е съобразено с изискванията в четвъртата поправка. Вж. дело *See c/y град Сиатъл*, 387 U.S. 541 (1967 г.).

Заключение

Всички правоприлагащи и регулаторни дейности в Съединените щати трябва да са съобразени с приложимото законодателство, включително с Конституцията на САЩ, законите, подзаконовите разпоредби и правилата. Тези дейности трябва да са съобразени също и с приложимите политики, включително с насоките на Министъра на правосъдието, от които се ръководят дейностите във федералното правоприлагане. Разгледаната по-горе правна уредба ограничава възможността за правоприлагащите и регулаторните органи на САЩ да получават информация от дружества в Съединените щати, независимо дали тя се отнася за граждани на САЩ или на други държави, и в допълнение към това позволява да се осъществява съдебен контрол на всяко искане за данни от страна на правителството съгласно тези правомощия.

Искрено Ваш,

Bruce C. Swartz

Заместник министъра на правосъдието и съветник по международните въпроси

РЕШЕНИЕ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2016/1251 НА КОМИСИЯТА

от 12 юли 2016 година

за приемане на многогодишна програма на Съюза за събиране, управление и използване на данни в секторите на рибарството и аквакултурите за периода 2017—2019 година

(нотифицирано под номер C(2016) 4329)

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид Регламент (ЕО) № 199/2008 на Съвета от 25 февруари 2008 г. за установяване на общностна рамка за събиране, управление и използване на данни в сектор Рибарство и за подкрепа на научните консултации във връзка с Общата политика в областта на рибарството ([1]), и по-специално член 3 от него,

като има предвид, че:

(1) Съгласно член 3 от Регламент (ЕО) № 199/2008 многогодишната програма на Съюза за събиране, управление и използване на данни в сектор „Рибарство“ се изготвя за тригодишен период, за да се осигури еднакво прилагане на задължението за събиране и управление на данни.

(2) Настоящата многогодишна програма на Съюза се основава на многогодишната програма за периода 2011—2013 г., който бе удължен с Решение за изпълнение C(2013) 5243 на Комисията, за да покрие периода между приемането на Регламент (ЕС) № 1380/2013 на Европейския парламент и на ([2]) и 31 декември 2016 г. Поради това е необходимо да се изготви многогодишна програма на Съюза за тригодишен период с начало 1 януари 2017 г.

(3) Съгласно член 25 от Регламент (ЕС) № 1380/2013 държавите членки събират биологични, екологични, технически и социално-икономически данни, необходими за управлението на рибарството. Многогодишната програма на Съюза е необходима, за да могат държавите членки да определят и планират своите дейности по събиране на данни в националните си работни планове. В съответствие с член 21 от Регламент (ЕС) № 508/2014 на Европейския парламент и на Съвета ([3]) посочените национални работни планове трябва да бъдат представени на Комисията до 31 октомври на годината, предхождаща годината, през която трябва да се прилага работният план.

(4) В многогодишната програма на Съюза следва да се определят изисквания за събирането на данни в съответствие с член 1 от Регламент (ЕО) № 199/2008. Тя следва да съдържа елементите, необходими за изпълнението на общата политика в областта на рибарството, доколкото те вече не се изискват съгласно други законодателни рамки.

(5) С оглед постигането на целите на реформираната обща политика в областта на рибарството, посочени в член 2 от Регламент (ЕС) № 1380/2013, е необходимо да се актуализират изискванията на Съюза за надеждни научни становища за периода, който започва на 1 януари 2017 г.

(6) Освен това новите международни задължения и ангажименти, наложени на държавите членки и Съюза с многостранни и двустранни споразумения относно рибарството, водят до включване в многогодишната програма на Съюза на някои изисквания относно събирането на данни, по-специално произтичащите от споразумения за партньорство в областта на устойчивото рибарство (СПОУР).

([1]) ОВ L 60, 5.3.2008 г., стр. 1.

([2]) Регламент (ЕС) № 1380/2013 на Европейския парламент и на Съвета от 11 декември 2013 г. относно общата политика в областта на рибарството, за изменение на регламенти (ЕО) № 1954/2003 и (ЕО) № 1224/2009 на Съвета и за отмяна на регламенти (ЕО) № 2371/2002 и (ЕО) № 639/2004 на Съвета и Решение 2004/585/ЕО на Съвета (ОВ L 354, 28.12.2013 г., стр. 22).

([3]) Регламент (ЕС) № 508/2014 на Европейския парламент и на Съвета от 15 май 2014 г. за Европейския фонд за морско дело и рибарство и за отмяна на регламенти (ЕО) № 2328/2003, (ЕО) № 861/2006, (ЕО) № 1198/2006 и (ЕО) № 791/2007 на Съвета и Регламент (ЕС) № 1255/2011 на Европейския парламент и на Съвета (ОВ L 149, 20.5.2014 г., стр. 1).

(7) Оценката на настоящата рамка за събиране, управление и използване на данни в сектора на рибарството и последващите консултации със заинтересованите страни показаха, че многогодишната програма на Съюза следва да се съсредоточи върху естеството на изискваните от държавите членки данни, а не на методите за тяхното събиране. Методологичните изисквания са описани в работните планове на държавите членки, които трябва да бъдат одобрени от Комисията след тясно сътрудничество между държавите членки на равнището на морските региони.

(8) Поради това програмата на Съюза за периода 2017—2019 г. следва да отчита всички тези елементи, както и целите на Регламент (ЕС) № 1380/2013, по-специално членове 2 и 25 от него, доколкото това е възможно в рамките на настоящата правна рамка, предвидена в Регламент (ЕО) № 199/2008. Когато новите изисквания за данните надхвърлят настоящата законодателна рамка, те следва да бъдат незадължителни. След като влезе в сила нова правна рамка за изменение на Регламент (ЕО) № 199/2008, Комисията може да измени многогодишната програма на Съюза, ако е необходимо, за да отрази всички нови изисквания за събирането на данни.

(9) Комисията взе предвид препоръките от консултацията в рамките на регионалните координационни срещи, посочени в член 5 от Регламент (ЕО) № 199/2008 и с Научния, технически и икономически комитет по рибарство (НТИКР). Бяха проведени консултации и с други подходящи консултативни научни органи като Международния съвет за изследване на моретата (ICES), както и с представители на държавите членки, събрани в предназначени за целта експертни групи.

(10) От съображения за правна сигурност Решение за изпълнение C(2013) 5243 следва да бъдат отменено.

(11) Мерките, предвидени в настоящото решение, са в съответствие със становището на Управителния комитет по рибарство и аквакултури,

ПРИЕ НАСТОЯЩОТО РЕШЕНИЕ:

Член 1

Многогодишната програма на Съюза за събиране, управление и използване на данни в сектора на рибарството за периода 2017—2019 г. съгласно член 3 от Регламент (ЕО) № 199/2008 се съдържа в приложението към настоящия регламент.

Член 2

Решение за изпълнение C(2013)5243 се отменя, считано от 1 януари 2017 г.

Член 3

Адресати на настоящото решение са държавите членки.

Съставено в Брюксел на 12 юли 2016 година.

За Комисията
Karmenu VELLA
Член на Комисията

ПРИЛОЖЕНИЕ

ГЛАВА I

Определения

За целите на настоящото приложение се прилагат определенията от Регламент (ЕС) № 1224/2009 на Съвета ([1]), Регламент за изпълнение (ЕС) № 404/2011 на Комисията ([2]) и Регламент (ЕС) № 1380/2013 на Европейския парламент и на Съвета ([3]). В допълнение се прилагат и следните определения:

1) **Активни кораби**: кораби, които са участвали в каквато и да е риболовна операция (един или повече дни) през календарната година. Кораб, който не е участвал в риболовни операции през годината, се счита за „неактивен“.

2) **Анадромни видове**: живи водни ресурси с жизнен цикъл, започващ с излюпване в сладка вода, мигриране в солена вода, връщане и накрая хвърляне на хайвера в сладка вода.

3) **Катадромни видове**: живи водни ресурси с жизнен цикъл, започващ с излюпване в солена вода, мигриране в сладка вода, връщане и накрая хвърляне на хайвера в солена вода.

4) **Фракция от улова**: част от общия улов, като например частта от улова, разтоварена на брега над минималния референтен размер за опазване, разтоварената на брега част под минималния референтен размер за опазване, изхвърлената част под минималния референтен размер за опазване, изхвърлянето *de minimis* или изхвърлянето на улов.

5) **Дни в морето**: всеки непрекъснат период от 24 часа (или част от него), по време на който корабът присъства в рамките на дадена зона и отсъства от пристанище.

6) **Риболовни дни**: всеки календарен ден в морето, през който се извършва риболовна операция, без да се засягат международните задължения на Съюза и неговите държави членки. Един риболовен рейс може да е част както от сумата на риболовните дни за пасивни съоръжения, така и от сумата на риболовните дни за активни съоръжения по време на този рейс.

7) **Риболовно поле**: (група) географски единици, в които се извършва риболов. Тези единици трябва да бъдат съгласувани на равнище морски региони въз основа на съществуващи зони, определени от регионалните организации за управление на рибарството или научните органи.

8) **Сегмент от флота**: група кораби с един и същ клас по дължина (LOA, обща дължина) и едни и същи преобладаващи риболовни съоръжения през годината.

9) **Група сходни риболовни дейности**: група риболовни операции, които имат за цел сходен вид (съобщество) риби, при които се използват сходни съоръжения ([4]), през един и същ период от годината и/или в една и съща зона, и които се характеризират със сходен режим на експлоатация.

10) **Научни изследвания по море**: пътувания, извършвани от изследователски кораб или кораб, предназначен за научни изследвания на запасите и за наблюдение на екосистемите, и определен за тази дейност от органа, отговарящ за изпълнението на националния работен план, създаден в съответствие с член 21 от Регламент (ЕС) № 508/2014.

([1]) Регламент (ЕС) № 1224/2009 на Съвета от 20 ноември 2009 г. за създаване на система за контрол на Общността за гарантиране на спазването на правилата на общата политика в областта на рибарството, за изменение на регламенти (ЕО) № 847/96, (ЕО) № 2371/2002, (ЕО) № 811/2004, (ЕО) № 768/2005, (ЕО) № 2115/2005, (ЕО) № 2166/2005, (ЕО) № 388/2006, (ЕО) № 509/2007, (ЕО) № 676/2007, (ЕО) № 1098/2007, (ЕО) № 1300/2008, (ЕО) № 1342/2008 и за отмяна на регламенти (ЕИО) № 2847/93, (ЕО) № 1627/94 и (ЕО) № 1966/2006 (ОВ L 343, 22.12.2009 г., стр. 1).

([2]) Регламент за изпълнение (ЕС) № 404/2011 на Комисията от 8 април 2011 г. за определяне на подробни правила за прилагането на Регламент (ЕС) № 1224/2009 на Съвета за създаване на система за контрол на Общността за гарантиране на спазването на правилата на общата политика в областта на рибарството (ОВ L 112, 30.4.2011 г., стр. 1).

([3]) Регламент (ЕС) № 1380/2013 на Европейския парламент и на Съвета относно общата политика в областта на рибарството, за изменение на регламенти (ЕС) № 1954/2003 и (ЕС) № 1224/2009 на Съвета и за отмяна на регламенти (ЕО) № 2371/2002 и (ЕО) № 639/2004 на Съвета и Решение 2004/585/ЕО на Съвета (ОВ L 354, 28.12.2013 г., стр. 22).

([4]) Както е посочено в приложение XI към Регламент (ЕС) № 404/2011.

ГЛАВА II

Методи за събиране на данни

Методите за събиране на данни и качеството им са подходящи за целите, за които са предназначени, определени в член 25 от Регламент (ЕС) № 1380/2013, и се придържат към най-добрите практики и съответните методологии, препоръчани от компетентните научни органи. За тази цел, методите и резултатите от прилагането на методите се проверяват на равномерни интервали от независими научни органи, за да се провери тяхната целесъобразност по отношение на управлението на общата политика в областта на рибарството.

ГЛАВА III

Изисквания за данните

1. **Набори от данни**

1.1. В рамките на работните планове, изготвени в съответствие с член 21 от Регламент (ЕС) № 508/2014, държавите членки определят данните, които трябва да бъдат събрани измежду следните набори, както е посочено в точки 2 — 7 от настоящата глава:

а) Биологични данни, по фракции на улова, за запасите, уловени при търговски риболов на Съюза във и извън водите на Съюза и при любителски риболов във водите на Съюза;

б) Данни, с които да се оцени въздействието на рибарството на Съюза върху морската екосистема във и извън водите на Съюза;

в) Подробни данни за дейността на риболовните кораби на Съюза във водите на Съюза и извън водите на Съюза, докладвани съгласно Регламент (ЕС) № 1224/2009;

г) Социални и икономически данни относно риболова ([1]);

д) Социални, икономически и екологични данни за аквакултурите;

1.2. Данните, които трябва да се събират, са определени в съответствие с членове 3, 4 и 5 от Регламент (ЕО) № 199/2008 и като се вземат предвид праговете, установени в глава V от настоящото приложение.

1.3. Данни се събират, за да се получи възможност за валидна оценка, извлечена за вид риболов, временни срокове и зони, въз основа на нуждите на крайния потребител, съгласувана на равнище морски региони. Честотата на събиране на данни следва да се координира на равнище морски региони, освен ако е посочено друго в настоящото приложение и съответните таблици.

2. **Биологични данни за улова от търговски риболов на Съюза във водите на Съюза и извън водите на Съюза и от любителския риболов във водите на Съюза.**

Тези данни включват следната информация:

а) Количествата улов по видове и биологичните данни от отделни образци, позволяващи оценка на:

i) за търговския риболов —обема и честотата на дължината на всички фракции на улова (включително изхвърления и нежелания улов) за запасите, изброени в таблици 1A, 1B и 1C, представени на обобщено равнище 6, както е определено в таблица 2. Временната прецизност се координира на равнище морски региони въз основа на нуждите на крайния потребител;

ii) за търговския риболов — средно тегло и възрастово разпределение при улова на запасите, изброени в таблици 1A, 1B и 1C. Подборът на запаси, от които да се съберат посочените променливи и временната прецизност се координират на равнище морски региони въз основа на нуждите на крайния потребител;

([1]) Данните за преработвателната промишленост могат да се събират на доброволна основа, като в такъв случай може да се използва сегментирането и променливата от таблица 11.

iii) за търговския риболов — данните за съотношението по пол, зрелостта и плодовитостта на запасите, посочени в таблици 1A, 1B и 1C от улова при необходимите за научните консултации честоти. Подборът на запаси, от които да се съберат посочените променливи, както и временната прецизност, се координират на равнище морски региони въз основа на нуждите на крайния потребител;

iv) за любителския риболов — годишният обем (брой и тегло или дължина) на улова и обратното пускане във водата на видовете, изброени в таблица 3 и/или видовете, определени на равнище морски региони, както е необходимо за целите на управлението на риболовните стопанства. Нуждите на крайния потребител от данни за възрастта или други биологични данни, посочени в точки i) — iii), за любителски риболов се оценяват на равнище морски региони.

б) В допълнение към данните, събирани по силата на буква а), данните за анадромните и катадромните видове, изброени в таблица 1E, уловени от търговския риболов в сладководния стадий от жизнения им цикъл, независимо от начина, по който се извършват посочените риболовни дейности, както следва:

i) свързани със запаса променливи (за отделните екземпляри, за възраст, дължина, тегло, пол, зрелост и плодовитост, по жизнен стадий, но допълнително уточнени въз основа на видове и региони), и

ii) количества на годишния улов по възрастова категория или жизнен стадий.

в) Освен това:

по отношение на запасите от змиорки, се събира ежегодно информация (например данни, оценки, тенденции и т.н.) от поне един речен басейн на звено за управление на запасите от змиорки за следното:

i) изобилието на нови индивиди,

ii) изобилието на постоянни запаси (жълти змиорки), и

iii) броят или теглото, като и съотношението по пол на мигриращите сребърни змиорки,

и по отношение на всичката дива сьомга: ежегодно събираната информация — освен ако не е уговорено друго на равнище морски регион — за изобилието от млада сьомга преди и в процес на миграция към морето и броя на индивидите, които мигрират към реките.

Определянето на реките, които да се наблюдават за змиорката и сьомгата, се извършва на равнище региони. Подборът на запасите, от които да се съберат посочените променливи, се координира на равнище региони въз основа на нуждите на крайния потребител;

3. **Данни, за да се оцени въздействието на рибарството на Съюза върху морските екосистеми във водите на Съюза и извън водите на Съюза**

Тези данни включват следната информация:

а) За всички видове риболов, случайният прилов на всички птици, бозайници и влечуги и риби, защитени по силата на законодателството на Съюза и международните споразумения, включително видовете, посочени в таблица 1D, включително липсата в улова, по време на научните пътувания за наблюдение с риболовните кораби, или от самите рибари в риболовните дневници.

Когато за данните, събрани по време на пътувания за наблюдение, се счита, че не осигуряват достатъчни данни за случайния прилов за нуждите на крайния потребител, държавите членки прилагат други методологии. Подборът на тези методологии се координира на равнище морски региони и се основава на нуждите на крайния потребител.

б) Данните в подкрепа на оценката на въздействието на риболова във водите на Съюза и извън водите на Съюза върху морските местообитания.

Използваните променливи за оценката на въздействието на риболова върху морските местообитания са вписаните съгласно Регламент (ЕС) № 1224/2009. Разбивката на данните е на равнище на риболовна дейност 3 ([1]), освен ако на регионално ниво се изисква по-ниско ниво на обобщаване, по-специално в морските защитени зони.

([1]) Вж. таблица 2

Когато данните, вписани съгласно Регламент (ЕС) № 1224/2009, не са с нужната прецизност или с достатъчно качество или обхват за научното им предназначение, те се събират по алтернативен начин с прилагане на подходящи методи за изготвяне на извадка. Данните, вписвани съгласно Регламент (ЕС) № 1224/2009, трябва да се предоставят с подходящо ниво на обобщаване на националните институции, отговарящи за изпълнението на работните планове.

в) Данните за оценка на равнището на риболова и въздействието на риболовните дейности върху морските биологични ресурси и морските екосистеми, като например ефекта върху нетърговските видове, отношенията хищник — плячка и естествената смъртност на видовете риба във всеки морски регион.

Тези данни първоначално се оценяват в пилотни проучвания. Въз основа на резултатите от тези пилотни проучвания държавите членки определят бъдещото събиране на данни, специфични за всеки морски регион, координирани на равнище морски регион и основани на нуждите на крайния потребител.

4. **Подробни данни за дейността на риболовните кораби на Съюза** [1] **във водите на Съюза и извън водите на Съюза, вписвани съгласно Регламент (ЕС) № 1224/2009.**

Данните за оценката на дейността на риболовните кораби на Съюза във водите на Съюза и извън водите на Съюза се състоят от променливите, посочени в таблица 4. Данните, вписвани, докладвани и представяни съгласно Регламент (ЕС) № 1224/2009, се предоставят под формата на първични данни на националните институции, отговарящи за изпълнението на работните планове. Когато тези данни не се събират съгласно Регламент (ЕС) № 1224/2009 или когато данните, събирани съгласно Регламент (ЕС) № 1224/2009, не са с нужната прецизност или с достатъчно качество или обхват за научното им предназначение, те се събират чрез прилагане на подходящи методи за изготвяне на извадка. Тези методи позволяват оценката на променливите, изброени в таблица 4, на най-ниското съответно географско равнище по сегмент от флота (таблица 5а) и равнище на група сходни риболовни дейности 6 (таблица 2).

5. **Социално-икономически данни за риболова, даващи възможност за оценка на социално-икономическите показатели на сектора на рибарството в Съюза.**

Тези данни включват следната информация:

а) Икономическите променливи, както са посочени в таблица 5A, според сектора сегментация на таблица 5B, и според супрарегионите съгласно определението в таблица 5C.

Съвкупността са всички активни и неактивни кораби, регистрирани в регистъра на риболовния флот на Съюза съгласно определението в Регламент (ЕО) № 26/2004 на Комисията [2] на 31 декември на отчетната година, и кораби, които не са вписани в регистъра към посочената дата, но които извършват риболов най-малко един ден през отчетната година.

За неактивните кораби се събират само капиталовата стойност и капиталовите разходи.

В случаи, когато е налице риск от идентифициране на физически лица и/или юридически лица, за отчитането на икономическите променливи може да се използват гнезда, за да се осигури статистическа поверителност. Схемата с гнезда може да се използва също така, ако е необходимо да се изготви план за вземане на проби, статистически издържан. Схемата с гнезда е постоянна във времето.

Икономическите данни се събират на годишна основа.

б) Социалните променливи, както са посочени в таблица 6.

Социалните данни се събират на всеки три години, считано от 2018 г.

Данните за заетостта по образователна степен и заетостта по националност могат да се събират въз основа на пилотни проучвания.

---

[1] Включително специфичните изисквания за РОУР, посочени в Регламент (ЕС) № 1343/2011 на Европейския парламент и на Съвета от 13 декември 2011 година относно определени разпоредби за риболова в зоната по Споразумението за GFCM (Генералната комисия по рибарство в Средиземно море) и за изменение на Регламент (ЕО) № 1967/2006 на Съвета относно мерките за управление на устойчивата експлоатация на рибните ресурси в Средиземно море (ОВ L 347, 30.12.2011 г., стр. 44).

[2] Регламент (ЕО) № 26/2004 на Комисията от 30 декември 2003 г. относно регистъра на риболовния флот на Общността (ОВ L 5, 9.1.2004 г., стр. 25).

6. **Социални, икономически и екологични данни за морските аквакултури и по избор относно сладководните аквакултури, даващи възможност за оценка на социалните, икономическите и екологичните резултати на сектора на аквакултурите в Съюза**

Тези данни включват следната информация:

а) Икономически променливи, посочени в таблица 7 според сегментирането по сектор, определено в таблица 9.

Съвкупността са всички предприятия, чиято основна дейност се определя съгласно Европейската класификация на икономическите дейности NACE ([1]), кодове 03.21 и 03.22 и които развиват дейност с цел печалба.

Икономическите данни се събират на годишна основа.

б) Социалните променливи, както са посочени в таблица 6.

Социалните данни се събират на всеки три години, считано от 2018 г.

Данните за заетостта по образователна степен и за заетостта по националност могат да се събират въз основа на пилотни проучвания.

в) Данни за околната среда относно аквакултурите, както е посочено в таблица 8, позволяващи оценка на аспекти на техните показатели за околната среда.

Данни за околната среда могат да бъдат събирани въз основа на пилотни проучвания и екстраполирани, за да се получат крайни резултати, свързани с общия обем на произвежданата в държавата членка риба.

Данните за околната среда се събират на всеки две години.

ГЛАВА IV

Научни изследвания по море

1. Провеждат се най-малко всички научни изследвания по море, изброени в таблица 10, освен ако след преглед на изследванията се стигне до извода, че изследването вече не е подходящо за оценка на запасите и управление на рибарството. Въз основа на същите критерии за научен преглед към тази таблица могат да се добавят нови изследвания.

2. Държавите членки определят, в рамките на работните планове, определени в член 21 от Регламент (ЕС) № 508/2014 научни изследвания в открити води, които се извършват, и отговаря за тези проучвания.

3. Приносът на държавите членки за международните научни изследвания се координира в рамките на един и същ морски регион.

4. В националните си работни планове държавите членки осигуряват приемственост спрямо структурата на предишните изследвания.

ГЛАВА V

Прагове

1. Настоящата глава се прилага за рибарството на Съюза.

2. Не е необходимо да се събират биологични данни, ако за дадени рибни запаси или видове риба:

а) делът на държавата членка в съответния общ допустим улов (ОДУ) е по-малък от 10 % от общия за Съюза, или

([1]) Регламент (ЕО) № 1893/2006 на Европейския парламент и на Съвета от 20 декември 2006 г. за установяване на статистическа класификация на икономическите дейности NACE Rev. 2 и за изменение на Регламент (ЕИО) № 3037/90 на Съвета, както и на някои ЕО регламенти относно специфичните статистически области (ОВ L 393, 30.12.2006 г., стр. 1).

б) ако ОДУ не е определен, общите разтоварени на брега количества от запаса или вида риба от държавата членка са по-малко от 10 % от средните общи разтоварвания на брега в ЕС през предходните 3 години, или

в) общите годишни разтоварвания на брега на даден вид риба от държавата членка са под 200 тона. За видове с потребност от специфично управление може да се определи по-нисък праг на равнище морски региони.

Когато сумата от съответните квоти на няколко държави членки, чиито дял на ОДУ е под 10 %, е по-висока от 25 % от дела на ОДУ за определен запас, прагът от 10 % по буква а) не се прилага, а държавите членки си поделят задачите на равнище региони, за да гарантират, че запасите са включени в извадката в съответствие с нуждите на крайния потребител.

Не се прилага праг за големи пелагични видове и за анадромните и катадромните видове.

3. Без да се засягат по-конкретните разпоредби, свързани с международните задължения по РОУР, биологични данни не се събират, ако за някой международно експлоатиран рибен запаси, различен от едрите пелагични видове или далекомигриращите видове, делът на Съюза е по-малък от 10 %.

4. Държавите членки предоставят изчисления на улова от съществуващите изследвания на любителския риболов, включително проведените по рамката за събиране на данни, или от допълнително пилотно проучване, в срок от две години от датата, на която влиза в сила настоящото решение. Тези изследвания позволяват да се оцени дела на улова от любителски риболов, съотнесен към улова от търговски риболов, за всички видове в даден морски регион, за които съгласно настоящата многогодишна програма на Съюза се изискват данни за улова от любителски риболов. Последващата структура и обхват на националните изследвания на любителския риболов, включително праговете за събиране на данни, се координира на равнище морски региони и се основава на нуждите на крайния потребител.

Праг не се прилага за улова от любителски риболов на рибни запаси, които са обект на планове за възстановяване или на многогодишни планове за управление, например прилаганите за едрите пелагични видове и далекомигриращите видове.

5. Не се събират социални и икономически данни за аквакултурите, ако общото производство на държавата членка е по-малко от 1 % от общия обем на производството на Съюза и общата стойност. Не се събират данни за аквакултурите за видовете, представляващи по-малко от 10 % от обема и стойността на производството на аквакултури на държавата членка. Освен това държавите членки с общо производство, възлизащо на по-малко от 2,5 % от общия обем и общата стойност на производството на аквакултури в Съюза, могат да определят опростена методика, например пилотни проучвания с оглед екстраполирането на изискваните данни за видовете, които съставляват над 10 % от обема и стойността на производството на аквакултури на държавите членки.

Референтни данни са последните предоставени от държавите членки данни съгласно Регламент (ЕО) № 762/2008 на Европейския парламент и на Съвета ([1]) и съответните данни, публикувани от Евростат.

6. Не се събират данни за околната среда по отношение на аквакултури, когато общото производство на аквакултури в държавата членка е под от 2,5 % от общия обем и общата стойност на производството на аквакултури в Съюза.

Референтни данни са последните предоставени от държавите членки данни съгласно Регламент (ЕО) № 762/2008 на Европейския парламент и на Съвета и съответните данни, публикувани от Евростат.

7. Участието на дадена държава членка (физическо или финансово) в научните изследвания в открито море, посочени в таблица 10, не е задължително, когато нейният дял от ОДУ на Съюза на целевите видове в изследването е под прага от 3 %. Когато ОДУ не е определен, участието на дадена държава членка (физическо или финансово) в научните изследвания в открито море не е задължително, когато през предходните 3 години нейният дял от общия брой разтоварвания на Съюза на запас или вид е под прага от 3 %. Праговете за изследванията на множество видове и на екосистеми могат да се определят на равнище морски региони.

8. Независимо от точки 2—7, в рамките на един и същ морски регион държавите членки могат да се споразумеят за алтернативни прагове.

([1]) Регламент (ЕО) № 762/2008 на Европейския парламент и на Съвета от 9 юли 2008 г. за предоставянето от държавите членки на статистика относно аквакултурите и за отмяна на Регламент (ЕО) № 788/96 (ОВ L 218, 13.8.2008 г., стр. 1).

БИОЛОГИЧНИ ДАННИ

Таблица 1A

Запаси във водите на Съюза

Вид (общоприето наименование)	Вид (научно наименование)	Зона (на ICES [1]), МКРБМ [2]) или код на зоната на FAO [3])), в която се намира запасът/Код на запаса
Норвежко море и Източна Арктика, Баренцово море		
Европейска змиорка	*Anguilla anguilla*	I, II
Менек	*Brosme brosme*	I, II
Херинга	*Clupea harengus*	I, II
Атлантическа треска	*Gadus morhua*	I, II
Мойва	*Mallotus villosus*	I, II
Пикша	*Melanogrammus aeglefinus*	I, II
Син меджид	*Micromesistius poutassou*	I-II
Северна скарида	*Pandalus borealis*	I, II
Сайда	*Pollachius virens*	I, II
Черна писия	*Reinhardtius hippoglossoides*	I, II
Сьомга	*Salmo salar*	I, II
Скумрия	*Scomber scombrus*	II,
Златист костур	*Sebastes marinus.*	I, II
Морски костур	*Sebastes mentella.*	I, II
Сафрид	*Trachurus trachurus*	IIa,
Скагерак и Категат		
Пясъчница, видове	*Ammodytidae*	IIIa
Европейска змиорка	*Anguilla anguilla*	IIIa
Херинга	*Clupea harengus*	IIIa/22-24, IIIa
Гренадир	*Coryphaenoides rupestris*	IIIa
Сива морска лястовица	*Eutrigla gurnardus*	IIIa
Червена морска лястовица	*Aspitrigla cuculus*	IIIa,

Вид (общоприето наименование)	Вид (научно наименование)	Зона (на ICES [1]), МКРБМ [2]) или код на зоната на FAO [3])), в която се намира запасът/Код на запаса
Атлантическа треска	*Gadus morhua*	IIIaN
Атлантическа треска	*Gadus morhua*	IIIaS
Червена писия	*Glyptocephalus cynoglossus*	IIIa
Лиманда	*Limanda limanda*	IIIa
Пикша	*Melanogrammus aeglefinus*	IIIa
Меджид	*Merlangius merlangus*	IIIa
Мерлуза	*Merluccius merluccius*	IIIa,
Син меджид	*Micromesistius poutassou*	IIIa
Норвежки омар	*Nephrops norvegicus*	Функционална единица
Северна скарида	*Pandalus borealis*	IIIa
Морска писия	*Pleuronectes platessa*	IIIa
Сайда	*Pollachius virens*	IIIa
Сьомга	*Salmo salar*	IIIa
Калкан	*Psetta maxima*	IIIa
Скумрия	*Scomber scombrus*	IIIa
Средиземноморски калкан	*Scophthalmus rhombus*	IIIa
Морски език	*Solea solea*	IIIa
Цаца	*Sprattus sprattus*	IIIa
Норвежки паут	*Trisopterus esmarki*	IIIa
Всички акули, скатове и морски лисици за търговски цели [4])	*Selachii, Rajidae*	IIIa
	Балтийско море —	
Европейска змиорка	*Anguilla anguilla*	22—32
Херинга	*Clupea harengus*	22-24/25-29, 32/30/31/ Рижки залив
Чудски сиг	*Coregonus lavaretus*	IIId
Рипус	*Coregonus albula*	22—32
Атлантическа треска	*Gadus morhua*	22—24/25—32

Вид (общоприето наименование)	Вид (научно наименование)	Зона (на ICES (1), МКРБМ (2) или код на зоната на FAO (3)), в която се намира запасът/Код на запаса
Лиманда	*Limanda limanda*	22—32
Костур	*Perca fluviatilis*	IIId
Писия	*Platichtys flesus*	22—32
Морска писия	*Pleuronectes platessa*	22—32
Калкан	*Psetta maxima*	22—32
Сьомга	*Salmo salar*	22—31/32
Морска пъстърва	*Salmo trutta*	22—32
Бяла риба	*Sander lucioperca*	IIId
Средиземноморски калкан	*Scophthalmus rhombus*	22—32
Морски език	*Solea solea*	22
Цаца	*Sprattus sprattus*	22—32
	Северно море и Източен Ламанш	
Пясъчница	*Ammodytidae*	IV
Зъбатки	*Anarhichas* spp.	IV
Европейска змиорка	*Anguilla anguilla*	IV, VIId
Аргентина	*Argentina* spp.	IV
Сива морска лястовица	*Eutrigla gurnardus*	IV
Менек	*Brosme brosme*	IV
Херинга	*Clupea harengus*	IV, VIId
Обикновена скарида	*Crangon crangon*	IV, VIId
Лаврак	*Dicentrarchus labrax*	IV, VIId
Сива морска лястовица	*Eutrigla gurnardus*	IV
Треска	*Gadus morhua*	IV, VIId
Червена писия	*Glyptocephalus cynoglossus*	IV
Синя скропена	*Helicolenus dactylopterus*	IV
Петнист мегрим	*Lepidorhombus boscii*	IV, VIId

Вид (общоприето наименование)	Вид (научно наименование)	Зона (на ICES (1), МКРБМ (2) или код на зоната на FAO (3)), в която се намира запасът/Код на запаса
Мегрим	*Lepidorhombus whiffiagonis*	IV, VIId
Лиманда	*Limanda limanda*	IV, VIId
Чернокоремен морски дявол	*Lophius budegassa*	IV, VIId
Морски дявол	*Lophius piscatorius*	IV
Дългоопашата риба	*Macrourus berglax*	IV
Пикша	*Melanogrammus aeglefinus*	IV
Меджид	*Merlangius merlangus*	IV, VIId
Мерлуза	*Merluccius merluccius*	IV VII
Син меджид	*Micromesistius poutassou*	IV, VIId
Малоуста писия	*Microstomus kitt*	IV, VIId
Синя молва	*Molva dypterigia*	IV
Молва	*Molva molva*	IV
Червен барбун	*Mullus barbatus*	IV, VIId
Барбун ивичест	*Mullus surmuletus*	IV, VIId
Норвежки омар	*Nephrops norvegicus*	всички функционални единици
Северна скарида	*Pandalus borealis*	IVa East/IVa/IV
Миди Сен Жак	*Pecten maximus*	VIId
Брадата мерлуза	*Phycis blennoides*	IV
Налим	*Phycis phycis*	IV
Писия	*Platichthys flesus*	IV
Морска писия	*Pleuronectes platessa*	IV
Морска писия	*Pleuronectes platessa*	VIId
Сайда	*Pollachius virens*	IV
Калкан	*Psetta maxima*	IV, VIId
Черна писия	*Reinhardtius hippoglossoides*	IV

Вид (общоприето наименование)	Вид (научно наименование)	Зона (на ICES (1), МКРБМ (2) или код на зоната на FAO (3)), в която се намира запасът/Код на запаса
Сьомга	*Salmo salar*	IV, VIId
Скумрия	*Scomber scombrus*	IV, VIId
Средиземноморски калкан	*Scophthalmus rhombus*	IV, VIId
Морски костур	*Sebastes mentella.*	IV
Морски език	*Solea solea*	IV
Морски език	*Solea solea*	VIId
Цаца	*Sprattus sprattus*	IV/VIId
Сафрид	*Trachurus trachurus*	IV, VIId
Морска лястовица	*Trigla lucerna*	IV
Норвежки паут	*Trisopterus esmarki*	IV
Светипетрова риба	*Zeus faber*	IV, VIId
Всички акули, скатове и морски лисици за търговски цели (4)	*Selachii, Rajidae*	IV, VIId
Североизточна част на Атлантическия океан и Западен Ламанш		
Гладкоглава риба	*Alepocephalus bairdii*	VI, XII
Пясъчница	*Ammodytidae*	VIa
Капрови риби	*Phycis blennoides*	V, VI, VII
Кръгла раковина	*Pecten maximus*	IV, VI, VII
Кралска мида	*Aequipecten opercularis*	VII
Морски паяк	*Maja squinado*	V, VI, VII
Европейска змиорка	Anguilla anguilla	всички зони
Афанопус	*Aphanopus spp.*	всички зони
Аргентина	*Argentina* spp.	всички зони
Горбил	*Argyrosomus regius*	всички зони
Червена морска лястовица	*Aspitrigla cuculus*	всички зони
Берикс	*Beryx* spp.	всички зони без X и IXa
Берикс	*Beryx* spp.	IXa и X

Вид (общоприето наименование)	Вид (научно наименование)	Зона (на ICES (1), МКРБМ (2) или код на зоната на FAO (3)), в която се намира запасът/Код на запаса
Морски рак	*Cancer pagurus*	всички зони
Херинга	*Clupea harengus*	VIa/VIaN/ VIa S, VIIbc/VIIa/VIIj
Морска змиорка	*Conger conger*	всички зони без X
Морска змиорка	*Conger conger*	X
Гренадир	*Coryphaenoides rupestris*	всички зони
Черна акула	*Dalatias licha*	Всички зони
Обикновен скат	*Dasyatis pastinaca*	VII, VIII
Клюнеста акула	*Deania calcea*	V, VI, VII, IX, X, XII
Лаврак	*Dicentrarchus labrax*	всички зони без IX
Лаврак	*Dicentrarchus labrax*	IX
Морски език	*Dicologoglosa cuneata*	VIIIc, IX
Хамсия	*Engraulis encrasicolus*	IXa (единствено Кадис)
Хамсия	*Engraulis encrasicolus*	VIII
Нощна акула	*Etmopterus spinax*	VI, VII, VIII
Сива морска лястовица	*Eutrigla gurnardus*	VIId,e
Атлантическа треска	*Gadus morhua*	Va/Vb/VIa/VIb/VIIa/VIIe-k
Червена писия	*Glyptocephalus cynoglossus*	VI, VII
Синя скорпена	*Helicolenus dactylopterus*	всички зони
Омари	*Homarus gammarus*	всички зони
Атлантически големоглав	*Hoplostethus atlanticus*	всички зони
Сребриста риба сабя	*Lepidopus caudatus*	IXa
Петнист мегрим	*Lepidorhombus boscii*	VIIIc, IXa
Мегрим	*Lepidorhombus whiffiagonis*	VI/VII, VIIIabd/VIIIc, IXa
Лиманда	*Limanda limanda*	VIIe/VIIa,f-h
Обикновен калмар	*Loligo vulgaris*	всички зони без VIIIc, IXa
Обикновен калмар	*Loligo vulgaris*	VIIIc, IXa

Вид (общоприето наименование)	Вид (научно наименование)	Зона (на ICES (1), МКРБМ (2) или код на зоната на FAO (3)), в която се намира запасът/Код на запаса
Чернокоремен морски дявол	*Lophius budegassa*	IV, VI/VIIb-k, VIIIabd
Чернокоремен морски дявол	*Lophius budegassa*	VIIIc, IXa
Морски дявол	*Lophius piscatorious*	IV, VI/VIIb-k, VIIIabd
Морски дявол	*Lophius piscatorious*	VIIIc, IXa
Мойва	*Mallotus villosus*	XIV
Пикша	*Melanogrammus aeglefinus*	Va/Vb
Пикша	*Melanogrammus aeglefinus*	VIa/VIb/VIIa/VIIb-k
Меджид	*Merlangius merlangus*	VIII/IX, X
Меджид	*Merlangius merlangus*	Vb/VIa/VIb/VIIa/VIIe-k
Мерлуза	*Merluccius merluccius*	IIIa, IV, VI, VII, VIIIab/VIIIc, IXa
Морски език	*Microchirus variegatus*	всички зони
Син меджид	*Micromesistius poutassou*	I-IX, XII, XIV
Малоуста писия	*Microstomus kitt*	всички зони
Синя молва	*Molva dypterigia*	всички зони без X
Испанска молва	*Molva macrophtalma*	X
Молва	*Molva molva*	всички зони
Барбун ивичест	*Mullus surmuletus*	всички зони
Бялопетниста гладка кучешка акула	*Mustelus asterias*	VI, VII, VIII, IX
Гладка кучешка акула	*Mustelus mustelus*	VI, VII, VIII, IX
Чернопетниста кучешка акула	*Mustelus punctulatus*	VI, VII, VIII, IX
Норвежки омар	*Nephrops norvegicus*	VI функционална единица
Норвежки омар	*Nephrops norvegicus*	VII функционална единица
Норвежки омар	*Nephrops norvegicus*	VIII, IX функционална единица
Обикновен октопод	*Octopus vulgaris*	всички зони без VIIIc, IXa
Обикновен октопод	*Octopus vulgaris*	VIIIc, IXa

Вид (общоприето наименование)	Вид (научно наименование)	Зона (на ICES (1), МКРБМ (2) или код на зоната на FAO (3)), в която се намира запасът/Код на запаса
Червенопер пагел	*Pagellus bogaraveo*	IXa, X
Скарида пандалида	*Pandalus* spp.	всички зони
Розова скарида	*Parapenaeus longirostris*	IXa
Брадата мерлуза	*Phycis blennoides*	всички зони
Налим	*Phycis phycis*	всички зони
Морска писия	*Pleuronectes platessa*	VIIa/VIIe/VIIfg
Морска писия	*Pleuronectes platessa*	VIIbc/VIIh-k/VIII, IX, X
Сребриста сайда	*Pollachius pollachius*	всички зони без IX, X
Сребриста сайда	*Pollachius pollachius*	IX, X
Сайда	*Pollachius virens*	Va/Vb/IV, IIIa, VI
Сайда	*Pollachius virens*	VII, VIII
Американски бибан	*Polyprion americanus*	X
Калкан	*Psetta maxima*	всички зони
Черна писия	*Reinhardtius hippoglossoides*	V, XIV/VI
Атлантическа писия	*Hoplostethus atlanticus*	V, XIV
Сьомга	*Salmo salar*	всички зони
Сардина	*Sardina pilchardus*	VIIIabd/VIIIc, IXa
Испанска скумрия	*Scomber colias*	VIII, IX, X
Скумрия	*Scomber scombrus*	II, IIIa, IV, V, VI, VII, VIII, IX
Средиземноморски калкан	*Scophthalmus rhombus*	всички зони
Златист костур	*Sebastes marinus*	Подзони V, VI, XII, XIV на ICES и подзона 2 на NAFO + (участък 1F + 3K)
Морски костур	*Sebastes mentella*	Подзони V, VI, XII, XIV на ICES и подзона 2 на NAFO + (участък 1F + 3K)
Сепия	*Sepia officinalis*	всички зони
Морски език	*Solea solea*	VIIa/VIIfg
Морски език	*Solea solea*	VIIbc/VIIhjk/IXa/VIIIc

Вид (общоприето наименование)	Вид (научно наименование)	Зона (на ICES (1), МКРБМ (2) или код на зоната на FAO (3)), в която се намира запасът/Код на запаса
Морски език	*Solea solea*	VIIe
Морски език	*Solea solea*	VIIIab
Спаридови	*Sparidae*	всички зони
Средиземноморски сафрид	*Trachurus mediterraneus*	VIII, IX
Синя скумрия	*Trachurus mediterraneus*	VIII, IX, X
Сафрид	*Trachurus trachurus*	IIa, IVa, Vb, VIa, VIIa-c, e-k, VIIIabde/X
Сафрид	*Trachurus trachurus*	VIIIc, IXa
Паут	*Trisopterus* spp.	всички зони
Светипетрова риба	*Zeus faber*	всички зони
Всички акули, скатове и морски лисици за търговски цели (4)	*Selachii, Rajidae*	IV, VIId
	Средиземно море и Черно море	
Европейска змиорка	*Anguilla anguilla*	всички зони в Средиземно море
Гигантска червена скарида	*Aristeomorpha foliacea*	всички зони в Средиземно море
Червена скарида	*Aristeus antennatus*	всички зони в Средиземно море
Гопа	*Boops boops*	1.3, 2.1, 2.2, 3.1, 3.2
Корифена	*Coryphaena equiselis*	всички зони в Средиземно море
Корифена	*Coryphaena hippurus*	всички зони в Средиземно море
Лаврак	*Dicentrarchus labrax*	всички зони в Средиземно море
Обикновен октопод	*Eledone cirrhosa*	1.1, 1.3, 2.1, 2.2, 3.1
Мускусен октопод	*Eledone moschata*	1.3, 2.1, 2.2, 3.1
Хамсия	*Engraulis encrasicolus*	всички зони в Средиземно море
Хамсия	*Engraulis encrasicolus*	Черно море ГПЗ 29
Сива морска лястовица	*Eutrigla gurnardus*	2.2, 3.1
Калмар	*Illex* spp., *Todarodes* spp.	всички зони в Средиземно море
Марлина	*Istiophoridae*	всички зони в Средиземно море

Вид (общоприето наименование)	Вид (научно наименование)	Зона (на ICES (1), МКРБМ (2) или код на зоната на FAO (3)), в която се намира запасът/Код на запаса
Обикновен калмар	*Loligo vulgaris*	всички зони в Средиземно море
Морски дявол	*Lophius budegassa*	1.1, 1.2, 1.3, 2.2, 3.1
Морски дявол	*Lophius piscatorius*	1.1, 1.2, 1.3, 2.2, 3.1
Меджид	*Merlangius merlangus*	Черно море ГПЗ 29
Мерлуза	*Merluccius merluccius*	всички зони в Средиземно море
Син меджид	*Micromesistius poutassou*	1.1, 3.1
Кефалови	*Mugilidae*	1.3, 2.1, 2.2, 3.1
Червен барбун	*Mullus barbatus*	всички зони в Средиземно море
Червен барбун	*Mullus barbatus*	Черно море ГПЗ 29
Барбун ивичест	*Mullus surmuletus*	всички зони в Средиземно море
Обикновен октопод	*Octopus vulgaris*	всички зони в Средиземно море
Норвежки омар	*Nephrops norvegicus*	всички зони в Средиземно море
Червен пагел	*Pagellus erythrinus*	всички зони в Средиземно море
Розова скарида	*Parapenaeus longirostris*	всички зони в Средиземно море
Скарида Карамот	*Penaeus kerathurus*	3.1
Калкан	*Psetta maxima*	Черно море ГПЗ 29
Сардина	*Sardina pilchardus*	всички зони в Средиземно море
Скумрия	*Scomber* spp.	всички зони в Средиземно море
Сепия	*Sepia officinalis*	всички зони в Средиземно море
Морски език	*Solea vulgaris*	1.2, 2.1, 3.1
Златиста спара	*Sparus aurata*	1.2, 3.1
Смаридови	*Spicara smaris*	2.1, 3.1, 3.2
Цаца	*Sprattus sprattus*	Черно море ГПЗ 29
Рак богомолка	*Squilla mantis*	1.3, 2.1, 2.2
Средиземноморски сафрид	*Trachurus mediterraneus*	Всички области в Средиземно море

Вид (общоприето наименование)	Вид (научно наименование)	Зона (на ICES (1), МКРБМ (2) или код на зоната на FAO (3)), в която се намира запасът/Код на запаса
Средиземноморски сафрид	*Trachurus mediterraneus*	Черно море ГПЗ 29
Сафрид	*Trachurus trachurus*	всички зони в Средиземно море
Сафрид	*Trachurus trachurus*	Черно море ГПЗ 29
Морска лястовица	*Trigla lucerna*	1.3, 2.2, 3.1
Миди	*Veneridae*	2.1, 2.2
Стъкленка	*Aphia minuta*	ГПЗ 9,10,16 и 19
Голяма атерина	Atherina spp	ГПЗ 9,10,16 и 19
Треска от вида Trisopterus minutus	*Trsopterus minutus*	Всички региони
Всички акули, скатове и морски лисици за търговски цели (4)	*Selachii, Rajidae*	Всички региони

(1) Международен съвет за изследване на морето
(2) Международна комисия по риболова в Балтийско море
(3) Организацията на ООН по прехрана и земеделие
(4) Да се отчита на равнище видове.

БИОЛОГИЧНИ ДАННИ

Таблица 1B

Запаси от най-отдалечените региони на Съюза

Вид (общоприето наименование)	Видове (научно наименование)
Френска Гвиана	
Червен снапер	*Lutjanus purpureus*
Едри скариди	*Farfantepenaeus subtilis*
Риба от вида *Cynoscion acoupa*	*Cynoscion acoupa*
Риба от вида *Cynoscion steindachneri*	*Cynoscion steindachneri*
Риба от вида *Cynoscion virescens*	*Cynoscion virescens*
Морски котки	*Ariidae*
Риба от вида *Lobotes surinamensis*	*Lobotes surinamensis*
Риба от вида *Genyatremus luteus*	*Genyatremus luteus*
Видове от род *Centropomus*	Centropomus spp.

Вид (общоприето наименование)	Видове (научно наименование)
Групери	*Serranidae*
Кефал	Mugil spp.
Гваделупа и Мартиника	
Снапери	*Lutjanidae*
Риби от вида *Haemulidae*	*Haemulidae*
Групери	*Serranidae*
Риба лъв	*Pterois volitans*
Риби, подобни на риба тон	*Scombridae*
Син марлин	*Makaira nigricans*
Корифена	*Coryphaena hippurus*
Остров Реюнион и Майот	
Снапери	*Lutjanidae*
Групери	*Serranidae*
Риби, подобни на риба тон	*Scombridae*
Риба меч	*Xiphias gladius*
Други марлинови риби	*Istiophoridae*
Корифена	*Coryphaena hippurus*
Големоока сафрид	*Selar crumenophthalmus Bigeye scad*
Азорските острови, Мадейра и Канарските острови	
Атлантически сафрид	*Scomber colias*
Сардинела	*Sardinella maderensis*
Сафрид, видове	Trachurus spp.
Сардина	*Sardina pilchardus*
Риба папагал	*Sparisoma cretense*
Патела	*Patellidae*

БИОЛОГИЧНИ ДАННИ

Таблица 1C

Запаси в морски региони на регионалните организации за управление на рибните ресурси (РОУР) и на партньорствата в областта на устойчивото рибарство (ПОУР)

IATTC (Междуамериканска комисия за тропическата риба тон)

ВИД При изготвянето на планове за вземане на проби с цел събиране на биологични данни, както е посочено в глава III от настоящото приложение, се вземат предвид границите на запаса, определени от компетентните РОУР или регионалните риболовни организации (РРО), като за всеки запас се задели подходящ ресурс за вземане на проби.				Честота на събиране на биологични променливи
Научно наименование	Общоприето наименование	Географски район	Приоритет	Събирането на данни е годишно, а актуализирането/обработката на данните се извършва своевременно, за да се спази графикът на оценките на запасите.
Thunnus albacares	Жълтопер тунец (албакор)	Източна част на Тихия океан	Висок	
Thunnus obesus	Големоок тон	Източна част на Тихия океан	Висок	
Katsuwonus pelamis	Ивичест тунец	Източна част на Тихия океан	Висок	
Thunnus alalunga	Бял тон	Източна част на Тихия океан	Висок	
Thunnus orientalis	Тихоокеански червен тон	Източна част на Тихия океан	Висок	
Xiphias gladius	Риба меч	Източна част на Тихия океан	Висок	
Makaira nigricans (или Mazara)	Син марлин	Източна част на Тихия океан	Висок	
Makaira indica	Черен марлин	Източна част на Тихия океан	Висок	
Tetrapturus audax	Ивичест марлин	Източна част на Тихия океан	Висок	

ICCAT (Международната комисия за опазване на рибата тон в Атлантическия океан)

ВИД При изготвянето на планове за вземане на проби с цел събиране на биологични данни, както е посочено в глава III от настоящото приложение, се вземат предвид границите на запаса, определени от компетентните РОУР или РРО, като за всеки запас се задели подходящ ресурс за вземане на проби.				Честота на събиране на биологични променливи
Научно наименование	Общоприето наименование	Географски район	Приоритет	Събирането на данни е годишно, а актуализирането/обработката на данните се извършва своевременно, за да се спази графикът на оценките на запасите.
Thunnus albacares	Жълтопер тунец (албакор)	Атлантически океан и прилежащите морета	Висок	
Thunnus obesus	Големоок тон	Атлантически океан и прилежащите морета	Висок	
Katsuwonus pelamis	Ивичест тунец	Атлантически океан и прилежащите морета	Висок	
Thunnus alalunga	Бял тон	Атлантически океан и прилежащите морета	Висок	

ВИД При изготвянето на планове за вземане на проби с цел събиране на биологични данни, както е посочено в глава III от настоящото приложение, се вземат предвид границите на запаса, определени от компетентните РОУР или РРО, като за всеки запас се задели подходящ ресурс за вземане на проби.				Честота на събиране на биологични променливи
Thunnus thynnus	Червен тон	Атлантически океан и прилежащите морета	Висок	
Xiphias gladius	Риба меч	Атлантически океан и прилежащите морета	Висок	
Makaira nigricans (или Mazara)	Син марлин	Атлантически океан и прилежащите морета	Висок	
Istiophorus albicans	Риба ветроход	Атлантически океан и прилежащите морета	Висок	
Engraulis encrasicolus	Бял марлин	Атлантически океан и прилежащите морета	Висок	
Prionace glauca	Синя акула	Атлантически океан и прилежащите морета	Висок	
Auxis rochei	Ивичеста ауксида	Атлантически океан и прилежащите морета	Висок	
Atlantic bonito	Атлантически бонито	Атлантически океан и прилежащите морета	Висок	
Euthynnus alleteratus	Обикновен тон	Атлантически океан и прилежащите морета	Умерен	
Thunnus atlanticus	Чернопер тунец	Атлантически океан и прилежащите морета	Умерен	
Orcynopsis unicolor	Обикновен бонито	Атлантически океан и прилежащите морета	Умерен	
Scomberomorus brasiliensis	Испанска скумрия на тесни ивички	Атлантически океан и прилежащите морета	Умерен	
Scomberomorus regalis	Скумрия от вида *Scomberomorus regalis*	Атлантически океан и прилежащите морета	Умерен	
Auxis thazard	Обикновена ауксида	Атлантически океан и прилежащите морета	Умерен	
Scomberomorus cavalla	Кралска скумрия	Атлантически океан и прилежащите морета	Умерен	
Scomberomorus tritor	Западноафриканска испанска скумрия	Атлантически океан и прилежащите морета	Умерен	
Scomberomorus maculatus	Атлантическа испанска скумрия	Атлантически океан и прилежащите морета	Умерен	

ВИД При изготвянето на планове за вземане на проби с цел събиране на биологични данни, както е посочено в глава III от настоящото приложение, се вземат предвид границите на запаса, определени от компетентните РОУР или РРО, като за всеки запас се задели подходящ ресурс за вземане на проби.				Честота на събиране на биологични променливи
Acanthocybium solandri	Уаху	Атлантически океан и прилежащите морета	Умерен	
Coryphaena hippurus	Корифена	Атлантически океан и прилежащите морета	Умерен	

NAFO (Организация за риболова в северната част на Атлантическия океан)

ВИД При изготвянето на планове за вземане на проби с цел събиране на биологични данни, както е посочено в глава III от настоящото приложение, се вземат предвид границите на запаса, определени от компетентните РОУР или РРО, като за всеки запас се задели подходящ ресурс за вземане на проби.				Честота на събиране на биологични променливи
Научно наименование	Общоприето наименование	Рибни запаси, както са определени от РОУР	Приоритет	
Gadus morhua	Атлантическа треска	NAFO 2J 3KL	Ниско	
Gadus morhua	Атлантическа треска	NAFO 3M	Високо	
Gadus morhua	Атлантическа треска	NAFO 3NO	Високо	
Gadus morhua	Атлантическа треска	NAFO 3P	Високо	
Gadus morhua	Атлантическа треска	NAFO SA1	Високо	
Glyptocephalus cynoglossus	Червена писия	NAFO 3NO	Високо	
Glyptocephalus cynoglossus	Червена писия	NAFO 2J3KL	Ниско	Събирането на данни е годишно, а актуализирането/обработката на данните се извършва своевременно, за да се спази графикът на оценките на запасите.
Hippoglossoides platessoides	Американска писия	NAFO 3LNO	Високо	
Hippoglossoides platessoides	Американска писия	NAFO 3M	Високо	
Limanda ferruginea	Жълтоопашата лиманда	NAFO 3LNO	Умерен	
Coryphaenoides rupestris	Гренадир	NAFO SA0 + 1	Ниско	
Macrourus berglax	Дългоопашата риба	NAFO SA2 + 3	Високо	
Pandalus borealis	Северна скарида	NAFO 3LNO	Високо	
Pandalus borealis	Северна скарида	NAFO 3M	Високо	
Amblyraja radiata	Бодлива морска лисица	NAFO 3LNOP	Високо	
Reinhardtius hippoglossoides	Черна писия	NAFO 3KLMNO	Високо	

ВИД При изготвянето на планове за вземане на проби с цел събиране на биологични данни, както е посочено в глава III от настоящото приложение, се вземат предвид границите на запаса, определени от компетентните РОУР или РРО, като за всеки запас се задели подходящ ресурс за вземане на проби.				Честота на събиране на биологични променливи
Reinhardtius hippoglossoides	Черна писия	NAFO SA1	Високо	
Hippoglossus hippoglossus	Атлантическа писия	NAFO SA1	Ниско	
Sebastes mentella	Морски костур	NAFO SA1	Високо	
Sebastes spp.	Морски костур	NAFO 3LN	Високо	
Sebastes spp.	Морски костур	NAFO 3M	Високо	
Sebastes spp.	Морски костур	NAFO 3O	Високо	
Urophycis tenuis	Бяла мерлуза	NAFO 3NO	Високо	
Mallotus villosus	Мойва	NAFO 3NO	Високо	
Beryx spp.	Берикс	NAFO 6G	Високо	
Illex illecebrosus	Късоопашат калмар	NAFO SA 3 + 4	Ниско	
Salmo salar	Сьомга	NAFO S1+ подучастък XIV на ICES, NEAF, NASCO	Високо	

FAO морска зона 34 — Комисия по риболова в централната източна част на Атлантическия океан (CECAF)

ВИД При изготвянето на планове за вземане на проби с цел събиране на биологични данни, както е посочено в глава III от настоящото приложение, се вземат предвид границите на запаса, определени от компетентните РОУР или РРО, като за всеки запас се задели подходящ ресурс за вземане на проби.				Честота на събиране на биологични променливи
Научно наименование	Общоприето наименование	Географски район	Приоритет	
Brachydeuterus spp.	Пристипома	34.3.1, 34.3.1, 34.3.3-6	висок	
Caranx spp.	Сафрид	34.3.1, 34.3.3-6	висок	
Cynoglossus spp.	Морски език	34.1.1, 34.1.3, 34.3.1, 34.3.3-6	висок	Събирането на данни е годишно, а актуализирането/обработката на данните се извършва своевременно, за да се спази графикът на оценките на запасите.
Decapterus spp.	Сафрид	34.3.1., 34.3.3-6.	висок	
Dentex canariensis	Канарски зъбар	34.1.1, 34.1.3, 34.3.1, 34.3.3-6	умерен	
Dentex congoensis	Конгоански зъбар	34.1.1, 34.1.3, 34.3.1, 34.3.3-6	умерен	
Dentex macrophthalmus	Големоок зъбар	34.1.1, 34.1.3, 34.3.1, 34.3.3-6	висок	

ВИД При изготвянето на планове за вземане на проби с цел събиране на биологични данни, както е посочено в глава III от настоящото приложение, се вземат предвид границите на запаса, определени от компетентните РОУР или РРО, като за всеки запас се задели подходящ ресурс за вземане на проби.				Честота на събиране на биологични променливи
Dentex maroccanus	Марокански зъбар	34.1.1, 34.1.3, 34.3.1, 34.3.3-6	умерен	
Dentex spp.	Зъбар	34.1.1, 34.1.3, 34.3.1, 34.3.3-6	висок	
Engraulis encrasicolus	Хамсия	34.1.1, 34.1.3, 34.3.1, 34.3.3-6	висок	
Epinephelus aeneus	Епинефелус	34.3.1, 34.3.1, 34.3.3-6	висок	
Ethmalosa fimbriata	Бонга херинга	34.3.1, 34.3.3-6	висок	
Farfanepenaeus notialis	Южна розова дребна скарида	34.1.1, 34.1.3, 34.3.1, 34.3.3-6	висок	
Galeoides decadactylus	Малка африканска тънкопера риба	34.3.1, 34.3.1, 34.3.3-6	висок	Събирането на данни е годишно, а актуализирането/обработката на данните се извършва своевременно, за да се спази графикът на оценките на запасите.
Loligo vulgaris	Обикновен калмар	34.1.1, 34.1.3, 34.3.1, 34.3.3-6	висок	
Merluccius polli	Бенгелска мерлуза	34.1.1, 34.1.3, 34.3.1, 34.3.3-6	висок	
Merluccius senegalensis	Сенегалска мерлуза	34.1.1, 34.1.3, 34.3.1, 34.3.3-6	висок	
Merluccius spp.	Други мерлузи	34.1.1, 34.1.3, 34.3.1, 34.3.3-6	умерен	
Octopus vulgaris	Обикновен октопод	34.1.1, 34.1.3, 34.3.1, 34.3.3-6	висок	
Pagellus acarne	Сребрист пагел	34.1.1	висок	
Pagellus bellottii	Пагел на червени точки	34.1.1, 34.1.3, 34.3.1, 34.3.3-6	висок	
Pagellus bogaraveo	Червенопер пагел	34.1.1	умерен	
Pagellus spp.	Червен пагел	34.1.1, 34.1.3, 34.3.1, 34.3.3-6	висок	
Pagrus caeruleostictus	Син петнист пагел	34.1.1, 34.1.3, 34.3.1, 34.3.3-6	висок	
Parapenaeus longirostris	Дълбоководна розова скарида	34.1.1, 34.1.3, 34.3.1, 34.3 3-6	висок	
Pomadasys incisus	Боло (пристипома)	34.1.1	умерен	
Pomadasys spp.	Пристипома	34.1.1, 34.1.3, 34.3.1, 34.3.3-6	висок	

ВИД При изготвянето на планове за вземане на проби с цел събиране на биологични данни, както е посочено в глава III от настоящото приложение, се вземат предвид границите на запаса, определени от компетентните РОУР или РРО, като за всеки запас се задели подходящ ресурс за вземане на проби.				Честота на събиране на биологични променливи
Pseudotolithus spp.	Западноафрикански горбили	34.1.1	висок	
Sardina pilchardus	Сардина	34.1.1, 34.1.3	висок	
Sardinella aurita	Кръгла сардинела	34.1.1, 34.1.3, 34.3.1, 34.3.3-6	висок	
Sardinella maderensis	Плоска сардина	34.1.1, 34.1.3, 34.3.1, 34.3.3-6	висок	Събирането на данни е годишно, а актуализирането/обработката на данните се извършва своевременно, за да се спази графикът на оценките на запасите.
Scomber japonicus	Атлантическо-средиземноморска скумрия	34.1.1, 34.1.3, 34.3.1, 34.3.3-6	висок	
Scomber spp.	Други видове скумрии	34.1.1, 34.1.3, 34.3.1, 34.3.3-6	висок	
Sepia hierredda	Сепия	34.1.1, 34.1.3, 34.3.1, 34.3.3-6	висок	
Sepia officinalis	Обикновена сепия	34.1.1, 34.1.3, 34.3.1, 34.3.3-6	висок	
Sepia spp.	Сепия	34.1.1, 34.1.3, 34.3.1, 34.3.3-6	умерен	
Sparidae	Спаридови	34.1.1, 34.1.3, 34.3.1, 34.3.3-6	висок	
Sparus spp.	Ципура	34.1.1	висок	
Trachurus trachurus	Атлантически сафрид	34.1.1, 34.1.3, 34.3.1, 34.3.3-6	висок	
Trachurus trecae	Сафрид от вида *Trachurus trecae*	34.1.1, 34.1.3, 34.3.1, 34.3.3-6	висок	
Umbrina canariensis	Канарски горбил	34.3.3-6	умерен	

Организация за риболова в Югоизточния Атлантически океан (SEAFO)

ВИД При изготвянето на планове за вземане на проби с цел събиране на биологични данни, както е посочено в глава III от настоящото приложение, се вземат предвид границите на запаса, определени от компетентните РОУР или РРО, като за всеки запас се задели подходящ ресурс за вземане на проби.				Честота на събиране на биологични променливи
Научно наименование	Общоприето наименование	Географски район	Приоритет	Събирането на данни е годишно, а актуализирането/обработката на данните се извършва своевременно, за да се спази графикът на оценките на запасите.
Dissostichus eleginoides	Патагонски кликач	Югоизточен Атлантически океан	*Висок*	
Beryx spp.	Берикс	Югоизточен Атлантически океан	*Висок*	

ВИД При изготвянето на планове за вземане на проби с цел събиране на биологични данни, както е посочено в глава III от настоящото приложение, се вземат предвид границите на запаса, определени от компетентните РОУР или РРО, като за всеки запас се задели подходящ ресурс за вземане на проби.				Честота на събиране на биологични променливи
Chaceon spp.	Червен/Златен рак	Югоизточен Атлантически океан	*Висок*	
Pseudopentaceros richardsoni	Пелагична лъчеперка/Южна Капрова риба	Югоизточен Атлантически океан	*Висок*	
Helicolenus spp.	Чернокоремна риба	Югоизточен Атлантически океан	*Висок*	
Hoplostethus atlanticus	Атлантически големоглав	Югоизточен Атлантически океан	*Висок*	
Trachurus spp	Сафрид, видове	Югоизточен Атлантически океан	*Висок*	
Scomber spp	Скумрия	Югоизточен Атлантически океан	*Висок*	
Polyprion americanus	Американски бибан	Югоизточен Атлантически океан	*Умерен*	
Умерен	Скален омар Тристан	Югоизточен Атлантически океан	*Умерен*	
Lepidopus caudatus	Сребриста риба нож	Югоизточен Атлантически океан	*Умерен*	
Schedophilus ovalis	Черна риба от вида *Schedophilus ovalis*	Югоизточен Атлантически океан	*Нисък*	
Schedophilus velaini	Риба от вида *Schedophilus velaini*	Югоизточен Атлантически океан	*Нисък*	
Allocyttus verucossus	Риба от вида *Allocyttus verucossus*	Югоизточен Атлантически океан	*Нисък*	
Neocyttus romboidales		Югоизточен Атлантически океан		
Allocyttus guineensis		Югоизточен Атлантически океан		
Pseudocyttu smaculatus		Югоизточен Атлантически океан		
Emmelichthys nitidus	Риба от вида *Emmelichthys nitidus*	Югоизточен Атлантически океан	*Нисък*	
Ruvettus pretiosus	Маслена риба	Югоизточен Атлантически океан	*Нисък*	
Promethichthys prometheus	Риба от вида *Promethichthys prometheus*	Югоизточен Атлантически океан	*Нисък*	
Macrourus spp	Гренадир	Югоизточен Атлантически океан	*Нисък*	
Antimora rostrata	Синя антимора	Югоизточен Атлантически океан	*Нисък*	
Epigonus spp	Риба кардинал	Югоизточен Атлантически океан	*Нисък*	
Merluccius spp	Мерлуза	Югоизточен Атлантически океан	*Нисък*	

ВИД При изготвянето на планове за вземане на проби с цел събиране на биологични данни, както е посочено в глава III от настоящото приложение, се вземат предвид границите на запаса, определени от компетентните РОУР или РРО, като за всеки запас се задели подходящ ресурс за вземане на проби.				Честота на събиране на биологични променливи
Notopogon fernandezianus	Риба от вида *Notopogon fernandezianus*	Югоизточен Атлантически океан	*Нисък*	
Octopodidae и Loliginidae	Октоподи и сепии	Югоизточен Атлантически океан	*Нисък*	

Комисия за риболова в западен и централен Тихи океан

ВИД При изготвянето на планове за вземане на проби с цел събиране на биологични данни, както е посочено в глава III от настоящото приложение, се вземат предвид границите на запаса, определени от компетентните РОУР или РРО, като за всеки запас се задели подходящ ресурс за вземане на проби.				Честота на събиране на биологични променливи
Научно наименование	Общоприето наименование	Географски район	Приоритет	Събирането на данни е годишен и актуализиране/обработка на данни се извършва своевременно приноса на график на оценките на запасите.
Thunnus albacares	Жълтопер тунец (албакор)	Западна централна част на Тихия океан	Висок	
Thunnus obesus	Големоок тон	Западна централна част на Тихия океан	Висок	
Katsuwonus pelamis	Ивичест тунец	Западна централна част на Тихия океан	Висок	
Thunnus alalunga	Бял тон	Западна централна част на Тихия океан	Висок	
Thunnus orientalis	Тихоокеански червен тон	Западна централна част на Тихия океан	Висок	
Xiphias gladius	Риба меч	Западна централна част на Тихия океан	Висок	
Makaira nigricans (или Mazara)	Син марлин	Западна централна част на Тихия океан	Висок	
Makaira indica	Черен марлин	Западна централна част на Тихия океан	Висок	
Tetrapturus audax	Ивичест марлин	Западна централна част на Тихия океан	Висок	
Acanthocybium solandri	Уаху	Западна централна част на Тихия океан	Умерен	
Coryphaena hippurus	Корифена	Западна централна част на Тихия океан	Умерен	
Elagatis bipinnulata	Риба от вида *Elagatis bipinnulata*	Западна централна част на Тихия океан	Умерен	
Lepidocybium flavobrunneum	Риба от вида *Lepidocybium flavobrunneum*	Западна централна част на Тихия океан	Умерен	
Lampris regius	Риба от вида *Lampris regius*	Западна централна част на Тихия океан	Умерен	

ВИД При изготвянето на планове за вземане на проби с цел събиране на биологични данни, както е посочено в глава III от настоящото приложение, се вземат предвид границите на запаса, определени от компетентните РОУР или РРО, като за всеки запас се задели подходящ ресурс за вземане на проби.				Честота на събиране на биологични променливи
Mola Mola	Риба луна	Западна централна част на Тихия океан	Умерен	
Istiophorus platypterus	Риба ветроход	Западна централна част на Тихия океан	Умерен	
Tetrapturus angustirostris	Риба копие	Западна централна част на Тихия океан	Умерен	
Ruvettus pretiosus	Маслена риба	Западна централна част на Тихия океан	Умерен	
Prionace glauca	Синя акула	Западна централна част на Тихия океан	Висок	
Carcharhinus longimanus	Дългокрила акула	Западна централна част на Тихия океан	Висок	
Carcharhinus falciformis	Копринена акула	Западна централна част на Тихия океан	Висок	
Alopias superciliosus	Големоока акула скитница	Западна централна част на Тихия океан	Висок	
Alopias vulpinus	Обикновена акула скитница	Западна централна част на Тихия океан	Висок	
Alopias pelagicus	Пелагична акула скитница	Западна централна част на Тихия океан	Висок	

Забележка: за WCPF се добавят следните изисквания за докладване за кораби с парагада:

(1) Брой клонове между поплавъците. Броят клонове между поплавъците се отчита за всяка група.

(2) Брой на уловените риби за набор, за следните видове: Бял тон (*Thunnus alalunga*), големоок тон (*Thunnus obesus*), ивичест тон (*Katsuwonus pelamis*), жълтопер тунец (*Thunnus albacares*), ивичест марлин (*Tetrapturus audax*), син марлин (*Makaira mazara*), черен марлин (*Makaira indica*) и риба меч (*Xiphias gladius*), синя акула, копринена акула, дългокрила акула, акула мако, акула скитница, селдова акула (южно от 20° ю.ш., докато биологичните данни покажат, че е уместно това или друго географско ограничение), акули чук (от вида *Eusphyra blochii*, раковинна акула чук, голяма акула чук и гладка акула чук), китова акула и други видове, както са определени от Комисията.

Ако общото или средното тегло на уловени риби за набор от видове е регистрирано, се докладва и общото тегло или средното тегло на уловени риби за набор от видове. Ако общото или средното тегло на уловени риби за набор от видове не е регистрирано, общото тегло или средното тегло на уловени риби за набор от видове се изчислява приблизително и изчисленията се докладват. Общото тегло или средното тегло се отнася до общото тегло, а не до преработеното тегло.

WECAFC (Комисия по рибно стопанство в западноцентралната част на Атлантическия океан)

ВИД При изготвянето на планове за вземане на проби с цел събиране на биологични данни, както е посочено в глава III от настоящото приложение, се вземат предвид границите на запаса, определени от компетентните РОУР или РРО, като за всеки запас се задели подходящ ресурс за вземане на проби.				Честота на събиране на биологични променливи
Научно наименование	Общоприето наименование	Географски район	Приоритет	Събирането на данни е годишно, а актуализирането/обработката на данните се извършва своевременно, за да се спази графикът на оценките на запасите.
Panulirus argus	Карибска лангуста	Западна част на централния Атлантически океан	Висок	
Strombus gigas	Розов стромбус	Централна западна част на Атлантическия океан	Висок	

ВИД При изготвянето на планове за вземане на проби с цел събиране на биологични данни, както е посочено в глава III от настоящото приложение, се вземат предвид границите на запаса, определени от компетентните РОУР или РРО, като за всеки запас се задели подходящ ресурс за вземане на проби.				Честота на събиране на биологични променливи
Акулоподобни Selachii, Rajidae	Акули, скатове и морски лисици	Централна западна част на Атлантическия океан	Висок	
Coryphaena hippurus	Корифена	Централна западна част на Атлантическия океан	Висок	
Acanthocybium solandri	Уаху	Централна западна част на Атлантическия океан	Висок	
Epinephelus guttatus	Бодлоперка от вида *Epinephelus guttatus*	Централна западна част на Атлантическия океан	Висок	
Lutjanus vivanus	Копринен снапер	Централна западна част на Атлантическия океан	Висок	
Lutjanus buccanella	Чернопере снапер	Централна западна част на Атлантическия океан	Висок	
Lutjanus campechanus	Червен снапер	Централна западна част на Атлантическия океан	Висок	
Penaeus subtilis	Скариди от вида *Penaeus subtilis*	Френска Гвиана ИИЗ	Висок	

IOTC (Комисия за рибата тон в Индийския океан)

ВИД При изготвянето на планове за вземане на проби с цел събиране на биологични данни, както е посочено в глава III от настоящото приложение, се вземат предвид границите на запаса, определени от компетентните РОУР или РРО, като за всеки запас се задели подходящ ресурс за вземане на проби.				Честота на събиране на биологични променливи
Научно наименование	Общоприето наименование	Географски район	Приоритет	Събирането на данни е годишно, а актуализирането/обработката на данните се извършва своевременно, за да се спази графикът на оценките на запасите.
Thunnus albacares	Жълтопер тунец (албакор)	Източната и западната част на Индийския океан	Висок	
Thunnus obesus	Големоок тон	Източната и западната част на Индийския океан	Висок	
Katsuwonus pelamis	Ивичест тунец	Източната и западната част на Индийския океан	Висок	
Thunnus alalunga	Бял тон	Източната и западната част на Индийския океан	Висок	
Xiphias gladius	Риба меч	Източната и западната част на Индийския океан	Висок	
Makaira nigricans (или Mazara)	Син марлин	Източната и западната част на Индийския океан	Висок	
Makaira indica	Черен марлин	Източната и западната част на Индийския океан	Висок	
Tetrapturus audax	Ивичест марлин	Източната и западната част на Индийския океан	Висок	
Istiophorus platypterus	Индо-атлантически ветроход	Източната и западната част на Индийския океан	Висок	

ВИД При изготвянето на планове за вземане на проби с цел събиране на биологични данни, както е посочено в глава III от настоящото приложение, се вземат предвид границите на запаса, определени от компетентните РОУР или РРО, като за всеки запас се задели подходящ ресурс за вземане на проби.				Честота на събиране на биологични променливи
Auxis rochei	Ивичеста ауксида	Източната и западната част на Индийския океан	Умерен	
Auxis thazard	Обикновена ауксида	Източната и западната част на Индийския океан	Умерен	
Euthynnus affinis	Кауакауа	Източната и западната част на Индийския океан	Умерен	
Thunnus tonggol	Дългоопашата риба тон	Източната и западната част на Индийския океан	Умерен	
Scomberomorus guttatus	Индо-тихоокеанска кралска скумрия	Източната и западната част на Индийския океан	Умерен	
Scomberomorus commerson	Испанска скумрия на тесни ивички	Източната и западната част на Индийския океан	Умерен	
Prionace glauca	Синя акула	Източната и западната част на Индийския океан	Висок	
Alopias superciliosus	Големоока акула скитница	Източната и западната част на Индийския океан	Висок	
Carcharhinus falciformis	Копринени акули	Източната и западната част на Индийския океан	Висок	
Carcharhinus longimanus	Дългокрила акула	Източната и западната част на Индийския океан	Висок	
Alopias pelagicus	Големоока акула скитница	Източната и западната част на Индийския океан	Висок	
Sphyrna lewini	Бронзова акула чук	Източната и западната част на Индийския океан	Висок	

Други РОУР

ВИД При изготвянето на планове за вземане на проби с цел събиране на биологични данни, както е посочено в глава III от настоящото приложение, се вземат предвид границите на запаса, определени от компетентните РОУР или РРО, като за всеки запас се задели подходящ ресурс за вземане на проби.				Честота на събиране на биологични променливи
Научно наименование	Общоприето наименование	Географски район	Приоритет	Събирането на данни е годишно, а актуализирането/обработката на данните се извършва своевременно, за да се спази графикът на оценките на запасите.
Trachurus murphyi	Чилийски сафрид	Зона на Конвенцията SPRFMO	Висок	
Euphausia superba	Крил	Зона на Конвенцията CCAMLR	Висок	

ВИД При изготвянето на планове за вземане на проби с цел събиране на биологични данни, както е посочено в глава III от настоящото приложение, се вземат предвид границите на запаса, определени от компетентните РОУР или РРО, като за всеки запас се задели подходящ ресурс за вземане на проби.				Честота на събиране на биологични променливи
Dissostichus spp (Dissostichus eleginoides и Dissostichus mawsoni)	Кликач	Зона на Конвенцията CCAMLR	Висок	
Champsocephalus gunnari	Антарктическа ледена риба	Зона на Конвенцията CCAMLR	Нисък	
Ресурсите от риба, мекотели, ракообразни и други немигриращи видове в рамките на района, но с изключение на: i) немигриращи видове, предмет на риболовната юрисдикция на крайбрежните държави съгласно член 77, параграф 4 от Конвенцията на ООН от 1982 г. по морско право, и; ii) далекомигриращите видове, изброени в приложение I на Конвенцията на ООН от 1982 г. по морско право.		Зона на Конвенцията SIOFA		

БИОЛОГИЧНИ ДАННИ

Таблица 1D

Видове за наблюдение по програмите за защита в Съюза или съгласно международни задължения

Общоприето наименование	Научно наименование	Регион/РОУР	Правна рамка
Костни риби	Teleostei		
Есетрови	Acipenser spp.	Средиземно море и Черно море; Балтийско море; OSPAR II, IV	Приложение II към Конвенцията от Барселона ([1]), приложение IV към Протокола за опазване на биологичното и ландшафтното разнообразие на Черно море; OSPAR ([2]); HELCOM ([3])
Гладкоглави риби	*Alepocephalidae*	Всички региони	Свързана с дълбоководния риболов ([4])
Гладкоглава риба от вида *Alepocephalus bairdii*	*Alepocephalus bairdii*	Всички региони	Свързана с дълбоководния риболов
Гладкоглава риба от вида *Alepocephalus rostratus*	*Alepocephalus rostratus*	Всички региони	Свързана с дълбоководния риболов
Херинги понтика	*Alosa immaculata*	Черно море	Приложение IV към Протокола за опазване на биологичното и ландшафтното разнообразие на Черно море
Карагьоз	*Alosa alosa*	OSPAR II, III, IV	OSPAR
Чудски сиг	*Coregonus lavaterus*	OSPAR II	OSPAR
Атлантическа треска	*Gadus morhua*	OSPAR II, III; Балтийско море	OSPAR; HELCOM

Общоприето наименование	Научно наименование	Регион/РОУР	Правна рамка
Дългоносо морско конче	*Hippocampus guttulatus* (синоним: *Hippocampus ramulosus*)	OSPAR II, III, IV, V	OSPAR
Морско конче	*Hippocampus hippocampus*	OSPAR II, III, IV, V	OSPAR
Блеч	*Alosa tanaica*	Черно море	Приложение IV към Протокола за опазване на биологичното и ландшафтното разнообразие на Черно море
Синя антимора	*Antimora rostrata*	Всички региони	Свързана с дълбоководния риболов
Афанопус	*Aphanopus carbo*	Всички региони	Свързана с дълбоководния риболов
Афанопус	*Aphanopus intermedius*	Всички региони	Свързана с дълбоководния риболов
Раци	Astacus spp.	Черно море	Приложение IV към Протокола за опазване на биологичното и ландшафтното разнообразие на Черно море
Голяма пясъчна корюшка	*Atherina pontica*	Черно море	Приложение IV към Протокола за опазване на биологичното и ландшафтното разнообразие на Черно море
Зарган	*Belone belone euxini Günther*	Черно море	Приложение IV към Протокола за опазване на биологичното и ландшафтното разнообразие на Черно море
Берикс	Beryx spp.	Всички региони	Свързана с дълбоководния риболов
Бротула	*Cataetyx laticeps*	Всички региони	Свързана с дълбоководния риболов
Рипус	*Coregonus albula*	Балтийско море	Препоръка на РКС (регионална координационна среща) за Балтийско море
Панагора	*Cyclopterus lumpus*	Всички региони	Свързана с дълбоководния риболов
Пръстеновидна морска каракуда	*Diplodus annularis*	Средиземно море	Регламент (ЕО) № 1967/2006 на Съвета [5] (мин. размер на опазване)
Морска хиена	*Diplodus puntazzo*	Средиземно море	Регламент (ЕО) № 1967/2006 (минимален размер за опазване)
Ивичеста морска каракуда	*Diplodus sargus*	Средиземно море	Регламент (ЕО) № 1967/2006 (минимален размер за опазване)
Обикновена морска каракуда	*Diplodus vulgaris*	Средиземно море	Регламент (ЕО) № 1967/2006 (минимален размер за опазване)
Патагонски кликач	*Dissostichus eleginoides*	Всички региони	Свързана с дълбоководния риболов
Антарктически кликач	*Dissostichus mawsoni*	Всички региони	Свързана с дълбоководния риболов

Общоприето наименование	Научно наименование	Регион/РОУР	Правна рамка
Групери	Epinephelus spp.	Средиземно море	Регламент (ЕО) № 1967/2006 (минимален размер за опазване)
Черен кардинал	*Epigonus telescopus*	Всички региони	Уязвими видове, свързана с дълбоководния риболов
Попчета	*Gobiidae*	Черно море	Приложение IV към Протокола за опазване на биологичното и ландшафтното разнообразие на Черно море
Синя скорпена	*Helicolenus dactylopterus*	Всички региони	Свързана с дълбоководния риболов
Атлантическа писия	*Hippoglossus hippoglossus*	Всички региони	Свързана с дълбоководния риболов
Атлантически големоглав	*Hoplostethus atlanticus*	Всички региони; OSPAR I, V	Уязвими видове, свързана с дълбоководния риболов
Средиземноморски големоглав	*Hoplosthetus mediterraneus*	Всички региони	Свързана с дълбоководния риболов
Сребриста риба сабя	*Lepidopus caudatus*	Всички региони	Свързана с дълбоководния риболов
Спарид	*Lithognathus mormyrus*	Средиземно море	Регламент (ЕО) № 1967/2006 (минимален размер за опазване)
Златист морски кефал	*Liza aurata*	Черно море	Приложение IV към Протокола за опазване на биологичното и ландшафтното разнообразие на Черно море
Илария	*Liza saliens*	Черно море	Приложение IV към Протокола за опазване на биологичното и ландшафтното разнообразие на Черно море
Голям шарен ликод	*Lycods esmarkii*	Всички региони	Свързана с дълбоководния риболов
Макрурус, различна от гренадир и дългоопашата риба	Macrouridae различна от Coryphaenoides rupestris и Macrourus berglax	Всички региони	Свързана с дълбоководния риболов
Дългоопашата риба	*Macrourus berglax*	Всички региони	Свързана с дълбоководния риболов
Меджид	*Merlangius merlangus*	Балтийско море и Черно море	Препоръка за Балтийско море; Приложение IV към Протокола за опазване на биологичното и ландшафтното разнообразие на Черно море
Европейска змиорка	*Anguilla anguilla*	OSPAR I, II, III, IV, Балтийско море	OSPAR; HELCOM
Атлантическа сьомга	**Salmo salar*	OSPAR I, II, III, IV, Балтийско море	OSPAR; HELCOM
Червен тон	**Thunnus thynnus*	OSPAR V	OSPAR; HELCOM

Общоприето наименование	Научно наименование	Регион/РОУР	Правна рамка
Синя молва	*Molva dypterygia*	Всички региони	Свързана с дълбоководния риболов
Мора	*Mora moro*	Всички региони	Свързана с дълбоководния риболов
Кефал	Mugil spp.	Черно море	Приложение IV към Протокола за опазване на биологичното и ландшафтното разнообразие на Черно море
Гърбата змиорка	*Nesiarchus nasutus*	Всички региони	Свързана с дълбоководния риболов
Гърбата змиорка	*Notocanthus chemnitzii*	Всички региони	Свързана с дълбоководния риболов
Корюшка	*Osmerus eperlanus*	Балтийско море	Препоръка на РКС (регионална координационна среща) за Балтийско море, HELCOM
Испански пагел	*Pagellus acarne*	Средиземно море	Регламент (ЕО) № 1967/2006 (минимален размер за опазване)
Червенопер пагел	*Pagellus bogaraveo*	Средиземно море	Регламент (ЕО) № 1967/2006 (минимален размер за опазване)
Обикновена морска каракуда	*Pagrus pagrus*	Средиземно море	Регламент (ЕО) № 1967/2006 (минимален размер за опазване)
Американски бибан	*Polyprion americanus*	Средиземно море	Регламент (ЕО) № 1967/2006 (минимален размер за опазване)
Американски бибан	*Polyprion americanus*	Всички региони	Свързана с дълбоководния риболов
Лефер	*Pomatomus saltatrix*	Черно море	Приложение IV към Протокола за опазване на биологичното и ландшафтното разнообразие на Черно море
Норвежки бибан	*Sebastes viviparus*	Всички региони	Свързана с дълбоководния риболов
Моруна	*Huso huso*	Черно море	Приложение IV към Протокола за опазване на биологичното и ландшафтното разнообразие на Черно море
Дълбоководен бибан	*Trachyscorpia cristulata*	Всички региони	Свързана с дълбоководния риболов
Океански морски платики	Brama spp	ГПЗ 1.1, 1.2, 1.3 и Черно море ГПЗ 29	Приложение VIII към Регламент (ЕО) № 894/97 на Съвета [6]
Атлантически сафрид	*Scomber colias Gmelin*	Черно море	Приложение IV към Протокола за опазване на биологичното и ландшафтното разнообразие на Черно море
Попче от вида *Crystallogobius linearis*	*Crystallogobius linearis*	Черно море	Национални планове за управление
Химера	*Chimaera monstrosa*	Балтийско море	HELCOM

Общоприето наименование	Научно наименование	Регион/РОУР	Правна рамка
Карагьоз	*Alosa alosa*	Балтийско море	HELCOM
Средиземноморска финта	*Alosa fallax*	Балтийско море	HELCOM
Подвид на атлантическа херинга, хвърлящ хайвер през есента	Clupea harengus subsp.	Балтийско море	HELCOM
Чил косат	*Abramis ballerus*	Балтийско море	HELCOM
Уклей	*Alburnus alburnus*	Балтийско море	HELCOM
Распер	*Aspius aspius*	Балтийско море	HELCOM
Обикновена мряна	*Barbus barbus*	Балтийско море	HELCOM
Обикновена кротушка	*Gobio gobio*	Балтийско море	HELCOM
Сабица	*Pelecus cultratus*	Балтийско море	HELCOM
Лешанка	*Phoxinus phoxinus*	Балтийско море	HELCOM
Морунаш	*Vimba vimba*	Балтийско море	HELCOM
Обикновен щипок	*Cobitis taenia*	Балтийско море	HELCOM
Пъстърва	*Salmo trutta*	Балтийско море	HELCOM
Рипус	*Coregonus albula*	Балтийско море	HELCOM
Балтийски сиг	Coregonus balticus (синоним: Coregonus lavaretus, мигриращ)	Балтийско море	HELCOM
Марена	Coregonus maraena (синоним: Coregonus lavaretus, стационарен)	Балтийско море	HELCOM
Сиг от вида *Coregonus pallasii*	*Coregonus pallasii*	Балтийско море	HELCOM
Морска корюшка	*Osmerus eperlanomarinus*	Балтийско море	HELCOM
Чернокоремен морски дявол	*Lophius budegassa*	Балтийско море	HELCOM
Бодливка	*Spinachia spinachia*	Балтийско море	HELCOM
Игла от вида *Entelurus aequoreus*	*Entelurus aequoreus*	Балтийско море	HELCOM
Морско шило	*Nerophis ophidion*	Балтийско море	HELCOM
Игла от вида *Nerophis lumbriciformis*	*Nerophis lumbriciformis*	Балтийско море	HELCOM

Общоприето наименование	Научно наименование	Регион/РОУР	Правна рамка
Голяма морска игла	*Syngnathus acus*	Балтийско море	HELCOM
Широконоса морска игла	*Syngnathus typhle*	Балтийско море	HELCOM
Гренадир	*Coryphaenoides rupestris*	Балтийско море	HELCOM
Пикша	*Melanogrammus aeglefinus*	Балтийско море	HELCOM
Сребриста сайда	*Pollachius pollachius*	Балтийско море	HELCOM
Молва	*Lotidae Molva molva*	Балтийско море	HELCOM
Игла от рода *Lumpenus lampretaeformis*	*Lumpenus lampretaeformis*	Балтийско море	HELCOM
Океански костур	*Sebastidae Sebastes marinus*	Балтийско море	HELCOM
Норвежки костур	*Sebastes viviparus*	Балтийско море	HELCOM
Главоч	*Cottus gobio*	Балтийско море	HELCOM
Главоч от вида *Cottus poecilopus*	*Cottus poecilopus*	Балтийско море	HELCOM
Морски скорпион от вида *Myoxocephalus scorpius*	*Myoxocephalus scorpius*	Балтийско море	HELCOM
Главоч от вида *Taurulus bubalis*	*Taurulus bubalis*	Балтийско море	HELCOM
Морски скорпион от вида *Triglopsis quadricornis*	*Triglopsis quadricornis*	Балтийско море	HELCOM
Морски заек	*Cyclopterus lumpus*	Балтийско море	HELCOM
Морски охлюв от вида *Liparis liparis*	*Liparis liparis*	Балтийско море	HELCOM
Морски охлюв от вида *Liparis montagui*	*Liparis montagui*	Балтийско море	HELCOM
Светипетрова риба	*Zeus faber*	Балтийско море	HELCOM
Лаврак	*Dicentrarchus labrax*	Балтийско море	HELCOM
Зеленушка балан	*Labrus bergylta*	Балтийско море	HELCOM
Зеленушка от вида *Labrus mixtus*	*Labrus mixtus*	Балтийско море	HELCOM
Зеленушка от вида *Symphodus melops*	*Symphodus melops*	Балтийско море	HELCOM
Голям дракон	*Trachinus draco*	Балтийско море	HELCOM

Общоприето наименование	Научно наименование	Регион/РОУР	Правна рамка
Ивичеста зъбатка	*Anarhichas lupus*	Балтийско море	HELCOM
Малка пясъчница	*Ammodytes marinus*	Балтийско море	HELCOM
Дребна пясъчница	*Ammodytes tobianus*	Балтийско море	HELCOM
Попче от вида *Pomatoschistus pictus*	*Pomatoschistus pictus*	Балтийско море	HELCOM
Ивичеста ауксида	*Auxis rochei*	Балтийско море	HELCOM
Малък тунец	*Euthynnus alleteratus*	Балтийско море	HELCOM
Обикновен бонито	*Orcynopsis unicolor*	Балтийско море	HELCOM
Атлантическа скумрия	*Scomber scombrus*	Балтийско море	HELCOM
Атлантическа писия	*Hoplostethus atlanticus*	Балтийско море	HELCOM
Риба меч	*Xiphias gladius*	Балтийско море	HELCOM
Черна риба	*Centrolophus niger*	Балтийско море	HELCOM
Хрущялни риби	Chondrichthyes		
Риба трион от вида *Anoxypristis cuspidata*	*Anoxypristis cuspidata*	Всички океани	РОУР, висок приоритет
Клюнеста акула	*Deania calcea*	Всички океани	РОУР, висок приоритет
Гладка светеща акула	*Etmopterus pusillus*	Всички океани	РОУР, висок приоритет
Риба трион	*Pristis clavata*	Всички океани	РОУР, висок приоритет
Риба трион	*Pristis zijsron*	Всички океани	РОУР, висок приоритет
Норвежки скат	*Raja (Dipturus) nidarosiensis*	Всички океани	РОУР, висок приоритет
Морска лисица	*Raja clavata*	Всички океани	РОУР, висок приоритет OSPAR; HELCOM
Вълнист скат	*Raja undulata*	Всички океани	РОУР, висок приоритет
Пелагична акула скитница	*Alopias pelagicus*	Всички океани	РОУР, висок приоритет
Големоока акула скитница	*Alopias superciliosus*	Всички океани	РОУР, висок приоритет
Обикновена акула скитница	*Alopias vulpinus*	Всички океани	РОУР, висок приоритет; HELCOM
Бодлив скат	*Amblyraja radiata*	Всички океани	РОУР, висок приоритет

Общоприето наименование	Научно наименование	Регион/РОУР	Правна рамка
Исландска котешка акула	Apristuris spp	Всички океани	РОУР, висок приоритет, уязвими видове, свързана с дълбоководния риболов
Копринени акули	*Carcharhinus falciformis*	Всички океани	РОУР, висок приоритет
Галапагоска акула	*Carcharhinus galapagensis*	Всички океани	РОУР, висок приоритет
Дългокрила акула	*Carcharhinus longimanus*	Всички океани	РОУР, висок приоритет
Пясъчна акула	*Carcharhinus plumbeus*	Всички океани + Средиземно и Черно море	РОУР, висок приоритет, приложение II към Конвенцията от Барселона
Пясъчна тигрова акула	*Carcharias taurus*	Всички океани + Средиземно и Черно море	РОУР, висок приоритет, приложение II към Конвенцията от Барселона
Голяма бяла акула	*Carcharodon carcharias*	Всички океани	РОУР, висок приоритет
Гълтаща акула	*Centrophorus granulosus*	Всички океани и морета	РОУР, висок приоритет, приложение III към Конвенцията от Барселона; OSPAR
Гълтаща акула	Centrophorus spp	Всички региони	Свързана с дълбоководния риболов
Сива късошипа акула	*Centrophorus squamosus*	Всички океани и морета	РОУР, висок приоритет; OSPAR
Черна котешка акула	*Centroscyllium fabricii*	Всички океани	РОУР, висок приоритет, свързана с дълбоководния риболов
Португалска котешка акула	*Centroscymnus coelolepis*	Всички океани	РОУР, висок приоритет, свързана с дълбоководния риболов; OSPAR
Дългоноса кадифена котешка акула	*Centroscymnus crepidater*	Всички океани	РОУР, висок приоритет, уязвими видове, свързана с дълбоководния риболов
Гигантска акула	*Cetorhinus maximus*	Всички океани и морета	РОУР, висок приоритет; OSPAR; HELCOM
Европейска химера	*Chimaera monstrosa*	Всички региони	Свързана с дълбоководния риболов
Мантиева акула	*Chlamydoselachus anguineus*	Всички океани	РОУР, висок приоритет, уязвими видове, свързана с дълбоководния риболов
Черна акула	*Dalatias licha*	Всички океани	РОУР, висок приоритет, уязвими видове, свързана с дълбоководния риболов
Скат	*Dasyatis pastinaca*	Черно море	Приложение IV към Протокола за опазване на биологичното и ландшафтното разнообразие на Черно море, HELCOM

Общоприето наименование	Научно наименование	Регион/РОУР	Правна рамка
Клюнеста акула	*Deania calcea*	Всички океани	РОУР, висок приоритет, свързана с дълбоководния риболов
Обикновен скат	*Dipturus batis*	Всички океани и морета	РОУР, висок приоритет, приложение II към Конвенцията от Барселона; OSPAR; HELCOM
Бял скат	**Rostroraja alba*	OSPAR II, III, IV	OSPAR
Голяма светеща акула	*Etmopterus princeps*	Всички океани	РОУР, висок приоритет, уязвими видове, свързана с дълбоководния риболов
Нощна акула	*Etmopterus spinax*	Всички океани	РОУР, висок приоритет, свързана с дълбоководния риболов; HELCOM
Акула чук от вида *Eusphyra blochii*	*Eusphyra blochii*	Всички океани	РОУР, висок приоритет
Австралийска акула от вида *Galeorhinus galeus*	*Galeorhinus galeus*	Всички океани + Средиземно и Черно море	РОУР, висок приоритет, приложение II към Конвенцията от Барселона; HELCOM
Петниста котешка акула	*Galeus melastomus*	Всички океани	РОУР, висок приоритет, свързана с дълбоководния риболов
Миша котешка акула	*Galeus murinus*	Всички океани	РОУР, висок приоритет, свързана с дълбоководния риболов
Бодлив скат пеперуда	*Gymnura altavela*	Всички океани + Средиземно и Черно море	РОУР, висок приоритет, приложение II към Конвенцията от Барселона
Тесноглава седемхрилна гребенозъбеста акула	*Heptranchias perlo*	Всички океани + Средиземно и Черно море	РОУР, висок приоритет, приложение III към Конвенцията от Барселона
Шестхрилна акула	*Hexanchus griseus*	Всички океани + Средиземно и Черно море	РОУР, висок приоритет, приложение II към Конвенцията от Барселона; HELCOM
Химера от вида *Hydrolagus mirabilis*	*Hydrolagus mirabilis*	Всички региони	Свързана с дълбоководния риболов
Късопера мако	*Isurus oxyrinchus*	Всички океани	РОУР, висок приоритет
Дългопера мако	*Isurus paucus*	Всички океани	РОУР, висок приоритет
Селдова акула	*Lamna nasus*	Всички океани	РОУР, висок приоритет, OSPAR; HELCOM
Пясъчен скат	*Leucoraja circularis*	Всички океани + Средиземно и Черно море	РОУР, висок приоритет, приложение II към Конвенцията от Барселона

Общоприето наименование	Научно наименование	Регион/РОУР	Правна рамка
Малтийски скат	*Leucoraja melitensis*	Всички океани + Средиземно и Черно море	РОУР, висок приоритет, приложение II към Конвенцията от Барселона
Манта от вида *Manta alfredi*	*Manta alfredi*	Всички океани	РОУР, висок приоритет
Морски дявол	*Manta birostris*	Всички океани	РОУР, висок приоритет
Манта от вида *Mobula eregoodootenkee*	*Mobula eregoodootenkee*	Всички океани	РОУР, висок приоритет
Манта от вида *Mobula hypostoma*	*Mobula hypostoma*	Всички океани	РОУР, висок приоритет
Манта от вида *Mobula japanica*	*Mobula japanica*	Всички океани	РОУР, висок приоритет
Манта от вида *Mobula kuhlii*	*Mobula kuhlii*	Всички океани	РОУР, висок приоритет
Дяволска риба	*Mobula mobular*	Всички океани	РОУР, висок приоритет
Манта от вида *Mobula munkiana*	*Mobula munkiana*	Всички океани	РОУР, висок приоритет
Манта от вида *Mobula rochebrunei*	*Mobula rochebrunei*	Всички океани	РОУР, висок приоритет
Манта от вида *Mobula tarapacana*	*Mobula tarapacana*	Всички океани	РОУР, висок приоритет
Манта от вида *Mobula thurstoni*	*Mobula thurstoni*	Всички океани	РОУР, висок приоритет
Бялопетниста гладка кучешка акула	*Mustelus asterias*	Всички океани + Средиземно и Черно море	РОУР, висок приоритет, приложение III към Конвенцията от Барселона
Обикновена кучешка акула	*Mustelus mustelus*	Всички океани + Средиземно и Черно море	РОУР, висок приоритет, приложение III към Конвенцията от Барселона
Чернопетниста кучешка акула	*Mustelus punctulatus*	Всички океани + Средиземно и Черно море	РОУР, висок приоритет, приложение III към Конвенцията от Барселона
Акула от вида *Galeus melastomus*	*Galeus melastomus*	Балтийско море	HELCOM
Дребнопетниста акула от вида *Scyliorhinus canicula*	*Scyliorhinus canicula*	Балтийско море	HELCOM
Бодлива морска лисица	*Amblyraja radiata*	Балтийско море	HELCOM
Скат от вида *Leucoraja fullonica*	*Leucoraja fullonica*	Балтийско море	HELCOM
Петнист електрически скат	*Torpedo marmorata*	Балтийско море	HELCOM

Общоприето наименование	Научно наименование	Регион/РОУР	Правна рамка
Грапава акула	*Oxynotus paradoxus*	Всички океани	РОУР, висок приоритет, уязвими видове, свързана с дълбоководния риболов
Дребнозъба риба трион	*Pristis pectinata*	Всички океани + Средиземно и Черно море	РОУР, висок приоритет, приложение II към Конвенцията от Барселона
Обикновена риба трион	*Pristis pristis*	Всички океани + Средиземно и Черно море	РОУР, висок приоритет, приложение II към Конвенцията от Барселона
Крокодилова акула	*Pseudocarcharias kamoharai*	Всички океани	РОУР, висок приоритет
Син скат	*Pteroplatytrygon violacea*	Всички океани	РОУР, висок приоритет
Листовиден скат	*Raja fyllae*	Всички региони	Свързана с дълбоководния риболов
Арктически скат	*Raja hyperborea*	Всички региони	Свързана с дълбоководния риболов
Норвежки скат	*Raja nidarosiensus*	Всички региони	Свързана с дълбоководния риболов
Петнист скат	*Raja montagui*	OSPAR I, II, III, IV	OSPAR; HELCOM
Китова акула	*Rhincodon typus*	Всички океани	РОУР, висок приоритет
Атлантическа риба китара	*Rhinobatos cemiculus*	Всички океани + Средиземно и Черно море	РОУР, висок приоритет, приложение II към Конвенцията от Барселона
Обикновена риба китара	*Rhinobatos rhinobatos*	Всички океани + Средиземно и Черно море	РОУР, висок приоритет, приложение II към Конвенцията от Барселона
Носата атлантическа химера	*Rhinochimaera atlantica*	Всички региони	Свързана с дълбоководния риболов
Бял скат	*Rostroraja alba*	Всички океани + Средиземно и Черно море	РОУР, висок приоритет, приложение II към Конвенцията от Барселона
Острозъба котешка акула	*Dalatias licha*	Всички океани	РОУР, висок приоритет, свързана с дълбоководния риболов
Други акули	Selachimorpha (или Selachii), Batoidea (да се определи по видове според данните за разтоварване на брега, изследване или улов)	Всички океани	РОУР, висок приоритет; HELCOM
Гренландска акула	*Sonmnousus microcephalus*	Всички океани	РОУР, висок приоритет, свързана с дълбоководния риболов; HELCOM

Общоприето наименование	Научно наименование	Регион/РОУР	Правна рамка
Бронзова акула чук	*Sphyrna lewini*	Всички океани	РОУР, висок приоритет
Гигантска акула чук	*Sphyrna mokarran*	Всички океани	РОУР, висок приоритет
Гладка риба чук	*Sphyrna zygaena*	Всички океани	РОУР, висок приоритет
Черноморска бодлива акула	*Squalus acanthias*	Всички океани + Средиземно и Черно море	РОУР, висок приоритет, приложение III към Конвенцията от Барселона, OSPAR; HELCOM
Покривна морски ангел	*Squatina aculeata*	Всички океани + Средиземно и Черно море	РОУР, висок приоритет, приложение II към Конвенцията от Барселона
Морски ангел от вида *Squatina oculata*	*Squatina oculata*	Всички океани + Средиземно и Черно море	РОУР, висок приоритет, приложение II към Конвенцията от Барселона
Морски ангел	*Squatina squatina*	Всички океани + Средиземно и Черно море	РОУР, висок приоритет, приложение II към Конвенцията от Барселона, OSPAR; HELCOM
Морска минога	*Petromyzon marinus*	OSPAR I, II, III, IV	OSPAR; HELCOM
Речна минога	*Lampetra fluviatilis*	Балтийско море	HELCOM
Бозайници	Mammalia		
Китоподобни — всички видове	CETACEA — всички видове	Всички зони	Директива 92/43/ЕИО на Съвета ([7])
Кит джудже	*Balaenoptera acutorostrata*	Средиземно море	Препоръка ГКРСМ ([8])/36/2012/2 и приложение II на Конвенцията от Барселона
Кит от вида *Balaena mysticetus*	*Balaena mysticetus*	OSPAR I	OSPAR
Син кит	*Balaenoptera musculus*	Всички OSPAR	OSPAR
Бискайски кит	*Eubalaena glacialis*	Всички OSPAR	OSPAR
Сейвал	*Balaenoptera borealis*	Средиземно море	Препоръка на ГКРСМ/36/2012/2 и приложение II на Конвенцията от Барселона
Финвал	*Balaenoptera physalus*	Средиземно море	Препоръка на ГКРСМ/36/2012/2 и приложение II на Конвенцията от Барселона
Обикновен делфин	*Delphinus delphis*	Средиземно море	Препоръка на ГКРСМ/36/2012/2 и приложение II на Конвенцията от Барселона
Северната част на Атлантическия океан право кит	*Eubalaena glacialis*	Средиземно море	Препоръка на ГКРСМ/36/2012/2 и приложение II на Конвенцията от Барселона

Общоприето наименование	Научно наименование	Регион/РОУР	Правна рамка
Дългоопашата гринда	*Globicephala melas*	Средиземно море	Препоръка на ГКРСМ/36/2012/2 и приложение II на Конвенцията от Барселона
Сив делфин	*Grampus griseus*	Средиземно море	Препоръка на ГКРСМ/36/2012/2 и приложение II на Конвенцията от Барселона
Кашалот джудже	*Kogia simus*	Средиземно море	Препоръка на ГКРСМ/36/2012/2 и приложение II на Конвенцията от Барселона
Гърбат кит	*Megaptera novaeangliae*	Средиземно море	Препоръка на ГКРСМ/36/2012/2 и приложение II на Конвенцията от Барселона
Клюномуцунест кит на Бленвил	*Mesoplodon densirostris*	Средиземно море	Препоръка на ГКРСМ/36/2012/2 и приложение II на Конвенцията от Барселона
Косатка	*Orcinus orca*	Средиземно море	Препоръка на ГКРСМ/36/2012/2 и приложение II на Конвенцията от Барселона
Морска свиня	*Phocoena phocoena*	Средиземно море; OSPAR II, III	Препоръка на ГКРСМ/36/2012/2 и приложение II на Конвенцията от Барселона; Директива 92/43/ЕИО, OSPAR
Кашалоти	*Physeter macrocephalus*	Средиземно море	Препоръка на ГКРСМ/36/2012/2 и приложение II на Конвенцията от Барселона
Фалшива косатка	*Pseudorca crassidens*	Средиземно море	Препоръка на ГКРСМ/36/2012/2 и приложение II на Конвенцията от Барселона
Ивичест делфин	*Stenella coeruleoalba*	Средиземно море	Препоръка на ГКРСМ/36/2012/2 и приложение II на Конвенцията от Барселона
Грапавозъб делфин	*Steno bredanensis*	Средиземно море	Препоръка на ГКРСМ/36/2012/2 и приложение II на Конвенцията от Барселона
Афала	*Tursiops truncatus*	Средиземно море	Препоръка на ГКРСМ/36/2012/2 и приложение II на Конвенцията от Барселона
Клюномуцунест кит на Кювие	*Ziphius cavirostris*	Средиземно море	Препоръка на ГКРСМ/36/2012/2 и приложение II на Конвенцията от Барселона
Тюлени монаси	*Monachus monachus*	Всички зони	Препоръка на ГКРСМ/35/2011/5 и приложение II на Конвенцията от Барселона; Директива 92/43/ЕИО
Пръстенчати тюлени от от Саймаа	*Phoca hispida saimensis*	Всички зони	Директива 92/43/ЕИО
Дългомуцунест тюлен	*Halichoerus grypus*	Всички зони	Директива 92/43/ЕИО
Същински тюлени	*Phoca vitulina*	Всички зони	Директива 92/43/ЕИО
Балтийски пръстенчат тюлен	*Phoca hispida bottnica*	Всички зони	Директива 92/43/ЕИО

Общоприето наименование	Научно наименование	Регион/РОУР	Правна рамка
Птици	Aves		
Жълтоклюн буревестник	*Calonectris borealis*	Всички зони	Директива 2009/147/ЕО на Европейския парламент и на Съвета (9)
Голям корморан	*Phalacrocrax carbo*	Всички зони	Директива 2009/147/ЕО
Бял рибояд	*Morus bassanus*	Всички зони	Директива 2009/147/ЕО на Европейския парламент и на Съвета относно опазването на дивите птици
Тъпоклюна кайра	*Fratercula Arctica*	Всички зони	Директива 2009/147/ЕО
Балеарски буревестник	*Puffinus mauretanicus*	Всички зони	Директива 2009/147/ЕО
Речна чайка	*Larus ridibundus*	Всички зони	Директива 2009/147/ЕО
Обикновена траурна потапница	*Melanitta nigra*	Всички зони	Директива 2009/147/ЕО
Качулат корморан	*Phalacrocorax aristotelis*	Всички зони	Директива 2009/147/ЕО
Голям буревестник	*Ardenna gравис*	Всички зони	Директива 2009/147/ЕО
Обикновен буревестник	*Puffinus puffinus*	Всички зони	Директива 2009/147/ЕО
Полярен буревестник	*Fulmarus glacialis*	Всички зони	Директива 2009/147/ЕО
Буревестник от вида *Calonectris diomedea*	*Calonectris diomedea*	Всички зони	Директива 2009/147/ЕО
Сив буревестник	*Ardenna grisea*	Всички зони	Директива 2009/147/ЕО
Левантински буревестник	*Puffinus yelkouan*	Всички зони	Директива 2009/147/ЕО
Средиземноморска чайка	*Larus audouinii*	Всички зони	Директива 2009/147/ЕО
Исландска звънарка	*Bucephala islandica*	Всички зони	Директива 2009/147/ЕО
Булверов тайфунник	*Bulweria bulwerii*	Всички зони	Директива 2009/147/ЕО
Звънарка	*Bucephala clangula*	Всички зони	Директива 2009/147/ЕО
Европейска сребриста чайка	*Larus argentatus*	Всички зони	Директива 2009/147/ЕО
Полярна чайка	*Larus hyperboreus*	Всички зони	Директива 2009/147/ЕО
Голяма черногърба чайка	*Larus marinus*	Всички зони	Директива 2009/147/ЕО
Скуа	*Catharacta skua*	Всички зони	Директива 2009/147/ЕО

Общоприето наименование	Научно наименование	Регион/РОУР	Правна рамка
Планинска потапница	*Aythya marila*	Всички зони	Директива 2009/147/ЕО; приложение IV към Протокола за опазване на биологичното и ландшафтното разнообразие на Черно море
Кафявоглава потапница	*Aythya ferina*	Черно море	Приложение IV към Протокола за опазване на биологичното и ландшафтното разнообразие на Черно море
Малка черногърба чайка	*Larus fuscus*	Всички зони	Директива 2009/147/ЕО
Малка гагарка	*Alle alle*	Всички зони	Директива 2009/147/ЕО
Дългоопашат морелетник	*Stercorarius longicaudus*	Всички зони	Директива 2009/147/ЕО
Дебелоклюна гагарка	*Alca torda*	Всички зони	Директива 2009/147/ЕО
Остроопашат морелетник	*Stercorarius parasiticus*	Всички зони	Директива 2009/147/ЕО
Черногуш гмуркач	*Gavia arctica*	Всички зони	Директива 2009/147/ЕО
Буревестник от вида *Puffinus lherminieri*	*Puffinus lherminieri*	Всички зони	Директива 2009/147/ЕО
Чистик	*Cepphus grylle*	Всички зони	Директива 2009/147/ЕО
Черна потапница	*Melanitta americana*	Всички зони	Директива 2009/147/ЕО
Черноврат гмурец	*Podiceps nigricollis*	Всички зони	Директива 2009/147/ЕО
Каспийска чайка	*Larus cachinnans*	Всички зони	Директива 2009/147/ЕО
Обикновена гага	*Somateria mollissima*	Всички зони	Директива 2009/147/ЕО
Кайра	*Uria aalge*	Всички зони	Директива 2009/147/ЕО
Черноклюн гмуркач	*Gavia immer*	Всички зони	Директива 2009/147/ЕО
Обикновен нирец	*Mergus merganser*	Всички зони	Директива 2009/147/ЕО
Голям гмурец	*Podiceps cristatus*	Всички зони	Директива 2009/147/ЕО
Исландска потапница	*Histrionicus histrionicus*	Всички зони	Директива 2009/147/ЕО
Ушат гмурец	*Podiceps auritus*	Всички зони	Директива 2009/147/ЕО
Грендладска чайка	*Larus glaucoides*	Всички зони	Директива 2009/147/ЕО
Гребенчата гага	*Somateria spectabilis*	Всички зони	Директива 2009/147/ЕО

Общоприето наименование	Научно наименование	Регион/РОУР	Правна рамка
Ледена потапница	*Clangula hyemalis*	Всички зони	Директива 2009/147/ЕО
Малка черноглава чайка	*Larus melanocephalus*	Всички зони	Директива 2009/147/ЕО
Чайка буревестница	*Larus canus*	Всички зони	Директива 2009/147/ЕО
Среден нирец	*Mergus serrator*	Всички зони	Директива 2009/147/ЕО
Червеноврат гмурец	*Podiceps grisegena*	Всички зони	Директива 2009/147/ЕО
Червеногуш гмуркач	*Gavia stellata*	Всички зони	Директива 2009/147/ЕО
Дългоклюна чайка	*Larus genei*	Всички зони	Директива 2009/147/ЕО
Стелерова гага	*Polysticta stelleri*	Всички зони	Директива 2009/147/ЕО
Голям морелетник	*Stercorarius pomarinus*	Всички зони	Директива 2009/147/ЕО
Дебелоклюна кайра	*Uria lomvia*	Всички зони	Директива 2009/147/ЕО
Кадифена потапница	*Melanitta fusca*	Всички зони	Директива 2009/147/ЕО
Жълтоклюн гмуркач	*Gavia adamsii*	Всички зони	Директива 2009/147/ЕО
Средиземноморска жълтонога чайка	*Larus michahellis*	Всички зони	Директива 2009/147/ЕО
Буревестник от Мадейра	*Pterodroma madeira*	Всички зони	Директива 2009/147/ЕО
Средиземноморска чайка	*Larus ichthyaetus*	Всички зони	Директива 2009/147/ЕО
Трипръста чайка	*Rissa tridactyla*	Всички зони	Директива 2009/147/ЕО
Голям бял пеликан	*Pelecanus onocrotalus*	Всички зони	Директива 2009/147/ЕО
Северна вълнолюбка	*Oceanodroma leucorhoa*	Всички зони	Директива 2009/147/ЕО
Плоскоклюн листоног	*Phalaropus fulicarius*	Всички зони	Директива 2009/147/ЕО
Тънкоклюн листоног	*Phalaropus lobatus*	Всички зони	Директива 2009/147/ЕО
Уилсънова вълнолюбка	*Oceanites oceanicus*	Всички зони	Директива 2009/147/ЕО
Полярна рибарка	*Sterna paradisaea*	Всички зони	Директива 2009/147/ЕО
Вълнолюбка от вида *Hydrobates Castro*	*Hydrobates Castro*	Всички зони	Директива 2009/147/ЕО
Черна рибарка	*Chlidonias niger*	Всички зони	Директива 2009/147/ЕО
Каспийска рибарка	*Hydroprogne caspia*	Всички зони	Директива 2009/147/ЕО

Общоприето наименование	Научно наименование	Регион/РОУР	Правна рамка
Обикновена дебелоклюна рибарка	*Gelochelidon nilotica*	Всички зони	Директива 2009/147/ЕО
Речна рибарка	*Sterna hirundo*	Всички зони	Директива 2009/147/ЕО
Буревестник от вида *Pterodroma deserta*	*Pterodroma deserta*	Всички зони	Директива 2009/147/ЕО
Чайка от вида *Pagophila eburnea*	*Pagophila eburnea*	Всички зони	Директива 2009/147/ЕО
Рибарка от вида *Thalasseus bengalensis*	*Thalasseus bengalensis*	Всички зони	Директива 2009/147/ЕО
Малка чайка	*Hydrocoloeus minutus*	Всички зони	Директива 2009/147/ЕО
Белочела рибарка	*Sternula albifrons*	Всички зони	Директива 2009/147/ЕО
Северна вълнолюбка	*Hydrobates monteiroi*	Всички зони	Директива 2009/147/ЕО
Розова рибарка	*Sterna dougallii*	Всички зони	Директива 2009/147/ЕО
Розова чайка	*Rhodostethia rosea*	Всички зони	Директива 2009/147/ЕО
Вилоопашата чайка	*Xema sabini*	Всички зони	Директива 2009/147/ЕО
Гривеста рибарка	*Thalasseus sandvicensis*	Всички зони	Директива 2009/147/ЕО
Чайка от вида *Larus thayeri*	*Larus thayeri*	Всички зони	Директива 2009/147/ЕО
Морска вълнолюбка	*Pelagodroma marina*	Всички зони	Директива 2009/147/ЕО
Вълнолюбка	*Hydrobates pelagicus*	Всички зони	Директива 2009/147/ЕО
Малка черногърба чайка	*Larus fuscus fuscus*	OSPAR I	Списък на OSPAR на застрашените и намаляващите видове
Бяла чайка	*Pagophila eburnea*	OSPAR I	Списък на OSPAR на застрашените и намаляващите видове
Стелерова гага	*Polysticta stelleri*	OSPAR I	Списък на OSPAR на застрашените и намаляващите видове
Малък буревестник	Puffinus assimilis baroli (auct.incert.)	OSPAR V	Списък на OSPAR на застрашените и намаляващите видове
Мавритански буревестник	*Puffinus mauretanicus*	OSPAR II, III, IV, V	Списък на OSPAR на застрашените и намаляващите видове
Трипръста чайка	*Rissa tridactyla*	OSPAR I, II,	Списък на OSPAR на застрашените и намаляващите видове
Розова рибарка	*Sterna dougallii*	OSPAR II, III, IV, V	Списък на OSPAR на застрашените и намаляващите видове

Общоприето наименование	Научно наименование	Регион/РОУР	Правна рамка
Тънкоклюна кайра	Uria aalge — иберийска популация (синоними: Uria aalge albionis, Uria aalge ibericus)	OSPAR IV	Списък на OSPAR на застрашените и намаляващите видове
Дебелоклюна кайра	*Uria lomvia*	OSPAR I	Списък на OSPAR на застрашените и намаляващите видове
Влечуги	Reptilia		
Сива морска костенурка от вида *Lepidochelys kempii*	*Lepidochelys kempii*	Всички зони	Директива 92/43/ЕИО; Препоръка на ГКРСМ/35/2011/4 и приложение II към Конвенцията от Барселона
Карета	*Caretta caretta*	Всички зони	Директива 92/43/ЕИО; Препоръка на ГКРСМ/35/2011/4 и приложение II на Конвенцията от Барселона; OSPAR
Кожести костенурки	*Dermochelys coriacea*	Всички зони	Директива 92/43/ЕИО; Препоръка на ГКРСМ/35/2011/4 и приложение II на Конвенцията от Барселона; OSPAR
Морска костенурка от вида *Eretmochelys imbricata*	*Eretmochelys imbricata*	Всички зони	Директива 92/43/ЕИО; Препоръка на ГКРСМ/35/2011/4 и приложение II на Конвенцията от Барселона
Зелена морска костенурка	*Chelonia mydas*	Всички зони	Директива 92/43/ЕИО; Препоръка на ГКРСМ/35/2011/4 и приложение II на Конвенцията от Барселона
Мекочерупчеста костенурка от вида *Trionyx triunguis*	*Trionyx triunguis*	Средиземно море	Препоръка на ГКРСМ/35/2011/4 и приложение II на Конвенцията от Барселона
Мекотели	Mollusca		
Пясъчна бяла мида	*Chamelea gallina*	Черно море	Приложение IV към Протокола за опазване на биологичното и ландшафтното разнообразие на Черно море
Миди от вида *Donacilla cornea*	*Donacilla cornea*	Черно море	Приложение IV към Протокола за опазване на биологичното и ландшафтното разнообразие на Черно море
Октоподи от рода *Eledone*	Eledone spp.	Всички зони	Национални планове за управление
Средиземноморски миди от вида *Mytilus galloprovincialis*	*Mytilus galloprovincialis*	Всички зони в Средиземно море	Национални планове за управление
Черна морска мида	*Mytilus galloprovincialis*	Черно море	Приложение IV към Протокола за опазване на биологичното и ландшафтното разнообразие на Черно море
Патела	Patella spp.	Средиземно море	Приложение II към Конвенцията от Барселона
Рапан от вида *Rapana venosa*	*Rapana venosa*	Черно море	Приложение IV към Протокола за опазване на биологичното и ландшафтното разнообразие на Черно море
Миди от вида *Acanthocardia tuberculata*	*Acanthocardia tuberculata*	Всички зони	Национални планове за управление
Мурекс	*Bolinus brandaris*	Всички зони	Национални планове за управление

Общоприето наименование	Научно наименование	Регион/РОУР	Правна рамка
Твърда мида	*Callista chione*	Всички зони	Национални планове за управление
Мида от вида *Donax trunculus*	*Donax trunculus*	Всички зони	Национални планове за управление
Океански куахог	*Arctica islandica*	OSPAR II	OSPAR
Ракообразно от вида *Megabalanus azoricus*	*Megabalanus azoricus*	OSPAR V Навсякъде, където се среща	OSPAR
Морски охлюв от вида *Nucella lapillus*	*Nucella lapillus*	OSPAR II, III, IV	OSPAR
Стрида	*Ostrea edulis*	OSPAR II	OSPAR
Мида от вида *Patella ulyssiponensis aspera*	*Patella ulyssiponensis aspera*	Всички зони OSPAR, където се среща	OSPAR
Ракообразни	Crustacea		
Омари	*Homarus gammarus*	Средиземно море	Регламент (ЕО) № 1967/2006 (минимален размер за опазване)
Дълбоководен червен рак	*Chaceon (Geryon) affinis*	Всички региони	Свързана с дълбоководния риболов
Сива скарида	*Crangon crangon*	Черно море	Приложение IV към Протокола за опазване на биологичното и ландшафтното разнообразие на Черно море
Балтийска скарида	*Palaemon adspersus*	Черно море	Приложение IV към Протокола за опазване на биологичното и ландшафтното разнообразие на Черно море
Скарида от вида *Palaemon elegans*	*Palaemon elegans*	Черно море	Приложение IV към Протокола за опазване на биологичното и ландшафтното разнообразие на Черно море
Лангуста	*Palinuridae*	Средиземно море	Регламент (ЕО) № 1967/2006 (минимален размер за опазване)
Мешести	Cnidaria		
Червени корали	*Corallium rubrum*	Средиземно море	Препоръка на ГКРСМ/36/2012/1 и Препоръка на ГКРСМ/35/2011/2

([1]) По-специално Конвенцията от Барселона за защита на морската среда и на крайбрежните райони в Средиземноморието.
([2]) OSPAR Конвенция за защита на морската среда на Североизточния Атлантически океан
([3]) HELCOM Конвенция за защита на морската среда на района на Балтийско море
([4]) Регламент (ЕО) № 2347/2002 на Съвета от 16 декември 2002 г. за определяне на специалните условия за достъп до риболовните полета на дълбоководни запаси и за определяне на съответните изисквания (ОВ L 351, 28.12.2002 г., стр. 6).
([5]) Регламент (ЕО) № 1967/2006 на Съвета от 21 декември 2006 г. относно мерките за управление на устойчивата експлоатация на рибните ресурси в Средиземно море, за изменение на Регламент (ЕИО) № 2847/93 и за отмяна на Регламент (ЕО) № 1626/94 (ОВ L 409, 30.12.2006 г., стр. 11).
([6]) Регламент (ЕО) № 894/97 на Съвета от 29 април 1997 г. за установяване на някои технически мерки за опазване на рибните ресурси (ОВ L 132, 23.5.1997 г., стр. 1).
([7]) 92/43/ЕИО на Съвета за опазване на естествените местообитания и на дивата флора и фауна (ОВ L 206, 22.7.1992 г., стр. 7).
([8]) Генерална комисия по рибарство за Средиземно море
([9]) Директива 2009/147/ЕО на Европейския парламент и на Съвета от 30 ноември 2009 година относно опазването на дивите птици (ОВ L 20, 26.1.2010 г., стр. 7).)

За забранени видове: Използват се само индивиди, уловени мъртви. Те се изхвърлят след измерването. Събирането на данни е годишно, а актуализирането/обработката на данните се извършва своевременно, за да се спази графикът на оценките на запасите.

БИОЛОГИЧНИ ДАННИ

Таблица 1E

Сладководни анадромни и катадромни видове

Вид (общоприето наименование)	Вид (научно наименование)	Без морски райони, в които запасът се намира/Код на запаса
Европейска змиорка	*Anguilla anguilla*	Единици за управление на запасите от змиорки, определени в съответствие с Регламент (ЕО) № 1100/2007 на Съвета [1]
Сьомга	*Salmo salar*	всички области на естествено разпространение
Морска пъстърва	*Salmo trutta*	Че всички вътрешни води в Балтийско море за напускане

[1] Регламент (ЕО) № 1100/2007 на Съвета от 18 септември 2007 г. относно установяване на мерки за възстановяване на запасите от европейска змиорка (ОВ L 248, 22.9.2007 г., стр. 17).

Таблица 2

Риболовна дейност (група сходни риболовни дейности) по региони

Ниво 1	Ниво 2	Ниво 3	Ниво 4	Ниво 5	Ниво 6	Класове LOA (m)					
Дейност	Класове съоръжения	Групи съоръжения	Вид уред	Целева група (б)	Размер на отвора и други селективни съоръжения	< 10	10- < 12	12- < 18	18- < 24	24- < 40	40 и +
Риболовна дейност	Драги	Драги	Корабна драга [DRB]	Анадромни видове (ANA) Катадромни видове (CAT) Главоноги (CEP) Ракообразни (CRU) Дънни видове (DEF) Дълбоководни видове (DWS) Същински риби (FIF) Сладководни видове (без код) Разни (MIS) Смесени главоноги и дънни риби (MCF) Смесени ракообразни и дънни риби (MCD) Смесени дълбоководни видове и дънни риби (MDD) Смесени пелагични и дънни риби (MPD) Мекотели (MOL) Едри пелагични риби (LPF) Дребни пелагични риби (SPF) Едри пелагични риби (LPF) и Дребни пелагични риби (SPF)	б)						
			Механична/Засмукваща драга [HMD]		б)						
	Тралове	Дънни тралове	Дънен трал [OTB]		б)						
			Близнецов трал [OTT]		б)						
			Дънен трал, теглен от два кораба [PTB]		б)						
			Бим трал [TBB]		б)						
		Пелагични тралове	Пелагичен трал [OTM]		б)						
			Пелагичен трал, теглен от два кораба [PTM]		б)						

Ниво 1	Ниво 2	Ниво 3	Ниво 4	Ниво 5	Ниво 6	Класове LOA (m)					
Дейност	Класове съоръжения	Групи съоръжения	Вид уред	Целева група (б)	Размер на отвора и други селективни съоръжения	< 10	10- < 12	12- < 18	18- < 24	24- < 40	40 и +
	Куки и влакна	Пръти и влакна	Чепарета (ръчни и механизирани) [LHP] [LHM]		б)						
			Влачещи се въдичарски уреди [LTL]		б)						
		Парагади	Плаващи парагади [LLD]		б)						
			Парагади и кърмаци [LLS]		б)						
	Капани	Капани	Винтери и капанни съоръжения [FPO]		б)						
			Конусовидни мрежи [FYK]		б)						
			Непокрити стационарни мрежи [FPN]		б)						
			Стационарни инсталации за огради и заграждения		б)						
	Мрежи	Мрежи	Тройна мрежа [GTR]		б)						
			Хрилна мрежа (закотвена) [GNS]		б)						
			Плаваща хрилна мрежа [GND]		б)						
	Грибове	Ограждащи мрежи	Мрежа гъргър [PS]		б)						
			Лампари [LA]		б)						
		Грибове в)	Гриб шотландски [SSC]		б)						
			Гриб датски [SDN]		б)						

Ниво 1	Ниво 2	Ниво 3	Ниво 4	Ниво 5	Ниво 6	Класове LOA (m)					
Дейност	Класове съоръжения	Групи съоръжения	Вид уред	Целева група (б)	Размер на отвора и други селективни съоръжения	< 10	10- < 12	12- < 18	18- < 24	24- < 40	40 и +
			Двоен гриб [SPR]		б)						
			Гриб плажен и корабен [SB] [SV]		б)						
	Други съоръжения	Други съоръжения	Риболов на змиорки (без код)	Змиорка	б)						
	Разни (да се посочи)	Разни (да се посочи)			б)						
Друга дейност освен риболов				Друга дейност освен риболов							
Неактивен				Неактивен							

Бележки под линия:
а) съгласно съществуващите кодове в съответните регламенти
б) съгласно съществуващите кодове в съответните регламенти
в) с устройства за концентриране на риба (YCP)/в свободни пасажи
г) < 6 m и 6—12 метра в Средиземно море

Таблица 3

Видове, които се събират за любителски риболов

	Зона	Вид
1	Балтийско море (подучастъци 22—32 на ICES)	Сьомга, змиорки и морска пъстърва (включително в сладка вода) и треска.
2	Северно море (зони на ICES IIIa, IV и VIId)	Сьомга и змиорки (включително в сладка вода). Лаврак, атлантическа треска, сребриста сайда и подклас Пластинчатохрили
3	Източна Арктика (зони на ICES I и II)	Сьомга и змиорки (включително в сладка вода). Атлантическа треска, сребриста сайда и подклас Пластинчатохрили
4	Северната част на Атлантическия океан (зони V-XIV на ICES и зони на NAFO)	Сьомга и змиорки (включително в сладка вода). Лаврак, атлантическа треска, сребристра сайда, подклас Пластинчатохрили и далекомигриращи видове, обхванати от ICCAT.
5	Средиземно море	Змиорки (включително в сладка вода), подклас Пластинчатохрили и далекомигриращи видове, обхванати от ICCAT.
6	Черно море	Змиорки (включително в сладка вода), подклас Пластинчатохрили и далекомигриращи видове, обхванати от ICCAT.

Таблица 4

Променливи на риболовната дейност

	Променливи [1]	Единица
	Капацитет	
	Брой на корабите	Брой
	Бруто тонаж, kW, възраст на кораба	Брой
	Усилие	
	Дни в морето	Дни
	Риболовни часове (по избор)	Часове
	Риболовни дни	Дни
	kW * риболовни дни	Брой
	GT * риболовни дни	Брой
	Брой рейсове	Брой
	Брой на риболовните операции	Брой
	Брой на мрежите/дължина (*)	Брой/метри
	Брой на куките, брой на въдиците (*)	Брой
	Брой на винтерите, капанните съоръжения (*)	Брой
	Разтоварвания на брега	
	Стойност на разтоварванията — общо и по търговски видове	Евро
	Живо тегло на целия разтоварен улов на сушата и по видове	Тонове
	Цени по търговски видове	EUR/kg

[1] Всички променливи, които трябва да се отчитат с ниво на обобщаване (групи сходни риболовни дейности и сегмент на флота), посочени в таблица 3 и таблица 5B. и по подрегион/риболовно поле, както е посочено в таблица 5Cb.

(*) Събирането на посочените променливи за кораби с дължина под 10 метра следва да бъде договорено равнище морски региони

ИКОНОМИЧЕСКИ ДАННИ НА ФЛОТА

Таблица 5A

Икономически променливи за флота

Група променливи	Променлива	Единица
Приходи	Брутна стойност на разтоварванията на брега	Евро
	Приходи от лизинг на квота или други риболовни права	Евро
	Други приходи	Евро
Разходи за труд	Разходи за персонал	Евро
	Стойност на труда на лицата, които работят без заплащане	Евро
Разходи за енергия	Разходи за енергия	Евро
Разходи за ремонт и поддръжка	Разходи за ремонт и поддръжка	Евро
Други оперативни разходи	Променливи разходи	Евро
	Фиксирани разходи	Евро
	Лизингови плащания или плащане на наем за квота или други риболовни права	Евро
Субсидии	Субсидии за дейността	Евро
	Субсидии за инвестиции	Евро
Капиталови разходи	Потребление на основен капитал	Евро
Капиталова стойност	Стойност на материалните активи	Евро
	Стойност на квотата и на други риболовни права	Евро
Инвестиции	Инвестиции в материални активи, нетен размер	Евро
Финансово състояние	Дългосрочен/краткосрочен дълг	Евро
	Общи активи	Евро
Заетост	Наемен екипаж	Брой
	Лица, които работят без заплащане	Брой
	Общо отработени часове годишно	Брой

Група променливи	Променлива	Единица
Флот	Брой на корабите	Брой
	Средна LOA на корабите	Метри
	Общ тонаж на кораба	Бруто тонаж (GT)
	Обща мощност на кораба	kW
	Средна възраст на корабите	Години
Усилие	Дни в морето	Дни
	Потребление на енергия	Литри
Брой на риболовните предприятия/единици	Брой на риболовните предприятия/единици	Брой
Стойност на продукцията по видове	Стойност на разтоварванията по видове	Евро
	Средна цена по видове	EUR/kg

ИКОНОМИЧЕСКИ ДАННИ НА ФЛОТА

Таблица 5B

Сегментиране на флота

		Класове на дължина (LOA) [1]					
Активни кораби		0-< 10 m 0-< 6 m	10-< 12 m 6-< 12 m	12-< 18 m	18-< 24 m	24-< 40 m	40 m или повече
Използващи активни съоръжения	Бим траулери						
	Дънни траулери и/или дънни сейнери						
	Пелагични траулери						
	Кораби с мрежи гъргър						
	Кораби с драги						
	Кораби, използващи други активни съоръжения						
	Кораби, използващи само поливалентни активни съоръжения						

Активни кораби		Класове на дължина (LOA) [1]					
		0-< 10 m 0-< 6 m	10-< 12 m 6-< 12 m	12-< 18 m	18-< 24 m	24-< 40 m	40 m или повече
Използващи пасивни съоръжения	Кораби, използващи куки	[2]	[2]				
	Кораби, използващи плаващи или статични мрежи						
	Кораби, използващи кошове и/или капанни съоръжения						
	Кораби, използващи други пасивни съоръжения						
	Кораби, използващи единствено поливалентни пасивни съоръжения						
Използващи поливалентни съоръжения	Кораби, използващи активни и пасивни съоръжения						
Неактивни кораби							

[1] За кораби, по-къси от 12 метра в Средиземно и Черно море, категориите по дължина са 0-< 6, 6-< 12 метра. За всички останали региони категориите по дължина са определени като 0-< 10, 10-< 12 метра.

[2] Корабите, по-къси от 12 метра и използващи пасивни съоръжения в Средиземно и Черно море, могат да бъдат категоризирани по тип уреди. Дефиницията на сегмента на флота също така включва посочване на супрарегиона и, ако има на разположение, географски показател за идентифициране на корабите, които извършват риболов в най-отдалечените региони и изключително извън водите на ЕС

ИКОНОМИЧЕСКИ ДАННИ НА ФЛОТА

Таблица 5C

Географско разделение по региони

Подрегион/Риболовно място	Регион	Супрарегион
I	II	III
Групиране на пространствени единици на равнище 3, определено в теблица 3 (участък на NAFO)	NAFO (зона 21 на FAO)	Балтийско море Северно море Източна Арктика; NAFO Разширени северозападни води (зони на ICES V, VI и VII) и югозападни води
Групиране на пространствени единици на равнище 4, определено в таблица 3 (подучастък на ICES)	Балтийско море (зони III b-d на ICES)	
Групиране на пространствени единици на равнище 3, определено в таблица 3 (участък на ICES)	Северно море (зони на ICES IIIa и IV), Източна Арктика (зони на ICES I и II)	
	Северозападните води (зони на ICES Vb (само водите на Съюза), VI и VII)	
	Извън Съюза, северозападните води (зони на ICES Va и Vб) (Само води извън Съюза))	

Подрегион/Риболовно място	Регион	Супрарегион
I	II	III
Групиране на пространствени единици на равнище 3, определено в таблица 3 (участък на ICES/NAFO)	Югозападни води (зони VIII, IX и X (водите около Азорските острови), Зони на CECAF 34.1.1, 34.1.2 и 34.2.0 (водите около Мадейра и Канарските острови)	
Групиране на пространствени единици на равнище 4, определено в Таблица 3 (ГПЗ)	Средиземно море (водите на Средиземно море на изток от 5°36′ з.д.), Черно море (географската подзона на ГКРСМ съгласно определението в Резолюция FCM/33/2009/2)	Средиземно море и Черно море
Подзони на РОУР за вземане на проби (с изключение на ГКРСМ)	Други региони, където се извършват риболовни дейности от кораби на Съюза и са управлявани от РОУР, към които Съюзът е договаряща страна или наблюдател (напр. ICCAT, IOTC, CECAF…)	Други региони

Таблица 6

Социални променливи за сектора на риболова и аквакултурите

Променлива	Единица
Заетост по пол	Брой
Еквивалент на пълно работно време, по пол	Брой
Лица, които работят без заплащане, по пол	Брой
Заетост по възраст	Брой
Заетост по степен на образование	Брой за всяка степен на образование
Заетост по националност	Брой от ЕС, ЕИП и извън ЕС/ЕИП
Заетост по трудов статус	Брой
Национален еквивалент на пълно работно време	Брой

Таблица 7

Списък на икономическите променливи за сектора на аквакултурите

Група променливи	Променлива	Единица
Доходи (*)	Брутни продажби по видове	Евро
	Други приходи	Евро

Група променливи	Променлива	Единица
Разходи за персонал	Разходи за персонал	Евро
	Стойност на труда на лицата, които работят без заплащане	Евро
Разходи за енергия	Разходи за енергия	Евро
Разходи за суровини	Разходи за зарибителен материал	Евро
	Разходи за изхранване	Евро
Ремонт и поддръжка	Ремонт и поддръжка	Евро
Други оперативни разходи	Други оперативни разходи	Евро
Субсидии	Субсидии за дейността	Евро
	Субсидии за инвестиции	Евро
Капиталови разходи	Потребление на основен капитал	Евро
Капиталова стойност	Обща стойност на активите	Евро
Финансови резултати	Финансови приходи	Евро
	Финансови разходи	Евро
Инвестиции	Нетни инвестиции	Евро
Дълг	Дълг	Евро
Разходи за суровини	Използван зарибителен материал	kg
	Използвани рибни фуражи	kg
Тегло на продажбите	Тегло на продажбите по видове	Kg
Заетост	Наети лица	Брой/еквивалент на пълно работно време
	Лица, които работят без заплащане	Брой/еквивалент на пълно работно време
	Брой часове, изработени от заетите лица и неплатените работници	Часове
Брой предприятия	Брой предприятия (по категории за броя на заетите лица)	Брой

(*) Включва директни плащания, напр. компенсация за спиране на търговията, възстановяване на мито за гориво или подобни компенсаторни еднократни плащания; изключват се социалните плащания и косвените субсидии, напр. намалено мито за изходни суровини като гориво или инвестиционни субсидии.

Таблица 8

Списък на икономическите променливи за сектора на аквакултурите

Променлива	Спецификация:	Единица
Приложени лекарства или лечения (1)	Вид	Грам
Смъртност (2)		Процент

(1) Екстраполирано от данни, вписвани съгласно приложение I, точка 8, буква б) към Регламент (ЕО) № 852/2004 на Европейския парламент и на Съвета (ОВ L 139, 30.4.2004 г., стр. 1).
(2) Екстраполирано като процент от националното производство, от данни, регистрирани съгласно Директива 2006/88/ЕО на Съвета (ОВ L 328, 24.11.2006 г., стр. 14), член 8, параграф 1, буква б)

Таблица 9

Сегментиране, което се прилага при събирането на данни за аквакултурите (1)

	Техники на рибовъдство (2)						Поликултурно отглеждане	Люпилни и развъдници (3)	Техники за отглеждане на черупчести			
	Басейни	Резервоари и канали	Прегради места и заграждения (6)	Системи за рециркулация (5)	Други методи	Клетки (7)	Всички методи		Над дъното		По дъното (4)	Други
									Платформи	Парагада		
Сьомга												
Пъстърва												
Морски костур и северен пагел												
Шарани												
Тон												
Змиорки												
Есетра (хайвер за консумация от човека)												
Други сладководни риби												
Други морски риби												
Миди от вида Mytilus												

	Техники на рибовъдство ([2])						Поликултурно отглеждане	Люпилни и развъдници ([3])	Техники за отглеждане на черупчести			
	Басейни	Резервоари и канали	Прегради места и заграждения ([6])	Системи за рециркулация ([5])	Други методи	Клетки ([7])	Всички методи		Над дъното		По дъното ([4])	Други
									Платформи	Парагада		
Стриди												
Миди												
Ракообразни												
Други мекотели												
Многовидов												
Морски водорасли												
Други водни организми												

([1]) За определения на методите за събиране вж. Регламент (ЕО) № 762/2008.
([2]) Предприятията следва да бъдат сегментирани в съответствие с основните техники за отглеждане, които прилагат.
([3]) Люпилните и развъдниците са места за изкуствено оплождане, излюпване и отглеждане през ранните етапи от живота на водните животни. За статистически цели люпилните се ограничават до производството на оплодени яйца. Счита се, че по-нататъшните етапи от развитието на младите водни животни преминават в развъдници. Когато люпилните и развъдниците са тясно свързани, статистиките трябва да се отнасят само за последния етап отгледани животни. (COM (2006) 864 от 19 юли 2007 г.)
([4]) „Дънните“ техники обхващат отглеждането на черупчести в зоните между прилива и отлива (директно на дъното или повдигнати)
([5]) „Системи за рециркулация“ означава системи, в които водата се използва повторно след някаква форма на обработка (напр. филтриране).
([6]) „Прегради места и заграждения“ означават водни пространства, оградени с мрежи или други средства, които позволяват свободен воден обмен и се отличават с това, че тези прегради места заемат целия воден стълб от дъното до повърхността; по принцип заграждения и прегради места обхващат относително голям воден обем. (COM (2006) 864 от 19 юли 2007 г.)
([7]) Клетките са непокрити или покрити заградени структури от мрежа или какъвто и да е порест материал, позволяващ естествения обмен на водата. Тези структури могат да бъдат плаващи, окачени или закрепени за дъното, но така, че отдолу да се осигурява воден обмен (COM (2006) 864 от 19 юли 2007 г.).

Таблица 10

Научни изследвания по море

Наименование на изследването	Съкращение	Зона	Период	Основни целеви видове
Балтийско море				
Baltic International Trawl Survey	BITS Q1 BITS Q4	IIIaS, IIIb-d	1-во и 4-то тримесечие	Атлантическа треска и други дънни видове
Baltic International Acoustic Survey (Autumn)	BIAS	IIIa, IIIb-d	Септември—октомври	Херинга и цаца
Gulf of Riga Acoustic Herring Survey	GRAHS	IIId	3-то тримесечие	Херинга

Наименование на изследването	Съкращение	Зона	Период	Основни целеви видове
Sprat Acoustic Survey	SPRAS	IIId	Май	Цаца и херинга
Rügen Herring Larvae Survey	RHLS	IIId	Март — юни	Херинга
Северно море и Източна Арктика (зони на ICES I и II)				
International Bottom Trawl Survey	IBTS Q1 IBTS Q3	IIIa, IV	1-во и 3-то тримесечие	Пикша, атлантическа треска, сайда, херинга, цаца, меджид, скумрия, норвежки паут
North Sea Beam Trawl Survey	BTS	IVb,IVc,VIId	3-то тримесечие	Морска писия, морски език
Demersal Young Fish Survey	DYFS	Бреговете на Северно море	3-то и 4-то тримесечие	Писия (морска), обикновен морски език, кафява скарида
Sole Net Survey	SNS	IVb, IVc	3-то тримесечие	Обикновен морски език, писия (морска)
North Sea Sandeels Survey	NSSS	IVa, IVb	4-то тримесечие	Пясъчница, видове
International Ecosystem Survey in the Nordic Seas	ASH	IIa	Май	Херинга, син меджид
Redfish Survey in the Norwegian Sea and adjacent waters	REDNOR	II	август — септември	Морски костур
Mackerel egg Survey (на всеки три години)	NSMEGS	IV	май — юли	Хвърляне на хайвер на скумрия
Herring Larvae survey	IHLS	IV,VIId	1-во и 3-то тримесечие	Херинга, ларви на цаца
NS Herring Acoustic Survey	NHAS	IIIa, IV,VIa	юни, юли	Херинга, цаца
Nephrops TVsurvey (FU 3&4)	NTV3&4	IIIA	2-ро или 3-то тримесечие	Норвежки омар
Nephrops TVsurvey (FU 6)	NTV6	IVb	септември	Норвежки омар
Nephrops TVsurvey (FU 7)	NTV7	IVa	2-ро или 3-то тримесечие	Норвежки омар
Nephrops TVsurvey (FU 8)	NTV8	IVb	2-ро или 3-то тримесечие	Норвежки омар
Nephrops TVsurvey (FU 9)	NTV9	IVa	2-ро или 3-то тримесечие	Норвежки омар

Наименование на изследването	Съкращение	Зона	Период	Основни целеви видове
Северната част на Атлантическия океан (зони V-XIV на ICES и зони на NAFO)				
International Redfish Trawl and Acoustic Survey (Biennial)	REDTAS	Va, XII, XIV; NAFO SA 1-3	Юни/юли	Морски костур
Flemish Cap Groundfish survey	FCGS	3M	Юли	Дънни видове
Greenland Groundfish survey	GGS	XIV, NAFO SA1	октомври/ноември	Атлантическа треска, морски костур и други дънни видове
3LNO Groundfish survey	PLATUXA	NAFO 3LNO	2-ро и 3-то тримесечие	Дънни видове
Western IBTS 4-то тримесечие (вкл. Porcupine survey)	IBTS Q4	VIa, VII, VIII, IXa	4-то тримесечие	Дънни видове
Scottish Western IBTS	IBTS Q1	VIa,VIIa	Март	Трескови риби, херинга, скумрия
ISBCBTS септември	ISBCBTS	VIIa f g	Септември	Морски език, морска писия
WCBTS	VIIe BTS	VIIe	Октомври	Морски език, морска писия, морски дявол, малоуста писия
Blue whiting survey		VI, VII	1-во и 2-ро тримесечие	Син меджид
International Mackerel and Horse Mackerel Egg Survey (на всеки три години)	MEGS	VIa, VII,VIII, IXa	януари—юли	Хвърляне на хайвер на скумрия и сафрид
Sardine, Anchovy Horse Mackerel Acoustic Survey		VIII, IX	март, април, май	Показатели за изобилие на сардина, хамсия, скумрия, сафрид
DEPM на сардина (на всеки три години)		VIIIc, IXa	2-ро и 4-то тримесечие	SSB на сардина и използване на CUFES
Spawning/Pre spawning Herring acoustic survey		VIa, VIIa-g	Юли, септември, ноември, март, януари	Херинга, цаца
Biomass of Anchovy	BIOMAN	VIII	Май	SSB на хамсия (DEP)
Nephrops UWTV survey (крайбрежие)	UWTV (FU 11—13)	VIa	2-ро или 3-то тримесечие	Норвежки омар

Наименование на изследването	Съкращение	Зона	Период	Основни целеви видове
Nephrops UWTV Ирландско море	UWTV (FU 15)	VIIa	Август	Норвежки омар
Nephrops UWTV survey Aran Grounds	UWTV (FU 17)	VIIb	Юни	Норвежки омар
Nephrops UWTV survey Келтско море	UWTV (FU 20—22)	VIIg,h,j	Юли	Норвежки омар
Nephrops TV Survey Offshore Portugal NepS	UWTV (FU 28—29)	IXa	Юни	Норвежки омар
Водите на Средиземно море и Черно море				
Pan-Mediterranean Acoustic Survey ()	MEDIAS	ГПЗ 1, 6, 7, 9, 10, 15, 16, 17, 18, 20, 22	Пролет-лято (тримесечия 2-3)	Дребни пелагични видове
Bottom Trawl Survey в Черно море,	BTSBS	ГПЗ 29	Пролет - есен (тримесечия 2,3,4)	Калкан
Pelagic Trawl Survey в Черно море,	PTSBS	ГПЗ 29	Пролет-есен (тримесечия 2,3,4)	Цаца и меджид
International Bottom Trawl Survey в Средиземно море,	MEDITS	ГПЗ 1, 2, 3, 5, 6, 7, 8, 9, 10, 11, 15, 16, 17, 18, 19, 20, 22, 23, 25	Пролет — лято (тримесечия 2-3)	Дънни видове

Таблица 11

Икономически и социални променливи за сектора на преработвателната промишленост, които могат да бъдат събирани на доброволна основа

Група променливи	Променлива	Единица
ИКОНОМИЧЕСКИ ПРОМЕНЛИВИ		
Приходи	Оборот	Евро
	Други доходи	Евро
Разходи за персонала	Разходи за персонала	Евро
	Стойност на труда на лицата, които работят без заплащане	Евро
	Заплащане за външни работници от агенции (по избор)	Евро
Разходи за енергия	Разходи за енергия	Евро
Разходи за суровини	Закупуване на риба и други суровини за производството	Евро

Група променливи	Променлива	Единица
Други експлоатационни разходи	Други експлоатационни разходи	Евро
Субсидии	Оперативни субсидии	Евро
	Субсидии за инвестиции	Евро
Капиталови разходи	Потребление на основен капитал	Евро
Капиталова стойност	Обща стойност на активите	Евро
Финансови резултати	Финансов приход	Евро
	Финансови разходи	Евро
Инвестиции	Нетни инвестиции	Евро
Дълг	Дълг	Евро
Заетост	Брой на заетите лица	Брой
	Национален еквивалент на пълно работно време	Брой
	Лица, които работят без заплащане	Брой
	Брой на часовете работа на служителите и лицата, които работят без заплащане	Брой
Брой предприятия	Брой предприятия (1)	Брой
Тегло на суровината (ПО ИЗБОР)	Тегло на суровината по видове и по произход (ПО ИЗБОР)	Kg

СОЦИАЛНИ ПРОМЕНЛИВИ

Заетост по пол	Брой
Заетост по възраст	Брой
Заетост по образователна степен	Брой по образователна степен
Заетост по националност	Брой по държави в света
Национален еквивалент на пълно работно време	Брой

ISSN 1977-0618 (електронно издание)
ISSN 1830-3617 (печатно издание)

Служба за публикации на Европейския съюз
2985 Люксембург
ЛЮКСЕМБУРГ

BG