ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 24.6.2020 г.
SWD(2020) 115 final

РАБОТЕН ДОКУМЕНТ НА СЛУЖБИТЕ НА КОМИСИЯТА

[…]

придружаващ

СЪОБЩЕНИЕТО ОТ КОМИСИЯТА ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И СЪВЕТА

Защитата на данните като стълб в оправомощаването на гражданите и подхода на ЕС спрямо цифровия преход — две години прилагане на Общия регламент за защита на данните

{COM(2020) 264 final}

BG

Съдържание

1 КОНТЕКСТ

Общият регламент относно защитата на данните[1] (наричан по-нататък „ОРЗД“) е плод на осем години подготовка, съставяне и междуинституционални преговори и започна да се прилага на 25 май 2018 г. след двугодишен преходен период (май 2016 г. — май 2018 г.). В член 97 от ОРЗД е предвидено изискване Комисията да представя доклад относно оценката и прегледа на регламента, като започне с първия доклад след две години на прилагане и продължи със следващ на всеки четири години след това.

Оценката е също така част от многоаспектен подход, който Комисията вече следваше преди влизането в сила на ОРЗД и към който активно продължава да се придържа оттогава насам. Като част от този подход Комисията започна постоянни двустранни диалози с държавите членки относно съответствието на националното законодателство с ОРЗД, допринесе активно за работата на Европейския комитет по защита на данните (наричан по-нататък „Комитетът“ или „ЕКЗД“), като предостави своя опит и експертни познания, подкрепи органите за защита на данните и поддържаше тесни контакти с широк кръг заинтересовани страни във връзка с практическото прилагане на регламента.

Като основа за оценката е използван прегледът на постигнатите резултати, извършен от Комисията за първата година от прилагането на ОРЗД, който беше обобщен в публикуваното през юли 2019 г. съобщение[2]. Оценката е също така последващо действие по съобщението относно прилагането на ОРЗД, публикувано през януари 2018 г.[3]. Освен това Комисията прие Насоки относно използването на лични данни в контекста на избори, публикувани през септември 2018 г., и Насоки относно електронните приложения в подкрепа на борбата срещу пандемията от COVID-19, публикувани през април 2020 г.

Макар че настоящата оценка е съсредоточена върху двата въпроса, посочени в член 97, параграф 2 от ОРЗД, а именно международното предаване на данни и механизмите за сътрудничество и съгласуваност, в нея е възприет по-широк подход с цел да се разглеждат въпросите, повдигнати от различни участници през последните две години.

За да подготви оценката, Комисията взе предвид приноса на:

- Съвета[4];

---

[1] 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 (ОВ L 119, 4.5.2016 г., стр. 1—88.

[2] Съобщение на Комисията до Европейския парламент и Съвета „Правилата за защита на данните като катализатор на доверието в ЕС и извън него — преглед на постигнатите резултати“, COM(2019) 374 final, 24.7.2019 г.

[3] Съобщение от Комисията до Европейския парламент и Съвета: „По-силна защита, нови възможности — насоки на Комисията относно прякото прилагане, считано от 25 май 2018 г., на Общия регламент относно защитата на данните“, COM/2018/043 final

[4] Позиция и констатации на Съвета относно прилагането на Общия регламент относно защитата на данните (ОРЗД) — 14994/2/19 Rev2, 15.1.2020 г.: https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-2/bg/pdf

- Европейския парламент (Комисията по граждански свободи, правосъдие и вътрешни работи — LIBE)[5];
- Комитета[6] и отделните органи за защита на данните[7] въз основа на въпросник, изпратен от Комисията;
- отзивите от членовете на многостранната експертна група на заинтересованите страни за подкрепа на прилагането на ОРЗД[8], също въз основа на въпросник, изпратен от Комисията;
- и *ad hoc* принос, получен от заинтересовани страни.

2 ПРИЛАГАНЕ НА ОРЗД И ФУНКЦИОНИРАНЕ НА МЕХАНИЗМИТЕ ЗА СЪТРУДНИЧЕСТВО И СЪГЛАСУВАНОСТ

С ОРЗД бе установена новаторска система за управление и бе положена основата за истинска европейска култура за защита на данните, която има за цел да осигури не само хармонизирано тълкуване, но и хармонизирано прилагане и изпълнение на правилата за защита на данните. Нейни стълбове са независимите национални органи за защита на данните и новоучреденият Комитет.

Тъй като органите за защита на данните са от ключово значение за функционирането на цялата система на ЕС за защита на данните, Комисията внимателно следи за тяхната ефективна независимост, включително по отношение на достатъчните финансови, човешки и технически ресурси.

Все още е твърде рано да се направи цялостна оценка на функционирането на механизмите за сътрудничество и съгласуваност предвид досегашния кратък период за натрупване на опит[9]. Освен това органите за защита на данните все още не са използвали пълния спектър от инструменти, предвидени в ОРЗД, за да засилят допълнително сътрудничеството помежду си.

2.1 Използване на засилените правомощия от страна на органите за защита на данните

С ОРЗД се създават независими органи за защита на данните и им се предоставят хармонизирани и засилени правомощия за прилагане. Откакто се

---

[5] Писмо на Комисията LIBE на Европейския парламент от 21 февруари 2020 г. до члена на Комисията Райндерс, реф. №: IPOL-COM-LIBE D (2020)6525.

[6] Принос на Комитета към оценката на ОРЗД съгласно член 97, приет на 18 февруари 2020 г.: https://edpb.europa.eu/our-work-tools/our-documents/other/contribution-edpb-evaluation-gdpr-under-article-97_bg

[7] https://edpb.europa.eu/individual-replies-data-protection-supervisory-authorities_bg

[8] Многостранната експертна група на заинтересованите страни по въпросите на ОРЗД, създадена от Комисията, включва представители на гражданското общество, стопанските и академичните среди и практикуващи юристи: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537&Lang=BG
Докладът на многостранната експертна група на заинтересованите страни е на разположение на адрес: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=21356

[9] Този факт е изтъкнат по-специално от Съвета в неговата позиция и констатации относно прилагането на ОРЗД и от Комитета в неговия принос към оценката.

прилага ОРЗД, тези органи използват широк кръг от корективни правомощия, предвидени в регламента, като например административни наказания „глоба“ или „имуществена санкция“ (22 органа от ЕС/ЕИП)[10], предупреждения и официални предупреждения (23), разпореждания за изпълнение на исканията на субекта на данните (26), разпореждания за съобразяване на операциите по обработване на данни с разпоредбите на ОРЗД (27) и разпореждания за коригиране, заличаване или ограничаване на обработването на данни (17). Приблизително половината от органите за защита на данните (13) са наложили временно или окончателно ограничаване, в т.ч. забрани, на обработването на данни. Това показва съзнателно използване на всички коригиращи мерки, предвидени в ОРЗД; органите за защита на данните не се колебаят да налагат административни наказания „глоба“ или „имуществена санкция“ в допълнение към други корективни мерки или вместо тях, в зависимост от обстоятелствата по отделните случаи.

Административни наказания „глоба“ или „имуществена санкция“

През периода от 25 май 2018 г. до 30 ноември 2019 г. 22 органа за защита на данните от ЕС/ЕИП са наложили приблизително 785 глоби. Само няколко органа все още не са налагали административни наказания „глоба“ или „имуществена санкция“, въпреки че в момента текат производства, които може да доведат до такива глоби. Повечето глоби се отнасят до нарушения на: принципа на законосъобразност; действителното съгласие; защитата на чувствителни данни; задължението за прозрачност, правата на субектите на данните; както и нарушения на сигурността на данните.

Примерите за глоби, наложени от органите за защита на данните, включват[11]:

- 200 000 EUR за неспазване на правото на възражение срещу директен маркетинг в Гърция;
- 220 000 EUR на дружество посредник за данни в Полша, което не е уведомило физическите лица за това, че данните им се обработват;
- 250 000 EUR, наложени на испанската футболна лига La Liga, поради липсата на прозрачност при изготвянето на нейното приложение за смартфон;
- 14,5 милиона евро за нарушение на принципите за защита на данните, по-конкретно неправомерно съхранение, от страна на германско дружество за недвижими имоти;
- 18 милиона евро за неправомерно обработване на специални категории данни в голям мащаб от австрийските пощенски служби;
- 50 милиона евро на Google във Франция поради условията за получаване на съгласие от страна на потребителите.

[10] Цифрите в скобите показват броя на органите за защита на данните от ЕС/ЕИП, които са използвали описаните правомощия през периода от май 2018 г. до края на ноември 2019 г. Вж. приноса на Комитета, стр. 32—33.

[11] Няколко от решенията за налагане на глоби все още подлежат на съдебен контрол.

Успехът на ОРЗД не следва да се измерва с броя наложени глоби, тъй като в регламента е предвиден по-широк спектър от коригиращи правомощия. Например в зависимост от обстоятелствата възпиращият ефект от дадена забрана върху обработването на данни или преустановяването на потоците от данни може да бъде много по-силен.

Въпроси, специфични за публичния сектор

ОРЗД дава възможност на държавите членки да определят дали и до каква степен могат да бъдат налагани административни наказания „глоба“ или „имуществена санкция“ на публични органи и структури. В случаите, когато държавите членки се възползват от тази възможност, това не възпрепятства органите за защита на данните да използват всички останали корективни правомощия спрямо публични органи и структури[12].

Друг специфичен въпрос е съдебният надзор: макар ОРЗД да се прилага и спрямо дейностите на съдилищата, те са освободени от надзора на органите за защита на данните, когато действат при изпълнение на своите съдебни функции. Въпреки това в Хартата и ДФЕС са предвидени задължения държавите членки да възлагат на независим орган в рамките на своите съдебни системи надзора на тези операции по обработване[13].

Сътрудничество с други регулаторни органи

Както обяви в своето съобщение от юли 2019 г., Комисията подкрепя взаимодействието с други регулаторни органи при пълно зачитане на съответните им компетентности. Сред обещаващите области на сътрудничество са защитата на потребителите и конкуренцията. Комитетът изрази своята готовност да си сътрудничи с други регулаторни органи по-конкретно във връзка с концентрацията на цифровите пазари[14]. Комисията призна значението на неприкосновеността на личния живот и защитата на данните като качествен параметър на конкуренцията[15]. Членовете на Комитета взеха участие в съвместни работни форуми с Мрежата за сътрудничество в областта на защитата на потребителите относно сътрудничеството за по-успешно прилагане на законодателството на ЕС в областта на защитата на потребителите и данните. Този подход ще бъде следван, за да се насърчи общо разбиране и да се разработят практически начини за решаване на конкретни проблеми, с които се сблъскват потребителите, по-конкретно в цифровата икономика.

С цел да се осигури последователен подход към неприкосновеността на личния живот и защитата на данните и до приемането на Регламента за неприкосновеността на личния живот и електронните съобщения, е абсолютно необходимо тясното сътрудничество с органите, компетентни по прилагането на *lex specialis* в областта на електронните съобщения — Директивата за правото

---

12 Член 83, параграф 7 от ОРЗД.

13 Член 8, параграф 3 от Хартата; член 16, параграф 2 от ДФЕС; съображение 20 от ОРЗД.

14 Вж. изявлението на Комитета относно въздействието на икономическата концентрация върху защитата на данните на адрес https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_economic_concentration_en.pdf.

15 Вж. дело M.8124 — Microsoft/LinkedIn.

на неприкосновеност на личния живот и електронни комуникации[16]. По-тясното сътрудничество с органите, компетентни съгласно Директивата за мрежова и информационна сигурност (МИС)[17], и групата за сътрудничество за МИС би било от взаимна полза за тези органи и органите за защита на данните.

2.2 Механизмите за сътрудничество и съгласуваност

С ОРЗД бяха създадени механизмът за сътрудничество (система за „обслужване на едно гише“ на операторите, съвместни операции и взаимопомощ между органите за защита на данните) и механизмът за съгласуваност, за да се насърчи еднаквото прилагане на правилата за защита на данните чрез последователно тълкуване и разрешаване на евентуални разногласия между органите от страна на Комитета.

Комитетът, в който участват всички органи за защита на данните, е създаден като орган на ЕС с юридическа правосубектност и функционира пълноценно, подпомаган от секретариат[18]. Това е от решаващо значение за функционирането на двата механизма, посочени по-горе. До края на 2019 г. Комитетът е приел 67 документа, включително 10 нови насоки[19] и 43 становища[20],[21].

Важната роля на Комитета се прояви, когато възникна необходимост бързо да се осигури последователно тълкуване на ОРЗД и незабавно да се намерят приложими решения на равнището на ЕС. Например във връзка с избухването на епидемията от COVID-19, през март 2020 г. Комитетът прие изявление относно обработването на лични данни, в което наред с друго е разгледана законосъобразността на обработването и използването на данни за местонахождение в този контекст[22], а през април 2020 г. той прие Насоки относно обработването на данни за здравословното състояние с научноизследователска цел в контекста на пандемията от COVID-19 [23], както и Насоки относно използването на данни за местонахождение и инструменти за

---

[16] Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 година относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронни комуникации) — ОВ L 201, 31.7.2002 г., стр. 37—47.

[17] Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 година относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза — ОВ L 194, 19.7.2016 г., стр. 1—30.

[18] Подробна информация относно дейността на секретариата вж. в приноса на Комитета, стр. 24—26.

[19] В допълнение към 10-те документа с насоки, приети от Работната група по член 29 в хода на подготовката за влизането в сила на ОРЗД и утвърдени от Комитета. Освен това Комитетът е приел 4 допълнителни насоки и е актуализирал една съществуваща през периода от януари до края на май 2020 г.

[20] 42 от тези становища са приети съгласно член 64 от ОРЗД, а едно е прието съгласно член 70, параграф 1, буква т) от ОРЗД и се отнася до решението относно адекватното ниво на защита по отношение на Япония.

[21] За пълен преглед на дейностите на Комитета вж. приноса на Комитета, стр. 18—23.

[22] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf

[23] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032020-processing-data-concerning-health-purpose_bg.

проследяване на контакти в контекста на пандемията от COVID-19[24]. Комитетът също така оказа съществен принос за разработването от страна на Комисията и държавите членки на подхода на ЕС за приложения за проследяване.

Сътрудничеството между органите за защита на данните в ежедневната работа, независимо дали действат в изпълнение на собствените си функции или в качеството на членове на Комитета, се основава на обмен на информация и на уведомления за случаите, заведени от органите. С цел да улесни комуникацията между органите Комисията осигури значителна подкрепа, като им предостави система за обмен на информация[25]. Повечето органи считат, че тя е адаптирана към нуждите на механизмите за сътрудничество и съгласуваност, въпреки че би могла да бъде допълнително прецизирана, например като се направи по-лесна за ползване.

Въпреки че етапът все още е начален, вече могат да бъдат идентифицирани редица постижения и предизвикателства, които са представени по-долу. Те показват, че досега органите за защита на данните са използвали ефективно инструментите за сътрудничество, като предпочитат по-гъвкавите решения.

Обслужване на едно гише

Като общо правило при трансгранични случаи органът за защита на данните на дадена държава членка може да бъде включен или i) като водещ орган, когато основното място на установяване на оператора се намира в тази държава членка, или ii) като засегнат орган, когато операторът има място на установяване на територията на тази държава членка, когато физически лица в тази държава членка са съществено засегнати или когато до този орган са подадени жалби.

Това тясно сътрудничество се е превърнало в ежедневна практика: след датата на прилагане на ОРЗД органите за защита на данните във всички държави членки на някакъв етап бяха определени или като водещи, или като засегнати органи при трансгранични случаи, макар и в различна степен.

От май 2018 г. до края на 2019 г. органът за защита на данните в Ирландия е изпълнявал функциите на водещ орган по най-голям брой трансгранични случаи (127), следван от Германия (92), Люксембург (87), Франция (64) и Нидерландия (45). Това класиране отразява по-специално специфичното положение на Ирландия и Люксембург, където са седалищата на няколко големи мултинационални технологични предприятия.

Класирането е различно от гледна точка на участието като засегнати органи за защита на данните, като в най голям брой случаи са участвали органите в Германия (435), следвана от Испания (337), Дания (327), Франция (332) и Италия (306)[26].

Между 25 май 2018 г. и 31 декември 2019 г. бяха представени 141 проекта за решения чрез процедурата „обслужване на едно гише“, като по 79 от тях бяха

[24] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_bg.pdf

[25] Информационна система за вътрешния пазар (IMI)

[26] Вж. приноса на Комитета, стр. 8.

приети окончателни решения. Към датата на публикуване на настоящия доклад са в ход няколко важни решения с трансгранично измерение, подлежащи на механизма „обслужване на едно гише“. Някои от тях включват големи мултинационални технологични предприятия[27]. Очаква се чрез тях да се дадат разяснения и да се допринесе за по-голяма хармонизация при тълкуването на ОРЗД.

Взаимопомощ

Органите за защита на данните са се възползвали в голяма степен от инструмента за взаимопомощ.

До края на 2019 г. са осъществени 115 процедури за взаимопомощ[28], по-специално за провеждане на разследвания, повечето от органите за защита на данните в Испания (26), Германия (20), Дания (13), Полша (12) и Чешката република (10). От друга страна, най-много искания са получили Ирландия (19), Франция (11), Австрия (10), Германия (10) и Люксембург (9) [29].

Преобладаващата част от органите намират взаимопомощта за много полезен инструмент за сътрудничество и не са срещнали някакви особени пречки пред прилагането на процедурата за взаимопомощ. Доброволният обмен на взаимопомощ, при който няма законоустановен срок или не се налага строго задължение за отговор, е използван по-често — в 2 427 процедури. Органът за защита на данните на Ирландия е изпратил и получил най-много искания за взаимопомощ (527 изпратени и 359 получени), следван от германските органи (260 изпратени/356 получени).

От друга страна, все още не са провеждани съвместни операции[30], които биха позволили органи за защита на данните от няколко държави членки да участват още на етапа на разследването на трансгранични случаи. В рамките на Комитета е в ход процес на размисъл относно практическото прилагане на този инструмент и начините за насърчаване на неговото използване.

Механизъм за съгласуваност

Досега се използва само първият етап от механизма за съгласуваност, а именно приемането на становища на Комитета[31]. От друга страна, досега не са задействани процедури за разрешаване на спорове от Комитета[32] или процедури по спешност[33].

---

[27] Така например, на 22 май 2020 г. ирландският орган за защита на данните е представил проект за решение на други засегнати органи съгласно член 60 от регламента във връзка с разследване на Twitter International Company относно уведомление за нарушения на сигурността на данните. На същия ден ирландският орган за защита на данните също така е обявил, че е в процес на изготвяне проект за решение за подаване по член 60 относно WhatsApp Ireland Limited, свързано с прозрачността, включително прозрачност относно това каква информация се споделя с Facebook.

[28] Член 61 от ОРЗД.

[29] Вж. приноса на Комитета, стр. 12—14.

[30] Член 62 от ОРЗД.

[31] Въз основа на член 64 от ОРЗД.

[32] Член 65 от ОРЗД.

[33] Член 66 от ОРЗД.

Между 25 май 2018 г. и 31 декември 2019 г. Комитетът е издал 36 становища в контекста на приемането на мерки от един от неговите членове[34]. Повечето от тях (31) са свързани с приемането на национални списъци на операциите по обработване, които подлежат на изискването за оценка на въздействието по отношение на защитата на лични данни. Две становища се отнасят до задължителни фирмени правила, други две се отнасят до проекти за критериите за акредитиране на орган за наблюдение на кодекси на поведение, а едно се отнася до стандартните договорни клаузи[35].

Освен това Комитетът е приел шест становища въз основа на отправени искания[36]. Три от тези становища се отнасят до национални списъци на видовете обработване, които не подлежат на изискването за оценка на въздействието по отношение на защитата на лични данни. Останалите се отнасят съответно до административна договореност за предаването на лични данни между органи за финансов надзор от ЕИП и органи за финансов надзор извън ЕИП, взаимодействието между Директивата за правото на неприкосновеност на личния живот и електронни комуникации и ОРЗД и компетентността на надзорния орган в случай на промяна в обстоятелствата, свързана с основното или единственото място на установяване[37].

Предизвикателства, които трябва да бъдат преодолени

Въпреки че органите за защита на данните работиха особено усилено заедно в рамките на Комитета и вече активно използват инструмента за сътрудничество за взаимопомощ, истинска обща култура за защита на данните все още е в процес на изграждане.

По-специално разглеждането на трансгранични случаи изисква по-ефикасен и хармонизиран подход и ефективно използване на всички инструменти за сътрудничество, предвидени в ОРЗД. По този въпрос има много широк консенсус, тъй като той беше повдигнат по различни начини от Европейския парламент, Съвета, Европейския надзорен орган по защита на данните, заинтересованите страни (в рамките на многостранната група на заинтересованите страни и извън нея) и от органите за защита на данните.

Сред основните въпроси, които трябва да бъдат разгледани в този контекст, са разликите в:

- националните административни процедури, отнасящи се по-специално до процедурите за разглеждане на жалби, критериите за допустимост на жалбите, продължителността на производствата поради различни срокове или липсата на срокове, момента в процедурата, когато се предоставя правото на изслушване, информацията за жалбоподателите и участието им в хода на процедурата;
- тълкуванията на понятия, свързани с механизма за сътрудничество, като например значима информация, понятията „незабавно“, „жалба“, документа,

[34] Съгласно член 64, параграф 1 от ОРЗД.
[35] Член 28, параграф 8 от ОРЗД.
[36] Съгласно член 64, параграф 2 от ОРЗД.
[37] Вж. приноса на Комитета, стр. 15.

който се определя като „проект за решение“ на водещия орган за защита на данните, уреждането по взаимно съгласие (по-специално процедурата, водеща до уреждане по взаимно съгласие, и правната форма на споразумението); и

- подхода към момента на започване на процедурата за сътрудничество, включването на засегнатите органи за защита на данните и съобщаването на информация на тези органи. Жалбоподателите също така нямат яснота относно начина, по който се разглеждат случаите им при трансгранични ситуации, както беше подчертано от няколко членове на многостранната група на заинтересованите страни. Освен това предприятията посочват, че в някои случаи националните органи за защита на данните не са отнесли случаите им до водещия орган за защита на данните, а са ги разгледали като местни случаи.

Комисията приветства изявлението на Комитета, че е започнал процес на размисъл относно начините за справяне с тези въпроси. По-специално Комитетът посочи, че ще изясни процедурните стъпки, свързани със сътрудничеството между водещия орган за защита на данните и засегнатите органи за защита на данните, ще анализира националното административно процесуално право, ще работи за изготвяне на общо тълкуване на ключови понятия и ще засили комуникацията и сътрудничеството (включително съвместните операции). Процесът на размисъл и анализът на Комитета следва да доведат до създаване на по-ефикасни работни договорености по трансграничните случаи[38], включително чрез надграждане върху експертния опит на неговите членове и чрез засилване на участието на неговия секретариат. Освен това следва да се отбележи, че отговорността на Комитета да осигури последователно тълкуване на ОРЗД не може да бъде изпълнена само чрез намиране на „най-малкия общ знаменател“.

И накрая, като орган на ЕС Комитетът трябва също така да прилага административното право на ЕС и да гарантира прозрачност в процеса на вземане на решения.

2.3 Становища и насоки

Повишаване на осведомеността и предоставяне на становища от страна на органите за защита на данните

Няколко органа за защита на данните създадоха нови инструменти, като например линии за помощ за отделните лица и предприятията и набори от инструменти за предприятията[39]. Много оператори приветстват прагматизма, демонстриран от тези органи при оказването на подкрепа по прилагането на ОРЗД. По-конкретно, няколко от тях активно и тясно си сътрудничиха и комуникираха с длъжностни лица по защита на данните, включително чрез сдружения на длъжностните лица по защита на данните. Много органи също така публикуваха насоки, обхващащи ролята и задълженията на длъжностните лица по защита на данните, за да се подпомогнат длъжностните лица по защита

[38] Както беше посочено и в Позицията и констатациите на Съвета.
[39] Вж. точка 7 по-долу.

на данните в ежедневната им работа, и проведоха специално предназначени за тях семинари. Това обаче не се отнася за всички органи за защита на данните.

Отзивите, получени от заинтересованите страни, също показват редица въпроси във връзка с насоките и становищата:

- липсата на последователен подход и насоки по определени въпроси между националните органи за защита на данните (например относно „бисквитките“[40], прилагането на законен интерес, уведомленията за нарушения на сигурността на данните или оценките на въздействието по отношение на защитата на лични данни) или дори между органите за защита на данните в рамките на едни и същи държави членки (например в Германия относно понятията „администратор“ и „обработващ лични данни“);
- непоследователността на насоките, приети на национално равнище, с приетите от Комитета;
- липса на обществени консултации относно някои насоки, приети на национално равнище;
- различни равнища на ангажираност със заинтересованите страни сред органите за защита на данните;
- закъснения при получаването на отговори на искания за информация;
- трудности при получаването на практически и полезни становища от органите за защита на данните;
- необходимостта от увеличаване на равнището на експертни познания по отделни сектори в някои органи за защита на данните (например в сектора на здравеопазването и фармацевтиката).

Няколко от тези въпроси са свързани и с липсата на ресурси в няколко органа за защита на данните (вж. по-долу).

Различни практики по отношение на уведомленията за нарушения на сигурността на данните[41]

Въпреки че Съветът подчертава тежестта вследствие на тези уведомления, съществуват значителни несъответствия по отношение на уведомленията между държавите членки: през периода от май 2018 г. до края на ноември 2019 г. в повечето държави членки общият брой на уведомленията за нарушения на сигурността на данните е бил по-малко от 2 000, а в 7 държави членки между

[40] До приемането на Регламента за неприкосновеността на личния живот и електронните съобщения е необходимо тясно сътрудничество с компетентните органи, отговарящи за прилагането в държавите членки на Директивата за правото на неприкосновеност на личния живот и електронни комуникации. В съответствие с тази директива в някои държави членки органите, компетентни да прилагат член 5, параграф 3 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации (в който се определят условията, при които в крайното оборудване на ползвателя могат да се съхраняват „бисквитки“ и да се получава достъп до тях), не са същите като надзорните органи в рамките на ОРЗД.

[41] Член 33 от ОРЗД.

2 000 и 10 000, докато нидерландските и германските органи за защита на данните са докладвали съответно 37 400 и 45 600 уведомления[42].

Това може да е признак за липса на последователно тълкуване и прилагане, въпреки наличието на насоки на равнище ЕС относно уведомленията за нарушения на сигурността на данните.

Насоки на Европейския комитет по защита на данните

Към днешна дата Комитетът е приел повече от 20 насоки, които обхващат ключови аспекти на ОРЗД[43]. Насоките са основен инструмент за последователното прилагане на ОРЗД и поради това до голяма степен са приветствани от заинтересованите страни. Заинтересованите страни оцениха системното организиране на публични консултации (в продължение на 6—8 седмици). Те обаче искат по-редовен диалог с Комитета. В този контекст практиката за организиране на работни семинари по целеви теми преди изготвянето на насоки следва да бъде продължена и разширена, за да се гарантират прозрачност, приобщаване и целесъобразност на работата на Комитета. Заинтересованите страни също така изискват тълкуването на най-спорните въпроси да се разглежда в насоките, тъй като те са предмет на обществени консултации, а не в становища съгласно член 64, параграф 2 от ОРЗД. Някои заинтересовани страни също така призовават за насоки с по-практическа насоченост, в които подробно се описва прилагането на понятията и разпоредбите на ОРЗД[44]. Членовете на многостранната група на заинтересованите страни подчертават необходимостта от повече конкретни примери, за да се намали във възможно най-голяма степен възможността за различни тълкувания на органите по защита на данните. В същото време исканията да се изясни как да се прилага ОРЗД и да се осигури правна сигурност не следва да водят до допълнителни изисквания или да намаляват предимствата на основания на риска подход и на принципа на отчетност.

Темите, по които заинтересованите страни биха желали Комитетът да изготви допълнителни насоки, включват: обхвата на правата на субектите на данните (включително в контекста на трудовите правоотношения); актуализиране на становището относно обработването на данни на основание на законен интерес; понятията „администратор“, „съвместен администратор“ и „обработващ лични данни“ и необходимите договорености между страните[45]; прилагането на ОРЗД по отношение на нови технологии (като например блокова верига и изкуствен интелект); обработването на данни в контекста на научните изследвания (включително във връзка с международното сътрудничество); обработването на данни на деца; псевдонимизацията и анонимизацията; и обработването на данни за здравословното състояние.

---

[42] Вж. приноса на Комитета, стр. 35.

[43] Работата по насоките започна още преди влизането в сила на ОРЗД на 25 май 2018 г. в рамките на Работната група по член 29. Вж. пълния списък с насоки на адрес https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_bg

[44] Това беше подчертано също и от Европейския парламент и от Съвета.

[45] Понастоящем се подготвят насоки на Комитета относно администраторите и обработващите лични данни.

Комитетът вече е посочил, че ще публикува насоки по много от тези въпроси и че работата по няколко от тях вече е започнала (например относно прилагането на законния интерес като правно основание за обработването на данни).

Заинтересованите страни приканват Комитета да актуализира и преразгледа съществуващите насоки, като вземе предвид, когато е целесъобразно, натрупания след публикуването им опит и като се възползва от възможността при необходимост да разгледа въпросите по-подробно.

2.4 Ресурси на органите за защита на данните

Предоставянето на необходимите човешки, технически и финансови ресурси, помещения и инфраструктура на всеки орган за защита на данните е предпоставка за ефективното изпълнение на техните задачи и упражняването на техните правомощия и следователно е съществено условие за тяхната независимост[46].

След влизането в сила на ОРЗД през 2016 г.[47] на повечето органи за защита на данните е осигурено увеличение на персонала и ресурсите. Много от тях обаче все още съобщават, че не разполагат с достатъчно ресурси[48].

Брой на служителите, работещи за националните органи за защита на данните

Между 2016 г. и 2019 г. общият брой на служителите, работещи в органи за защита на данните от ЕИП, се е увеличил с 42 % (с 62 %, ако се вземе предвид прогнозата за 2020 г.).

През този период броят на служителите в повечето органи е нараснал, като най-голямо увеличение (като процент) е регистрирано за органите в Ирландия (+ 169 %), Нидерландия (+ 145 %), Исландия (+ 143 %), Люксембург (+ 126 %) и Финландия (+ 114 %). От друга страна, в няколко органа за защита на данните броят на служителите е намалял, като най-резките спадове са наблюдавани в Гърция (- 15 %), България (- 14 %), Естония (- 11 %), Латвия (- 10 %) и Литва (- 8 %). В някои органи намаляването на служителите се дължи също така на преминаване на експертите по защита на данните в частния сектор, който предлага по-привлекателни условия.

Като цяло прогнозата за 2020 г. предвижда увеличение на служителите в сравнение с 2019 г., с изключение на органите в Австрия, България, Италия, Исландия и Швеция (където броят на служителите се очаква да остане стабилен), Кипър и Дания (където броят на служителите се очаква да намалее).

Германските органи за защита на данните[49], взети заедно, имат най-голям брой служители (888 през 2019 г./1002 според прогнозата за 2020 г.), следвани от

[46] Вж. член 52, параграф 4 от ОРЗД.

[47] Регламентът влезе в сила през май 2016 г. и започна да се прилага през май 2018 г. след двугодишен преходен период.

[48] Вж. приноса на Комитета, стр. 26—30.

[49] В Германия има 18 органа, единият от които е федерален орган, а 17 са регионални органи (включително два в Бавария).

органите за защита на данните в Полша (238/260), Франция (215/225), Испания (170/220), Нидерландия (179/188), Италия (170/170) и Ирландия (140/176).

Органите за защита на данните с най-малък брой служители са тези в Кипър (24/22), Латвия (19/31), Исландия (17/17), Естония (16/18) и Малта (13/15).

Бюджет на националните органи за защита на данните

Между 2016 г. и 2019 г. общият бюджет на органите за защита на данните от ЕИП, взети заедно, се е увеличил с 49 % (с 64 %, ако се вземе предвид прогнозата за 2020 г.).

През този период бюджетът на повечето органи се е увеличил, като най-голямо увеличение (като процент) е регистрирано за органите в Ирландия (+ 223 %), Исландия (+ 167 %), Люксембург (+ 165 %), Нидерландия (+ 130 %) и Кипър (+ 114 %). От друга страна, при някои органи се наблюдава само малко увеличение на бюджета, като най-малко увеличение е регистрирано за органите за защита на данните в Естония (7 %), Латвия (4 %), Румъния (3 %) и Белгия (1 %), докато във Франция органът отбелязва спад (- 2 %).

Като цяло прогнозата за 2020 г. предвижда увеличение на бюджета в сравнение с 2019 г., с изключение на органите в Австрия, България, Естония и Нидерландия (чиито бюджети се очаква да се запазят стабилни).

Органите за защита на данните с най-висок бюджет са тези на Германия (76,6 милиона евро през 2019 г./85,8 милиона евро в прогнозата за 2020 г.), Италия (29,1/30,1 милиона евро), Нидерландия (18,6/18,6 милиона евро), Франция (18,5/20,1 милиона евро) и Ирландия (15,2/16,9 милиона евро).

Органите с най-нисък бюджет са тези на Хърватия (1,2 милиона евро през 2019 г./1,4 милиона евро в прогнозата за 2020 г.), Румъния (1,1/1,3 милиона евро), Латвия (0,6/1,2 милиона евро), Кипър (0,5/0,5 милиона евро) и Малта (0,5/0,6 милиона евро).

В таблицата в приложение II е представен преглед на човешките и бюджетните ресурси на националните органи за защита на данните.

Освен че засяга капацитета им за прилагане на правилата на национално равнище, липсата на ресурси също така ограничава капацитета на органите за защита на данните да участват и да допринасят за механизмите за сътрудничество и съгласуваност, както и за работата, извършвана в рамките на Комитета. Както беше подчертано от Комитета, успехът на механизма „обслужване на едно гише“ зависи от времето и усилията, които органите за защита на данните могат да насочат към разглеждането на отделните трансгранични случаи и сътрудничеството по тях. Въпросът за ресурсите се усложнява от нарасналата роля на органите в надзора на широкомащабните информационни системи, които се разработват понастоящем. Освен това органите за защита на данните в Ирландия и Люксембург имат специфични нужди от ресурси, предвид тяхната роля на водещи органи за прилагането на ОРЗД по отношение на големите технологични предприятия, които се намират предимно в тези държави членки.

Съветът от една страна изтъква влиянието на механизма за сътрудничество и неговите срокове върху работата на органите за защита на данните[50], но от друга страна ОРЗД задължава държавите членки да предоставят на своите национални органи за защита на данните достатъчни човешки, финансови и технически ресурси[51].

Секретариатът на Комитета, който се осигурява от Европейския надзорен орган по защита на данните (ЕНОЗД)[52], понастоящем се състои от 20 души, включително експерти в областта на правото, информационните технологии и комуникациите. Трябва да се прецени дали е необходимо тази бройка да се промени в бъдеще с оглед на ефективното изпълнение на функцията му за предоставяне на аналитична, административна и логистична подкрепа на Комитета и неговите подгрупи, включително чрез управлението на системата за обмен на информация.

3 ХАРМОНИЗИРАНИ ПРАВИЛА, НО ВСЕ ОЩЕ СЪЩЕСТВУВАЩА ИЗВЕСТНА ФРАГМЕНТИРАНОСТ И РАЗЛИЧАВАЩИ СЕ ПОДХОДИ

В ОРЗД е предвиден последователен подход към правилата за защита на данните в целия ЕС, който заменя различните национални режими съгласно Директивата за защита на личните данни от 1995 г.

3.1 Прилагане на ОРЗД от държавите членки

ОРЗД се прилага пряко във всички държави членки от 25 май 2018 г. Той задължава държавите членки да приемат законодателни актове, по-специално да създадат национални органи за защита на данните и да приемат общи условия за техните членове, за да се гарантира, че всеки орган действа напълно независимо при изпълнението на задачите си и упражняването на правомощията си съгласно ОРЗД. Правните задължения и обществените задачи могат да представляват правно основание за обработването на лични данни само ако са установени в (правото на Съюза или) националното право. Освен това държавите членки трябва да определят правила за санкции, по-специално за нарушения, които не подлежат на административни наказания „глоба“ или „имуществена санкция“, и трябва да съгласуват правото на защита на личните данни с правото на свобода на изразяване и информация. В националното право може също така да бъде предвидено правно основание за освобождаване от общата забрана за обработване на специални категории лични данни, например поради причини, свързани със значим обществен интерес в областта на общественото здраве, включително защитата срещу сериозни трансгранични заплахи за здравето. Освен това държавите членки трябва да осигурят акредитацията на сертифициращи органи.

Комисията наблюдава прилагането на ОРЗД в националното законодателство. Към момента на изготвяне на настоящия доклад всички държави членки с

[50] Член 60 от ОРЗД.
[51] Член 52, параграф 4 от ОРЗД.
[52] Член 75 от ОРЗД.

изключение на Словения са приели ново законодателство за защита на данните или са адаптирали своето законодателство в тази област. Поради това Комисията поиска от Словения да предостави разяснения относно постигнатия до момента напредък и настоятелно я прикани да приключи този процес[53].

Освен това съответствието на националното законодателство с правилата за защита на данните по отношение на достиженията на правото от Шенген се оценява също така в контекста на механизма за оценка по Шенген, координиран от Комисията. Комисията и държавите членки оценяват съвместно как държавите изпълняват и прилагат достиженията на правото от Шенген в редица области; по отношение на защитата на данните това засяга широкомащабните информационни системи като Шенгенската информационна система и Визовата информационна система и включва ролята на органите за защита на данните за надзора на обработването на лични данни в рамките на тези системи.

Работата на национално равнище по адаптирането на секторните закони все още продължава. След включването на ОРЗД в Споразумението за Европейското икономическо пространство обхватът на неговото прилагане се разпростря до Норвегия, Исландия и Лихтенщайн. Тези държави също са приели свои национални закони за защита на данните.

Комисията ще използва всички инструменти, с които разполага, включително производства за установяване на нарушение, за да гарантира спазването на ОРЗД от страна на държавите членки.

Основни въпроси, свързани с прилагането на национално равнище

Основните въпроси, набелязани до момента като част от текущата оценка на националното законодателство и двустранния обмен с държавите членки, включват:

- ограничения за прилагането на ОРЗД — някои държави членки например напълно изключват дейността на националния парламент;
- различия в приложимостта на националните уточняващи закони. Някои държави членки обвързват приложимостта на националното си право с мястото, където се предлагат стоките или услугите, други — с мястото на установяване на администратора или обработващия лични данни. Това противоречи на целта за хармонизиране, преследвана от ОРЗД;
- национални закони, които пораждат въпроси относно пропорционалността на намесата в правото на защита на данните. Комисията например започна производство за установяване на нарушение срещу държава членка, която е приела законодателен акт, изискващ съдиите да оповестяват конкретна информация относно своята неслужебна дейност, което е несъвместимо с

[53] Следва да се отбележи, че националният орган за защита на данните в Словения е създаден въз основа на действащото национално законодателство за защита на данните и контролира прилагането на ОРЗД в тази държава членка.

правото на зачитане на личния живот и правото на защита на личните данни[54];

- липсата на независим орган за надзор на обработването на лични данни от страна на съдилищата, когато действат при изпълнение на своите съдебни функции[55];
- законодателството в области, които са изцяло регулирани от ОРЗД, надхвърлящо рамките за уточнения и ограничения. Такъв е по-специално случаят, когато националните разпоредби определят условията за обработването на данни на основание на законен интерес, като предвиждат постигането на баланс между съответните интереси на администратора и на засегнатите лица, докато ОРЗД задължава всеки администратор да постига този баланс за всеки отделен случай и да се възползва от това правно основание;
- уточнения и допълнителни изисквания отвъд обработването с цел спазване на правно задължение или изпълнение на задача от обществен интерес (например за видеонаблюдение в частния сектор или за целите на директния маркетинг); както и за понятията, използвани в ОРЗД (например „мащабно“ или „изтриване“).

Някои от тези въпроси може да бъдат изяснени от Съда в рамките на дела, които все още са висящи[56].

Съгласуване на правото на защита на личните данни със свободата на изразяване на мнение и на информация

Конкретен въпрос е свързан с изпълнението на задължението на държавите членки да съгласуват със закон правото на защита на личните данни със свободата на изразяване на мнение и на информация[57]. Този въпрос е много сложен, тъй като при оценката на баланса между тези основни права трябва да се вземат предвид също така разпоредбите и гаранциите в законите за печата и медиите.

Оценката на законодателството на държавите членки показва различни подходи към съгласуването на правото на защита на личните данни със свободата на изразяване на мнение и на информация:

- някои държави членки са установили принципа за предимство на свободата на изразяване на мнение или изключват по принцип прилагането на цели глави, посочени в член 85, параграф 2 от ОРЗД, ако става дума за обработване, извършвано за журналистически цели и за целите на академичното, художественото или литературното изразяване. Законите за

[54] Това производство за установяване на нарушение се отнася до полския Закон за съдебната власт от 20 декември 2019 г., който засяга независимостта на съдиите и е свързан, наред с другото, с оповестяването на участието на съдии в неслужебни дейности: https://ec.europa.eu/commission/presscorner/detail/bg/ip_20_772.

[55] Вж. член 8, параграф 3 от Хартата; член 16 от ДФЕС; съображение 20 от ОРЗД.

[56] Например освобождаването на парламентарна комисия от прилагането на ОРЗД се разглежда във висящо съдебно производство (дело C-272/19).

[57] Член 85 от ОРЗД.

медиите до известна степен осигуряват някои гаранции по отношение на правата на субектите на данните;

- някои държави членки са установили предимство на защитата на личните данни и предвиждат изключения от прилагането на правилата за защита на данните само в конкретни ситуации, например когато става въпрос за лице с публичен статут;
- други държави членки предвиждат известна степен на постигане на баланс от страна на законодателя и/или оценка за всеки отделен случай по отношение на дерогациите от някои разпоредби на ОРЗД.

Комисията ще продължи своята оценка на националното законодателство въз основа на изискванията на Хартата. Съгласуването трябва да бъде предвидено в закон и да зачита основното съдържание на посочените права и свободи, както и да бъде пропорционално и необходимо (член 52, параграф 1 от Хартата). Правилата за защита на данните не следва да засягат упражняването на свободата на изразяване на мнение и на информация, особено чрез създаване на възпиращ ефект, или като се тълкуват по такъв начин, че да се оказва натиск върху журналисти да разкриват своите източници.

3.2 Клаузи за незадължителни уточнения и ограничения за тях

В ОРЗД на държавите членки се предоставя възможността да уточнят допълнително прилагането на своя територия в ограничен брой области. Тази свобода за национални законодателни актове следва да се разграничава от задължението за прилагане на някои други разпоредби на ОРЗД, посочени по-горе. Клаузите за незадължителни уточнения са изброени в приложение I.

Свободата за законодателство на държавите членки подлежи на условията и ограниченията, определени от ОРЗД, и не позволява успореден национален режим за защита на данните[58]. Държавите членки са задължени да изменят или отменят националните закони за защита на данните, включително секторното законодателство с аспекти, свързани със защитата на данните.

Освен това законодателството на съответната държава членка не трябва да включва разпоредби, които биха могли да породят объркване по отношение на прякото прилагане на ОРЗД. Поради това, когато в ОРЗД се предвиждат уточнения или ограничения на съдържащите се в него правила от правото на държавите членки, държавите членки могат, доколкото това е необходимо за гарантиране на последователността и разбираемостта на националните разпоредби за лицата, по отношение на които те се прилагат, да включат елементи на ОРЗД в собственото си право[59].

Заинтересованите страни считат, че държавите членки следва да ограничат или да се въздържат от използването на клаузите за незадължителни уточнения, тъй като те не допринасят за хармонизацията. Националните различия както в

[58] Широко използваният термин „отворени клаузи“ в смисъл на клаузи за уточнения е подвеждащ, тъй като може да създаде впечатлението, че държавите членки имат свобода на действие отвъд разпоредбите на регламента.

[59] Съображение 8 от ОРЗД.

прилагането на законите, така и в тяхното тълкуване от страна на органите за защита на данните значително повишават разходите за спазване на правните изисквания в целия ЕС.

Разпокъсаност, свързана с използването на клаузите за незадължителни уточнения

- Възрастова граница за съгласие на деца за услуги на информационното общество

Редица държави членки са се възползвали от възможността да предвидят по-ниска възраст от 16 години за съгласие във връзка с услуги на информационното общество (член 8, параграф 1 от ОРЗД). Докато девет държави членки прилагат възрастовата граница от 16 години, осем държави членки са избрали 13 години, шест — 14 години, а три — 15 години[60].

Следователно дружество, което предоставя услуги на информационното общество на непълнолетни лица в целия ЕС, трябва да прави разграничение между възрастта на потенциалните ползватели в зависимост от това в коя държава членка пребивават. Това е в противоречие с основната цел на ОРЗД да осигурява еднакво ниво на защита на физическите лица и на възможности за стопанска дейност във всички държави членки.

Тези разлики водят до ситуации, при които държавата членка, в която е установен администраторът, предвижда различна възрастова граница от държавите членки, в които се намират субектите на данните.

- Здравеопазване и научни изследвания

Когато се прилагат дерогации от общата забрана за обработване на специални категории лични данни[61], в законодателството на държавите членки се следват различни подходи по отношение на равнището на уточняване и гаранциите, включително за целите на здравеопазването и научните изследвания. Повечето държави членки са въвели или запазили допълнителни условия за обработването на генетични данни, биометрични данни или данни за здравословното състояние. Това е валидно и за дерогациите, свързани с правата на субектите на данни за научноизследователски цели[62], както по отношение на обхвата на дерогациите, така и по отношение на съответните гаранции.

Бъдещите насоки на Комитета относно използването на лични данни в областта на научните изследвания ще допринесат за хармонизиран подход в тази област. Комисията ще предостави на Комитета входни данни, по-специално във връзка с научни изследвания в областта на здравеопазването, включително под формата на конкретни въпроси и анализ на конкретни сценарии, които е получила от научноизследователската общност. Би било полезно тези насоки да бъдат приети преди стартирането на рамковата програма „Хоризонт Европа“ с

---

[60] 13 години в Белгия, Дания, Естония, Финландия, Латвия, Малта, Португалия и Швеция; 14 години в Австрия, България, Испания, Италия, Кипър и Литва; 15 години в Чешката република, Гърция и Франция; 16 години в Германия, Ирландия, Люксембург, Нидерландия, Полша, Румъния, Словакия, Унгария и Хърватия.

[61] Член 9 от ОРЗД.

[62] Член 89, параграф 2 от ОРЗД.

оглед на хармонизирането на практиките за защита на данните и улесняването на обмена на данни за научни постижения. От полза биха били също така насоки на Комитета относно обработването на лични данни в областта на здравеопазването.

В ОРЗД е предвидена солидна рамка за националното законодателство в областта на общественото здраве и изрично са включени трансгранични заплахи за здравето и наблюдение на епидемии и тяхното разпространение[63], което беше от значение в контекста на борбата срещу пандемията от COVID-19.

На равнището на ЕС на 8 април 2020 г. Комисията прие препоръка относно инструментариум за използване на технологии и данни в този контекст, включително мобилни приложения и използване на анонимизирани данни за мобилността[64], а на 16 април 2020 г. — насоки за мобилните приложения, които подпомагат борбата с пандемията, във връзка със защитата на данните[65]. В този контекст на 19 март 2020 г. Комитетът публикува изявление относно обработването на данни, последвано на 21 април 2020 г.[66] от насоки относно обработването на данни с научноизследователска цел и относно използването на данни за местонахождение и инструменти за проследяване на контакти в този контекст[67]. С тези препоръки и насоки се разяснява как се прилагат принципите и правилата за защита на личните данни в контекста на борбата с пандемията.

- Значителни ограничения на правата на субектите на данните

В повечето национални закони в областта на защитата на данните, с които се ограничават правата на субектите на данните, не са посочени целите от широк обществен интерес, защитавани с тези ограничения, и/или не се спазват в достатъчна степен условията и гаранциите, изисквани от член 23, параграф 2 от ОРЗД[68]. Няколко държави членки не са оставили възможност за проверка за пропорционалност или са разширили обхвата на ограниченията дори извън приложното поле на член 23, параграф 1 от ОРЗД. В някои национални закони например се отказва правото на достъп по причини, свързани с непропорционално големи усилия от страна на администратора, до лични данни, съхранявани въз основа на задължение за запазване на данни или свързани с изпълнението на задачи от обществен интерес, без това ограничение да бъде лимитирано до цели от широк обществен интерес.

- Допълнителни изисквания за дружествата

Въпреки че изискването за задължително длъжностно лице по защита на данните се прилага съгласно основан на риска подход[69], една държава членка[70]

---

63 Вж. член 9, параграф 2, буква и) от ОРЗД и съображение 46.
64 https://eur-lex.europa.eu/legal-content/bg/TXT/PDF/?uri=CELEX:32020H0518&from=EN.
65 https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:52020XC0417(08)&from=EN.
66 https://edpb.europa.eu/news/news/2020/statement-processing-personal-data-context-covid-19-outbreak_bg.
67 https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_bg.
68 В някои случаи защото те просто възпроизвеждат текста на член 23, параграф 1 от ОРЗД.
69 Член 37, параграф 1 от ОРЗД.
70 Германия.

разшири обхвата му, като включи в него количествени критерии, задължаващи дружества, в които 20 или повече служители участват постоянно в автоматизираното обработване на лични данни, да определят длъжностно лице по защита на данните, независимо от рисковете, свързани с дейностите по обработване[71]. Това е довело до допълнителни тежести.

4 Предоставяне на правомощия на физическите лица да контролират своите данни

С ОРЗД се осигурява ефективно упражняване на основните права, по-специално правото на защита на личните данни, но също така и на другите основни права, признати от Хартата, включително зачитане на личния и семейния живот, свобода на изразяване на мнение и свобода на информация, недискриминация, свобода на мисълта, съвестта и религията, свобода на стопанската инициатива и право на ефективни правни средства за защита. Между тези права трябва да се постига равновесие съгласно принципа на пропорционалност[72].

С ОРЗД на физическите лица се предоставят приложими права, като право на достъп, коригиране, изтриване, възражение, преносимост и по-голяма прозрачност. С регламента също така на физическите лица се дава правото да подават жалби до орган за защита на данните, включително чрез представителни искове, както и правото на съдебна защита.

Физическите лица все повече осъзнават своите права, както е видно от резултатите от проучването на Евробарометър от юли 2019 г.[73] и проучването, проведено от Агенцията за основните права[74].

Според проучването на основните права, извършено от Агенцията за основните права:

- 69 % от населението на възраст над 16 години в ЕС са чували за ОРЗД;
- 71 % от респондентите в ЕС са чували за органа за защита на данните в своята държава; тази цифра варира от 90 % в Чешката република до 44 % в Белгия;
- 60 % от респондентите в ЕС са запознати със закон, който им позволява да имат достъп до своите лични данни, съхранявани от публичната администрация; този процент обаче намалява до 51 % за частните дружества;
- повече от един на всеки петима респонденти (23 %) в ЕС не желаят да споделят лични данни (като адрес, гражданство или дата на раждане) с публичната администрация, а 41 % не желаят да споделят тези данни с частни дружества.

[71] Като се е възползвала от клаузата за уточняване в член 37, параграф 4 от ОРЗД.
[72] Вж. съображение 4 от ОРЗД.
[73] https://ec.europa.eu/commission/presscorner/detail/bg/IP_19_2956
[74] Агенция на Европейския съюз за основните права (FRA) (2020 г.): Проучване на основните права за 2019 г. Защита на данните и технологии: https://fra.europa.eu/en/publication/2020/fundamental-rights-survey-data-protection

Физическите лица все по-често използват правото си да подават жалби до органите за защита на данните, индивидуално или чрез представителни искове[75]. Само няколко държави членки са позволили на неправителствени организации да завеждат искове без мандат в съответствие с възможността, предоставена от ОРЗД. След като бъде приета, предложената Директива относно представителни искове за защита на колективните интереси на потребителите[76] се очаква да подсили рамката за представителните искове също и в областта на защитата на данните.

Жалби

Общият брой жалби през периода май 2018 г. — края на ноември 2019 г., докладвани от Комитета, е около 275 000[77]. Тази цифра обаче следва да се разглежда много предпазливо, като се има предвид, че определението за жалба не е еднакво сред отделните органи. Абсолютният брой на жалбите, получени от органите за защита на данните[78], е много различен в отделните държави членки. Най-голям брой жалби са регистрирани в Германия (67 000), Нидерландия (37 000), Испания и Франция (по 18 000), Италия (14 000), Полша и Ирландия (по 12 000). Две трети от органите са докладвали, че броят на жалбите варира между 8 000 и 600. Най-нисък брой жалби е бил регистриран в Естония и Белгия (по около 500 във всяка), Малта и Исландия (по по-малко от 200 във всяка).

Броят на жалбите не е непременно свързан с броя на населението или с БВП, например жалбите в Германия са близо два пъти повече в сравнение с тези в Нидерландия и са четири пъти повече в сравнение с тези в Испания и Франция.

Обратната информация от многостранната група на заинтересованите страни показва, че организациите са въвели разнообразни мерки за улесняване на упражняването на правата на субектите на данните, в това число процедури, които гарантират индивидуален преглед на исканията и отговор от страна на администратора, използването на няколко канала (поща, специален адрес на електронна поща, уебсайт и др.), актуализирани вътрешни процедури и политики за своевременно вътрешно обработване на исканията и обучение на персонала. Някои дружества са създали цифрови портали, достъпни чрез уебсайта на дружеството (или чрез вътрешната мрежа за служителите на дружеството), за да се улесни упражняването на правата от страна на субектите на данните.

Въпреки това е необходим по-нататъшен напредък в следните направления:

- не всички администратори на данни изпълняват задължението си да съдействат за упражняването на правата на субектите на данните[79]. Те трябва да гарантират, че субектите на данните имат ефективно звено за контакт, където могат да обяснят проблемите си. Това може да бъде длъжностното лице по защита на данните, чиито координати за връзка

[75] Член 80 от ОРЗД.
[76] COM/2018/184 final - 2018/0089 (COD)
[77] Съгласно член 77 и член 80 от ОРЗД.
[78] Вж. приноса на Комитета, стр. 31—32.
[79] Член 12, параграф 2 от ОРЗД.

трябва да бъдат предоставени активно на субекта на данните[80]; условията за осъществяване на контакти не трябва да се ограничават до електронни съобщения, а трябва също така да се дава възможност на субекта на данните да се обърне към администратора чрез други средства;

- физическите лица все още срещат трудности, когато искат достъп до своите данни, например от платформи, брокери на данни и технологични предприятия за реклама („adtech“);
- правото на преносимост на данните не се използва пълноценно. В приетата от Комисията на 19 февруари 2020 г. Европейска стратегия за данните (наричана по-нататък „Стратегията за данните“)[81] се подчертава необходимостта от улесняване на всички възможни начини на използване на това право (например чрез даване на мандат за технически интерфейси и машинно четими формати, позволяващи преносимост на данните в режим, (близък до) реално време. Операторите отбелязват, че понякога има трудности при предоставянето на данните в структуриран, широко използван машинно четим формат (поради липсата на стандарт). Само организации в определени сектори, като банково дело, далекосъобщения, водоподаване и енергоразпределение, съобщават, че са въвели необходимите интерфейси[82]. Разработени са нови технологични инструменти, за да се улесни упражняването от страна на физическите лица на техните права съгласно ОРЗД, които не се изчерпват с преносимост на данните (например пространство за лични данни и услуги за управление на личната информация).
- Права на децата: няколко членове на многостранната група на заинтересованите страни подчертават необходимостта от предоставяне на информация на децата и факта, че много организации пренебрегват обстоятелството, че децата могат да бъдат засегнати от обработването на данни от тяхна страна. Съветът подчерта, че при изготвянето на кодекси за поведение би могло да се обърне специално внимание на защитата на децата. Защитата на децата също така е в центъра на вниманието на органите за защита на данните[83];
- право на информация: някои дружества имат твърде легалистичен подход и възприемат известията относно защитата на данните като упражнение по законотворчество, представяйки информацията по доста сложен, труден за разбиране или непълен начин, докато ОРЗД изисква всяка информация да

---

80 Член 13, параграф 1, буква б) и член 14, параграф 1, буква б) от ОРЗД.

81 https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:52020DC0066&qid=1596384191105&from=BG

82 Вж. доклада на многостранната група на заинтересованите страни.

83 Вж. резултатите от обществената консултация относно правата на децата в областта на защитата на данните, проведена от ирландския орган за защита на данните: https://www.dataprotection.ie/sites/default/files/uploads/2019-09/Whose%20Rights%20Are%20They%20Anyway_Trends%20and%20Hightlights%20from%20Stream%201.pdf. Френският орган за защита на данните също започна обществена консултация през април 2020 г.: https://www.cnil.fr/fr/la-cnil-lance-une-consultation-publique-sur-les-droits-des-mineurs-dans-lenvironnement-numerique

бъде кратка и да се използва ясен и прост език[84]. Изглежда някои дружества не спазват препоръките на Комитета, например по отношение на вписването на имената на образуванията, пред които те разкриват данни;

- няколко държави членки са ограничили в значителна степен правата на субектите на данните чрез националното си законодателство, а някои са направили това дори извън рамките на член 23 от ОРЗД;
- упражняването на правата на физическите лица понякога се възпрепятства от практиките на няколко основни участници в цифровата сфера, които затрудняват физическите лица да изберат настройките, които в най-голяма степен защитават неприкосновеността на личния им живот (в нарушение на изискването за защита на данните на етапа на проектирането и по подразбиране[85])[86].

Насоките на Комитета относно правата на субектите на данни се очакват с голям интерес от заинтересованите страни.

5 ВЪЗМОЖНОСТИ И ПРЕДИЗВИКАТЕЛСТВА ЗА ОРГАНИЗАЦИИТЕ, ПО-СПЕЦИАЛНО ЗА МАЛКИТЕ И СРЕДНИТЕ ПРЕДПРИЯТИЯ

Възможности за организациите

В ОРЗД се насърчават конкуренцията и иновациите. Заедно с Регламента за свободното движение на нелични данни[87], с ОРЗД се гарантира свободното движение на данни в рамките на ЕС и се създават еднакви условия на конкуренция с дружества, които не са установени в ЕС. Чрез създаването на хармонизирана рамка за защита на личните данни ОРЗД гарантира, че всички участници на вътрешния пазар са обвързани от едни и същи правила и се ползват от едни и същи възможности, независимо от това къде са установени и къде се извършва обработването. Технологичната неутралност, заложена в ОРЗД, осигурява рамката за защита на данните за новите технологични разработки. Принципите на защита на данните на етапа на проектирането и по подразбиране стимулират иновативни решения, които включват от самото начало съображения за защита на данните и могат да намалят разходите за спазване на правилата за защита на данните.

---

[84] Член 12, параграф 1 от ОРЗД.

[85] Член 25 от ОРЗД.

[86] Вж. доклада на Норвежкия съвет за защита на потребителите „Заблудени на етапа на проектирането“ (Deceived by Design), в който се изтъкват „сенчестите“ модели, настройки по подразбиране и други характеристики и техники, използвани от дружествата, за да подтикнат потребителите да избират варианти, позволяващи намеса: https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/
Вж. също проучването, публикувано през декември 2019 г. от Трансатлантическия диалог на потребителите (TACD) и фондация „Хайнрих Бьол“, Брюксел, Европейски съюз, в което се анализират практиките на три големи глобални платформи: https://eu.boell.org/en/2019/12/11/privacy-eu-and-us-consumer-experiences-across-three-global-platforms

[87] Регламент (ЕС) 2018/1807 на Европейския парламент и на Съвета от 14 ноември 2018 г. относно рамка за свободното движение на нелични данни в Европейския съюз, ОВ L 303, 28.11.2018 г., стр. 59—68.

Освен това неприкосновеността на личния живот се превръща във важен параметър на конкуренцията, който хората все по-често вземат предвид при избора на своите услуги. Онези, които са по-информирани и чувствителни към съображенията, свързани със защитата на данните, търсят продукти и услуги, които гарантират ефективна защита на личните данни. Прилагането на правото на преносимост на данните има потенциала да намали пречките за навлизане на пазара за предприятията, които предлагат новаторски услуги, съобразени със защитата на данните. Въздействието от потенциално по-широко използване на това право върху пазара в различни сектори следва да се проследи. Спазването на правилата за защита на данните и тяхното прозрачно прилагане ще създадат доверие по отношение на използването на личните данни на хората, а по този начин и нови възможности за предприятията.

Както всички разпоредби, правилата за защита на данните водят до присъщи разходи за привеждане в съответствие за дружествата. Тези разходи обаче се компенсират от възможностите и предимствата от засиленото доверие в цифровите иновации и ползите за обществото, произтичащи от зачитането на основно право. Чрез осигуряването на еднакви условия на конкуренция и обезпечаването на органите за защита на данните с ресурсите, необходими им за ефективно прилагане на правилата, ОРЗД възпрепятства дружествата, които не спазват правилата, да се възползват от доверието, изградено от онези, които ги спазват.

Особени предизвикателства за малките и средните предприятия (МСП)

Заинтересованите страни, но също и Европейският парламент, Съветът и органите за защита на данните споделят общо разбиране, че прилагането на ОРЗД е особено предизвикателство за микро-, малките и средните предприятия, както и за малките доброволчески и благотворителни организации.

Според основания на риска подход не би било уместно да се предоставят дерогации въз основа на размера на операторите, тъй като техният размер сам по себе си не е показател за рисковете, които обработването на лични данни от въпросния оператор може да породи за физическите лица. Основаният на риска подход съчетава гъвкавост и ефективна защита. При него се вземат предвид нуждите на МСП, чиято основна дейност не е обработване на данни, и техните задължения се прецизират по-специално въз основа на вероятността и тежестта на рисковете, свързани със специфичното обработване, което извършват[88].

Обработването в малки мащаби и при нисък риск не следва да се третира по същия начин, както честото обработване при висок риск — независимо от размера на дружеството, което го извършва. Ето защо, както заключи Комитетът, „във всеки случай следва да се запази основаният на риска подход, насърчаван от законодателя в текста, тъй като рисковете за субектите на данните не зависят от размера на администраторите“[89]. Органите за защита на данните следва напълно да възприемат този принцип при прилагането на ОРЗД, за предпочитане в рамките на общ европейски подход, за да не се създават пречки пред единния пазар.

---

[88] Член 24, параграф 1 от ОРЗД.

[89] Вж. приноса на Комитета, стр. 35.

Органите за защита на данните разработиха няколко инструмента и подчертаха намерението си да продължат да ги подобряват. Някои органи са предприели кампании за повишаване на осведомеността и дори ще провеждат безплатни „часове за обучение по ОРЗД“ за МСП.

Примери за насоки и инструменти, предоставени от органите за защита на данните специално за МСП:

- публикуване на информация, предназначена за МСП;
- семинари за длъжностни лица по защита на данните и събития за МСП, които не са задължени да определят длъжностно лице по защита на данните;
- интерактивни ръководства в помощ на МСП;
- горещи линии за консултации;
- образци на договори за обработване на данни и записи относно дейности по обработване.

В приноса на Комитета е представено описание на дейностите, извършвани от органите за защита на данните[90].

За няколко от действията, с които се подкрепят конкретно МСП, е получено финансиране от ЕС. Комисията предостави финансова подкрепа чрез три транша на безвъзмездни средства на обща стойност 5 милиона евро, като двата последни бяха специално насочени към подпомагане на националните органи за защита на данните в усилията им да достигнат до гражданите и до МСП. В резултат на това през 2018 г. бяха отпуснати 2 милиона евро на девет органа за защита на данните за дейности през периода 2018—2019 г. (Белгия, България, Дания, Унгария, Литва, Латвия, Нидерландия, Словения и Исландия)[91], а през 2019 г. бяха отпуснати 1 милион евро на четири органа за защита на данните за дейности през 2020 г. (Белгия, Малта, Словения и Хърватия в партньорство с Ирландия)92. През 2020 г. ще бъдат отпуснати допълнителни 1 милион евро.

Въпреки тези инициативи МСП и новосъздадените предприятия често съобщават, че се затрудняват да прилагат принципа на отчетност, предвиден в ОРЗД[93]. По-конкретно те съобщават, че невинаги получават достатъчно насоки и практически консултации от националните органи за защита на данните или че времето, необходимо за получаване на насоки и консултации, е твърде продължително. Има и случаи, в които органите не са били склонни да се занимават с правни въпроси. Когато са изправени пред подобни ситуации, МСП често се обръщат към външни консултанти и адвокати, за да се справят с прилагането на принципа на отчетност и основания на риска подход (включително изискванията за прозрачност, регистрите на дейностите по

---

90 Вж. приноса на Комитета, стр. 35—45.

91 https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/rec-rdat-trai- ag-2017.

92 https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules/eu-funding-supporting-implementation-gdpr_en

93 Вж. доклада на многостранната група на заинтересованите страни.

обработване и уведомленията за нарушения на сигурността на данните). Това може също така да доведе до допълнителни разходи за тях.

Специфичен проблем е документирането на дейностите по обработване, което МСП и малките сдружения определят като значителна административна тежест. Действително обхватът на освобождаването от това задължение в член 30, параграф 5 от ОРЗД е твърде тесен. Въпреки това усилията, свързани с изпълнението на това задължение, не следва да бъдат надценявани. Когато основната дейност на МСП не е свързана с обработването на лични данни, тези регистри могат да бъдат опростени и да не създават административна тежест. Същото се отнася и за доброволческите и други сдружения. Воденето на такива опростени регистри ще бъде улеснено чрез предоставянето на образци, каквато вече е практиката при някои органи за защита на данните. Във всеки случай всеки субект, който обработва лични данни, следва да има общ поглед върху обработването им като основно изискване на принципа на отчетност.

Разработването на практически инструменти на равнище ЕС от страна на Комитета, като например хармонизирани формуляри за нарушения на сигурността на данните и опростени регистри на дейностите по обработване, може да помогне на МСП и на малките сдружения[94], чиято основна дейност не е съсредоточена върху обработването на лични данни, да изпълняват своите задължения.

Различни браншови организации са положили усилия за повишаване на осведомеността и информиране на своите членове, например чрез конференции и семинари, предоставяне на информация на предприятията относно наличните насоки или разработване на услуга за подпомагане на своите членове в областта на неприкосновеността на личния живот. Те също така докладват за все по-голям брой семинари, срещи и прояви, организирани от аналитични центрове и сдружения на МСП, по свързани с ОРЗД въпроси.

С цел да се подобри свободното движение на всички данни в рамките на ЕС и да се установи последователно прилагане на ОРЗД и на Регламента за свободното движение на нелични данни, Комисията също така изготви практически насоки относно правилата, уреждащи обработването на набори от смесени данни, съставени както от лични, така и от нелични данни, и насочени специално към МСП[95].

Инструментариум за предприятията

В ОРЗД са предвидени инструменти, които спомагат за доказването на съответствие, като кодекси за поведение, механизми за сертифициране и стандартни договорни клаузи.

- Кодекси за поведение

[94] Вж. приноса на Съвета.

[95] Съобщение на Комисията до Европейския парламент и Съвета „Насоки във връзка с Регламента относно рамка за свободното движение на нелични данни в Европейския съюз“, COM(2019) 250 final.

Комитетът е издал насоки[96] за подкрепа и улесняване на „субектите на кодекси“ при изготвянето, внасянето на изменения или разширяването на обхвата на кодексите и за предоставяне на практически насоки и съдействие при тълкуването. В тези насоки също така са изяснени процедурите за представяне, одобрение и публикуване на кодекси както на национално равнище, така и на равнище ЕС, като са определени изискваните минимални критерии.

Заинтересованите страни считат кодексите за поведение за много полезни инструменти. Въпреки че много кодекси се прилагат на национално равнище, понастоящем се подготвят редица кодекси за поведение, обхващащи целия ЕС (например относно мобилните приложения, свързани със здравословното състояние, здравните научни изследвания в областта на геномиката, компютърните услуги „в облак“, директния маркетинг, застраховането, обработването за целите на предотвратяването на престъпления и услугите за консултиране на деца)[97]. Според операторите кодексите за поведение, обхващащи целия ЕС, следва да бъдат популяризирани по-широко, тъй като те способстват за последователното прилагане на ОРЗД във всички държави членки.

Въпреки това за разработването на кодексите за поведение, както и за създаването на необходимите независими органи за наблюдение се изискват време и инвестиции от страна на операторите. Представители на МСП подчертават значението и ползата от кодекси за поведение, които са съобразени с тяхното положение и не водят до прекомерни разходи.

Вследствие на това стопански асоциации в редица сектори са приложили други видове инструменти за саморегулиране, като например кодекси за добри практики или насоки. Въпреки че тези инструменти могат да предоставят полезна информация, те нямат одобрението на органите за защита на данните и не могат да служат като инструмент, спомагащ за доказването на съответствие с ОРЗД.

Съветът подчертава, че при изготвянето на кодекси за поведение трябва да се отделя особено внимание на обработването на данни на деца и данни за здравословното състояние. Комисията подкрепя кодекс(и) за поведение, чрез който(ито) ще се хармонизира подходът в областта на здравеопазването и научните изследвания и ще се улесни трансграничното обработване на лични данни[98]. Понастоящем в Комитета се извършва одобряване на проекти за критерии за акредитиране на органи за наблюдение на кодекси на поведение, предложени от редица органи за защита на данните[99]. След като транснационалните или европейските кодекси за поведение бъдат готови за представяне за одобрение пред органите за защита на данните, ще бъде поискано становището на Комитета по тях. Експедитивното въвеждане на транснационални кодекси за поведение е особено важно за области, свързани с обработването на значителни обеми от данни (например компютърни услуги „в

---

96 https://edpb.europa.eu/our-work-tools/our-documents/wytyczne/guidelines-12019-codes-conduct-and-monitoring-bodies-under_bg.

97 Вж. доклада на многостранната група на заинтересованите страни.

98 Вж. действията, обявени в Европейската стратегия за данните, стр. 30.

99 Съгласно член 41, параграф 3 от ОРЗД. Вж. становищата на ЕКЗД на адрес https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_bg

облак“) или на чувствителни данни (например за здравословното състояние/научноизследователски).

- Сертифициране

Сертифицирането може да бъде полезен инструмент за доказване на съответствие със специфичните изисквания на ОРЗД. Чрез него може да се повиши правната сигурност за предприятията и да се популяризира ОРЗД в световен план.

Както е посочено в проучването относно сертифицирането, публикувано през април 2019 г.[100], целта следва да бъде да се улесни навлизането на съответните схеми. Разработването на схеми за сертифициране в ЕС ще бъде подпомогнато с издадените от Комитета насоки относно критериите за сертифициране[101] и относно акредитацията на сертифициращите органи[102].

Сигурността и защитата на данните на етапа на проектирането са ключови елементи, които трябва да бъдат взети предвид в схемите за сертифициране съгласно ОРЗД и спрямо които е полезно прилагането на единен и амбициозен подход в целия ЕС. Комисията ще продължи да подкрепя текущите контакти между Агенцията на Европейския съюз за киберсигурност (ENISA), органите за защита на данните и Комитета.

Що се отнася до киберсигурността, след приемането на Акта за киберсигурността Комисията поиска от ENISA да подготви две схеми за сертифициране, включително една схема за компютърни услуги „в облак“[103]. Обмислят се допълнителни схеми, насочени към киберсигурността на услугите и продуктите за потребителите. Макар в схемите за сертифициране, създадени в съответствие с Акта за киберсигурността, да не се разглеждат изрично защитата на данните и неприкосновеността на личния живот, те допринасят за повишаването на доверието на потребителите в цифровите услуги и продукти. Такива схеми могат да предоставят доказателства за придържане към принципите на сигурност на етапа на проектирането, както и за прилагане на подходящи технически и организационни мерки, свързани със сигурността на обработването на лични данни.

- Стандартни договорни клаузи

Комисията работи по стандартни клаузи в договорите между администраторите и обработващите лични данни[104], също и с оглед на осъвременяването на стандартните договорни клаузи за международни предавания на данни (вж. раздел 7.2). Чрез приет от Комисията акт на Съюза ще се осигури

---

[100] https://ec.europa.eu/info/study-data-protection-certification-mechanisms_en

[101] https://edpb.europa.eu/our-work-tools/our-documents/nasoki/guidelines-12018-certification-and-identifying-certification_bg.

[102] https://edpb.europa.eu/our-work-tools/our-documents/pokyny/guidelines-42018-accreditation-certification-bodies-under_bg. Няколко надзорни органа вече са представили своите изисквания за акредитация на ЕКЗД, както за органите за наблюдение на кодекси за поведение, така и за сертифициращите органи. Вж. общия преглед на следния адрес: https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_bg.

[103] https://ec.europa.eu/digital-single-market/en/news/towards-more-secure-and-trusted-cloud-europe

[104] Член 28, параграф 7 от ОРЗД.

задължителен за целия ЕС ефект, който ще гарантира пълна хармонизация и правна сигурност.

6 ПРИЛАГАНЕТО НА ОРЗД ПО ОТНОШЕНИЕ НА НОВИТЕ ТЕХНОЛОГИИ

Технологично неутрална рамка, отворена за нови технологии

ОРЗД е технологично неутрален, играе ролята на катализатор на доверието и е основан на принципи[105]. Тези принципи, включително законосъобразното и прозрачно обработване, ограничението на целите и свеждането на данните до минимум, предоставят солидна основа за защита на личните данни, независимо от прилаганите операции и техники по обработване.

Членовете на многостранната група на заинтересованите страни докладват, че като цяло ОРЗД оказва положително въздействие върху разработването на нови технологии и предоставя добра основа за иновации. ОРЗД се възприема като важен и гъвкав инструмент за гарантиране, че новите технологии се разработват в съответствие с основните права. Прилагането на основните му принципи е особено важно при интензивното обработване на данни. Чрез основания на риска и технологично неутрален подход, заложен в ОРЗД, се осигурява ниво на защита на данните, което е достатъчно за справяне със свързания с обработването риск, включително при нововъзникващи технологии.

По-специално заинтересованите страни посочват, че принципите на ОРЗД за ограничение на целите и допълнително съвместимо обработване, свеждане на данните до минимум, ограничение на съхранението, прозрачност, отчетност и условията, при които в законите могат да бъдат заложени процеси на автоматизирано вземане на решения[106], до голяма степен разсейват опасенията, свързани с използването на изкуствен интелект.

Ориентираният към бъдещето и основан на риска подход, заложен в ОРЗД, ще бъда приложен също така при евентуалната бъдеща рамка за изкуствения интелект и при изпълнението на стратегията за данните. Стратегията за данните има за цел да се насърчат наличието на данни и създаването на общи европейски пространства за данни, които се поддържат чрез услуги за федерирани облачни инфраструктури. По отношение на личните данни в ОРЗД е предвидена основната правна рамка, в съответствие с която могат да се разработват ефективни решения за всеки отделен случай, в зависимост от естеството и съдържанието на всяко пространство за данни.

Чрез ОРЗД осведомеността относно защитата на личните данни беше повишена както в рамките на ЕС, така и извън него, и дружествата бяха подтикнати да адаптират своите практики, за да зачитат принципите на защита на данните, когато въвеждат иновации. Организациите на гражданското общество обаче отбелязват, че макар въздействието на ОРЗД върху разработването на нови технологии да изглежда положително, практиките на основните участници в

[105] Както се припомня от Съвета, Европейския парламент и Комитета в техните приноси към оценката.

[106] Заинтересованите страни обаче отбелязват, че не всички процеси на автоматизирано вземане на решения в контекста на изкуствения интелект попадат в обхвата на член 22 от ОРЗД.

цифровата сфера все още не са променени съществено в посока на обработване, съобразено в по-голяма степен с неприкосновеността на личния живот. Стриктното и ефективно прилагане на ОРЗД по отношение на големите цифрови платформи и интегрираните дружества, включително в области като онлайн рекламите и микротаргетирането, е съществен елемент за защитата на физическите лица.

Комисията понастоящем анализира по-широките въпроси, свързани с пазарното поведение на големите участници в цифровата сфера, в контекста на пакета на законодателния акт за цифровите услуги[107]. По отношение на научните изследвания в областта на социалните медии Комисията припомня, че платформите на социалните медии не могат да използват ОРЗД като претекст за ограничаване на достъпа на изследователите и проверителите на факти до нелични данни, като например статистически данни за това какви целеви реклами са били изпратени на кои категории групи, критериите за насочване, информация относно фалшиви профили и др.

Технологично неутралният и ориентиран към бъдещето подход, заложен в ОРЗД, беше подложен на изпитание по време на пандемията от COVID-19 и се оказа успешен. Чрез основаните на принципи правила на регламента беше подкрепено разработването на инструменти за противодействие и наблюдение на разпространението на вируса.

Предизвикателства, които трябва да бъдат преодолени

При разработването и прилагането на нови технологии тези принципи не се поставят под въпрос. Предизвикателствата се състоят в това да се изясни как доказаните принципи да се прилагат в полза на конкретни технологии, като изкуствен интелект, блокова верига, интернет на предметите, разпознаване на лица или квантови изчисления.

В този контекст Европейският парламент и Съветът подчертаха необходимостта от непрекъснато наблюдение, за да се изясни начинът, по който ОРЗД се прилага по отношение на новите технологии и големите технологични дружества. Освен това заинтересованите страни предупреждават, че преценката дали ОРЗД продължава да е подходящ за заложените цели също изисква непрекъснато наблюдение.

Заинтересованите страни от промишления сектор подчертават, че за целите на иновациите е необходимо ОРЗД да се прилага по основан на принципи начин, съответстващ на неговия замисъл, а не по стриктен и формален начин. Те са на мнение, че с оглед на основания на риска подход насоките на Комитета относно начините на прилагане на принципите, концепциите и правилата на ОРЗД спрямо новите технологии, например изкуствен интелект, блокова верига или интернет на предметите, ще спомогнат за предоставянето на разяснения и за по-голяма правна сигурност. Такива актове с незадължителен характер са подходящи да съпътстват прилагането на ОРЗД спрямо новите технологии, тъй като те предвиждат по-голяма правна сигурност и могат да бъдат преразглеждани с оглед на технологичното развитие. Някои заинтересовани

[107] https://ec.europa.eu/commission/presscorner/detail/bg/ip_20_962

страни предполагат също така, че от полза могат да бъдат секторни насоки относно начините на прилагане на ОРЗД по отношение на новите технологии.

Комитетът посочи, че ще продължи да разглежда въздействието на нововъзникващите технологии върху защитата на личните данни.

Заинтересованите страни подчертават също така, че е важно регулаторните органи да добият задълбочено разбиране за начина на използване на технологиите и да започнат диалог с промишлеността относно разработките на нововъзникващи технологии. Те считат, че подходът „регулаторна лаборатория“ — като средство за получаване на насоки за прилагането на правилата — може да бъде интересна възможност за изпитване на нови технологии и да подпомогне предприятията при прилагането на защитата на данните в новите технологии на етапа на проектирането и по подразбиране.

По отношение на допълнителните мерки на политиката заинтересованите страни препоръчват бъдещите предложения за политика в областта на изкуствения интелект да се основават на съществуващите правни рамки и да бъдат приведени в съответствие с ОРЗД. Преди да бъдат предложени нови предписателни правила, следва да се направи внимателна оценка на потенциалните специфични въпроси, основана на подходящи доказателства.

В Бялата книга на Комисията за изкуствения интелект се предлагат редица варианти на политиката, по които до 14 юни 2020 г. бяха потърсени мнения от заинтересованите страни По отношение на разпознаването на лица — технология, която може да окаже значително въздействие върху правата на физическите лица, в Бялата книга се припомня настоящата законодателна рамка и се започва открит дебат относно конкретните обстоятелства, ако има такива, които биха могли да оправдаят използването на изкуствен интелект за целите на разпознаването на лица и други цели, свързани с дистанционна биометрична идентификация на обществени места, както и относно общите гаранции.

7 МЕЖДУНАРОДНО ПРЕДАВАНЕ НА ДАННИ И СЪТРУДНИЧЕСТВО В СВЕТОВЕН МАЩАБ

7.1 Неприкосновеност на личния живот: въпрос от световно значение

За необходимостта от защита на личните данни няма граници, тъй като физическите лица от цял свят все повече ценят неприкосновеността на личния живот и сигурността на своите данни.

В същото време значението на потоците от данни за физическите лица, правителствата, дружествата и в по-общ план, за обществото като цяло е неизбежен факт във взаимосвързания свят, в който живеем. Те представляват неразделна част от търговията, сътрудничеството между публичните органи и социалните взаимодействия. Във връзка с това настоящата пандемия от COVID-19 също показа колко решаващи са предаването и обменът на лични данни за много съществени дейности, включително осигуряването на непрекъснатост на работата на правителството и на стопанската дейност — чрез осигуряване на възможност за дистанционна работа и други решения, които в голяма степен разчитат на информационни и комуникационни технологии — развиването на научноизследователско сътрудничество в областта на диагностиката, лечението

и ваксините, както и борбата с новите форми на киберпрестъпност, като например схеми за онлайн измами с предлагане на фалшиви лекарства, за които се твърди, че предотвратяват или лекуват COVID-19.

В този контекст и повече от всякога защитата на неприкосновеността на личния живот и улесняването на потока от данни трябва да вървят ръка за ръка. Със своя режим на защита на данните, който съчетава подготвеност за международно предаване на данни с високо равнище на защита на физическите лица, ЕС е в много добра позиция да насърчава безопасни и сигурни потоци от данни. ОРЗД вече се е наложил като еталон на международно равнище и е подействал като катализиращ фактор за много държави по света да започнат да обмислят въвеждането на съвременни правила за защита на неприкосновеността на личния живот.

Това действително е световна тенденция, като примерите са навсякъде — от Чили до Южна Корея, от Бразилия до Япония, от Кения до Индия, от Тунис до Индонезия и от Калифорния до Тайван. Тези промени са забележителни не само от гледна точка на количеството, но и от гледна точка на качеството: много от законите за защита на неприкосновеността на личния живот, които са приети наскоро или са в процес на приемане, се основават на набор от общи гаранции, права и механизми за правоприлагане, споделяни от ЕС. В свят, който твърде често се характеризира с различни регулаторни подходи, които понякога са и разнопосочни, тази тенденция към сближаване на световно равнище представлява много положителна промяна, с която се създават нови възможности за повишаване на защитата на физическите лица в Европа, като в същото време се улесняват потоците от данни и се намаляват разходите по сделките за стопанските субекти.

С цел да се възползва от тези възможности и да приложи стратегията, изложена в нейното съобщение от 2017 г. „Обмен и защита на личните данни в един глобализиран свят“[108], Комисията засили значително работата си по международното измерение на неприкосновеността на личния живот, като използва пълноценно наличния „инструментариум“ за предаване на данни, както е обяснено по-долу. Това включваше активно ангажиране с ключови партньори с оглед на достигането до „констатация за адекватно ниво на защита“ и доведе до важни резултати, като например създаването на най-голямото пространство в света за свободни и безопасни потоци от данни между ЕС и Япония.

Наред с работата си по адекватното ниво на защита, Комисията работи в тясно сътрудничество с органите за защита на данните в рамките на Комитета, както и с други заинтересовани страни, за да използва пълния потенциал на гъвкавите правила на ОРЗД за международното предаване на данни. Това се отнася до модернизирането на инструменти, като стандартни договорни клаузи, разработването на схеми за сертифициране, кодекси за поведение или административни договорености за обмен на данни между публичните органи,

[108] Съобщение на Комисията до Европейския парламент и Съвета „Обмен и защита на личните данни в един глобализиран свят“, 10.1.2017 г. (COM(2017) 7 final).

както и изясняването на ключови понятия, свързани например с териториалния обхват на правилата на ЕС за защита на данните или с използването на т.нар. „дерогации“ за предаването на лични данни.

И накрая, Комисията активизира диалога в редица двустранни, регионални и многостранни форуми с цел насърчаване в световен мащаб на култура на зачитане на неприкосновеността на личния живот и разработване на елементи на сближаване на различните системи за неприкосновеност на личния живот. В своята работа Комисията може да разчита на активната подкрепа на Европейската служба за външна дейност и на мрежата от делегации на ЕС в трети държави и мисии на международни организации. Това също така гарантира съгласуваност и по-добро взаимно допълване между различните аспекти на външното измерение на политиките на ЕС — от търговията до новото партньорство между Африка и ЕС.

7.2 Инструментариумът на ОРЗД за предаване на данни

Тъй като все повече частни и публични оператори разчитат на международните потоци от данни като част от рутинните си операции, нараства необходимостта от гъвкави инструменти, които могат да бъдат адаптирани към различните сектори, бизнес модели и ситуации на предаване на данни. В отражение на тази необходимост, в ОРЗД е предложен осъвременен инструментариум, който улеснява предаването на лични данни от ЕС на трета държава или международна организация, като същевременно се гарантира, че за данните продължава да се прилага високо ниво на защита. Тази непрекъснатост на защитата е важна, като се има предвид, че в днешния свят данните се движат лесно през границите, и гарантираната в ОРЗД защита би била непълна, ако се ограничаваше до обработването в рамките на ЕС.

В глава V от ОРЗД законодателят е потвърдил структурата на правилата за предаване на данни, която вече съществуваше съгласно Директива 95/46/ЕО: предаване на данни може да се извършва, когато Комисията е достигнала до констатация за адекватно ниво на защита по отношение на трета държава или международна организация или, при липса на такова, когато администраторът или обработващият лични данни в ЕС („износителят на данни“) е предоставил подходящи гаранции, например чрез договор с получателя („вносителя на данни“). Освен това продължават да съществуват законови основания за предаване на данни (т.нар. „дерогации“) за специфични ситуации, за които законодателят е решил, че балансът на интересите позволява предаване на данни при определени условия. Същевременно чрез реформата съществуващите правила са изяснени и опростени, например чрез подробно определяне на условията за достигане до констатация за адекватно ниво на защита или задължителните фирмени правила, чрез ограничаване на изискванията за издаване на разрешения до много редки и специфични случаи и чрез пълно премахване на изискванията за уведомяване. Освен това бяха въведени нови инструменти за предаване на данни, като кодекси за поведение или схеми за сертифициране, и възможностите за използване на съществуващите инструменти (например стандартни договорни клаузи) бяха разширени.

Днешната цифрова икономика позволява на чуждестранните оператори да участват (от разстояние, но) пряко във вътрешния пазар на ЕС и да се

конкурират за европейските клиенти и техните лични данни. Когато се насочват конкретно към европейците, като предлагат стоки или услуги или като наблюдават тяхното поведение, те следва да спазват правото на ЕС по същия начин, както операторите от ЕС. Това е отразено в член 3 от ОРЗД, в който пряката приложимост на правилата на ЕС за защита на данните е разширена така, че да обхване някои операции по обработване, извършвани от администратори и обработващи лични данни извън ЕС. Това осигурява необходимите гаранции, както и еднакви условия на конкуренция за всички дружества, които извършват дейност на пазара на ЕС.

Широкият му обхват е една от причините, поради които ефектите от ОРЗД са усетени и в други части на света. Ето защо подробните насоки относно териториалния обхват на ОРЗД, изготвени от Комитета след всеобхватна обществена консултация, са важни, за да се помогне на чуждестранните оператори, включително чрез конкретни примери, да определят дали и кои дейности по обработване подлежат пряко на неговите гаранции[109].

Разширяването на обхвата на законодателството на ЕС в областта на защитата на данните обаче само по себе си не е достатъчно, за да се гарантира неговото спазване на практика. Както беше подчертано и от Съвета[110], от решаващо значение е да се гарантира спазването от страна на чуждестранните оператори и ефективното прилагане спрямо тях. Определянето на представител в ЕС (член 27, параграфи 1 и 2 от ОРЗД), към който физическите лица и надзорните органи могат да се обръщат освен или вместо към отговорното дружество, което извършва дейност в чужбина[111], следва да играе ключова роля в това отношение. Този подход, който се използва все по-често и в други контексти[112], следва да се прилага по-усърдно, за да се изпрати ясно послание, че липсата на място на установяване в ЕС не освобождава чуждестранните оператори от тяхната отговорност съгласно ОРЗД. Когато тези оператори не изпълнят задължението си да определят представител[113], надзорните органи следва да използват пълния инструментариум за правоприлагане, предвиден в член 58 от ОРЗД (например публични предупреждения, временни или окончателни

---

[109] ЕКЗД, Насоки № 2/2018 относно териториалния обхват на ОРЗД, 12.11.2019 г. В насоките са разгледани няколко от въпросите, повдигнати по време на обществената консултация, например тълкуването на критериите за насочване и наблюдение.

[110] Вж. Позицията и констатациите на Съвета, точки 34, 35 и 38.

[111] Вж. член 27, параграф 4 и съображение 80 от ОРЗД („Посоченият представител следва да бъде обект на правоприлагащи процедури, в случай на нарушение от страна на администратора или обработващия лични данни“).

[112] Предложение за Директива на Европейския парламент и на Съвета за установяване на хармонизирани правила относно определянето на юридически представители за целите на събирането на доказателства по наказателни производства (COM/2018/226 final), член 3; Предложение за Регламент на Европейския парламент и на Съвета за предотвратяване на разпространението на терористично съдържание онлайн (COM(2018) 640 final), член 16, параграфи 2 и 3.

[113] Според едно становище, представено в рамките на обществената консултация, един от основните въпроси за разглеждане „е ефективното прилагане и действителните последици за онези, които са решили да пренебрегнат това изискване […]. Следва да се има предвид по-специално, че това също така поставя предприятията, установени в Съюза, в неблагоприятно положение от гледна точка на конкуренцията спрямо тези предприятия, които не спазват изискванията и са установени извън местата за търговия в Съюза“. Вж. становище на бизнес партньори на ЕС от 29 април 2020 г.

забрани за обработване в ЕС, правоприлагане спрямо съвместните администратори на лични данни, установени в ЕС).

И накрая, много е важно Комитетът да приключи работата си по допълнителното изясняване на връзката между член 3 относно прякото прилагане на ОРЗД и правилата относно международното предаване на данни, предвидени в глава V[114].

Решения относно адекватното ниво на защита

Получените мнения от заинтересованите страни потвърждават, че решенията относно адекватното ниво на защита продължават да бъдат съществен инструмент, чрез който операторите от ЕС да предават по сигурен начин лични данни на трети държави[115]. Тези решения предоставят най-всеобхватното, просто и разходно ефективно решение за предаването на данни, тъй като те се приравняват на предаване на данни в рамките на ЕС, като по този начин се осигурява безопасен и свободен поток от лични данни без допълнителни условия или необходимост от разрешение. Поради това решенията относно адекватното ниво на защита отварят търговски канали за операторите от ЕС и улесняват сътрудничеството между публичните органи, като същевременно осигуряват привилегирован достъп до единния пазар на ЕС. Въз основа на практиката по прилагане на Директивата от 1995 г. разпоредбите на ОРЗД изрично дават възможност за преценка за наличието на адекватно ниво на защита по отношение на отделна територия на трета държава или на конкретен сектор или промишлен отрасъл в трета държава (т.нар. „частично“ адекватно ниво на защита).

В ОРЗД са използвани опитът от последните години и поясненията, предоставени от Съда, като е установен подробен набор от елементи, които Комисията трябва да вземе предвид при оценката си. Стандартът за адекватното ниво на защита изисква ниво на защита, което е подобно (или „по същество равностойно“) на нивото, гарантирано в ЕС[116]. Това включва изчерпателна оценка на системата на третата държава като цяло, включително същността на защитата на неприкосновеността на личния живот, ефективното ѝ прилагане и изпълнение, както и правилата относно достъпа до лични данни от страна на

[114] Този въпрос беше повдигнат в няколко становища, представени в рамките на обществената консултация, например по отношение на предаването на лични данни на получатели, които се намират извън ЕС, но са обхванати от ОРЗД.

[115] Позиция и констатации на Съвета, точка 17; принос на Комитета, стр. 5—6. В няколко становища в рамките на обществената консултация, включително от редица бизнес асоциации (като Френската асоциация на големите дружества (French Association of Large Companies), Цифрова Европа (Digital Europe), Световния алианс за данни (Global Data Alliance)/Бизнес Софтуер Алианс (Business Software Alliance — BSA), Асоциацията за компютърната и комуникационната индустрия (Computer & Communication Industry Association — CCIA) или Търговската камара на САЩ (US Chamber of Commerce) бяха отправени призиви за ускоряване на работата по констатациите за адекватно ниво на защита, особено с важни търговски партньори.

[116] Решение на Съда от 6 октомври 2015 г. по дело C-362/14, *Maximillian Schrems/Data Protection Commissioner* (решението *„Schrems“*), точки 73, 74 и 96. Вж. също съображение 104 от ОРЗД, което се отнася до стандарта за равностойност по същество.

публичните органи, по-специално за целите на правоприлагането и националната сигурност[117].

Това е отразено и в насоките, приети от предишната Работна група по член 29 (и одобрени от Комитета), по-специално т.нар. „Референтен документ относно адекватното ниво на защита“, в който допълнително се изясняват елементите, които Комисията трябва да вземе предвид при извършването на оценка на адекватното ниво на защита, включително като предостави преглед на „гаранциите по същество“ за достъп до лични данни от страна на публичните органи[118]. Посоченият документ се основава по-специално на съдебната практика на Европейския съд по правата на човека. Въпреки че стандартът за „равностойност по същество“ не включва буквално възпроизвеждане („фотокопие“) на правилата на ЕС, като се има предвид, че средствата за осигуряване на подобно ниво на защита може да се различават между отделните системи за неприкосновеност на личния живот, което често отразява различни правни традиции, той все пак изисква високо ниво на защита.

Този стандарт е обоснован от факта, че с решението относно адекватно ниво на защита по същество ползите от единния пазар по отношение на свободния поток от данни се разпростират до трети държави. Това обаче означава и че понякога ще има относителни разлики между нивото на защита, гарантирано във въпросната трета държава, в сравнение с ОРЗД, които трябва да бъдат преодолени, например чрез договарянето на допълнителни гаранции. На тези гаранции следва да се гледа положително, тъй като те допълнително укрепват защитата, с която разполагат физическите лица в ЕС. Същевременно Комисията изразява съгласие с Комитета за това колко важно е постоянното наблюдение на прилагането им на практика, включително ефективното прилагане от страна на органа за защита на данните на третата държава[119].

В ОРЗД се пояснява, че решенията относно адекватното ниво на защита са „динамични инструменти“, които следва да се наблюдават непрекъснато и периодично да бъдат подлагани на преглед[120]. В съответствие с тези изисквания Комисията осъществява редовен обмен на информация с компетентните органи за активно проследяване на новите промени. Например, от приемането през 2016 г. на решението относно Щита за личните данни в отношенията между ЕС

---

[117] Член 45, параграф 2 и съображение 104 от ОРЗД. Вж. също решението *„Schrems“*, точки 75, 91—91.

[118] Референтен документ относно адекватното ниво на защита, WP 254 rev. 01 (Работна група по член 254), 6 февруари 2018 г. (на разположение на адрес: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108).

[119] Принос на Комитета, стр. 5—6.

[120] Съгласно член 45, параграфи 4 и 5 от ОРЗД се изисква Комисията да осъществява постоянно наблюдение на развитието в трети държави и да извършва периодичен преглед — най-малко веднъж на четири години — на констатация за адекватно ниво на защита. Освен това посочените разпоредби предоставят на Комисията правомощието да отменя, изменя или спира прилагането на решение относно адекватното ниво на защита, ако установи, че съответната държава или международна организация вече не осигурява адекватно ниво на защита. В член 97, параграф 2, буква а) от ОРЗД също така се изисква Комисията да представи на Европейския парламент и на Съвета доклад относно оценката до 2020 г. Вж. също решение на Съда от 6 октомври 2015 г. по дело C-362/14, *Maximillian Schrems/Data Protection Commissioner*, точка 76.

и САЩ[121] Комисията, заедно с представители на Комитета, извърши три годишни прегледа, за да оцени всички аспекти на функционирането на рамката[122]. Тези прегледи се основаваха на информация, получена чрез обмен с органите на САЩ, както и на принос на други заинтересовани страни, като органи за защита на данните от ЕС, гражданското общество и търговски сдружения. Те дадоха възможност за подобряване на практическото функциониране на различни елементи на рамката. В по-широк план годишните прегледи допринесоха за установяването на по-всеобхватен диалог с администрацията на САЩ относно неприкосновеността на личния живот като цяло, и в частност ограниченията и гаранциите по отношение на националната сигурност.

Като част от първата оценка на ОРЗД Комисията е длъжна също така да направи преглед на решенията относно адекватното ниво на защита, приети съгласно Директивата от 1995 г.[123]. Службите на Комисията започнаха активен диалог с всяка от 11-те съответни държави и територии, за да оценят доколко са се развили техните системи за защита на личните данни след приемането на решението относно адекватното ниво на защита и дали отговарят на стандарта, определен в ОРЗД. Необходимостта да се гарантира непрекъснатост в прилагането на тези решения, тъй като те са ключов инструмент за търговията и международното сътрудничество, е един от факторите, подтикнали няколко от тези държави и територии да осъвременят и укрепят законодателствата си в областта на защитата на личните данни. Тези промени безспорно се посрещат с одобрение. С някои от тези държави и територии се обсъждат допълнителни гаранции за преодоляване на съответните различия в защитата.

Въпреки това, като се има предвид, че в решение, което предстои да бъде произнесено на 16 юли, Съдът може да предостави разяснения, които могат да бъдат от значение за някои елементи на стандарта за адекватно ниво на защита,

---

[121] 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. Това решение относно адекватното ниво на защита е специфичен случай, който, при липсата на общо законодателство за защита на данните в САЩ, се основава на ангажиментите, поети от участващите дружества (които подлежат на принудително изпълнение съгласно правото на САЩ) да прилагат стандартите за защита на данните, определени в посочената договореност. Освен това Щитът за личните данни се основава на конкретните писмени изявления и уверения, дадени от правителството на САЩ по отношение на достъпа за целите на националната сигурност, които подкрепят констатацията за адекватно ниво на защита.

[122] Прегледи бяха извършени през 2017 г. (доклад на Комисията до Европейския парламент и Съвета относно първия годишен преглед на функционирането на Щита за личните данни в отношенията между ЕС и САЩ, COM (2017) 611 final), 2018 г. (доклад на Комисията до Европейския парламент и Съвета относно втория годишен преглед на функционирането на Щита за личните данни в отношенията между ЕС и САЩ, COM (2018) 860 final) и 2019 г. (доклад на Комисията до Парламента и Съвета относно третия годишен преглед на функционирането на Щита за личните данни в отношенията между ЕС и САЩ, COM (2019) 495 final).

[123] Тези съществуващи решения относно адекватното ниво на защита се отнасят до държави, които са тясно интегрирани с Европейския съюз и неговите държави членки (Швейцария, Андора, Фарьорските острови, Гърнзи, Джърси, остров Ман), до важни търговски партньори (например Аржентина, Канада, Израел) и до държави, които са изиграли водеща роля за развитието на законодателство за защита на данните в своя регион (Нова Зеландия, Уругвай).

Комисията ще докладва отделно за оценката на посочените 11 решения относно адекватното ниво на защита след като Съдът постанови решението си по това дело[124].

В изпълнение на стратегията, изложена в нейното съобщение от 2017 г. „Обмен и защита на личните данни в един глобализиран свят“, Комисията се ангажира и с нови диалози относно адекватното ниво на защита[125]. С тези действия вече са постигнати значителни резултати с участието на ключови партньори на ЕС. През януари 2019 г. Комисията прие решение относно адекватното ниво на защита по отношение на Япония, което се основава на висока степен на сближаване, включително чрез специфични гаранции, например в областта на последващото предаване на данни, и чрез създаването на механизъм за разследване и разрешаване на жалби на физически лица във връзка с достъпа на държавните органи до лични данни за целите на правоприлагането и националната сигурност.

Като първа констатация за адекватно ниво на защита, приета съгласно ОРЗД, договорената с Япония рамка предоставя полезен прецедент за бъдещи решения[126]. Това включва факта, че Япония от своя страна е издала реципрочна констатация за адекватно ниво на защита за ЕС. Взети заедно, тези взаимни констатации за адекватно ниво на защита създават най-голямото пространство на сигурни и свободни потоци от лични данни в света, като по този начин допълват Споразумението между Европейския съюз и Япония за икономическо партньорство. Действително всяка година споразумението способства за търговия със стоки на стойност около 124 милиарда евро и търговия с услуги на стойност 42,5 милиарда евро.

Процесът на оценяване на адекватното нивото на защита по отношение на Република Корея също е на напреднал етап. Важен резултат от това е неотдавнашната законодателна реформа на Южна Корея, която доведе до създаването на независим орган за защита на данните, разполагащ с широки правомощия по правоприлагане. Това онагледява начина, по който диалогът

[124] Вж. решение по дело C-311/18, *Data Protection Commissioner/Facebook Ireland Limited, Maximillian Schrems („Schrems II“)*, което се отнася до преюдициално запитване относно така наречените стандартни договорни клаузи. Някои елементи от стандарта за адекватно ниво на защита обаче също може да бъдат допълнително изяснени от Съда. Изслушването по това дело е проведено на 9 юли 2019 г. и решението е обявено за 16 юли 2020 г.

[125] Вж. по-горе бележка под линия 109. Комисията обясни, че при преценката с кои трети държави следва да се проведе диалог относно адекватното ниво на защита ще бъдат взети предвид следните критерии: i) обемът на търговските отношения на ЕС (настоящи или потенциални) с третата държава, включително наличието на споразумение за свободна търговия или текущи преговори; ii) обемът на потоците от лични данни от ЕС, отразяващ географски и/или културни връзки; iii) ролята на пионер, която държавата играе в областта на неприкосновеността на личния живот и защитата на данните, поради която тя може да послужи за образец на други държави в региона; и iv) цялостните политически отношения с държавата, по-специално във връзка с насърчаването на общи ценности и споделени цели на международно равнище.

[126] Резолюция на Европейския парламент от 13 декември 2018 г. относно адекватността на нивото на защитата на личните данни, предоставяна от Япония (2018/2979 (RSP). Принос на Комитета, стр. 5—6.

относно адекватното ниво на защита може да допринесе за по-голямо сближаване на правилата на ЕС за защита на данните с тези на чужда държава.

Комисията изразява пълно съгласие с призива на заинтересованите страни за засилване на диалога с избрани трети държави с оглед на евентуални нови констатации за адекватно ниво на защита[127]. Тя активно проучва тази възможност с други важни партньори в Азия, Латинска Америка и съседните на Съюза държави, като се основава на настоящата тенденция към възходящо сближаване в световен мащаб на стандартите за защита на данните. Така например, в Латинска Америка (Бразилия, Чили) е прието или е в напреднал етап на законодателния процес всеобхватно законодателство в областта на неприкосновеността на личния живот, а в Азия (например Индия, Индонезия, Малайзия, Шри Ланка, Тайван и Тайланд), Африка (например Етиопия, Кения), както и в източните и южните съседни на ЕС държави (например Грузия, Тунис) се наблюдават обещаващи промени. Когато е възможно, Комисията ще работи за постигането на всеобхватни решения относно адекватното ниво на защита, обхващащи както частния, така и публичния сектор[128].

Освен това в ОРЗД е предвидена възможност Комисията да приема констатации за адекватно ниво на защита по отношение на международни организации. Във време, когато някои международни организации осъвременяват своите режими за защита на данните, като въвеждат всеобхватни правила, както и механизми, които осигуряват независим надзор и правна защита, тази възможност може да бъде проучена за първи път.

Адекватното ниво на защита играе важна роля и в контекста на отношенията с Обединеното кралство след оттеглянето му от ЕС, при условие че са изпълнени съответните условия. То е способстващ фактор за търговията, включително цифровата търговия, и е съществена предпоставка за тясно и амбициозно сътрудничество в областта на правоприлагането и сигурността[129]. Освен това, като се има предвид значението на потоците от данни с Обединеното кралство и близостта му до пазара на ЕС, високата степен на сближаване между правилата за защита на данните от двете страни на Ламанша е важен елемент за осигуряването на еднакви условия на конкуренция. В съответствие с Политическата декларация относно бъдещите отношения между ЕС и Обединеното кралство[130] в момента Комисията извършва оценка на

[127] Вж. например Резолюция на Европейския парламент от 12 декември 2017 г. относно „Към стратегия за електронна търговия“ (2017/2065 (INI), точки 8 и 9; Позиция и констатации на Съвета относно прилагането на Общия регламент относно защитата на данните (ОРЗД), 19.12.2019 г. (14994/1/19), точка 17; Принос на Комитета, стр. 5.

[128] Както беше поискано от Съвета, вж. Позиция и констатации на Съвета относно прилагането на Общия регламент относно защитата на данните (ОРЗД), 19.12.2019 г. (14994/1/19), точки 17 и 40. За това обаче е необходимо да са изпълнени условията за констатация за адекватно ниво на защита по отношение на предаването на данни на публични органи, включително по отношение на независимия надзор.

[129] Вж. указанията за водене на преговори, приложени към Решение на Съвета за разрешаване на започването на преговори за ново споразумение за партньорство с Обединеното кралство Великобритания и Северна Ирландия (ST 5870/20 ADD 1 REV 3), точки 13 и 118.

[130] Вж. преразгледания текст на политическата декларация, очертаваща рамката на бъдещите отношения между Европейския съюз и Обединеното кралство, договорен на равнище

адекватното ниво на защита както съгласно ОРЗД, така и съгласно Директивата относно правоприлагането в областта на защитата на данните. Като се има предвид автономният и едностранен характер на оценката на адекватното ниво на защита, тези разговори се водят по отделни направления от тези на преговорите за споразумение относно бъдещите отношения между ЕС и Обединеното кралство.

И накрая, Комисията приветства факта, че други държави понастоящем въвеждат механизми за предаване на данни, подобни на констатация за адекватно ниво на защита. По този начин те често признават ЕС и държавите, по отношение на които Комисията е приела решение относно адекватното ниво на защита, като сигурни местоназначения за предаване на данни[131]. От една страна, нарастващият брой държави, които се ползват от решения на ЕС относно адекватното ниво на защита, и от друга страна, тази форма на признаване от други държави, имат потенциала да създадат мрежа от държави, в които данните могат да се движат свободно и безопасно. Комисията счита това за положителна промяна, която допълнително ще увеличи ползите от решение относно адекватното ниво на защита за трети държави и ще допринесе за сближаването в световен мащаб. Този вид полезни взаимодействия може успешно да допринесе и за разработването на рамки за сигурен и свободен поток от данни, например в контекста на инициативата за „свободно и надеждно движение на данни“ (вж. по-долу).

Подходящи гаранции

ОРЗД предвижда редица други инструменти за предаване на данни извън всеобхватното решение за констатация за адекватно ниво на защита. Гъвкавостта на този „инструментариум“ е видна от член 46 от ОРЗД, който урежда предаването на данни въз основа на „подходящи гаранции“, включително приложими права на субектите на данни и ефективни правни средства за защита. С цел да се гарантират подходящи гаранции съществуват различни инструменти, за да се отговори на нуждите от предаване на данни както на търговските оператори, така и на публичните органи.

- Стандартни договорни клаузи (СДК)

Първата група от тези инструменти се отнася до договорни инструменти, които могат да бъдат или индивидуални *ad hoc* клаузи за защита на данните, договорени между износител на данни от ЕС и вносител на данни извън ЕС, упълномощен от компетентния орган за защита на данните (член 46, параграф 3, буква а) от ОРЗД), или типови клаузи, предварително одобрени от Комисията (член 46, параграф 2, букви в) и г) от ОРЗД[132]). Най-важните от тези инструменти са т.нар. стандартните договорни клаузи (СДК), т.е. типови клаузи

преговарящи на 17 октомври 2019 г., точки 8—10 (на разположение на адрес: https://ec.europa.eu/commission/sites/beta-political/files/revised_political_declaration.pdf).

131 Например до Аржентина, Колумбия, Израел, Швейцария или Уругвай.

132 За стандартните договорни клаузи (СДК) за международно предаване на данни винаги е необходимо одобрение от Комисията, но могат да бъдат изготвени или от самата Комисия, или от национален орган за защита на данните. Всички съществуващи СДК попадат в първата категория.

за защита на данните, които износителят на данни и вносителят на данни могат да включват в договорните си споразумения (например договор за услуги, изискващ предаването на лични данни) на доброволни начала и в които се определят изискванията, свързани с подходящи гаранции.

СДК като цяло са най-използваният механизъм за предаване на данни[133]. Хиляди дружества от ЕС разчитат на СДК, за да предоставят широк набор от услуги на своите клиенти, доставчици, партньори и служители, включително услуги, които са от съществено значение за функционирането на икономиката. Тяхното широко използване показва, че те са много полезни за предприятията в техните усилия за спазване на изискванията и са от особена полза за дружествата, които не разполагат с ресурси да договарят индивидуални договори с всеки от своите търговски партньори. Чрез стандартизацията и предварителното одобрение на СДК на дружествата се предоставя лесен за прилагане инструмент за удовлетворяване на изискванията за защита на данните в контекста на предаването на данни.

Съществуващите набори от СДК[134] бяха приети и одобрени въз основа на Директивата от 1995 г. Тези СДК остават в сила, докато не бъдат изменени, заменени или отменени, ако е необходимо, с решение на Комисията (член 46, параграф 5 от ОРЗД). ОРЗД разширява възможностите за използване на СДК както в рамките на ЕС, така и за международно предаване на данни. Комисията работи съвместно със заинтересованите страни, за да се възползват от тези възможности и да актуализират съществуващите клаузи[135]. С цел да се гарантира, че бъдещата структура на СДК е подходяща за заложените цели, Комисията събра обратна информация относно опита на заинтересованите страни със СДК чрез многостранната група на заинтересованите страни по въпросите на ОРЗД и специален работен форум, който бе проведен през септември 2019 г., но също и чрез множество контакти с дружества, които използват СДК, както и организации на гражданското общество. Комитетът

---

[133] Според годишния доклад от 2019 г. на Международната асоциация на специалистите в областта на поверителността на данните (International Association of Privacy Professionals — IAPP) и Ърнст и Янг (Ernst & Young — EY) „Управление на поверителността на данните“ (Privacy Governance), „всяка година измежду тези инструменти [за предаване на данни] най-популярни с голяма преднина са стандартните договорни клаузи: 88 % от респондентите в тазгодишното проучване са посочили СДК като техен основен метод за извънтериториално предаване на данни, следван от спазването на договореността относно Щита за личните данни в отношенията между ЕС и САЩ (60 %). За респондентите, които прехвърлят данни от ЕС към Обединеното кралство (52 %), 91 % съобщават, че възнамеряват да използват СДК, за да спазват изискванията за предаване на данни след излизането на Обединеното кралство от ЕС“.

[134] Понастоящем съществуват три набора от стандартни договорни клаузи, приети от Комисията за предаването на лични данни на трети държави: два за предаване на данни от администратор от ЕИП на администратор извън ЕИП и един за предаване на данни от администратор от ЕИП на преработващ лични данни извън ЕИП. Те бяха изменени през 2016 г. вследствие на решението на Съда по делото „*Schrems I*“ (C-362/14), за да бъдат премахнати всички ограничения на компетентните надзорни органи да упражняват своите правомощия за контрол върху предаването на данни. Вж. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_bg.

[135] Вж. също приноса на Комитета, стр. 6—7. По същия начин Съветът призова Комисията да „преразгледа и преработи [СДК] в близко бъдеще, така че да бъдат отразени потребностите на администраторите и обработващите данните“. Вж. Позицията и констатациите на Съвета.

също понастоящем актуализира редица насоки, които биха могли да бъдат от значение за прегледа на СДК, например по отношение на понятията „администратор на лични данни“ и „обработващ лични данни“.

Въз основа на получените отзиви службите на Комисията понастоящем работят по преразглеждането на СДК. В този контекст бяха набелязани редица области, в които е необходимо подобрение, по-специално по отношение на следните аспекти:

1. актуализиране на СДК в контекста на новите изисквания, въведени с ОРЗД, като например изискванията във връзка с отношенията между администраторите и обработващите лични данни съгласно член 28 от ОРЗД (по-специално задълженията на обработващия лични данни), задълженията за прозрачност на вносителя на данни (по отношение на необходимата информация, която трябва да бъде предоставена на субекта на данните) и т.н.;
2. разглеждане на редица сценарии за предаване на данни, които не са обхванати от действащите СДК, като предаване на данни от обработващ лични данни от ЕС на обработващ данни (подизпълнител) извън ЕС, но също и случаи, при които управлението на администратора е разположено извън ЕС[136];
3. по-добро отразяване на реалностите на операциите по обработване в съвременната цифрова икономика, където тези операции често включват множество вносители и износители на данни, дълги и често сложни процеси на обработване, развиващи се търговски отношения и т.н. С цел да се вземат предвид тези ситуации проучените решения включват например възможността за подписване на СДК от множество страни или присъединяването на нови страни през целия срок на договора.

При разглеждането на тези въпроси Комисията обмисля също така начини да направи сегашната „архитектура“ на СДК по-удобна за потребителите, например като замени множеството набори от СДК с един изчерпателен документ. Предизвикателството е да се постигне добър баланс, от една страна, между необходимостта от яснота и определена степен на стандартизация, и от друга, необходимата гъвкавост, която ще позволи на редица оператори да използват клаузите с различни изисквания, в различен контекст и за различни видове предаване на данни.

Друг важен аспект, който трябва да се разгледа, е евентуалната необходимост в контекста на настоящия съдебен спор в Съда[137] да се изяснят допълнително гаранциите по отношение на достъпа на чуждестранни публични органи до

[136] Този последен сценарий беше коментиран в няколко становища, получени в рамките на обществената консултация, като често се изразяваха опасения, че изискването за обработващите лични данни от ЕС да осигуряват подходящи гаранции в своите отношения с администраторите извън ЕС ще ги постави в неблагоприятно положение от гледна точка на конкуренцията по отношение на чуждестранните обработващи лични данни, които предлагат подобни услуги.

[137] Вж. решението по делото *Schrems II*.

данни, предавани въз основа на СДК, по-специално за целите на националната сигурност. Това може да включва изискване вносителят или износителят на данни или и двамата, да предприемат действия и да изяснят ролята на органите за защита на данните в този контекст. Въпреки че преразглеждането на СДК е доста напреднало, ще трябва да се изчака решението на Съда да отрази евентуалните допълнителни изисквания в преразгледаните клаузи, преди проектът за решение за нов набор от СДК да може да бъде представен на Комитета, за да изготви становището си, и след това да бъде предложен за приемане чрез „процедурата на комитет“[138].

Успоредно с това Комисията поддържа контакт с международни партньори, които разработват подобни инструменти[139]. Този диалог, който дава възможност за обмен на опит и най-добри практики, би могъл значително да допринесе за по-нататъшно развитие на сближаването „на практика“ и по този начин да улесни спазването на правилата за трансгранично предаване на данни от страна на дружествата, които извършват дейност в различни региони на света.

- Задължителни фирмени правила (ЗФП)

Друг важен инструмент са т.нар. „задължителни фирмени правила (ЗФП)“. Това са правно обвързващи политики и договорености, които се прилагат за членовете на дадена корпоративна група, включително за нейните служители (член 46, параграф 2, буква б) и член 47 от ОРЗД). Използването на ЗФП позволява свободното движение на лични данни между различните членове на групата в целия свят — премахване на необходимостта от сключване на договорни споразумения с всяко корпоративно образувание, като същевременно се гарантира спазването на еднакво високо ниво на защита на личните данни в цялата група. Те предлагат особено добро решение за сложни и големи корпоративни групи и за тясно сътрудничество между дружествата, обменящи данни в множество юрисдикции. За разлика от предвиденото в Директивата от 1995 г., съгласно ОРЗД ЗФП може да се използват от група дружества, които развиват съвместна стопанска дейност, но не са част от една и съща корпоративна група.

От процедурна гледна точка ЗФП трябва да бъдат одобрени от компетентните органи за защита на данните въз основа на необвързващо становище на Комитета[140]. За да даде насока на този процес, Комитетът извърши преглед на

---

[138] В съответствие с член 46, параграф 2, буква в) от ОРЗД следва да бъдат приети стандартни договорни клаузи чрез процедурата по разглеждане, предвидена в член 5 от Регламент (ЕС) № 182/2011 на Европейския парламент и на Съвета от 16 февруари 2011 г. за установяване на общите правила и принципи относно реда и условията за контрол от страна на държавите членки върху упражняването на изпълнителните правомощия от страна на Комисията (ОВ L 55, 28.2.2011 г., стр. 13—18). Това включва по-специално положително решение на комитет, съставен от представители на държавите членки.

[139] Това включва например текущите дейности на държавите — членки на АСЕАН, по разработване на „типови договорни клаузи на АСЕАН“. Вж. АСЕАН, „Ключови подходи за механизъм на АСЕАН по отношение на трансграничните потоци от данни“ (Key Approaches for ASEAN Cross Border Data Flows Mechanism) (на разположение на адрес: https://asean.org/storage/2012/05/Key-Approaches-for-ASEAN-Cross-Border-Data-Flows-Mechanism.pdf).

[140] За преглед на представените до момента становища на ЕКЗД вж. https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_bg.

референтните документи (материалноправните стандарти) за администраторите[141] и обработващите лични данни[142] в контекста на ОРЗД и продължава да актуализира тези документи въз основа на натрупания от надзорните органи практическия опит. Той също така прие различни документи с насоки, за да помогне на заявителите, както и да рационализира процеса на подаване на молба за и одобрение на ЗФП[143]. Според Комитета понастоящем са в процес на одобрение повече от 40 ЗФП, половината от които се очаква да бъдат одобрени до края на 2020 г.[144]. Важно е органите за защита на данните да продължат да работят за по-нататъшно рационализиране на процеса на одобрение, тъй като продължителността на тези процедури често се споменава от заинтересованите страни като практическа пречка пред по-широкото използване на ЗФП.

На последно място, що се отнася специално до ЗФП, одобрени от органа за защита на данните на Обединеното кралство — Службата на комисаря по информацията (Information Commissioner Office) — дружествата ще могат да продължат да ги използват като валиден механизъм за предаване на данни съгласно ОРЗД след края на преходния период, предвиден в Споразумението за оттегляне между ЕС и Обединеното кралство, но само ако бъдат изменени, така че всяка връзка с правния ред на Обединеното кралство да бъде заменена със съответните позовавания на корпоративни образувания и компетентни органи в рамките на ЕС. Одобряването на нови ЗФП следва да се изисква от един от надзорните органи в ЕС.

- Механизми за сертифициране и кодекси за поведение

В допълнение към осъвременяването и разширяването на прилагането на вече съществуващите инструменти за предаване на данни, чрез ОРЗД бяха въведени и нови инструменти, с което бяха разширени възможностите за международно предаване на данни. Това включва използването, при определени условия, на одобрени кодекси за поведение и механизми за сертифициране (като например печати или маркировки за защита на данните), с цел да се осигурят подходящи гаранции. Това са инструменти „от долу нагоре“, които дават възможност за индивидуални решения — като например общи механизъм за отчетност (вж. членове 40—42 от ОРЗД), и по-специално за международно предаване на данни, което отразява например специфичните характеристики и нужди на даден сектор или промишленост, или на конкретни потоци от данни. Прецизирайки задълженията в зависимост от рисковете, кодексите за поведение също могат да бъдат много полезен и разходно ефективен начин за изпълнение на задълженията по ОРЗД от страна на малките и средните предприятия.

---

[141] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109.

[142] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614110.

[143] Тези документи бяха приети (от предишната Работна група по член 29) след влизането в сила на ОРЗД, но преди края на преходния период. Вж. Работната група по член 263 (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623056); Работната група по член 264 (https://edpb.europa.eu/sites/edpb/files/files/file2/wp264_art29_wp_bcr-c_application_form.pdf); Работната група по член 265 (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623848).

[144] Принос на Комитета, стр. 7.

Що се отнася до механизмите за сертифициране, въпреки че Комитетът е приел насоки за насърчаване на тяхното използване в рамките на ЕС, неговата работа по разработването на критерии за одобряване на механизми за сертифициране като международни инструменти за предаване на данни все още продължава. Същото важи и за кодексите за поведение, по отношение на които понастоящем Комитетът работи върху насоки за използването им като инструмент за предаване на данни.

Предвид значението на предоставянето на операторите на широк набор от инструменти за предаване на данни, които са адаптирани към техните потребности, и потенциала за улесняване на предаването на данни, който имат по-специално механизмите за сертифициране, като същевременно гарантират високо ниво на защита на данните, Комисията настоятелно призовава Комитета да финализира възможно най-скоро своите насоки в това отношение. Това се отнася както за материалноправните (т.е. критерии), така и за процедурните аспекти (т.е. одобрение, наблюдение и т.н.). Заинтересованите страни изразиха голям интерес към тези механизми за предаване на данни и следва да могат да използват пълноценно инструментариума, предвиден в ОРЗД. Насоките на Комитета също така ще допринесат за насърчаване на модела на ЕС за защита на данните в световен мащаб и за насърчаване на сближаването, тъй като при други системи за неприкосновеност на личния живот се използват подобни инструменти.

Могат да се извлекат ценни поуки от съществуващите усилия за стандартизация в областта на неприкосновеността на личния живот както на европейско, така и на международно равнище. Интересен пример е наскоро публикуваният международен стандарт ISO 27701[145], който има за цел да се помогне на предприятията да отговарят на изискванията за защита на личните данни и да управляват рисковете, свързани с обработването на лични данни, чрез „системи за управление на неприкосновеността на информацията“. Въпреки че сертифицирането по стандарта само по себе си не отговаря на изискванията на членове 42 и 43 от ОРЗД, прилагането на системи за управление на неприкосновеността на информацията може да допринесе за отчетността, включително в контекста на международното предаване на данни.

- Международни споразумения и административни договорености

ОРЗД дава възможност също така да се осигурят подходящи гаранции за предаването на данни между публични органи или организации въз основа на международни споразумения (член 46, параграф 2, буква а) или административни договорености (член 46, параграф 3, буква б). Въпреки че и двата инструмента трябва да осигурят един и същ резултат по отношение на гаранциите, включително приложими права на субектите на данни и ефективни правни средства за защита, те се различават по правния си характер и процедурата за приемане.

За разлика от международните споразумения, които създават обвързващи задължения съгласно международното право, административните

[145]Списъкът на специфичните изисквания, които съставляват този стандарт на ISO, е достъпен на адрес: https://www.iso.org/standard/71670.html.

договорености (например под формата на меморандум за разбирателство) обикновено са незадължителни и следователно изискват предварително разрешение от компетентния орган за защита на данните (вж. също съображение 108 от ОРЗД). Един от първите примери се отнася до административната договореност за предаването на лични данни между органи за финансов надзор от ЕИП и органи за финансов надзор извън ЕИП, сътрудничещи си под егидата на Международната организация на комисиите по ценни книжа (IOSCO), по която Комитетът е дал своето становище[146] в началото на 2019 г. Оттогава Комитетът допълнително разви своето тълкуване на „минималните гаранции“, които международните споразумения (за сътрудничество) и административните договорености между публични органи или структури (включително международни организации) трябва да осигурят, за да се спазват изискванията на член 46 от ОРЗД. На 18 януари 2020 г. той прие проект на насоки[147], с които отговори на искането на държавите членки за допълнителни разяснения и насоки относно това какво може да се счита за подходящи гаранции за предаването между публични органи[148]. Комитетът настоятелно препоръчва публичните органи да използват тези насоки като отправна точка за преговорите си с трети страни[149].

Насоките отразяват гъвкавостта при разработването на такива инструменти, включително по важни аспекти, като например надзор[150] и правна защита[151].

---

[146] ЕКЗД, Становище № 4/2019 относно проекта на административна договореност за предаването на лични данни между органи за финансов надзор от Европейското икономическо пространство (ЕИП) и органи за финансов надзор извън ЕИП, 12.2.2019 г.

[147] ЕКЗД, Насоки № 2/2020 относно член 46, параграф 2, буква а) и член 46, параграф 3, буква б) от Регламент (ЕС) 2016/679 за предаване на лични данни между публични от ЕИП и публични органи извън ЕИП (проектът е достъпен на адрес: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_bg). Според ЕКЗД „[к]омпетентният [надзорен орган] ще извърши прегледа въз основа на общите препоръки, изложени в настоящите насоки, но също така може да поиска повече гаранции в зависимост от конкретния случай.“ ЕКЗД представи този проект на насоки на обществена консултация, която приключи на 18 май 2020 г.

[148] Позиция и констатации на Съвета, точка 20;

[149] В същото време ЕКЗД пояснява, че публичните органи продължават да разполагат със „свободата да разчитат на други съответни инструменти, предвиждащи подходящи гаранции съгласно член 46 от ОРЗД“. Във връзка с избора на инструмент ЕКЗД подчертава, че „[с]ледва да се прецени внимателно дали да се използват правно необвързващи административни договорености за предоставяне на гаранции в публичния сектор, с оглед на целта на обработването и естеството на наличните данни. Ако в националното законодателство на третата държава не са предвидени права за защита на данните и правна защита за физически лица от ЕИП, следва да се отдаде предпочитание на сключването на правно обвързващо споразумение. Независимо от вида на приетия инструмент, действащите мерки трябва да бъдат ефективни, за да се гарантира правилното прилагане, изпълнение и надзор“ (точка 67).

[150] Това може да включва например съчетаването на вътрешни проверки (с ангажимент за информиране на другата страна за всеки случай на неспазване изискванията за независим надзор чрез външни или поне чрез функционално независими механизми, както и възможността предаващият данни публичен орган да преустанови или да прекрати предаването на данни).

[151] Това може да включва например квазисъдебни обвързващи механизми (например арбитраж) или механизми за алтернативно разрешаване на спорове, съчетани с възможността предаващият данни публичен орган да преустанови или да прекрати предаването на лични данни, ако страните не успеят да уредят спор доброволно, заедно с ангажимент от страна на

Това следва да даде възможност на публичните органи да преодолеят трудностите, например при осигуряването на приложими права на субектите на данни чрез незадължителни договорености. Важен елемент от тези договорености е постоянното им наблюдение от страна на компетентния орган за защита на данните, подкрепено от изискванията за информация и за поддържане на регистър, и преустановяването на потоците от данни, ако на практика вече не може да се осигурят подходящи гаранции.

Дерогации

И накрая, в ОРЗД е изяснено използването на така наречените „дерогации“. Това са специфични основания за предаване на данни (например изрично съгласие[152], изпълнение на договор или важни съображения от обществен интерес), признати от закона, и на които субектите могат да разчитат при липсата на други инструменти за предаване на данни и при определени условия.

С цел да изясни използването на тези законови основания Комитетът е изготвил конкретни насоки[153] и е предоставил тълкуване на член 49 в редица случаи по отношение на конкретни сценарии за предаване на данни[154]. Поради изключителния характер на дерогациите Комитетът счита, че те трябва да се тълкуват ограничително за всеки отделен случай. Въпреки тяхното строго тълкуване, тези основания обхващат широк спектър от сценарии за предаване на данни. Това включва по-специално предаването както от публични органи, така и от частни субекти на данни, които са необходими за „важни причини от обществен интерес“, например между органи за защита на конкуренцията, финансови органи или митнически органи, служби, компетентни по въпросите на социалната сигурност или общественото здраве (например в случай на проследяване на контакти при заразни болести или с цел намаляване и/или премахване на употребата на допинг в спорта)[155]. Друга област е трансграничното сътрудничество за целите на наказателното правоприлагане, по-специално по отношение на тежките престъпления[156].

получаващия публичен орган да върне или заличи личните данни. При избора на алтернативни механизми за правна защита в рамките на обвързващи и приложими инструменти, тъй като не съществува възможност за осигуряване на ефективни средства за правна защита, ЕКЗД препоръчва да се потърси становището на компетентния надзорен орган, преди да бъдат приети тези инструменти.

[152] Това е промяна спрямо разпоредбите на Директива 95/46/ЕО, които изискват само „недвусмислено“ съгласие. Освен това се прилагат общите изисквания за съгласие в съответствие с член 4, параграф 11 от ОРЗД.

[153] ЕКЗД, Насоки № 2/2018 относно дерогациите по член 49 съгласно Регламент 2016/679, 25.5.2018 г. (на разположение на адрес: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_bg.pdf).

[154] Това включва например международното предаване на данни за здравословното състояние за научноизследователски цели в контекста на пандемията от COVID-19. Вж.ЕКЗД, Насоки 03/2020 относно обработването на данни за здравословното състояние с научноизследователска цел в контекста на пандемията от COVID-19, 21.4.2020 г. (на разположение на адрес https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_bg.pdf).

[155] Вж. съображение 112.

[156] Вж. „Заключения на Европейската комисия от името на Европейския съюз като *Amicus Curiae*, в които не се подкрепя нито една от страните по делото *US/Microsoft*“ (Brief of the

Комитетът изясни, че макар и съответният обществен интерес да трябва да бъде признат в правото на ЕС или правото на държава членка, той може да бъде установен и въз основа на това, че „международно споразумение или конвенция, в която се признава определена цел и се предвижда международно сътрудничество за насърчаване на тази цел, може да бъде показател при оценката на наличието на обществен интерес съгласно член 49, параграф 1, буква г), доколкото ЕС или държавите членки са страна по това споразумение или конвенция.“[157]

Решения на чуждестранни съдилища или органи, които не са основание за предаване на данни

В допълнение към изричното излагане на основанията за предаване на данни в глава V от ОРЗД, в неговия член 48 също така се пояснява, че постановленията на съдилищата и решенията на административни органи извън ЕС *сами по себе си* не представляват такива основания, освен ако те са признати или подлежат на изпълнение въз основа на международно споразумение (например договор за правна взаимопомощ). Всяко разкриване от субекта в ЕС, до който е отправено искането, на чуждестранен съд или орган в отговор на такова постановление или решение представлява международно предаване на данни, което трябва да се основава на един от посочените инструменти за предаване на данни[158].

ОРЗД не представлява „закон за блокиране“ и при определени условия позволява предаване на данни в отговор на подходящо искане за правоприлагане от трета държава. Важното е, че именно правото на ЕС следва да определи дали случаят е такъв и въз основа на кои гаранции може да се осъществя такова предаване на данни.

Комисията обясни функционирането на член 48 от ОРЗД, включително

European Commission on behalf of the European Union as *Amicus Curiae* in Support of Neither Party in the Case *US v. Microsoft)*, стр. 15: „По принцип правото на Съюза, както и правото на държавите членки признават значението на борбата срещу тежката престъпност, а оттам и на наказателното правоприлагане и международното сътрудничество в това отношение като цел от общ интерес. […] В член 83 от ДФЕС са определени няколко области на престъпност, които са особено тежки и имат трансгранични измерения, като например незаконния трафик на наркотици.“ (на разположение на адрес: https://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf).

[157] ЕКЗД, Насоки относно дерогациите (по-горе бележка под линия 153), стр. 12. Освен това ЕКЗД поясни, че докато предаването на данни въз основа на дерогацията поради основания от обществен интерес не трябва да се извършва „в голям мащаб“ или „системно“ но „трябва да се ограничава до конкретни ситуации, и […] да отговаря на строгия критерий за необходимост“, няма изискване то да „засяга отделни случаи“.

[158] Това става ясно от текста на член 48 от ОРЗД („без да се засягат другите основания за предаване на данни съгласно настоящата глава“) и съпътстващото съображение 115 („[п]редаванията на данни следва да са разрешени само когато са изпълнени условията на настоящия регламент относно предаването на данни на трети държави. Такъв може да бъде случаят, *inter alia*, когато разкриването е необходимо поради важно основание от обществен интерес, признато в правото на Съюза или в правото на държава членка, на което е подчинен администраторът“). Това е признато и от ЕКЗД, вж. Насоките относно дерогациите (по-горе бележка под линия 153), стр. 5 Що се отнася до всички операции по обработване, трябва да се спазват и другите гаранции съгласно регламента (например тези данни да се предават с конкретна цел, да са свързани със и да са ограничени до необходимото за целите на искането и т.н.).

евентуалното позоваване на дерогация поради основания от обществен интерес в контекста на заповед за предоставяне (заповед) от чуждестранен правоприлагащ орган в областта на наказателното право по делото *Microsoft*, което се разглежда от Върховния съд на САЩ[159]. В своето становище Комисията подчерта интереса на ЕС да гарантира, че сътрудничеството в областта на правоприлагането се осъществява „в правна рамка, при която се избягват стълкновения на закони, и се основава на […] зачитане на основните интереси на другите държави както в областта на неприкосновеността на личния живот, така и правоприлагането“[160]. По-специално „от гледна точка на международното публично право, когато публичен орган изисква от дружество, установено в собствената си юрисдикция, да предостави електронни данни, съхранявани на сървър в чужда юрисдикция, се спазват принципите на териториалност и на зачитане съгласно международното публично право“[161].

Това е отразено и в предложението на Комисията за Регламент относно европейските заповеди за предоставяне и за запазване на електронни доказателства по наказателноправни въпроси[162], което съдържа специална „клауза за зачитане“, осигуряваща възможност за повдигане на възражение срещу заповед за предоставяне, ако съответствието би било в стълкновение със законите на трета държава, като по този начин се забранява разкриването, по-специално на основание, че това е необходимо за защитата на основните права на засегнатите физически лица[163].

---

[159] Становище по делото *Microsoft* (по-горе бележка под линия 156). Както беше обяснено от Комисията, съответно в ОРЗД „предпочитан вариант“ за предаването на данни са договорите за правна взаимопомощ (MLAT), тъй като тези договори „предвиждат събиране на доказателства въз основа на съгласие и представляват внимателно договорен баланс между интересите на различни държави, чиято цел е да се смекчат последиците от спорове за компетентност, които в противен случай могат да възникнат“. Вж. също ЕКЗД, Насоки относно дерогациите (по-горе бележка под линия 153), стр. 5 („В случай че е налице международно споразумение, например договор за правна взаимопомощ (MLAT), дружествата от ЕС като цяло следва да отказват преки молби и да насочват изискващия орган от трета държава към съществуващ MLAT или споразумение“).

[160] Становище по делото *Microsoft* (по-горе бележка под линия 156), стр. 4

[161] Становище по делото *Microsoft* (по-горе бележка под линия 156), стр. 6

[162] Европейска комисия, Предложение за регламент на Европейския парламент и на Съвета относно европейските заповеди за предоставяне и за запазване на електронни доказателства по наказателноправни въпроси, 17.4.2018 г. (COM(2018) 225 final). Съветът прие общ подход по предложението за регламент на 7.12.2018 г. (на разположение на адрес: https://www.consilium.europa.eu/bg/press/). Вж. също ЕНОЗД, „Становище 7/19 относно предложения във връзка с европейските заповеди за предоставяне и за запазване на електронни доказателства по наказателноправни въпроси“ (Opinion 7/19 on proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters) (на разположение на адрес: https://edps.europa.eu/data-protection/ourwork/publications/opinions/electronic-evidence-criminal-matters_en).

[163] В обяснителния меморандум, стр. 21, се пояснява, че освен да се гарантира зачитане на суверенните интереси на трети държави, защитата на съответното физическо лице и избягването на стълкновение на закони за доставчиците на услуги, една важна мотивация за клаузата за зачитане е реципрочността, т.е. гарантиране на спазването на правилата на ЕС, включително относно защитата на личните данни (член 48 от ОРЗД). Вж. също становището на Работната група по член 29 от 29 ноември 2017 г., „Аспекти, свързани със защитата на данните и неприкосновеността на личния живот при трансграничния достъп до електронни доказателства (Data protection and privacy aspects of cross-border access to electronic evidence)(становище на Работната група по член 29) (на разположение на адрес:

Гарантирането на зачитане е важно, като се има предвид, че правоприлагането — като например по отношение на престъпността, и по-специално киберпрестъпността — във все по-голяма степен става трансгранично и съответно често поражда въпроси, свързани с компетентността, и създава потенциални стълкновения на закони[164]. Не е изненадващо, че най-добрият начин за разрешаване на тези въпроси е чрез международни споразумения, които предвиждат необходимите ограничения и гаранции за трансграничен достъп до лични данни, включително чрез гарантиране на високо ниво на защита на данните от страна на органа, отправил искането.

Комисията, действайки от името на ЕС, понастоящем участва в многостранни преговори за втори допълнителен протокол към Конвенцията на Съвета на Европа за престъпления в кибернетичното пространство (Конвенцията от Будапеща), чиято цел е да се укрепят съществуващите правила за получаване на трансграничен достъп до електронни доказателства в наказателни разследвания, като същевременно се гарантират подходящи гаранции за защита на данните като част от протокола[165]. Също така започнаха двустранни преговори по споразумение между ЕС и САЩ относно трансграничния достъп до електронни доказателства за целите на съдебното сътрудничество по наказателноправни въпроси[166]. По време на тези преговори Комисията разчита на подкрепата на Европейския парламент и на Съвета, както и на насоките на ЕКЗД.

В по-общ план е важно да се гарантира, че когато дружествата, осъществяващи дейност на европейския пазар, са приканени въз основа на законосъобразно искане да споделят данни за целите на правоприлагането, те могат да направят

---

file:///C:/Users/ralfs/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/20171207_e-Evidence_Statement_FINALpdf%20(1).pdf), стр. 9.

164 Вж. становището на работната група по член 29 (по-горе бележка под линия 163), стр. 6

165 Вж. Препоръка за решение на Съвета за разрешаване на участието в преговори по втори допълнителен протокол към Конвенцията на Съвета на Европа за престъпления в кибернетичното пространство (CETS № 185), 5.2.2019 г. (COM(2019) 71 final). Вж. също ЕНОЗД, „Становище 3/2019 относно участието в преговорите с оглед на втори допълнителен протокол към Конвенцията от Будапеща за престъпления в кибернетичното пространство“ (Opinion 3/2019 regarding the participation in the negotiations in view of a Second Additional Protocol to the Budapest Cybercrime Convention) 2.4.2019 г. (на разположение на адрес: https://edps.europa.eu/sites/edp/files/publication/19-04-02_edps_opinion_budapest_convention_en.pdf); ОНЗД, „Принос към консултацията относно проект за втори допълнителен протокол към Конвенцията на Съвета на Европа за престъпления в кибернетичното пространство“ (Конвенцията от Будапеща), (Contribution to the consultation on a draft second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention) 13.11.2019 г. (на разположение на адрес: https://edpb.europa.eu/sites/edpb/files/files/file1/edpbcontributionbudapestconvention_en.pdf).

166 Вж. Препоръка за решение на Съвета за разрешаване на започването на преговори по споразумение между Европейския съюз и Съединените американски щати относно трансграничния достъп до електронни доказателства за целите на съдебното сътрудничество по наказателноправни въпроси, 5.2.2019 г. (COM(2019) 70 final). Вж. също ЕНОЗД, „Становище 2/2019 относно мандата за преговори за споразумение между ЕС и САЩ относно трансграничния достъп до електронни доказателства“ (Opinion 2/2019 on the negotiating mandate of an EU-US agreement on cross-border access to electronic evidence) (на разположение на адрес: https://edps.europa.eu/sites/edp/files/publication/19-04-02_edps_opinion_on_eu_us_agreement_on_e-evidence_en.pdf).

това, без да са изправени пред стълкновение на закони и при пълно зачитане на основните права на ЕС. С оглед на подобряването на това предаване на данни, Комисията се ангажира да разработи подходяща правна рамка с международните си партньори с цел да се избегне стълкновението на закони и да се спомогне за ефективни форми на сътрудничество, по-специално като се осигурят необходимите гаранции за защита на данните и по този начин се допринесе за по-ефективна борба срещу престъпността.

7.3 Международно сътрудничество в областта на защитата на данните

Насърчаването на сближаването между различните системи за неприкосновеност на личния живот означава също да се учим едни от други чрез обмен на знания, опит и най-добри практики. Този обмен е от съществено значение за справяне с новите предизвикателства, които придобиват все по-глобален характер и обхват. Ето защо Комисията засили своя диалог относно защитата на данните и потоците от данни с широк кръг от участници и на различни форуми на двустранно, регионално и многостранно равнище.

Двустранното измерение

След приемането на ОРЗД е налице все по-голям интерес към опита на ЕС в изготвянето, договарянето и прилагането на съвременни правила за защита на неприкосновеността на личния живот. Диалогът с държавите, които преминават през сходни процеси, се осъществява под няколко форми.

Службите на Комисията представиха становища за редица обществени консултации, организирани от чуждестранни правителства, в които се обсъжда законодателството в областта на неприкосновеността на личния живот, например от САЩ[167], Индия[168], Малайзия и Етиопия. В някои трети държави службите на Комисията имат привилегията да дават показания пред компетентните парламентарни органи, например в Бразилия[169], Чили[170], Еквадор и Тунис[171].

---

[167] Вж. становището на ГД „Правосъдие и потребители“ от 9 ноември 2018 г. в отговор на искане за коментари от страна на обществеността относно предложен от Националната телекомуникационна и информационна администрация на САЩ подход за защита на неприкосновеността на личния живот на потребителите [Docket № 180821780-8780-01] (на разположение на адрес: https://ec.europa.eu/info/sites/info/files/european_commission_submission_on_a_proposed_approach_to_consumer_privacy.pdf)

[168] Вж. становището на ГД „Правосъдие и потребители“ от 19 ноември 2018 г. относно проекта на Закон за защита на личните данни на Индия за 2018 г. на Министерството на електрониката и информационните технологии (достъпен на адрес: ahttps://eeas.europa.eu/delegations/india/53963/submission-draft-personal-data-protection-bill-india-2018-directorate-general-justice_en).

[169] Вж. пленарното заседание от 17 април 2018 г. на Сената на Бразилия (https://www25.senado.leg.br/web/atividade/sessao-plenaria/-/pauta/23384), заседанието от 10 април 2019 г. на Съвместния комитет относно временната мярка (ВМ) 869/2018 на Конгреса на Бразилия (https://www12.senado.leg.br/ecidadania/visualizacaoaudiencia?id=15392) и заседанието на Специалния комитет на Камарата на депутатите на Бразилия от 26 ноември 2019 г. (https://www.camara.leg.br/noticias/616579-comissao-discutira-protecao-de-dados-no-ambito-das-constituicoes-de-outros-paises/).

Освен това в контекста на текущите реформи на законите за защита на данните бяха проведени специални срещи с представители на правителството или парламентарни делегации от много региони на света (например Грузия, Кения, Тайван, Тайланд, Мароко). Това включваше организирането на семинари и проучвателни посещения, например с представители на индонезийското правителство и делегация от служители на Конгреса на САЩ. По този начин бяха предоставени възможности за изясняване на важни понятия от ОРЗД, за подобряване на взаимното разбиране на въпросите, свързани с неприкосновеността на личния живот, и за илюстриране на ползите от сближаването с цел осигуряване на високо ниво на защита на правата на физическите лица, търговията и сътрудничеството. В някои случаи беше позволено и да се направи предупреждение относно определени погрешни схващания за защитата на данните, които могат да доведат до въвеждането на протекционистки мерки, като например изисквания за задължително локализиране.

След приемането на ОРЗД Комисията също така се ангажира с няколко международни организации, включително с оглед на значението на обмена на данни с тези организации в редица области на политиката. По-специално беше установен специален диалог с Организацията на обединените нации с оглед да се улеснят дискусиите с всички участващи заинтересовани страни, за да се гарантира безпрепятственото предаване на данни и да се развие по-нататъшното сближаване на съответните режими за защита на данните. Като част от този диалог Комисията ще работи в тясно сътрудничество с ЕКЗД, за да изясни допълнително как публичните и частните оператори от ЕС могат да изпълняват задълженията си по ОРЗД, когато обменят данни с международни организации като ООН.

Комисията е готова да продължи да споделя извлечените поуки от процеса на реформи със заинтересовани държави и международни организации по същия начин, по който е извлякла поуки от други системи при разработването на своето предложение за нови правила на ЕС за защита на данните. Този вид диалог е от взаимно полезен за ЕС и неговите партньори, тъй като дава възможност за по-добро разбиране на бързо променящата се област на неприкосновеността на личния живот и за обмен на мнения относно нововъзникващите правни и технологични решения.

Именно в този дух Комисията понастоящем създава „Академия за защита на данните“ с цел насърчаване на обмена между европейските регулаторни органи

[170] Вж. заседанията от 29 май 2018 г. (https://senado.cl/appsenado/index.php?mo=comisiones&ac=asistencia_sesion&idcomision=186&idsesion=12513&idpunto=15909&sesion=29/05/2018&listado=1), 24 април 2019 г. (https://www.senado.cl/appsenado/index.php?mo=comisiones&ac=sesiones_celebradas&idcomision=186&tipo=3&legi=485&ano=2019&desde=0&hasta=0&idsesion=13603&idpunto=17283&listado=2) и на комисията по конституционни, законодателни и съдебни въпроси на Сената на Чили.

[171] Вж. заседанието на комисията по свободи, права и външни отношения на Събранието на народните представители на Тунис от 2 ноември 2018 г. (https://www.facebook.com/1515094915436499/posts/2264094487203201/).

и регулаторните органи от трети държави и по този начин подобрява сътрудничеството „на практика“.

Освен това е необходимо да се разработят подходящи правни инструменти за по-тясно сътрудничество и взаимопомощ, включително като се даде възможност за необходимия обмен на информация в контекста на разследванията. Поради това Комисията ще използва правомощията, предоставени ѝ в тази област по силата на член 50 от ОРЗД, и по-специално ще иска разрешение за започване на преговори за сключване на споразумения за сътрудничество в областта на правоприлагането със съответните трети държави. В този контекст Комисията ще вземе предвид и становището на Комитета относно това кои държави следва да имат приоритет с оглед на обема на предаването на данни, ролята и правомощията на правоприлагащия орган в областта на неприкосновеността на личния живот в третата държава и необходимостта от сътрудничество в областта на правоприлагането за разглеждане на случаи от общ интерес.

Многостранното измерение

Освен двустранния обмен, Комисията понастоящем участва активно и в редица многостранни форуми за насърчаване на общи ценности и постигане на сближаване на регионално и световно равнище.

Все по-голямото участие в „Конвенция № 108“ на Съвета на Европа — единственият правно обвързващ многостранен инструмент в областта на защитата на личните данни — е ясен признак за тази тенденция към (възходящо) сближаване[172]. Конвенция, отворена и за държави, които не са членки на Съвета на Европа, вече е ратифицирана от 55 държави, включително редица държави от Африка и Латинска Америка[173]. Комисията допринесе значително за успешното приключване на преговорите относно осъвременяването на Конвенцията[174] и гарантира, че тя отразява същите принципи като тези, залегнали в правилата на ЕС за защита на данните. Понастоящем повечето държави — членки на ЕС, вече са подписали Протокола за изменение, макар че подписите на Дания, Малта и Румъния все още не са положени. Досега само четири държави членки (България, Хърватия, Литва и Полша) са ратифицирали Протокола за изменение. Комисията настоятелно призовава останалите три държави членки да подпишат осъвременената Конвенция и всички държави членки бързо да пристъпят към ратифициране, за

[172] Важно е да се отбележи, че осъвременената Конвенция не е просто договор, в който са определи строги гаранции за защита на данните, но също така с нея се създава мрежа от надзорни органи с инструменти за сътрудничество в областта на правоприлагането, а с помощта на Комитета по Конвенцията — се създава форум за дискусии, обмен на най-добри практики и разработване на международни стандарти.

[173] Вж. пълния списък на членовете: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures. Сред държавите от Африка са Кабо Верде, Мавриций, Мароко, Сенегал и Тунис, а от Латинска Америка — Аржентина, Мексико и Уругвай. Буркина Фасо бе поканена да се присъедини към Конвенцията.

[174] Вж. текста на осъвременената Конвенция: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf.

да се даде възможност за влизането ѝ в сила в близко бъдеще[175]. Освен това тя ще продължи активно да насърчава присъединяването на трети държави.

Наскоро потоците от данни и защитата на данните бяха разгледани и от държавите от Г-20 и Г-7. През 2019 г. световните лидери за първи път подкрепиха идеята, че чрез защитата на данните се допринася за доверието в цифровата икономика се и улесняват потоците от данни. С активната подкрепа на Комисията[176] лидерите подкрепиха концепцията за „свободно и надеждно движение на данни“, първоначално предложена от Япония в Декларацията от Осака на лидерите на държавите от Г-20[177], както и на Срещата на върха на Г-7 в Биариц[178]. Този подход е отразен и в съобщението на Комисията от 2020 г. относно „Европейска стратегия за данните“[179], в което се изтъква намерението ѝ да продължи да насърчава обмена на данни с ползващи се с доверие партньори, като същевременно се бори със злоупотребите, като например непропорционалния достъп на (чуждестранни) публични органи до данните.

По този начин ЕС ще може да разчита също така на редица инструменти в различни области на политиката, в които във все по-голяма степен се отчита въздействието върху неприкосновеността на личния живот: например първата по рода си рамка на ЕС за скрининг на чуждестранните инвестиции, която ще започне да се прилага изцяло през октомври 2020 г., дава възможност на ЕС и неговите държави членки да извършват скрининг на инвестиционни сделки, които имат отражение върху „достъпа до чувствителна информация,

---

[175] В съответствие с решението си относно Протокола за изменение от 18 май 2018 г. Комитетът на министрите „настойчиво прикани държавите членки и други страни по Конвенцията да предприемат без забавяне необходимите мерки, които да позволят влизането в сила на Протокола в срок от три години след откриването му за подписване и да започнат незабавно, но във всички случаи не по-късно от една година след датата, на която протоколът е бил открит за подписване, процеса съгласно тяхното национално право, водещ до ратификация...“ Той също така „инструктира своите заместници да проверяват два пъти годишно и да го направят за първи път една година след датата на откриването за подписване на Протокола, постигнатия цялостен напредък по ратифицирането въз основа на информацията, която трябва да бъде предоставена на генералния секретар от всяка държава членка и от другите страни по Конвенцията най-късно един месец преди началото на тази проверка.“ Вж. https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016808a3c9f.

[176] В рамките на срещата на върха ЕС—Япония през април 2019 г. председателят Юнкер изрази подкрепа за инициативата на Япония за „свободно и надеждно движение на данни“, както и за стартирането на инициативата на Япония, известна като „подходът Осака“ и пое ангажимент Комисията да „играе активна роля и в двете инициативи“.

[177] Вж. текста на Декларацията от Осака на лидерите на държавите от Г-20: https://www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf

[178] Вж. текста на Стратегията от Биариц на Г-7 за отворена, свободна и сигурна цифрова трансформация: https://www.elysee.fr/admin/upload/default/0001/05/62a9221e66987d4e0d6ffcb058f3d2c649fc6d9d.pdf

[179] Съобщение на Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите, Европейска стратегия за данните, 19.2.2020 г. (COM(2020) 66 final) (https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:52020DC0066&qid=1596384191105&from=BG), стр. 23—24.

включително лични данни, или способността да се контролира такава информация“, ако засягат сигурността или обществения ред[180].

Комисията работи с единомислещи държави в рамките на няколко други многостранни форума, за да популяризира активно своите ценности и стандарти. Значим сред тях форум е наскоро създадената от ОИСР Работна група по въпросите на управлението на данни и неприкосновеността на личния живот, която се занимава с редица важни инициативи, свързани със защитата на данни, обмена на данни и предаването на данни. Това включва оценката на насоките на ОИСР от 2013 г. относно неприкосновеността на личния живот. Освен това Комисията активно допринесе за изготвянето на Препоръката на Съвета на ОИСР относно изкуствения интелект (ИИ)[181] и направи необходимото, за да гарантира, че в окончателния текст е отразен ориентираният към човека подход на ЕС, което означава, че приложенията на изкуствения интелект трябва да спазват основните права, и по-специално защитата на данните. Важно е да се отбележи, че в Препоръката относно ИИ, която впоследствие беше включена в принципите за ИИ на Г-20, приложени към Декларацията от Осака на лидерите на държавите от Г-20[182], са заложени принципите на прозрачност и възможност за обясняване, с цел „да се даде възможност на онези, които са неблагоприятно засегнати от система с изкуствен интелект, да оспорят резултата от нея въз основа на проста и лесна за разбиране информация относно факторите и логиката, послужили като основа за прогнозата, препоръката или решението“, като стриктно се отразяват принципите на ОРЗД във връзка с автоматизираното вземане на решения[183].

Комисията също така активизира своя диалог с регионалните организации и мрежи, които все по-често играят централна роля за формулирането на общи стандарти за защита на данните[184], насърчаването на обмена на най-добри практики и стимулирането на сътрудничеството между правоприлагащите органи. Става въпрос по-специално за Асоциацията на народите от Югоизточна Азия (АСЕАН) — включително в контекста на нейната текуща работа по инструментите за предаване на данни, Африканския съюз, Форума на органите за защита на неприкосновеността на личния живот в Азиатско-тихоокеанския регион (АРРА), както и Ибероамериканската мрежа за защита на данните, които поставиха началото на важни инициативи в тази област и предоставят форуми за ползотворен диалог между регулаторните органи в областта на неприкосновеността на личния живот и други заинтересовани страни.

Африка е показателен пример за взаимното допълване между националното, регионалното и глобалното измерение на неприкосновеността на личния

[180] Член 4, параграф 1, буква г) от Регламент (ЕС) 2019/452 на Европейския парламент и на Съвета от 19 март 2019 година за създаване на рамка за скрининг на преки чуждестранни инвестиции в Съюза (ОВ L 79I, 21.3.2019 г.).

[181] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

[182] Декларацията на министрите на държавите от Г-20 относно търговията и цифровата икономика: https://g20trade-digital.go.jp/dl/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf

[183] Вж. член 13, параграф 2, буква е), член 14, параграф 2, буква ж) и член 22 от ОРЗД.

[184] Вж. например *Конвенцията на Африканския съюз за киберсигурност и защита на личните данни* („Конвенция Malabo“) и *Стандартите за защита на данните за ибероамериканските държави*, разработени от Ибероамериканската мрежа за защита на данните.

живот. Цифровите технологии бързо и дълбоко трансформират африканския континент. Това има потенциала да ускори постигането на целите за устойчиво развитие чрез стимулиране на икономическия растеж, намаляване на бедността и подобряване на живота на хората. Наличието на съвременна рамка за защита на данните, която привлича инвестиции и насърчава развитието на конкурентоспособни предприятия, като същевременно допринася за зачитането на правата на човека, демокрацията и принципите на правовата държава, е ключов елемент от тази трансформация. Хармонизирането на правилата за защита на данните в цяла Африка ще даде възможност за интегриране на цифровия пазар, а доближаването до световните стандарти ще улесни обмена на данни с ЕС. Тези различни измерения на защитата на данните са свързани помежду си и взаимно се подсилват.

Понастоящем в много африкански държави се наблюдава нарастващ интерес към защитата на данните, а броят на африканските държави, които са приели или понастоящем приемат съвременни правила за защита на данните, ратифицирали са Конвенция № 108[185] или Конвенцията от Малабо[186], продължава да се увеличава[187]. В същото време на африканския континент регулаторната рамка продължава да е твърде неоднородна и разпокъсана. Много държави все още предлагат малко или изобщо не предлагат гаранции за защита на данните. Мерките, ограничаващи потоците от данни, все още са широко разпространени и възпрепятстват развитието на регионална цифрова икономика.

С оглед извличане на взаимни ползи от сближаването на правилата за защита на данните, Комисията ще се ангажира с африканските си партньори както на двустранна основа, така и в рамките на регионални форуми[188]. Това се основава на работата на Работната група на ЕС и Африканския съюз по въпросите на цифровата икономика в контекста на новото партньорство между Африка и Европа в областта на цифровата икономика[189]. В подкрепа на

[185] Конвенция на Съвета на Европа за защита на лицата при автоматизираната обработка на лични данни https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=DW5jevqD

[186] Конвенция на Африканския съюз за киберсигурност и защита на личните данни https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection. В допълнение няколко от регионалните икономически общности са разработили правила за защита на данните, например Икономическата общност на западноафриканските държави (ECOWAS) и Южноафриканската общност за развитие (ЮАОР). Вж. съответно http://www.tit.comm.ecowas.int/wp-content/uploads/2015/11/SIGNED-Data-Protection-Act.pdf и http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/docs/SA4docs/data%20protection.pdf.

[188] Наред с другото, и чрез Инициативата за политическа и регулаторна рамка за изграждане на цифрова Африка (Policy and Regulation Initiative for Digital Africa — PRIDA); вж. информация на следния адрес: https://www.africa-eu-partnership.org/en/projects/policy-and-regulation-initiative-digital-africa-prida.

[189] Вж. съвместното съобщение на Европейската комисия и върховния представител по въпросите на външните работи и политиката на сигурност „Към цялостна стратегия с Африка“ (на разположение на адрес: https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:52020JC0004&qid=1596463988028&from=BG); Работна група по въпросите на цифровата икономика, „Ново партньорство между Африка и Европа в областта

тези цели е също и осъществяването на обхвата на инструмента за партньорство на Комисията „Подобряване на защитата на данните и потоците от данни“ (Enhanced Data Protection and Data Flows), така че да включва и Африка. По проекта ще бъдат мобилизирани ресурси в подкрепа на африканските държави, които възнамеряват да разработят съвременни рамки за защита на данните, или които желаят да подсилят капацитета на своите регулаторни органи чрез обучение, обмен на знания и обмен на най-добри практики.

И накрая, като насърчава сближаването на стандартите за защита на данните на международно равнище като начин за улесняване на потоците от данни, а оттук и на търговията, Комисията същевременно е решена да се справи с цифровия протекционизъм, както неотдавна беше подчертано в Стратегията за данните[190]. За тази цел тя е разработила специални разпоредби относно потоците от данни и защитата на данни в търговските споразумения, които системно представя в рамките на двустранните преговори — най-често с Австралия, Нова Зеландия и Обединеното кралство — както и в рамките на многостранни преговори, като например настоящите преговори в рамките на СТО относно електронната търговия. Тези хоризонтални разпоредби изключват необоснованите ограничения, като например изисквания за задължително локализиране на данните, като същевременно запазват регулаторната независимост на страните да отстояват основното право на защита на данните.

Макар че диалозите относно защитата на данните и търговските преговори трябва да се водят по отделни направления, те могат да се допълват взаимно: всъщност сближаването, основаващо се на високи стандарти и подкрепено от ефективно правоприлагане, осигурява най-солидната основа за обмен на лични данни — нещо, което все повече се признава от нашите международни партньори. Като се има предвид, че дружествата работят все по-често през граница и предпочитат да прилагат сходни набори от правила във всички свои стопански дейности по света, това сближаване спомага за създаването на среда, която благоприятства преките инвестиции, улеснява търговията и повишава доверието между търговските партньори. Поради това полезните взаимодействия между инструментите за търговия и за защита на данните следва да бъдат допълнително проучени, за да се гарантират свободни и безопасни международни потоци от данни, които са от съществено значение за стопанските операции, конкурентоспособността и растежа на европейските дружества, включително МСП, в нашата все по-цифровизирана икономика.

на цифровата икономика: ускоряване на постигането на целите за устойчиво развитие“ (New Africa-Europe Digital Economy Partnership: Accelerating the Achievement of the Sustainable Development Goals) (на разположение на адрес: https://www.africa-eu-partnership.org/sites/default/files/documents/finaldetfreportpdf.pdf).

[190] https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:52020DC0066&qid=1596384191105&from=BG, стр. 23.

Приложение I — Клаузи за незадължителни уточнения в националното законодателство

Предмет	Обхват	Членове от ОРЗД
Уточнения относно правни задължения и задача от обществен интерес	Адаптиране на прилагането на разпоредбите по отношение на обработването с цел спазване на правно задължение или изпълнение на задача от обществен интерес, включително за особени ситуации на обработване съгласно глава IX	Член 6, параграфи 2 и 3
Възрастова граница за съгласие във връзка с услуги на информационното общество	Определяне на минимална възраст между 13 и 16 години	Член 8, параграф 1
Обработване на специални категории данни	Запазване или въвеждане на допълнителни условия, включително и ограничения, по отношение на обработването на генетични данни, биометрични данни или данни за здравословното състояние.	Член 9, параграф 4
Дерогация по отношение на изискванията за информация	Получаване или оповестяване на информация, изрично уредени по закон, или регулиране със закон на професионалната тайна	Член 14, параграф 5, букви в) и г)
Автоматизирано вземане на индивидуални решения	Разрешаване на автоматизирано вземане на решения чрез дерогация от общата забрана	Член 22, параграф 2, буква б)
Ограничения на правата на субекта на данни	Ограничения от разпоредбите на членове 12—22, член 34 и съответните разпоредби в член 5, когато е необходимо и пропорционално, за да се гарантират изчерпателно изброените важни цели	Член 23, параграф 1
Изискване за консултация и разрешение	Изискване към администраторите да се консултират с органа за защита на данните или да получават разрешение от него във връзка с обработването за изпълнението на задача в полза на обществения интерес	Член 36, параграф 5
Определяне на длъжностно	Определяне на длъжностно лице по	Член 37,

лице по защита на данните в допълнителни случаи	защита на данните в случаи, различни от посочените в член 37, параграф 1	параграф 4
Ограничения за предаване на данни	Ограничение за предаването на специални категории лични данни	Член 49, параграф 5
Жалби и съдебни искове от организации по собствена инициатива	Упълномощаване на организации за защита на неприкосновеността на личния живот да подават жалби и искове пред съдилища независимо от възложения от субекта на данни мандат	Член 80, параграф 2
Достъп до официални документи	Съгласуване на публичния достъп до официални документи с правото на защита на личните данни	Член 86
Обработване на националния идентификационен номер	Специални условия за обработване на националния идентификационен номер	Член 87
Обработване на данни в контекста на трудово правоотношение	По-конкретни правила за обработване на лични данни на наетите лица	Член 88
Дерогации за обработването за целите на архивирането в обществен интерес, за научни изследвания или за статистически цели	Дерогации от определени права на субекта на данни, доколкото има вероятност тези права да направят невъзможно или сериозно да затруднят постигането на конкретни цели	Член 89, параграфи 2 и 3
Съгласуване на защитата на данните със задълженията за опазване на тайна	Специални правила относно правомощията на органите за защита на данните по отношение на администраторите или обработващите лични данни, които са обвързани със задължение за опазване на професионална тайна	Член 90

Приложение II — Преглед на ресурсите на органите за защита на данните

В таблицата по-долу е представен преглед на ресурсите (персонал и бюджет) на органите за защита на данните за всяка държава — членка на ЕС/ЕИП[191].

При сравняване на цифрите за различните държави членки е важно да се има предвид, че на органите може да са възложени задачи извън онези по силата на ОРЗД и че те могат да се различават в отделните държави членки. Съотношението на наетия от органите персонал към един милион жители и съотношението на бюджета на органите към един милион евро от БВП са включени единствено с цел да се осигурят допълнителни елементи за сравнение между държавите членки със сходен размер и не следва да се разглеждат изолирано. Абсолютните стойности, съотношенията и развитието през последните години следва да се разглеждат заедно при оценката на ресурсите на даден орган.

	ПЕРСОНАЛ (в еквивалент на пълно работно време)					БЮДЖЕТ (в EUR)				
Държави — членки на ЕС/ЕИП	**2019 г.**	**Прогноза за 2020 г.**	**Увеличение в % за периода 2016—2019 г.**	**Увеличение в % за периода 2016—2020 г. (прогноза)**	**Персонал на 1 милион жители (2019 г.)**	**2019 г.**	**Прогноза за 2020 г.**	**Увеличение в % за периода 2016—2019 г.**	**Увеличение в % за периода 2016—2020 г. (прогноза)**	**Бюджет на 1 млн. EUR БВП (2019 г.)**
Австрия	34	34	48 %	48 %	3,8	2 282 000	2 282 000	29 %	29 %	5,7
Белгия	59	65	9 %	20 %	5,2	8 197 400	8 962 200	1 %	10 %	17,3
България	60	60	- 14 %	- 14 %	8,6	1 446 956	1 446 956	24 %	24 %	23,8
Хърватия	39	60	39 %	114 %	9,6	1 157 300	1 405 000	57 %	91 %	21,5
Кипър	24	22	Няма данни	Няма данни	27,4	503 855	Няма данни	114 %	Няма данни	23,0
Чешка република	101	109	0 %	8 %	9,5	6 541 288	6 720 533	10 %	13 %	29,7
Дания	66	63	106 %	97 %	11,4	5 610 128	5 623 114	101 %	101 %	18,0
Естония	16	18	- 11 %	0 %	12,1	750 331	750 331	7 %	7 %	26,8
Финландия	45	55	114 %	162 %	8,2	3 500 000	4 500 000	94 %	150 %	14,6
Франция	215	225	9 %	14 %	3,2	18 506 734	20 143 889	- 2 %	7 %	7,7
Германия	888	1 002	52 %	72 %	10,7	76 599 800	85 837 500	48 %	66 %	22,3
Гърция	33	46	- 15 %	18 %	3,1	2 849 000	3 101 000	38 %	50 %	15,2
Унгария	104	117	42 %	60 %	10,6	3 505 152	4 437 576	102 %	155 %	24,4
Исландия	17	17	143 %	143 %	47,6	2 272 490	2 294 104	167 %	170 %	105,2
Ирландия	140	176	169 %	238 %	28,5	15 200 000	16 900 000	223 %	260 %	43,8
Италия	170	170	40 %	40 %	2,8	29 127 273	30 127 273	46 %	51 %	16,3
Латвия	19	31	- 10 %	48 %	9,9	640 998	1 218 978	4 %	98 %	21,0
Литва	46	52	- 8 %	4 %	16,5	1 482 000	1 581 000	40 %	49 %	30,6
Люксембург	43	48	126 %	153 %	70,0	5 442 416	6 691 563	165 %	226 %	85,7
Малта	13	15	30 %	50 %	26,3	480 000	550 000	41 %	62 %	36,3
Нидерландия	179	188	145 %	158 %	10,4	18 600 000	18 600 000	130 %	130 %	22,9
Норвегия	49	58	2 %	21 %	9,2	5 708 950	6 580 660	27 %	46 %	15,9
Полша	238	260	54 %	68 %	6,3	7 506 345	9 413 381	66 %	108 %	14,2
Португалия	25	27	- 4 %	4 %	2,4	2 152 000	2 385 000	67 %	86 %	10,1
Румъния	39	47	- 3 %	18 %	2,0	1 103 388	1 304 813	3 %	22 %	4,9

[191] С изключение на Лихтенщайн.

Словакия	49	51	20 %	24 %	9,0	1 731 419	1 859 514	47 %	58 %	18,4
Словения	47	49	42 %	48 %	22,6	2 242 236	2 266 485	68 %	70 %	46,7
Испания	170	220	13 %	47 %	3,6	15 187 680	16 500 000	8 %	17 %	12,2
Швеция	87	87	81 %	81 %	8,5	8 800 000	10 300 000	96 %	129 %	18,5
ОБЩО	**2 966**	**3 372**	**42 %**	**62 %**	**6,6**	**249 127 139**	**273 782 870**	**49 %**	**64 %**	**17,4**

Източник на първичните данни: приносът на Комитета. Изчисленията са на Комисията