



Брюксел, 25.7.2024 г.  
COM(2024) 357 final

**СЪОБЩЕНИЕ НА КОМИСИЯТА ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И  
СЪВЕТА**

**Втори доклад за прилагането на Общия регламент относно защитата на данните**

## 1 ВЪВЕДЕНИЕ

Това е вторият доклад на Комисията за прилагането на Общия регламент относно защитата на данните (ОРЗД), приет в съответствие с член 97 от ОРЗД. Първият доклад беше приет на 24 юни 2020 г. („доклада от 2020 г.“) <sup>(1)</sup>.

ОРЗД е един от крайъгълните камъни на подхода на ЕС към цифровата трансформация. Неговите основни принципи — справедливо, безопасно и прозрачно обработване на лични данни, гарантиращо, че физическите лица продължават да имат контрол — са в основата на всички политики на ЕС, включващи обработването на лични данни.

След доклада от 2020 г. ЕС прие редица инициативи, чиято цел е поставянето на физическите лица в центъра на цифровия преход. Всяка инициатива преследва конкретна цел, като например създаване на по-безопасна онлайн среда, създаване на по-справедлива и по-конкурентоспособна цифрова икономика, улесняване на революционните научни изследвания, осигуряване на разработването на безопасен и надежден изкуствен интелект (ИИ) и създаване на истински единен пазар за данни. Когато става въпрос за лични данни, тези инициативи се основават на ОРЗД. В ОРЗД се осигурява и основа за секторни инициативи, които оказват въздействие върху обработването на лични данни, например в областта на финансовите услуги, здравеопазването, заетостта, мобилността и правоприлагането.

Сред заинтересованите страни, органите за защита на данните и държавите членки е налице широк консенсус, че въпреки някои предизвикателства ОРЗД е дал значителни резултати за физическите лица и предприятията. С основания на риска технологично неутрален подход се осигуряват силна защита на субектите на данни и пропорционални задължения за администраторите и обработващите лични данни. В същото време следва да се постигне допълнителен напредък в редица области. По-специално акцентът през следващите години следва да бъде върху подкрепата на усилията на заинтересованите страни за спазване на изискванията — особено на малките и средните предприятия (МСП), малките оператори и изследователите и научноизследователските организации — като органите за защита на данните ще предоставят по-ясни и по-приложими насоки, и върху постигането на по-последователно тълкуване и прилагане на ОРЗД в ЕС.

Съгласно член 97 от ОРЗД Комисията следва да разгледа по-специално прилагането и функционирането на международното предаване на лични данни на трети държави (т.е. държави извън ЕС/ЕИП) (глава V от ОРЗД), както и механизмите за сътрудничество и съгласуваност между националните органи за защита на данните (Глава VII от ОРЗД). В настоящия доклад обаче, както и в доклада от 2020 г., се предоставя обща оценка на прилагането на ОРЗД, надхвърляща тези два елемента — набелязани са редица действия, необходими за подпомагане на ефективното прилагане на ОРЗД в ключови приоритетни области.

В настоящия доклад се вземат предвид следните източници: i) позицията и констатациите на Съвета, приети през декември 2023 г. <sup>(2)</sup>; ii) информация, събрана от заинтересовани страни, по-специално чрез Многостранната група на

---

<sup>(1)</sup> Защитата на данните като стълб на оправомощаването на гражданите и на подхода на ЕС по отношение на цифровия преход — две години от прилагането на Общия регламент относно защитата на данните, 24.6.2020 г., COM(2020) 264 final.

<sup>(2)</sup> <https://data.consilium.europa.eu/doc/document/ST-15507-2023-INIT/bg/pdf>

заинтересованите страни по въпросите на ОРЗД<sup>(3)</sup>, и публична покана за предоставяне на данни<sup>(4)</sup>; както и iii) информация от органите за защита на данните (чрез приноса на Европейския комитет по защита на данните<sup>(5)</sup> („Комитета“) и доклад, изготвен от Агенцията на Европейския съюз за основните права (FRA) въз основа на интервюта, проведени с отделни органи за защита на данните<sup>(6)</sup> („докладът на FRA“). Докладът се основава и на текущото наблюдение от страна на Комисията на прилагането на ОРЗД, включително двустранни диалози с държавите членки относно съответствието на националното законодателство, активен принос към работата на Комитета и тесни контакти с широк кръг от заинтересовани страни относно практическото прилагане на регламента.

## **2 ПРИЛАГАНЕ НА ОБЩИЯ РЕГЛАМЕНТ ОТНОСНО ЗАЩИТАТА НА ДАННИТЕ И ФУНКЦИОНИРАНЕ НА МЕХАНИЗМИТЕ ЗА СЪТРУДНИЧЕСТВО И СЪГЛАСУВАНОСТ**

Системата на ОРЗД за прилагане от единно звено за контакт има за цел да осигури хармонизирано тълкуване и прилагане от независими органи за защита на данните. Това изисква сътрудничество между органите за защита на данните в случаи на трансгранично обработване, когато в значителна степен са засегнати субекти на данни в множество държави членки. Споровете между органите се разрешават от Комитета съгласно механизма за съгласуваност на ОРЗД.

### **2.1 По-ефективно обработване на трансгранични случаи: предложение за процедурни правила**

В доклада от 2020 г. беше отбелязана необходимостта от по-ефикасно и хармонизирано обработване на трансграничните случаи в ЕС, по-специално с оглед на големите разлики в националните административни процедури и тълкуванията на понятия в рамките на механизма на ОРЗД за сътрудничество. Поради това през юли 2023 г. Комисията прие предложение за Регламент относно процедурните правила<sup>(7)</sup>, като се основа също на списък с въпроси, представен от Комитета на Комисията през октомври 2022 г.<sup>(8)</sup>, както и на информацията от заинтересованите страни<sup>(9)</sup> и държавите членки<sup>(10)</sup>. С предложението се допълва ОРЗД, като се определят подробни правила относно трансграничните жалби, участието на жалбоподателя, правата на справедлив съдебен процес на разследваните страни

---

<sup>(3)</sup> Обобщение на информацията от Многостранната група на заинтересованите страни по въпросите на ОРЗД е на разположение тук: [Доклад на Многостранната група на заинтересованите страни по въпросите на ОРЗД относно прилагането на ОРЗД — юни 2024 г. pdf](#). Информацията, получена в отговор на публичната покана за предоставяне на данни, и чрез двустранни срещи със заинтересованите страни, отразява до голяма степен възгледите, изразени от членовете на Многостранната група на заинтересованите страни по въпросите на ОРЗД.

<sup>(4)</sup> [https://ec.europa.eu/info/law/better-regulation/have-your-say\\_bg](https://ec.europa.eu/info/law/better-regulation/have-your-say_bg)

<sup>(5)</sup> [Принос на ЕКЗД към оценката на ОРЗД съгласно член 97 | Европейски комитет по защита на данните \(europa.eu\)](#).

<sup>(6)</sup> [ОРЗД на практика — Опитът на органите за защита на данните | Агенция на Европейския съюз за основните права \(europa.eu\)](#)

<sup>(7)</sup> Предложение за Регламент на Европейския парламент и на Съвета за определяне на допълнителни процедурни правила във връзка с изпълнението на Регламент (ЕС) 2016/679 (COM(2023) 348 final).

<sup>(8)</sup> [https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-letter-eu-commission-procedural-aspects-could-be\\_en](https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-letter-eu-commission-procedural-aspects-could-be_en).

<sup>(9)</sup> Чрез Многостранната група на заинтересованите страни по въпросите на ОРЗД и покана за предоставяне на данни, отправена през февруари 2023 г.

<sup>(10)</sup> Предимно чрез експертната група на държавите членки по ОРЗД: <https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=bg&do=groupDetail.groupDetail&groupID=3461>

(администратори и обработващи лични данни) и сътрудничеството между органите за защита на данните. Хармонизирането на тези процедурни аспекти би подпомогнало навременното приключване на разследванията и предоставянето на бързи средства за правна защита на физическите лица. Понастоящем предложението се договаря от Европейския парламент и Съвета.

## **2.2 Засилено сътрудничество между органите за защита на данните и използване на механизма за съгласуваност**

През последните години броят на трансграничните случаи се увеличи значително. Органите за защита на данните демонстрираха повишена готовност да използват инструментите за сътрудничество, предоставени от ОРЗД. Всички органи за защита на данните използват инструмента за взаимопомощ<sup>(11)</sup>, както и „неофициални“ искания с цел да си съдействат взаимно на доброволен принцип. Органите за защита на данните предпочитат неофициалните искания, които не налагат краен срок или стриктно задължение за отговор. Макар че през 2021 г. Комитетът прие насоки за съвместни операции<sup>(12)</sup>, органите все още не са използвали в значителна степен този инструмент<sup>(13)</sup> и като основни причини за ограничената му употреба посочват разликите в националните процедури и липсата на яснота относно процедурата.

С ОРЗД на съответните органи за защита на данните се предоставя възможността да повдигнат относимо и обосновано възражение, когато не са съгласни с проект на решение на водещия орган за защита на данните при трансграничен случай. Когато органите за защита на данните не могат да постигнат консенсус относно относимо и обосновано възражение, в ОРЗД се предвижда споровете да бъдат разрешавани от Комитета<sup>(14)</sup>. Най-често повдиганите теми в относими и обосновани възражения са: i) правното основание за обработването; ii) задълженията за информиране и прозрачност; iii) уведомяването за нарушения на данните; iv) права на субектите на данни; v) дерогации във връзка с международни предавания; vi) употребата на корективни мерки; и vii) размерът на административното наказание „глоба“ или „имуществена санкция“.

Системата за прилагане на ОРЗД се основава на предпоставката за искрено и ефективно сътрудничество между органите за защита на данните. Въпреки че процедурата за разрешаване на спорове играе важна роля в тази архитектура на правоприлагане, тя следва да се използва по предназначение, а именно като се отчита надлежно разделението на компетентността между органите за защита на данните, необходимостта от зачитане на справедлив съдебен процес и интересът за постигане на навременно разрешаване на случая за субектите на данни. Всяка процедура за разрешаване на спорове изисква значителни ресурси от страна на водещия орган, заинтересованите органи и секретариата на Комитета и забавя предоставянето на средства за правна защита на субектите на данни.

---

<sup>(11)</sup> Член 61 от ОРЗД.

<sup>(12)</sup> [internal edpb document 1 2021 on art 62 joint operations en.pdf \(europa.eu\)](#)

<sup>(13)</sup> Член 62 от ОРЗД.

<sup>(14)</sup> Член 65 от ОРЗД.

*Повишено използване на инструменти за сътрудничество от органите за защита на данните*

- В системата за обмен на информация на Комитета са регистрирани почти 2 400 вписвания на казуси <sup>(15)</sup>.
- Водещите органи за защита на данните са издали около 1 500 проекта на решения <sup>(16)</sup>, от които 990 са довели до окончателни решения, с които се установява нарушение на ОРЗД <sup>(17)</sup>.
- Органите за защита на данните са подали почти 1 000 „официални“ молби за взаимна помощ <sup>(18)</sup> и около 12 300 „неофициални“ молби <sup>(19)</sup>.
- Започнати са пет съвместни операции, в които са участвали органите за защита на данните от седем държави членки.
- Органите за защита на данните от 18 държави членки са повдигнали относими и обосновани възражения <sup>(20)</sup>.

Механизмът за съгласуваност на ОРЗД се използва все по-често от органите за защита на данните. Той се състои от три компонента: i) становища на Комитета; ii) разрешаване на спорове от Комитета; и iii) процедура по спешност <sup>(21)</sup>.

Все по-често Комитетът разглежда в своите становища важни въпроси от общ характер <sup>(22)</sup>. Той следва да гарантира провеждането на навременни и задълбочени консултации преди приемането на тези становища. Случаите, които са представени за разрешаване на спорове, се отнасят до въпроси като правното основание за обработване на данни за проследяване на поведението на потребителите в социалните медии и онлайн обработване на данни на деца. Повечето от последващите решения със задължителен характер са обжалвани пред Общия съд.

Прозрачността в процеса на вземане на решения от Комитета е от ключово значение за гарантиране на зачитането на правото на добра администрация съгласно Хартата на основните права на ЕС. Процедурата по спешност в ОРЗД позволява на органите за защита на данните да се отклонят от механизма за сътрудничество и съгласуваност, за да предприемат спешни мерки, когато това е необходимо, с цел да защитят правата и свободите на субектите на данни. Като дерогация от нормалната процедура за сътрудничество съгласно ОРЗД, инструменти като процедурата по спешност са предназначени да се използват само при извънредни обстоятелства и когато нормалната процедура за сътрудничество не може да защити правата и свободите на субектите на данни.

<sup>(15)</sup> От 3 ноември 2023 г. (принос на Комитета).

<sup>(16)</sup> Съгласно член 60, параграф 3 от ОРЗД.

<sup>(17)</sup> От 3 ноември 2023 г.

<sup>(18)</sup> Ирландският орган е отправил най-много официални молби (246), докато германските органи са получили най-много молби (516).

<sup>(19)</sup> Ирландските органи са отправили най-много неофициални молби (4 245), следвани от германските органи (2 036).

<sup>(20)</sup> От докладваните от органите 289 относими и обосновани възражения, 101 (35 %) са повдигнати от германските органи. Процентът на успеваемост при постигането на консенсус по относими и обосновани възражения варира от 15 % (от повдигнатите от германските органи възражения) до 100 % (от повдигнатите от полските органи възражения).

<sup>(21)</sup> Съответно членове 64, 65 и 66 от ОРЗД.

<sup>(22)</sup> Становища съгласно член 64, параграф 2 от ОРЗД.

### *Механизмът за съгласуваност*

- Комитетът е приел 190 становища относно съгласуваността.
- При разрешаване на спорове са приети девет решения със задължителен характер <sup>(23)</sup>. С всички тях на водещия орган за защита на данните са дадени указания да промени проекта на решението си, а няколко от тях са довели до значителни глоби.
- Пет органа за защита на данните са приели временни мерки в рамките на процедурата по спешност (Германия, Испания, Италия, Норвегия и Финландия).
- Два органа за защита на данните поискаха от Съвета спешно решение със задължителен характер <sup>(24)</sup>, а Съветът нареди в един от случаите налагането на спешни окончателни мерки.

### **2.3 Засилено прилагане**

През последните години се наблюдаваше значителен подем в дейността по правоприлагането от страна на органите за защита на данните, включително налагането на значителни глоби в знакови случаи срещу „големи технологични“ мултинационални дружества. Глоби бяха наложени например за: i) нарушаване на законосъобразността и сигурността на обработването; ii) нарушаване на обработването на специални категории лични данни; и iii) неспазването на правата на физическите лица <sup>(25)</sup>. Това накара частните дружества да „приемат сериозно защитата на данните“ <sup>(26)</sup> и спомогна за внедряването на култура на спазване в рамките на организациите. Органите за защита на данните приемат решения за установяване на нарушения на ОРЗД в случаи, основани на жалби и по собствена инициатива. Макар и да не са налични във всички държави членки, много органи за защита на данните са използвали ефективно процедурите за „уреждане на спора по взаимно съгласие“ за бързо разрешаване на случаи, основани на жалби, по задоволителен за жалбоподателя начин. В предложението за процедурни правила се признава възможността жалбите да бъдат разрешавани чрез уреждане на спора по взаимно съгласие <sup>(27)</sup>.

Органите за защита на данните са използвали в достатъчна степен корективните си правомощия, макар че броят на наложените корективни мерки варира значително между органите. Освен глобите, най-често използваните корективни мерки са предупреждения, официални предупреждения и разпореждания за спазване на ОРЗД. Администраторите и обработващите лични данни често оспорват решения за установяване на нарушения на ОРЗД в национални съдилища, най-често на процедурни основания <sup>(28)</sup>.

<sup>(23)</sup> Съгласно член 65, параграф 1, буква а) от ОРЗД.

<sup>(24)</sup> Съгласно член 66, параграфи 2 от ОРЗД.

<sup>(25)</sup> Вж. точка 5.3.4 от приноса на Комитета.

<sup>(26)</sup> Вж. доклада на FRA, стр. 36.

<sup>(27)</sup> Предложение за процедурни правила, член 5.

<sup>(28)</sup> В Румъния всичките 26 решения за установяване на нарушение са били обжалвани в съда, докато в Нидерландия процентът на обжалванията е бил 23 %. Процентът на уважените обжалвания е най-висок в Белгия (39 %).

### *Засилено прилагане*

- Органите за защита на данните са започнали над 20 000 разследвания по собствена инициатива <sup>(29)</sup>.
- Те получават общо над 100 000 жалби годишно <sup>(30)</sup>.
- Средната продължителност на времето за разглеждане на жалби от органите за защита на данните (от получаването до приключване на случая) варира в диапазона 1—12 месеца, като тя е 3 месеца или по-малко в пет държави членки (Дания (1 месец), Испания (1,5 месеца), Естония (3 месеца), Гърция (3 месеца) и Ирландия (3 месеца)).
- Над 20 000 жалби са разрешени чрез споразумение за уреждане на спора по взаимно съгласие. То е използвано най-често в Австрия, Ирландия, Люксембург и Унгария.
- През 2022 г. органите за защита на данните в Германия са приели най-голям брой решения за налагане на корективна мярка (3 261), следвани от Испания (774), Литва (308) и Естония (332). Най-малък брой корективни мерки са наложени в Лихтенщайн (8), Чехия (8), Исландия (10), Нидерландия (17) и Люксембург (22).
- Органите за защита на данните са наложили над 6 680 глоби на обща стойност около 4,2 милиарда евро <sup>(31)</sup>. Органът в Ирландия е наложил най-висок общ размер на глобите (2,8 милиарда евро), следван от Люксембург (746 милиона евро), Италия (197 милиона евро) и Франция (131 милиона евро). Най-малък е размерът на глобите, наложени в Лихтенщайн (9 600 EUR), Естония (201 000 EUR) и Литва (435 000 EUR).

Макар че повечето органи за защита на данните считат своите инструменти за разследване за подходящи, някои изискват допълнителни инструменти на национално равнище, като например подходящи санкции, когато администраторите не сътрудничат или не предоставят необходимата информация <sup>(32)</sup>. Органите за защита на данните считат, че недостатъчните ресурси и пропуските в техническата и правната квалификация са основният фактор, който влияе върху капацитета им за правоприлагане <sup>(33)</sup>.

## **2.4 Комитетът**

Комитетът се състои от ръководителя на един орган за защита на данните от всяка държава членка и Европейския надзорен орган по защита на данните, като Комисията участва без право на глас. Комитетът, който е подпомаган в работата си от своя секретариат, има за задача да осигури последователното прилагане на

---

<sup>(29)</sup> Органите за защита на данните в Германия са започнали най-голям брой разследвания по собствена инициатива (7 647), следвани от Унгария (3 332), Австрия (1 681) и Франция (1 571).

<sup>(30)</sup> През 2022 г. девет органа за защита на данните са получили над 2 000 жалби. Най-много жалби са регистрирани в Германия (32 300), Италия (30 880), Испания (15 128), Нидерландия (13 133) и Франция (12 193), а най-малко в Лихтенщайн (40), Исландия (140) и Хърватия (271).

<sup>(31)</sup> Всички органи са налагали административни наказания „глоба“ или „имуществена санкция“, с изключение на Дания, която не предвижда такъв вид наказание. Най-много глоби са наложени в Германия (2 106) и Испания (1 596). Най-малко глоби са наложени в Лихтенщайн (3), Исландия (15) и Финландия (20).

<sup>(32)</sup> Доклад на FRA, стр. 38.

<sup>(33)</sup> Доклад на FRA, стр. 20 и 23. Вж. също позиция и констатации на Съвета, точка 17.



ОРЗД<sup>(34)</sup>. Повечето органи за защита на данните смятат, че Комитетът е изиграл положителна роля за укрепване на сътрудничеството между тях<sup>(35)</sup>. Много органи за защита на данните отделят значителни ресурси за дейностите на Комитета, макар че по-малките органи посочват, че размерът им пречи да се ангажират напълно<sup>(36)</sup>. Някои органи смятат, че ефикасността на процесите на Комитета следва да се подобри, по-специално като се намали броят на заседанията и като се обръща по-малко внимание на второстепенни въпроси<sup>(37)</sup>. В зависимост от резултата от преговорите по предложението относно процедурните правила на ОРЗД, чиято цел е да се намали броят на подадените до Комитета случаи за разрешаване на спорове, може да е необходимо да се обмисли дали Комитетът се нуждае от допълнителни ресурси.

От ноември 2023 г. Комитетът е приел 35 насоки. Макар че заинтересованите страни и органите за защита на данните намират насоките за полезни, всички те считат, че следва да им бъдат предоставяни по-бързо и че качеството им следва да бъде подобро<sup>(38)</sup>. Заинтересованите страни отбелязват, че насоките са често прекалено теоретични, твърде дълги и не отразяват основания на риска подход на ОРЗД<sup>(39)</sup>. Органите за защита на данните и Комитетът следва да предоставят кратки и практически насоки, които да дават отговори на конкретни проблеми и да отразяват баланса между защитата на данните и други основни права. Насоките следва да са лесни за разбиране и за лица без юридическо обучение, например в МСП и доброволчески организации<sup>(40)</sup>. Един начин за постигане на това е подготовката на насоките да стане по-прозрачна, а провеждането на консултациите да се случва на ранен етап, така че да се даде възможност за по-добро разбиране на динамиката на пазара, търговските практики и начина, по който насоките да се прилагат на практика<sup>(41)</sup>. Приветства се фактът, че като част от своята стратегия за периода 2024—2027 г. Комитетът е изтъкнал целта си да предостави практически насоки, които са достъпни за съответната аудитория<sup>(42)</sup>.

Заинтересованите страни подчертават необходимостта от допълнителни насоки, по-специално относно анонимизирането и псевдонимизирането<sup>(43)</sup>, законния интерес и научните изследвания<sup>(44)</sup>. В доклада от 2020 г. Комисията призова Комитета да приеме насоки в областта на научните изследвания, но насоките все още не са приети. Като се признава значението на научните изследвания в обществото, по-специално за наблюдение на заболявания и разработване на лечения, както и за насърчаване на иновациите, от съществено значение е органите за защита на данните да действат за изясняване тези въпроси без допълнително забавяне<sup>(45)</sup>. Публичните

---

<sup>(34)</sup> Член 70, параграф 1 от ОРЗД.

<sup>(35)</sup> Доклад на FRA, стр. 64.

<sup>(36)</sup> Доклад на FRA, стр. 67. През 2023 г. германските органи за защита на данните са отделили най-много ресурси за дейностите на Комитета (26 еквивалента на пълно работно време (ЕППВ), следвани от Ирландия (16) и Франция (12) (принос на Комитета).

<sup>(37)</sup> Доклад на FRA, стр. 67.

<sup>(38)</sup> Доклад на FRA, стр. 67; обобщение на обратната информация от Многостранната група на заинтересованите страни по въпросите на ОРЗД.

<sup>(39)</sup> Обобщение на обратната информация от Многостранната група на заинтересованите страни по въпросите на ОРЗД.

<sup>(40)</sup> Вж. също позиция и констатации на Съвета, точка 45.

<sup>(41)</sup> Вж. също позиция и констатации на Съвета, точка 34.

<sup>(42)</sup> [https://www.edpb.europa.eu/system/files/2024-04/edpb\\_strategy\\_2024-2027\\_en.pdf](https://www.edpb.europa.eu/system/files/2024-04/edpb_strategy_2024-2027_en.pdf)

<sup>(43)</sup> Вж. също позиция и констатации на Съвета, точка 31, буква г).

<sup>(44)</sup> Те по-специално изискват яснота относно значението на понятието „научно изследване“, ролята на съгласието за обработване на лични данни за научни изследвания, съответното правно основание и ролите и отговорността на участниците.

<sup>(45)</sup> Вж. също позиция и констатации на Съвета, точка 31, буква б).



органи биха имали полза и от насоки, насочени към конкретните предизвикателства, пред които са изправени <sup>(46)</sup>.

## 2.5 Органи за защита на данните

### 2.5.1 Независимост и ресурси

Независимостта на органите за защита на данните е заложена в Хартата на основните права на Европейския съюз и Договора за функционирането на ЕС. В ОРЗД се определят изисквания за гарантиране на „пълна независимост“ на органите за защита на данните <sup>(47)</sup>. В доклада на FRA се установява, че повечето органи за защита на данните работят независимо от правителство, парламент или други публични органи <sup>(48)</sup>.

Органите за защита на данните изискват подходящи човешки, технически и финансови ресурси, за да могат ефективно и независимо да изпълняват задачите си съгласно ОРЗД. В доклада от 2020 г. Комисията отбелязва, че ресурсите на органите за защита на данните все още не са задоволителни и многократно повдигна този въпрос пред държавите членки. Оттогава насам ситуацията се е подобрила.

#### *Увеличаване на ресурсите за органите за защита на данните <sup>(49)</sup>*

- В периода 2020—2024 г. всички органи за защита на данните с изключение на два се възползваха от увеличение на персонала и увеличението надхвърли 25 % в 14 държави членки.
- Органът за защита на данните в Ирландия отбелязва най-голямо увеличение на персонала (79 %), следван от Естония, Швеция (и двете по 57 %) и България (56 %).
- Леко намаление в персонала се наблюдаваше в органа в Чехия (-1 %), докато в Лихтенщайн не се наблюдаваше увеличение, а увеличенията в Кипър (4 %) и в Унгария (8 %) бяха незначителни.
- В периода 2020—2024 г. всички органи за защита на данните с изключение на един отбелязаха увеличение на бюджета, като увеличението надхвърли 50 % в 13 държави членки.
- Органът за защита на данните в Кипър отбелязва най-голямо увеличение на бюджета (130 %), следван от Австрия (107 %), България (100 %) и Естония (97 %).
- Бюджетът на гръцкия орган за защита на данните е намалял с 15 %, като същевременно се наблюдават незначителни увеличения на бюджета за органите на Лихтенщайн (1 %), Словакия (6 %) и Чехия (8 %).

Въпреки че тези статистически данни показват обща възходяща тенденция в ресурсите на органите за защита на данните, самите органи смятат, че все още им липсват достатъчно човешки ресурси <sup>(50)</sup>. Те подчертават необходимостта от много

<sup>(46)</sup> Позиция и констатации на Съвета, точки 27—28.

<sup>(47)</sup> Член 52 от ОРЗД.

<sup>(48)</sup> Доклад на FRA, стр. 31.

<sup>(49)</sup> Вж. раздел 4.4.1 от приноса на Комитета, също и за абсолютните стойности.

<sup>(50)</sup> Само пет органа за защита на данните считат, че разполагат с подходящи човешки ресурси (принос на Комитета, стр. 33).

специализирани технически познания, по-специално относно новите и нововъзникващите технологии <sup>(51)</sup>, липсата на които се отразява на количеството и качеството на тяхната работа, както и относно трудностите при конкуренцията за човешки ресурси с частния сектор. Органите за защита на данните посочват недостатъчните правни познания и липсата на езикови умения като фактори, влияещи върху работата им. Ниското възнаграждение, неспособността за самостоятелен подбор на персонала и голямото натоварване са изтъкнати като ключови фактори, влияещи върху способността на органите да наемат и задържат персонал <sup>(52)</sup>. Органите за защита на данните изтъкват и необходимостта от финансови ресурси, в случай че решат да модернизират и цифровизират процесите си и да придобият техническо оборудване <sup>(53)</sup>. Всички органи за защита на данните изпълняват задачи извън възложените им съгласно ОРЗД <sup>(54)</sup>, например като надзорни органи за Директивата относно правоприлагането в областта на защитата на данните и Директивата за правото на неприкосновеност на личния живот и електронни комуникации, макар че мнозина изразяват опасения относно поемането на допълнителни отговорности съгласно новото цифрово законодателство <sup>(55)</sup>.

### 2.5.2 Трудности при разглеждането на голям брой жалби

Няколко органа за защита на данните посочват, че твърде голяма част от техните ресурси се използват за разглеждане на голям брой жалби, повечето от които смятат за маловажни и неоснователни, тъй като съгласно ОРЗД разглеждането на всяка жалба е задължение, чието изпълнение подлежи на съдебен контрол <sup>(56)</sup>. Това означава, че органите за защита на данните не могат да отделят достатъчно ресурси за други дейности, като разследвания по собствена инициатива, кампании за повишаване на осведомеността на обществеността и работата с администратори <sup>(57)</sup>. В качеството си на публични органи, органите за защита на данните имат правото да разпределят ресурсите си по своя преценка, така че да изпълнят всяка от задачите си (посочени в член 57, параграф 1 от ОРЗД) в обществен интерес. Много органи за защита на данните са приели стратегии за повишаване на ефикасността на разглеждането на жалби, като например автоматизация <sup>(58)</sup>, използване на процедури за уреждане на спора по взаимно съгласие <sup>(59)</sup> и „групиране“ на жалби, които се отнасят до сходни проблеми <sup>(60)</sup>.

### 2.5.3 Тълкуване на ОРЗД от националните органи за защита на данните

Основна цел на ОРЗД беше премахването на фрагментирия подход спрямо защитата на данните, който съществуваше при предишната Директива за защита на личните данни (Директива 95/46/ЕО) <sup>(61)</sup>. Органите за защита на данните обаче

---

<sup>(51)</sup> Доклад на FRA, стр. 20. Някои органи за защита на данните възлагат определени задачи на външни изпълнители, като разглеждане на жалби, правен анализ и съдебно-техническа експертиза.

<sup>(52)</sup> Доклад на FRA, стр. 24.

<sup>(53)</sup> Доклад на FRA, стр. 22.

<sup>(54)</sup> Вж. раздел 4.4.5 от приноса на Комитета.

<sup>(55)</sup> Принос на Комитета, стр. 32.

<sup>(56)</sup> Доклад на FRA, стр. 48.

<sup>(57)</sup> Доклад на FRA, стр. 45. Органите за защита на данните считат служебните разследвания за особено важни, тъй като жалбоподателите може да не са осведомени за много нарушения на ОРЗД.

<sup>(58)</sup> Доклад на FRA, стр. 8.

<sup>(59)</sup> Доклад на FRA, стр. 39.

<sup>(60)</sup> Доклад на FRA, стр. 41.

<sup>(61)</sup> Съображение 9 от ОРЗД.

продължават да приемат различни тълкувания на основни понятия, свързани със защитата на данните <sup>(62)</sup>. Заинтересованите страни определят това като основната пречка пред последователното прилагане на ОРЗД в ЕС. Устойчивостта на различните тълкувания създава правна несигурност и увеличава разходите за предприятията (например като за няколко държави членки се изисква различна документация), нарушава свободното движение на лични данни в ЕС, възпрепятства трансграничната стопанска дейност и възпрепятства научните изследвания и иновациите, свързани с неотложни предизвикателства пред обществото.

Конкретните въпроси, повдигнати от заинтересованите страни, включват: i) факта, че всеки от органите за защита на данните в три държави членки има различно мнение относно подходящото правно основание за обработването на лични данни при провеждане на клинично изпитване; ii) честото изразяване на различни мнения относно това дали даден субект е администратор или обработващ лични данни; и iii) това, че в някои случаи органите за защита на данните не следват насоките на Комитета или публикуват на национално равнище насоки, които противоречат на тези на Комитета <sup>(63)</sup>. Тези проблеми се усложняват, когато множество органи за защита на данните в рамките на една държава членка приемат противоречиви тълкувания.

Някои заинтересовани страни също така смятат, че определени органи за защита на данните и Комитетът приемат тълкувания, които се отклоняват от основания на риска подход на ОРЗД, което представлява предизвикателство за развитието на цифровата икономика <sup>(64)</sup> и свободата и плурализма на медиите. Те посочват като проблемни области: i) тълкуването на анонимизирането; ii) правното основание на законния интерес и съгласието <sup>(65)</sup>; и iii) изключенията от забраната за автоматизираното вземане на индивидуални решения <sup>(66)</sup>. Следва да се припомни, че органите за защита на данните и Комитетът имат за задача да гарантират както защитата на физическите лица във връзка с обработването на техните лични данни, така и свободното движение на лични данни в рамките на ЕС. Както се признава в ОРЗД <sup>(67)</sup>, правото на защита на личните данни трябва да бъде разглеждано във връзка с функцията му в обществото и да бъде в равновесие с другите основни права съгласно принципа на пропорционалност.

#### *2.5.4 Работа с администратори и обработващи лични данни*

Заинтересованите страни подчертават ползата от възможността да участват в конструктивен диалог с органите за защита на данните, за да се гарантира, че спазват ОРЗД от самото начало, по-специално по отношение на нововъзникващите технологии. Заинтересованите страни отбелязват, че някои органи за защита на данните работят активно с администраторите, докато други реагират бавно, предоставят неясни отговори или изобщо не отговарят <sup>(68)</sup>.

---

<sup>(62)</sup> Обобщение на обратната информация от Многостранната група на заинтересованите страни по въпросите на ОРЗД.

<sup>(63)</sup> Обобщение на обратната информация от Многостранната група на заинтересованите страни по въпросите на ОРЗД.

<sup>(64)</sup> Обобщение на обратната информация от Многостранната група на заинтересованите страни по въпросите на ОРЗД.

<sup>(65)</sup> Съответно член 6, параграф 1, букви а и е) от ОРЗД.

<sup>(66)</sup> Член 22, параграф 2 от ОРЗД.

<sup>(67)</sup> Съображение 4.

<sup>(68)</sup> Обобщение на обратната информация от Многостранната група на заинтересованите страни по въпросите на ОРЗД.

### 3 ПРИЛАГАНЕ НА ОРЗД ОТ ДЪРЖАВИТЕ ЧЛЕНКИ

#### 3.1 Разпокъсаност на националното прилагане

Макар че ОРЗД е пряко приложим, тъй като е регламент, в него се изисква държавите членки да приемат закони в определени области и им се предоставя възможност да конкретизират допълнително прилагането му в ограничен брой области <sup>(69)</sup>. Когато приемат законодателство на национално равнище държавите членки трябва да го правят при условията и в границите, определени в ОРЗД. Както и през 2020 г. заинтересованите страни съобщават, че срещат трудности, произтичащи от фрагментирането на националните правила, когато държавите членки имат възможност да конкретизират ОРЗД, по-специално по отношение на:

- минималната възраст за съгласието на детето във връзка с предлагането на услугите на информационното общество на това дете <sup>(70)</sup>;
- въвеждането от държавите членки на допълнителни условия относно обработването на генетични данни, биометрични данни или данни за здравословното състояние <sup>(71)</sup>;
- обработването на лични данни, свързани с присъди и нарушения <sup>(72)</sup>, което създава трудности в определени регулирани сектори.

Същевременно е важно, че много заинтересовани страни съобщават, че проблемите с фрагментирането възникват главно от различни тълкувания на ОРЗД от органите за защита на данните, а не от използването от страна на държавите членки на незадължителни клаузи за спецификацията.

Държавите членки считат, че ограничена степен на фрагментиране може да бъде приемлива и предоставените в ОРЗД клаузи за спецификацията продължават да са полезни, по-специално за обработването от публични органи <sup>(73)</sup>. Съгласно ОРЗД при изготвянето на законодателство, което се отнася до обработването на лични данни <sup>(74)</sup>, от държавите членки се изисква да се консултират с националния си орган за защита на данните. В доклада на FRA се установява, че някои правителства поставят много кратки срокове за тези органи, а в някои случаи изобщо не се консултират с тях <sup>(75)</sup>.

#### 3.2 Извършване на наблюдение от страна на Комисията

Комисията извършва постоянно наблюдение на прилагането на ОРЗД. Комисията стартира процедури за нарушение срещу държави членки по въпроси като независимостта на органите за защита на данните (включително независимост от външно влияние и наличието на средства за правна защита в случай на оставяне без разглеждане) <sup>(76)</sup> и правото на ефективни средства за правна защита за субекти на данни, когато органът за защита на данните не разглежда жалбата <sup>(77)</sup>. Като част от извършването от нея наблюдение Комисията изисква от органите за защита на

---

<sup>(69)</sup> например минималната възраст за съгласието на детето във връзка с услугите на информационното общество (член 8, параграф 1 от ОРЗД).

<sup>(70)</sup> Член 8, параграф 1 от ОРЗД.

<sup>(71)</sup> Възможност, предвидена в член 9, параграф 4 от ОРЗД.

<sup>(72)</sup> Член 10 от ОРЗД.

<sup>(73)</sup> Позиция и констатации на Съвета, точка 30.

<sup>(74)</sup> Член 36 от ОРЗД.

<sup>(75)</sup> Доклад на FRA, стр. 11.

<sup>(76)</sup> Белгия (2021/4045) и Белгия (2022/2160).

<sup>(77)</sup> Финландия (2022/4010) и Швеция (2022/2022).

данните да предоставят редовно информация, на строго поверителна основа <sup>(78)</sup>, относно текущи широкомащабни трансгранични случаи, по-специално тези, засягащи големи технологични мултинационални дружества.

Комисията редовно обменя информация с държавите членки относно прилагането на ОРЗД. Както бе посочено в доклада от 2020 г., Комисията продължи да използва експертната група на държавите членки по ОРЗД <sup>(79)</sup> за улесняване на дискусиите и споделянето на опит относно ефективното прилагане на ОРЗД. Експертната група проведе конкретни дискусии по: i) надзора на съдилищата при изпълнение на съдебните им функции (член 55 от ОРЗД; член 8 от Хартата); ii) съгласуването на правото на защита на данните с правото на свобода на изразяване (член 85 от ОРЗД); и iii) правото на ефективна съдебна защита срещу надзорен орган (член 78 от ОРЗД). След тези обсъждания Комисията състави прегледи на възприетите в държавите членки подходи за прилагането на тези разпоредби <sup>(80)</sup>. Комисията използва тази група и за обмен на мнения с държавите членки при изготвянето на предложението относно процедурните правила.

Съответствието на националното законодателство и практика с правилата за защита на данните, определени в съвкупността от правото на ЕС относно Шенгенското пространство, също се оценява като част от оценките по Шенген, провеждани съвместно от държавите членки и Комисията. Всяка година се извършват най-малко пет оценки на място за защита на данните, като понастоящем се поставя акцент върху широкомащабни информационни системи и Шенгенската информационна система, Визовата информационна система, както и върху надзорната роля на националните органи за защита на данните върху тези системи.

Комисията активно допринася за големия брой дела пред Съда (с около 30 преюдициални заключения годишно през последните години), които играят централна роля в последователното тълкуване на ключови понятия на ОРЗД. В увеличаващата се съдебна практика на Съда са предоставени няколко разяснения, като например относно определенията за лични данни <sup>(81)</sup>, специални категории лични данни <sup>(82)</sup>, администратор <sup>(83)</sup>, съгласие <sup>(84)</sup>, законен интерес <sup>(85)</sup>, право на достъп <sup>(86)</sup>, право на изтриване <sup>(87)</sup>, право на обезщетение <sup>(88)</sup>, автоматизирано вземане на индивидуални решения <sup>(89)</sup>, административни наказания „глоба“ или „имуществена санкция“ <sup>(90)</sup>, длъжностни лица по защита на данните <sup>(91)</sup>,

---

<sup>(78)</sup> С информация за препратката към случая, вида на разследването (по собствена инициатива или въз основа на жалба), обобщение на обхвата на разследването, съответните органи за защита на данните, предприетите ключови процедурни стъпки и дати, предприетите разследващи или всякакви други мерки и дати.

<sup>(79)</sup> <https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=bg&do=groupDetail.groupDetail&groupID=3461>

<sup>(80)</sup> <https://ec.europa.eu/transparency/expert-groups-register/screen/meetings/consult?lang=en&meetingId=31754&fromExpertGroups=3461>

<sup>(81)</sup> Дело C-319/22, ECLI:EU:C:2023:837.

<sup>(82)</sup> Дела C-184/20, ECLI:EU:C:2022:601; C-252/21, ECLI:EU:C:2023:537.

<sup>(83)</sup> Дела C-683/21, ECLI:EU:C:2023:949; C-604/22, ECLI:EU:C:2024:214; C-231/22, ECLI:EU:C:2024:7.

<sup>(84)</sup> Дело C-61/19, ECLI:EU:C:2020:901.

<sup>(85)</sup> Дела C-597/19, ECLI:EU:C:2021:492; C-252/21, ECLI:EU:C:2023:537.

<sup>(86)</sup> Дела C-307/22, ECLI:EU:C:2023:811; C-154/21, ECLI:EU:C:2023:3.

<sup>(87)</sup> Дело C-460/20, ECLI:EU:C:2022:962.

<sup>(88)</sup> Дело C-300/21, ECLI:EU:C:2023:370; Дело C-687/21, ECLI:EU:C:2024:72; Дело C-667/21, ECLI:EU:C:2023:1022.

<sup>(89)</sup> Съединени дела C-26/22 и C-64/22, ECLI:EU:C:2023:958.

<sup>(90)</sup> Дела C-807/21, ECLI:EU:C:2023:950; Дело C-683/21, ECLI:EU:C:2023:949.

<sup>(91)</sup> Дело C-453/21, ECLI:EU:C:2023:79.

публикуване на лични данни в регистри <sup>(92)</sup> и прилагане на ОРЗД към дейностите на парламентите <sup>(93)</sup>.

#### 4 ПРАВА НА СУБЕКТИТЕ НА ДАННИ

*Осведоменост на физическите лица относно ОРЗД и органите за защита на данните (проучване на Евробарометър № 549 от 2024 г. относно правосъдието, правата и ценностите)*

- 72 % от анкетираните в ЕС посочват, че са чували за ОРЗД, включително 40 %, които знаят какво представлява.
- В 19 държави членки повече от 70 % от анкетираните посочват, че са запознати с ОРЗД, като анкетираните в Швеция (92 %) са най-запознати, следвани от Нидерландия (88 %), Малта и Дания (84 %), докато анкетираните в България (59 %) са най-малко запознати, следвани от Литва (63 %) и Франция (64 %).
- 68 % от респондентите в ЕС посочват, че са чували за национален орган, който отговаря за защитата на техните права на защита на данните, като 24 % от всички анкетиранци заявяват, че знаят и кой публичен орган е отговорен.
- Във всички държави членки най-малко половината от анкетираните са чували за такъв национален орган, като най-високи са процентите в Нидерландия (82 %), Чехия, Словения и Полша (всичките по 75 %) и Португалия (74 %). Анкетираните в Австрия (56 %) и Испания (58 %) са най-слабо запознати с този орган.

Физическите лица са все по-запознати с правата си съгласно ОРЗД и все по-активно ги упражняват <sup>(94)</sup>. Органите за защита на данните отделят значителни ресурси за повишаване на осведомеността за правата и задълженията за защита на данните сред широката общественост, като например чрез социални медии и телевизионни кампании, линии за помощ, бюлетини и представяния в образователни институции <sup>(95)</sup>. При много от тези инициативи е използвано финансиране от ЕС <sup>(96)</sup>. Агенцията на Европейския съюз за основните права отбелязва, че макар осведомеността за защитата на данните сред широката общественост да се е повишила, разбирането на защитата на данните все още липсва, както се вижда от големия брой маловажни или неоснователни жалби <sup>(97)</sup>. Разработени са няколко удобни за потребителя цифрови инструменти, чиято цел е да улеснят субектите на данни при упражняване на правата им <sup>(98)</sup>. Законодателните актове, най-вече Акът за управление на данните <sup>(99)</sup>, следва да доведат до създаването на допълнителни начини субектът на данни да упражнява правата си в бъдеще. Предприятията отбелязват, че правото на изтриване се използва все по-често, докато правото на коригиране и правото на възражение се прилагат рядко.

<sup>(92)</sup> Дела С-439/19, ECLI:EU:C:2021:504; С-184/20, ECLI:EU:C:2022:601.

<sup>(93)</sup> Дела С-33/22, ECLI:EU:C:2024:46; С-272/19, ECLI:EU:C:2020:535.

<sup>(94)</sup> Позиция и констатации на Съвета, точка 13.

<sup>(95)</sup> Принос на Комитета, раздел 6.

<sup>(96)</sup> [https://commission.europa.eu/law/law-topic/data-protection/eu-funding-supporting-implementation-general-data-protection-regulation-gdpr\\_en?prefLang=bg](https://commission.europa.eu/law/law-topic/data-protection/eu-funding-supporting-implementation-general-data-protection-regulation-gdpr_en?prefLang=bg)

<sup>(97)</sup> Доклад на FRA, стр. 9 и 48.

<sup>(98)</sup> Обобщение на обратната информация от Многостранната група на заинтересованите страни по въпросите на ОРЗД.

<sup>(99)</sup> Член 10 от Регламент (ЕС) 2022/868 (Акт за управление на данните), ОВ L 152, 3.6.2022 г., стр. 1—44.



## 4.1 Правото на достъп

Администраторите докладват, че правото на достъп (член 15 от ОРЗД) е най-често посочваното право от субектите на данни. Макар че през 2022 г. Комитетът прие насоки относно това право, администраторите продължават да съобщават за предизвикателства, например при тълкуване на понятието „неоснователни или прекомерни искания“<sup>(100)</sup>, когато отговарят на голям брой искания и когато се занимават с искания, отправени за цели, които не са свързани със защитата на данните, например за събиране на доказателства за съдебно производство<sup>(101)</sup>. Организациите на гражданското общество отбелязват, че отговорите на исканията за достъп често са забавени или непълни, а получените данни невинаги са в четим формат<sup>(102)</sup>. Публичните органи посочват трудности при взаимодействието между правото на достъп и правилата за публичен достъп до документи<sup>(103)</sup>. Поради това стартирането през февруари 2024 г. от Комитета на координирано съвместно действие по рамката за правоприлагане относно правото на достъп е прието положително<sup>(104)</sup>.

## 4.2 Правото на преносимост

В доклада от 2020 г. Комисията се ангажира да проучи практически начини за улесняване на по-широкото използване на правото на преносимост (член 20 от ОРЗД) от страна на физическите лица в съответствие със стратегията за данните. Оттогава насам Комисията прие редица инициативи, които допълват това право. С тези инициативи се улеснява лесното превключване между услугите, като по този начин се създава по-голям избор за физическите лица, подкрепят се конкуренцията и иновациите и се предоставя възможност на физическите лица да се възползват от предимствата от използването на техните данни. С Акта за данните на потребителите на интелигентни устройства се предоставя разширено право на преносимост на генерирани чрез такива устройства данни, като им се предоставя правомощие, с което дизайнът на продукта или сървър за данни и функционална логика на производителя или притежателя на данни прави такава преносимост технически възможна. Съгласно Акта за цифровите пазари от доставчиците на основни платформени услуги, идентифицирани като „контролиращи достъпа предприятия“, се изисква да осигурят ефективна преносимост на данните на потребителите, включително непрекъснат достъп в реално време до такива данни. Няколко други инициативи на Комисията, които в момента са в процес на преговори или по които е постигнато политическо споразумение, предвиждат подобрени права за преносимост в конкретни области, като например Директивата за работа през

---

<sup>(100)</sup> Член 12, параграф 5 от ОРЗД.

<sup>(101)</sup> Въпреки това Съдът изясни, че субектът на данните не е длъжен да посочва причините за искане на достъп до лични данни: дело C-307/22, ECLI:EU:C:2023:811, т. 38.

<sup>(102)</sup> Обобщение на обратната информация от Многостранната група на заинтересованите страни по въпросите на ОРЗД.

<sup>(103)</sup> Позиция и констатации на Съвета, точки 27—28.

<sup>(104)</sup> [https://www.edpb.europa.eu/news/news/2024/cef-2024-launch-coordinated-enforcement-right-access\\_bg](https://www.edpb.europa.eu/news/news/2024/cef-2024-launch-coordinated-enforcement-right-access_bg)

платформа<sup>(105)</sup>, Европейското пространство на здравни данни<sup>(106)</sup> и рамката за достъп до финансови данни<sup>(107)</sup>.

### 4.3 Правото на подаване на жалба

Както се вижда от големия брой жалби, е налице широка осведоменост за правото на подаване на жалба до орган за защита на данните. Организацията на гражданското общество подчертават неоправданите различия в националните практики за разглеждане на жалби, проблем, който се разглежда в предложението на Комисията относно процедурните правила. Малко държави членки са упражнили възможността съгласно ОРЗД да предоставят на организация с нестопанска цел правото да предприема действия, независимо от възложения от субекта на данни мандат (член 80, параграф 2). Въпреки това приетата през 2020 г. Директива относно представителни иски<sup>(108)</sup> ще доведе до по-голямо хармонизиране в това отношение чрез улесняване на подаването на колективни иски от физически лица за нарушение на ОРЗД. Националните мерки за прилагане на директивата започнаха да се прилагат през юни 2023 г.

### 4.4 Защита на личните данни на децата

Децата се нуждаят от специална защита при обработването на личните им данни<sup>(109)</sup>. ОРЗД е част от всеобхватна правна рамка, с която се гарантира, че децата са защитени офлайн, както и онлайн<sup>(110)</sup>. Като се има предвид повишеното присъствие на деца онлайн, през последните години бяха предприети редица действия на европейско и национално равнище в подкрепа на защитата на децата онлайн. Органите за защита на данните наложиха значителни глоби на дружествата в областта на социалните медии за нарушаване на ОРЗД при обработването на данни на деца. Те си сътрудничат и с други органи, за да призоват за по-голяма защита на децата в областта на рекламата. В доклада от 2020 г. Комисията прикани Комитета да приеме насоки относно обработването на данните на деца и понастоящем тази дейност е в ход<sup>(111)</sup>. Актът за цифровите услуги включва конкретни разпоредби за гарантиране на високо равнище на поверителност, безопасност и сигурност на децата, използващи онлайн платформи.

Някои заинтересовани страни съобщават за предизвикателства при упражняването на правата на субектите на данни, когато субектите на данни са деца. По-специално те съобщават, че децата не разбират напълно правата си, нямат умения за цифрова грамотност и могат да бъдат обект на неправомерно влияние<sup>(112)</sup>. Комисията

---

<sup>(105)</sup> [Работници през платформа: Съветът потвърждава споразумението за нови правила за подобряване на условията на труд — Consilium \(europa.eu\)](#).

<sup>(106)</sup> Предложение за Регламент относно европейското пространство на здравни данни (COM(2022) 197 final).

<sup>(107)</sup> Предложение за Регламент относно нормативната уредба на достъпа до финансови данни и за изменение на регламенти (ЕС) № 1093/2010, (ЕС) № 1094/2010, (ЕС) № 1095/2010 и (ЕС) 2022/2554 (COM(2023) 360 final).

<sup>(108)</sup> Директива (ЕС) 2020/1828 от 25 ноември 2020 г. относно представителни иски за защита на колективните интереси на потребителите и за отмяна на Директива 2009/22/ЕО, ОВ L 409, 4.12.2020 г., стр. 1—27.

<sup>(109)</sup> Съображение 38 от ОРЗД.

<sup>(110)</sup> Препоръка относно разработването и укрепването на интегрирани системи за закрила на детето във висшия интерес на детето [https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/rights-child/combating-violence-against-children-and-ensuring-child-protection\\_bg](https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/rights-child/combating-violence-against-children-and-ensuring-child-protection_bg).

<sup>(111)</sup> Вж. също позиция и констатации на Съвета, точка 31, буква а).

<sup>(112)</sup> Обобщение на обратната информация от Многостранната група на заинтересованите страни по въпросите на ОРЗД.

финансира няколко инициативи на национално равнище за защита на данните на децата и за насърчаване на осведомеността на децата относно защитата на данните<sup>(113)</sup>. Съгласно стратегията за по-добър интернет за децата (VIK+) Комисията предоставя ресурси за повишаване на осведомеността и обучения на децата относно техните цифрови права, включително защита на данните (например цифрово съгласие)<sup>(114)</sup>. Все по-голям акцент се поставя върху необходимостта от ефективни и благоприятни за неприкосновеността на личния живот инструменти за проверка на възрастта. В началото на 2024 г. Комисията създаде работна група по въпросите на проверката на възрастта заедно с държавите членки, Комитета и Групата на европейските регулатори за аудио-визуални медийни услуги, с цел да се обсъди и подкрепи разработването на рамка и подход за проверка на възрастта за целия ЕС. Тази работа ще продължи съгласно Акта за цифровите услуги в рамките на работната група за защита на малолетните и непълнолетните лица. В контекста на Регламента на ЕС за цифровата самоличност<sup>(115)</sup>, който влезе в сила през май 2024 г., Комисията работи, за да гарантира, че европейският портфейл за цифрова самоличност се предлага на всички граждани на ЕС и пребиваващи в ЕС лица през 2026 г., включително за проверка на възрастта. Междувременно, преди екосистемата на портфейла да започне да функционира пълноценно, ще бъде разработено краткосрочно решение за проверка на възрастта, което ще стане достъпно в целия ЕС.

## **5 ВЪЗМОЖНОСТИ И ПРЕДИЗВИКАТЕЛСТВА ЗА ОРГАНИЗАЦИИ, ПО-СПЕЦИАЛНО МСП**

С ОРЗД бяха създадени еднакви условия на конкуренция за предприятията, работещи на вътрешния пазар, а неговият технологично неутрален и благоприятен за иновациите подход позволява на предприятията да намалят бюрокрацията и да се ползват от по-голямо доверие сред потребителите<sup>(116)</sup>. Много предприятия са развили вътрешна култура на защита на данните и приемат неприкосновеността на личния живот и защитата на данните като на ключови параметри на конкуренцията. Предприятията оценяват основания на риска подход на ОРЗД като водещ принцип, предоставящ възможност за гъвкавост и увеличаване на мащаба на техните задължения<sup>(117)</sup>.

### **5.1 Инструментариум за предприятията**

ОРЗД предоставя инструментариум, които дават възможност на организациите да бъдат гъвкави в управлението и да покажат, че спазват изискванията, включително кодексите за поведение, механизмите за сертифициране и стандартните договорни клаузи. Както беше обявено в доклада от 2020 г., през 2021 г. Комисията прие

---

<sup>(113)</sup> [https://commission.europa.eu/law/law-topic/data-protection/eu-funding-supporting-implementation-general-data-protection-regulation-gdpr\\_en?prefLang=bg](https://commission.europa.eu/law/law-topic/data-protection/eu-funding-supporting-implementation-general-data-protection-regulation-gdpr_en?prefLang=bg).

<sup>(114)</sup> <https://digital-strategy.ec.europa.eu/bg/policies/strategy-better-internet-kids>

<sup>(115)</sup> Регламент (ЕС) 2024/1183 за изменение на Регламент (ЕС) № 910/2014 по отношение на създаването на европейска рамка за цифрова самоличност, ОВ L, 2024/1183, 30.4.2024 г.

<sup>(116)</sup> Както се признава в доклада за платформата „Готови за бъдещето“ — експертна група на високо равнище, създадена, за да помогне на Комисията в нейните усилия да опрости законите на ЕС и да намали свързаните с това ненужни разходи: [https://commission.europa.eu/law/law-making-process/evaluating-and-improving-existing-laws/refit-making-eu-law-simpler-less-costly-and-future-proof/fit-future-platform-f4f\\_bg](https://commission.europa.eu/law/law-making-process/evaluating-and-improving-existing-laws/refit-making-eu-law-simpler-less-costly-and-future-proof/fit-future-platform-f4f_bg). Вж. също обобщението на обратната информация от Многостранната група на заинтересованите страни по въпросите на ОРЗД и позицията и констатациите на Съвета, точка 12.

<sup>(117)</sup> Обобщение на обратната информация от Многостранната група на заинтересованите страни по въпросите на ОРЗД.

стандартни договорни клаузи за отношенията между администратора и обработващия лични данни <sup>(118)</sup>. Тези стандартни договорни клаузи предоставят готов и лесен за изпълнение инструмент за доброволно спазване на изискванията, който е особено полезен за МСП или организации, които може да не разполагат с ресурсите да договарят индивидуални договори със своите търговски партньори. Предприятията съобщават смесена обратна информация относно използването на стандартните договорни клаузи, което означава, че някои дружества (главно МСП) ги използват изцяло или частично, докато други (предимно по-големи дружества) са склонни да не ги използват, защото предпочитат да използват свои собствени клаузи.

Предприятията подчертават, че кодексите за поведение притежават голям потенциал като специфичен за сектора и рентабилен инструмент за спазване на изискванията <sup>(119)</sup>. Разработването на кодекси за поведение обаче е ограничено <sup>(120)</sup>. Според наличната към днешна дата информация в целия ЕС са одобрени само два кодекса (и двата в сектора на изчислителния облак), докато на национално равнище са одобрени шест кодекса <sup>(121)</sup>. Като основни фактори, ограничаващи възприемането на кодексите за поведение, заинтересованите страни съобщават утежняващите изисквания (включително необходимостта от създаване на акредитиран орган за наблюдение), липсата на ангажираност от страна на органите за защита на данните и дългия процес на одобрение <sup>(122)</sup>.

Необходими са по-голяма прозрачност на процеса и ясни срокове за одобрение. Органите за защита на данните и, в случай на кодекси за целия ЕС — Комитетът, следва по-активно да насърчават изготвянето на кодекси за поведение, като си сътрудничат с асоциациите, разработващи кодексите. Това ще спомогне за разрешаване на разликите в тълкуването и за ускоряване на процеса на одобрение. Заинтересованите страни изразяват съжаление за дългите забавяния в приемането на кодексите за поведение, причинени от въпроси, обсъждани паралелно като част от работата по насоките. Предприятията съобщават и че сертифицирането не се използва широко, тъй като процесът на развитие е бавен и сложен. Както при кодексите за поведение, органите за защита на данните следва да предоставят по-ясни срокове за преглед и одобрение на сертификатите.

В стратегията си за периода 2024—2027 г. Комитетът се е ангажирал да продължи да подкрепя мерките за спазване на изискванията като сертифициране и кодекси за поведение, включително чрез работа с ключови групи заинтересовани страни, за да поясни как могат да се използват инструментите <sup>(123)</sup>.

## 5.2 Специфични промени за МСП и малките оператори

В доклада от 2020 г. Комисията призова за засилване на усилията в подкрепа на спазването на ОРЗД от страна на МСП. През последните години органите за защита

---

<sup>(118)</sup> Решение за изпълнение (ЕС) 2021/915 на Комисията от 4 юни 2021 г. относно стандартни договорни клаузи между администратори и обработващи лични данни съгласно член 28, параграф 7 от ОРЗД и член 29, параграф 7 от ОРЗД (C/2021/3701) — ОВ L 199, 7.6.2021, стр. 18—30.

<sup>(119)</sup> Обобщение на обратната информация от Многостранната група на заинтересованите страни по въпросите на ОРЗД.

<sup>(120)</sup> Позиция и констатации на Съвета, точка 25.

<sup>(121)</sup> [https://www.edpb.europa.eu/our-work-tools/accountability-tools/register-codes-conduct-amendments-and-extensions-art-4011\\_bg?f%5B0%5D=coc\\_scope%3Anational](https://www.edpb.europa.eu/our-work-tools/accountability-tools/register-codes-conduct-amendments-and-extensions-art-4011_bg?f%5B0%5D=coc_scope%3Anational)

<sup>(122)</sup> Обобщение на обратната информация от Многостранната група на заинтересованите страни по въпросите на ОРЗД.

<sup>(123)</sup> [https://www.edpb.europa.eu/system/files/2024-04/edpb\\_strategy\\_2024-2027\\_en.pdf](https://www.edpb.europa.eu/system/files/2024-04/edpb_strategy_2024-2027_en.pdf)

на данните и Комитета продължиха да разработват инструменти за спазване на изискванията за МСП, като бяха отчасти подпомогнати с финансиране от Комисията <sup>(124)</sup>. През април 2023 г. Комитетът стартира ръководство за защита на данните за малки предприятия <sup>(125)</sup>, в което се предоставя практическа информация за МСП в достъпен и лесно разбираем формат.

МСП в много държави членки подчертават ползите от съобразена с нуждите им подкрепа от страна на техните местни органи за защита на данните. Различните подходи за повишаване на осведомеността и насоки от страна на органите за защита на данните обаче означават, че в определени държави членки МСП възприемат спазването на изискванията като сложно и имат опасения във връзка с правоприлагането <sup>(126)</sup>. Органите за защита на данните следва да удвоят усилията си за справяне с тези предизвикателства, включително чрез проактивна работа с МСП, за да разсеят всички неоснователни опасения относно спазването на изискванията. Органите за защита на данните следва да се съсредоточат върху предоставянето на съобразена с нуждите подкрепа и практически инструменти, като образци (например за извършване на оценки на въздействието върху защитата на данните), горещи телефонни линии, нагледни примери, контролни списъци и насоки за специфични операции по обработване (например фактуриране или бюлетини) и технически и организационни мерки. Тъй като повечето МСП не разполагат с лица с квалификация по защита на данните на равнището на предприятието, всички предназначени за МСП насоки следва да се разбират лесно от лица без юридическо обучение <sup>(127)</sup>.

В съответствие с основания на риска подход на ОРЗД, МСП, извършващи дейности по обработване с нисък риск, не носят значителна тежест за спазване на изискванията. Макар че дерогацията за запазване на записи на дейностите по обработване <sup>(128)</sup> се прилага при ограничени обстоятелства <sup>(129)</sup>, МСП, извършващи обработване с нисък риск, могат да се съобразят, като поддържат опростени записи въз основа на образци, предоставени от органите за защита на данните. Освен това подобни записи следва да се разглеждат като полезен инструмент за МСП при преразглеждането на дейностите им по обработване.

### 5.3 Длъжностни лица по защита на данните

Длъжностните лица по защита на данните играят важна роля при гарантиране на спазването на ОРЗД в рамките на организациите, в които работят. По принцип всички длъжностните лица по защита на данните, извършващи дейност в ЕС, притежават необходимите знания и умения, за да изпълнят задачите си съгласно

---

<sup>(124)</sup> [https://commission.europa.eu/law/law-topic/data-protection/eu-funding-supporting-implementation-general-data-protection-regulation-gdpr\\_en?prefLang=bg](https://commission.europa.eu/law/law-topic/data-protection/eu-funding-supporting-implementation-general-data-protection-regulation-gdpr_en?prefLang=bg)

<sup>(125)</sup> [https://edpb.europa.eu/sme-data-protection-guide/home\\_en](https://edpb.europa.eu/sme-data-protection-guide/home_en)

<sup>(126)</sup> Обобщение на обратната информация от Многостранната група на заинтересованите страни по въпросите на ОРЗД.

<sup>(127)</sup> Вж. позиция и констатации на Съвета, точка 24; обобщение на обратната информация от Многостранната група на заинтересованите страни по въпросите на ОРЗД.

<sup>(128)</sup> Член 30, параграф 5 от ОРЗД.

<sup>(129)</sup> Когато в организацията работят по-малко от 250 души, освен ако извършването от нея обработване има вероятност да доведе до риск за правата и свободите на субектите на данни, обработването не е случайно или включва специални категории данни, както е посочено в член 9, параграф 1 от ОРЗД, или лични данни, свързани с присъди и нарушения, посочени в член 10 от ОРЗД.



ОРЗД и тяхната независимост се зачита<sup>(130)</sup>. Все още са налице обаче няколко предизвикателства, включително: i) трудности при назначаването на длъжностни лица по защита на данните с необходимите експертни познания; ii) липса на общоевропейски стандарти за образование и обучение; iii) липса на адекватно включване на длъжностните лица по защита на данните в организационните процеси; iv) липса на ресурси; v) допълнителни задачи извън защитата на данните; и vi) недостатъчно старшинство на една и съща длъжност<sup>(131)</sup>. Комитетът отбеляза, че органите за защита на данните трябва да ускорят дейностите за повишаване на осведомеността, както и своите информационни и правоприлагащи действия, за да гарантират, че длъжностните лица по защита на данните могат да изпълняват ролята си съгласно ОРЗД<sup>(132)</sup>.

## **6 ОРЗД КАТО КРАЙЪГЪЛЕН КАМЪК НА ПОЛИТИКАТА НА ЕС В ЦИФРОВАТА СФЕРА**

### **6.1 Изграждане на цифрова политика въз основа на ОРЗД**

В доклада от 2020 г. Комисията се ангажира да подкрепи последователното прилагане на рамката за защита на данните по отношение на новите технологии, за да спомага за иновациите и технологичното развитие. Оттогава насам ЕС прие набор от инициативи, някои от които допълват ОРЗД или уточняват начина, по който следва да се прилага в конкретни области, за да се преследват определени цели, както е представено по-долу.

- С Акта за цифровите услуги<sup>(133)</sup>, чиято цел е да се осигури безопасна онлайн среда за физическите лица и предприятията, се въвежда забрана за онлайн платформите да представят реклами въз основа на профилиране, при което се използват „специални категории лични данни“, както е определено в ОРЗД.
- С цел цифровите пазари да станат по-справедливи и по-достъпни с Акта за цифровите пазари<sup>(134)</sup> на определените като „контролиращи достъпа предприятия“ оператори се забранява „съчетаването“ и „кръстосаното използване“ на лични данни между техните основни платформени услуги и други услуги, освен ако потребителят не е предоставил своето съгласие, както е определено в ОРЗД.
- В Законодателния акт за изкуствения интелект<sup>(135)</sup> се уточняват правилата на ЕС за защита на данните в конкретни области, в които се използва ИИ, например в системи за дистанционна биометрична идентификация, обработването на специални категории данни за откриване на предубеждения и по-нататъшното обработване на лични данни в регулаторни лаборатории.
- С Директивата за работа през платформа<sup>(136)</sup> се допълва ОРЗД в областта на заетостта, като се определят правила относно системите за автоматизирано

---

<sup>(130)</sup> Позиция и констатации на Съвета, точка 26; Определяне на координирано действие по правоприлагане на ЕКЗД за 2023 г. и позиция на длъжностните лица по защита на данните: [https://www.edpb.europa.eu/system/files/2024-01/edpb\\_report\\_20240116\\_cef\\_dpo\\_en.pdf](https://www.edpb.europa.eu/system/files/2024-01/edpb_report_20240116_cef_dpo_en.pdf)

<sup>(131)</sup> Обобщение на обратната информация от Многостранната група на заинтересованите страни по въпросите на ОРЗД.

<sup>(132)</sup> Вж. препоръки при координирано действие по правоприлагане на ЕКЗД.

<sup>(133)</sup> Регламент (ЕС) 2022/2065 на Европейския парламент и на Съвета от 19 октомври 2022 г. относно единния пазар на цифрови услуги и за изменение на Директива 2000/31/ЕО (Акт за цифровите услуги), ОВ L 277, 27.10.2022 г., стр. 1—102.

<sup>(134)</sup> Регламент (ЕС) 2022/1925 (Акт за цифровите пазари), ОВ L 265, 12.10.2022 г., стр. 1—66.

<sup>(135)</sup> Регламент (ЕС) 2024/1689 (Акт за изкуствения интелект), ОВ L, 2024/1689, 12.7.2024 г.

<sup>(136)</sup> [Работници през платформа: Съветът потвърждава споразумението за нови правила за подобряване на техните условия на труд — Consilium \(europa.eu\).](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024L0168)



наблюдение и вземане на решения, използвани от цифрови трудови платформи, и по-специално ограниченията върху обработването на лични данни, прозрачност, човешки надзор и преразглеждане и преносимост.

- В Регламента за политическото рекламиране <sup>(137)</sup> се забранява употребата на специални категории лични данни при политическа реклама и се изисква по-голяма прозрачност относно техниките за таргетиране или усилено разпространение.
- С Регламента за европейската цифрова самоличност се предоставя възможност за създаването на универсален, надежден и сигурен европейски портфейл за цифрова самоличност. Това ще позволи на лицата да доказват лични атрибути като възраст, шофьорска книжка, дипломи и банкови сметки, като запазват пълен контрол върху личните си данни и без ненужното им споделяне.

Предложението за Регламент за неприкосновеността на личния живот в сектора на електронните съобщения <sup>(138)</sup>, с който да се замени настоящата Директива за право на неприкосновеност на личния живот и електронни комуникации и да се допълни законодателната рамка в областта на неприкосновеността на личния живот и защитата на данните <sup>(139)</sup>, са в процес на водене на преговори от няколко години. Необходимо е да се обмислят следващите етапи за тази инициатива, включително връзката ѝ с ОРЗД.

С Акта за оперативно съвместима Европа <sup>(140)</sup> се цели постигането на оперативна съвместимост на цифровите обществени услуги в ЕС. С него се подкрепя сътрудничеството между органите за защита на данните, по-специално чрез регулаторни лаборатории за оперативна съвместимост.

Няколко инициативи на ЕС предоставят правно основание за обработването на лични данни от частни субекти за предотвратяване, разследване, разкриване или наказателно преследване на престъпления. Всяко подобно законодателство трябва да бъде внимателно насочено към свеждане до минимум на намесата в правото на защита на личните данни и трябва да бъде пропорционално на преследваната цел <sup>(141)</sup>. Хартата, ОРЗД и съдебната практика на Съда предоставят рамка, спрямо която следва да се измерват тези инициативи. В предложения пакет за борба с изпирането на пари <sup>(142)</sup> се съдържат съществени гаранции за защита на личните данни, без да се компрометира целта за смекчаване на рисковете от изпиране на пари и финансиране на тероризма и ефективното разкриване на престъпни опити за злоупотреба с финансовата система на ЕС.

В този контекст Съветът подчерта, че всяко ново законодателство на ЕС, съдържащо разпоредби относно обработването на лични данни, следва да бъде в съответствие с ОРЗД и съдебната практика на Съда.

---

<sup>(137)</sup> Регламент (ЕС) 2024/900 относно прозрачността и таргетирането на политическото рекламиране, ОВ L, 2024/900, 20.3.2024 г.

<sup>(138)</sup> Предложение за Регламент за неприкосновеността на личния живот и електронните съобщения — COM/2017/010 final.

<sup>(139)</sup> Директива 2002/58/ЕО (Директива за правото на неприкосновеност на личния живот и електронни комуникации) — ОВ L 201, 31/07/2002 P. 0037 — 0047

<sup>(140)</sup> Регламент (ЕС) 2024/903 (Акт за оперативно съвместима Европа), ОВ L, 2024/903, 22.3.2024 г.

<sup>(141)</sup> Вж. позиция и констатации на Съвета, точка 31, буква е).

<sup>(142)</sup> [https://finance.ec.europa.eu/publications/anti-money-laundering-and-countermeasures-financing-terrorism-legislative-package\\_bg](https://finance.ec.europa.eu/publications/anti-money-laundering-and-countermeasures-financing-terrorism-legislative-package_bg).

## 6.2 Правна рамка за подобряване на споделянето на данни

Стратегията за данните цели създаването на единен пазар на данни, където потоците от данни ще се движат свободно в рамките на ЕС и между отделните сектори в полза на предприятията, изследователите и публичните администрации. Основна цел на стратегията за данните е създаването на общи европейски пространства на данни, с което се улесняват обединяването, достъпът и споделянето на данни. По отношение на личните данни в ОРЗД се предоставя рамката за всички инициативи, с които се цели подобряване на свободното движение на данни в рамките на ЕС — което само по себе си е цел на ОРЗД. Що се отнася до личните данни, предоставяните съгласно ОРЗД защиты не са засегнати.

Актът за управление на данните<sup>(143)</sup> и Актът за данните<sup>(144)</sup> са стълбове на стратегията за данните. В Акта за управление на данните се определят конкретни правила в контекста на повторното използване на данни от публичния сектор, съдържащи лични данни, установява се законодателна рамка за посреднически услуги за данни — включително услуги за управление на лична информация (PIMS) или изчислителни облаци от лични данни, предлагани с цел да се оправомощат субектите на данни при упражняване на правата си съгласно ОРЗД. В него се посочват и условията за употребата на данни за алтруистични цели. С Акта за данните се засилва контролът на субектите на данни върху данните, които генерират чрез използването на интелигентни обекти, които притежават, наемат или получават по договор за лизинг, като се налагат технически изисквания за достъп и преносимост на данните.

Европейското пространство на здравни данни (ЕПЗД)<sup>(145)</sup> отразява специфичните нужди в сектора на здравните данни, като същевременно се основава на ОРЗД. С него на физическите лица се предоставя възможност да получат лесен достъп до своите здравни данни в електронен формат и да ги споделят със здравни специалисти, включително в други държави членки, като по този начин се подобрява предоставянето на здравни грижи и се увеличава контрола на пациентите върху техните данни. С него също така се въвежда обща правна рамка за повторно използване на здравни данни за цели, като например научни изследвания, иновации и обществено здраве, въз основа на разрешение, издадено от орган за достъп до здравни данни. За да се гарантира защитата на личните данни, ЕПЗД ще предостави надеждна настройка за сигурен достъп и обработка на здравни данни. Комисията продължава да подкрепя работата по разработването на общи европейски пространства на данни в 14 сектора чрез прилагане на новата законодателна рамка и финансиране на специфични за сектора инициативи.

## 6.3 Управление на нови цифрови правила

Разработването на цифрови разпоредби поражда необходимостта от тясно сътрудничество между регулаторните области<sup>(146)</sup>. Такова сътрудничество е още по-необходимо, тъй като въпросите, свързани със защитата на данните, все повече се преплитат с въпроси, свързани например с конкурентното право, потребителското право, правилата за цифровите пазари, регулирането на електронните комуникации

---

<sup>(143)</sup> Регламент (ЕС) 2022/868 (Акт за управление на данните), ОВ L 152, 3.6.2022 г., стр. 1—44.

<sup>(144)</sup> Регламент (ЕУ) 2023/2854 (Акт за данните), ОВ L, 2023/2854, 22.12.2023 г.

<sup>(145)</sup> [https://www.europarl.europa.eu/doceo/document/TA-9-2024-0331\\_BG.html](https://www.europarl.europa.eu/doceo/document/TA-9-2024-0331_BG.html).

<sup>(146)</sup> Вж. позиция и констатации на Съвета, точки 40—41; Обобщение на обратната информация от Многостранната група на заинтересованите страни по въпросите на ОРЗД.

и киберсигурността. Такъв е например случаят при оценката на съвместимостта на моделите „плащане или съгласие“ със законодателството на ЕС.

В някои случаи на органите за защита на данните е възложено да прилагат конкретни разпоредби на новото цифрово законодателство на ЕС <sup>(147)</sup>. С новите цифрови разпоредби се създават и съответстващи на нуждите структури, които обединяват компетентни регулаторни органи с цел да се осигури съгласувано прилагане, като например групата на високо равнище по Акта за цифровите пазари, Европейският комитет за иновации в областта на данните (създаден съгласно Акта за управление на данните) и Европейският съвет за цифровите услуги (създаден съгласно Акта за цифровите услуги). В Директивата за МИС 2 <sup>(148)</sup> се определят по-подробни правила за сътрудничество между регулаторните органи и органите за защита на данните при справяне с киберинциденти, които представляват нарушения на личните данни.

Извън тези официални структури, органите за защита на данните предприемат стъпки, за да гарантират, че техните действия са допълващи се и са съгласувани с други регулаторни области. През юли 2020 г. органите за защита на потребителите и данните създадоха „група от доброволци“, за да определят най-добрите практики и да споделят опит в прилагането. Органите за защита на данните продължават да участват в съвместни семинари с Мрежата за сътрудничество за защита на потребителите. През 2023 г. Комитетът създаде работна група за взаимодействието между защитата на данните, конкуренцията и защитата на потребителите.

Въпреки че тези развия са положителни, има нужда от по-структурирани и ефективни средства за сътрудничество, по-специално за справяне със ситуации, които засягат голям брой лица в ЕС и включват няколко регулаторни органа <sup>(149)</sup>. Всички подобни структури следва да гарантират, че органите продължават да са отговорни по всяко време за всички въпроси, свързани със спазването на правилата в техните области на компетентност. Държавите членки следва да работят и за да гарантират, че се осъществява подходящо сътрудничество на национално равнище <sup>(150)</sup>.

## **7 МЕЖДУНАРОДНО ПРЕДАВАНЕ НА ДАННИ И СЪТРУДНИЧЕСТВО В СВЕТОВЕН МАЩАБ**

### **7.1 Инструментариумът на ОРЗД за предаване на данни**

Потоците от данни са станали неразделна част от цифровата трансформация на обществото и глобализацията на икономиката. Повече от всякога зачитането на неприкосновеността на личния живот е условие за стабилни, сигурни и конкурентни търговски потоци, както и средство за много форми на международно сътрудничество. С предоставения в глава V от ОРЗД инструментариум за предаване на данни се предлага разнообразие от инструменти за справяне с различни сценарии за предаване на данни, като същевременно се гарантира, че данните продължават да се ползват от високо равнище на защита, когато напускат ЕС.

---

<sup>(147)</sup> Вж. например член 37, параграф 3 от Акта за данните.

<sup>(148)</sup> Директива (ЕС) 2022/2555 (Директива МИС 2), ОВ L 333, 27.12.2022, стр. 80—152.

<sup>(149)</sup> Вж. позицията и констатациите на Съвета, точки 18, 40—41 и обобщението на обратната информация от Многостранната група на заинтересованите страни по въпросите на ОРЗД.

<sup>(150)</sup> Германия създаде „цифрова група“, която включва регулаторни органи от различни области с цел разширяване на тяхното сътрудничество по всички аспекти на цифровизацията и споделянето на знания и най-добри практики: <https://www.dataguidance.com/news/germany-bsi-announces-formation-digital-cluster-bonn>

След доклада от 2020 г. изискванията за предаване на данни, посочени в законодателството на ЕС за защита на данните, бяха допълнително пояснени и инструментариумът за предаване на данни продължава да се развива. Важно пояснение се отнася до понятието „международно предаване на данни“, което е определено от Комитета <sup>(151)</sup> като обхващащо всяко оповестяване на лични данни от администратор или обработващ лични данни, чието обработване е обект на ОРЗД за друг администратор или обработващ лични данни в трета държава, независимо от това дали обработването от последния е обект на ОРЗД <sup>(152)</sup>. Тези насоки на Комитета бяха особено важни за осигуряване на правна сигурност на европейските администратори и обработващи лични данни относно сценариите, при които е необходим инструмент за предаване на данни съгласно глава V от ОРЗД.

Допълнителни пояснения бяха предоставени и от Съда в неговото решение по делото *Schrems II* <sup>(153)</sup> относно защитата, която трябва да бъде предоставена от различни инструменти за предаване данни, за да се гарантира, че нивото на защита, осигурено от ОРЗД, не се излага на риск <sup>(154)</sup>. По-специално тези инструменти трябва да гарантират, че физическите лица, чиито данни са предадени извън ЕС, се ползват с ниво на защитата, което по същество е равностойно на гарантираното в ЕС <sup>(155)</sup>. Отговорност на износителя на данни от ЕС е да прецени дали това е така, като вземе предвид специфичните обстоятелства на извършваните от него предавания на данни <sup>(156)</sup>.

За да оценят нивото на защита, износителите на данни трябва да вземат предвид както гаранциите за защита на данните, посочени в инструмента за прехвърляне на данни, сключен с вносител на данни от трета държава (например договор), така и съответните аспекти на правната система на държавата, в която се намира вносителят на данни, по-специално по отношение на възможен достъп до данните от страна на публични органи в тази държава <sup>(157)</sup>. Последните трябва да бъдат оценени с оглед на критериите за оценка на адекватното ниво на защита, посочени в член 45 от ОРЗД. Съдът доразви тези критерии, по-специално по отношение на правилата за достъп до лични данни от страна на публичните органи за целите на правоприлагането и националната сигурност.

Това тълкуване е отразено и в насоките на Комитета, който актуализира своя „референтен справочник за адекватно ниво на защита“ <sup>(158)</sup> (в който се предоставят насоки относно елементите, които Комисията трябва да вземе предвид при извършване на оценка на адекватното ниво на защита). Комитетът прие и нови насоки, с които се предоставят допълнителни разяснения относно: i) елементите, които трябва да се вземат предвид от отделните износители на данни, когато се оценява нивото на защита; ii) прегледа на потенциалните източници, които може да се използват; и iii) примери за възможни допълнителни мерки (например договорни и технически гаранции) <sup>(159)</sup>. В насоките изрично се подчертава, че всяка оценка, извършена от износителите на данни, е уникална, поради което те трябва да вземат предвид специфичните характеристики на всяко предаване на данни, които могат да се различават в зависимост от целта на предаването на данни, видовете участващи

---

<sup>(151)</sup> Насоки 05/2021 на ЕКЗД.

<sup>(152)</sup> Раздел 2 от Насоки 05/2021 на ЕКЗД.

<sup>(153)</sup> Дело C-311/18, ECLI:EU:C:2020:559 (*Schrems II*).

<sup>(154)</sup> *Schrems II*, точка 93.

<sup>(155)</sup> *Schrems II*, точки 96 и 105.

<sup>(156)</sup> *Schrems II*, точка 131.

<sup>(157)</sup> *Schrems II*, точка 105.

<sup>(158)</sup> Препоръки 02/2020 на ЕКЗД и адекватното ниво на защита на личните данни, WP 254 версия 01.

<sup>(159)</sup> Препоръки 01/2020 на ЕКЗД, допълнени от препоръки 02/2020.

субекти, сектора в които се извършва предаването на данни, категориите предадени лични данни и др. <sup>(160)</sup>.

През последните години, предвид тези различни разяснения относно изискванията за международни предавания на данни, бяха предприети значителни стъпки за по-нататъшно развитие и въвеждане в действие на инструментариума на ОРЗД за предаване на данни.

### *7.1.1 Решения относно адекватното ниво на защита*

Както е отразено и в получената от заинтересованите страни обратна информация, решенията относно адекватното ниво на защита продължават да играят ключова роля в инструментариума на ОРЗД за предаване на данни <sup>(161)</sup>, като предоставят директно и всеобхватно решение за предаване на данни, без да е необходимо износителят на данни да предоставя допълнителни гаранции или да получи каквото и да е разрешение. Чрез осигуряването на възможност за свободно движение на лични данни тези решения разкриха търговски канали за операторите от ЕС, включително като допълниха и увеличиха ползите от търговските споразумения, и улесниха сътрудничеството с чуждестранни партньори в широк кръг от области — от регулаторно сътрудничество до научни изследвания.

След доклада от 2020 г. продължава да расте броят на държавите, които са въвели модерни закони за защита на данните, с които се осигуряват, наред с другото, основни принципи за защита на данните, индивидуални права и ефективно правоприлагане от страна на независими регулатори. Тази тенденция <sup>(162)</sup> позволи на Комисията също така да засили работата си по адекватното ниво на защита. Това включва приемането на решение относно адекватното ниво на защита за Обединеното кралство <sup>(163)</sup>, което е от основно значение за гарантиране на правилното функциониране на различните споразумения, сключени с Обединеното кралство след Брексит. За да се гарантира, че остава устойчиво в бъдеще, решението относно адекватното ниво на защита включва „клауза за прекратяване на действието“, която изтича през 2025 г., след което може да бъде подновена, ако нивото на защита продължава да бъде адекватно. Комисията прие решение относно адекватното ниво на защита и във връзка с Република Корея <sup>(164)</sup>, което допълва споразумението за свободна търговия между ЕС и Корея относно потоците от лични данни и улеснява регулаторното сътрудничество. Първият преглед на решението относно адекватното ниво на защита е планиран за края на 2024 г.

Освен това след обявяването за невалидно на решението относно адекватното ниво на защита, стоящо в основата на Щита за личните данни в отношенията между ЕС и САЩ, Комисията започна преговори с правителството на Съединените щати (САЩ) за разработване на последващо споразумение в съответствие с пояснените от Съда изисквания <sup>(165)</sup>. Президентът на САЩ прие нова изпълнителна заповед относно „Enhancing Safeguards for United States Signals Intelligence Activities“ (Засилване на гаранциите за дейностите на САЩ за радиоелектронно разузнаване), с която бяха

---

<sup>(160)</sup> Вж. например т. 8—13, 32—33 от препоръки 01/2020 на ЕКЗД.

<sup>(161)</sup> Вж. например принос на Комитета, стр. 7—8; Позиция и констатации на Съвета, точка 36; Обобщение на обратната информация от Многостранната група на заинтересованите страни по въпросите на ОРЗД.

<sup>(162)</sup> Съобщение за изпълнение на Комисията „Обмен и защита на личните данни в един глобализиран свят“, 10.1.2017 г. (COM(2017) 7 final).

<sup>(163)</sup> Решение за изпълнение (ЕС) 2021/1772 на Комисията, ОВ L 360, 11.10.2021 г., стр. 1—68.

<sup>(164)</sup> Решение за изпълнение (ЕС) 2022/254 на Комисията, ОВ L 44, 24.2.2022 г., стр. 1—90.

<sup>(165)</sup> [https://commission.europa.eu/news/joint-press-statement-european-commissioner-justice-didier-reynders-and-us-secretary-commerce-wilbur-2020-08-10\\_en?prefLang=bg](https://commission.europa.eu/news/joint-press-statement-european-commissioner-justice-didier-reynders-and-us-secretary-commerce-wilbur-2020-08-10_en?prefLang=bg)



въведени нови обвързващи и изпълними гаранции, за да се гарантира, че данните могат да бъдат достъпни за целите на националната сигурност само до степента, която е необходима и пропорционална, и че за европейците са достъпни ефективни средства за правна защита. Въз основа на това Комисията прие решението си относно адекватното ниво на защита на Рамката за защита на личните данни в отношенията между ЕС и САЩ (РЗЛД) <sup>(166)</sup>, с което се позволява свободното предаване на личните данни от ЕС към американските дружества, които се присъединяват към РЗЛД. Тъй като въведените от правителството на САЩ гаранции в областта на националната сигурност се прилагат за всяко предаване на данни към дружества в САЩ, независимо от използвания механизъм на ОРЗД за предаване на данни, използването на други инструменти, като стандартни договорни клаузи и задължителни фирмени правила, е значително улеснено. Първият преглед на функционирането на РЗЛД ще се извърши през лятото на 2024 г., за да се провери дали всички съответни елементи са изцяло въведени в правната рамка на САЩ и дали функционират ефективно на практика.

В момента се водят преговори за адекватно ниво на защита с Бразилия и Кения, както и за първи път с няколко международни организации (в напреднал стадий са например разговорите за адекватното ниво на защита с Европейската патентна организация) <sup>(167)</sup>. В съответствие с призивите и на различни заинтересовани страни <sup>(168)</sup> Комисията се ангажира активно в проучвателни разговори с държави в различни региони на света.

Комисията също така непрекъснато наблюдава събитията в държавите, които вече се ползват от констатациите относно адекватното ниво на защита, и периодично преразглежда съществуващите решения в съответствие със съответните си задължения съгласно ОРЗД <sup>(169)</sup>. През април 2023 г. Комисията прие своя доклад относно първия периодичен преглед на решението относно адекватното ниво на защита за Япония <sup>(170)</sup>, в който се стигна до заключението, че Япония продължава да осигурява адекватно ниво на защита <sup>(171)</sup>. Прегледът показва, че рамките за защита на данните на ЕС и Япония са се сблизили още повече след приемането на решенията относно взаимното адекватно ниво на защита.

Освен това в съответствие с член 97 от ОРЗД първият преглед на 11-те решения относно адекватното ниво на защита <sup>(172)</sup>, приети съгласно предишната рамка на ЕС за защита на данните (Директивата за защита на личните данни), беше започнат като част от оценката на приложението през 2020 г. и функционирането на ОРЗД. Приключването на този аспект от прегледа беше отложено, по-специално за да се вземат предвид решенията на Съда по делото *Schrems II* и последващото тълкуване от Съвета. Горепосочените разяснения на Съда относно основни елементи от

---

<sup>(166)</sup> Решение за изпълнение (ЕС) 2023/1795 на Комисията, ОВ L 231, 20.9.2023 г., стр. 118—229.

<sup>(167)</sup> Европейската патентна конвенция е междуправителствена организация, създадена въз основа на Конвенцията за издаване на европейски патенти. Нейната основна задача е да предоставя европейски патенти. В този контекст тя си сътрудничи тясно с дружества и публични органи в държавите — членки на ЕС, както и с различни институции и органи на ЕС.

<sup>(168)</sup> Принос на Комитета, стр. 7—8.

<sup>(169)</sup> Член 45, параграфи 4 и 5 от ОРЗД. Вж. също *Schrems I*, т. 76.

<sup>(170)</sup> Решение за изпълнение (ЕС) 2019/419 на Комисията, ОВ L 76, 19.3.2019 г., стр. 1—58. Вж. също [https://ec.europa.eu/commission/presscorner/detail/bg/IP\\_19\\_421](https://ec.europa.eu/commission/presscorner/detail/bg/IP_19_421). Това решение представлява първото решение относно адекватното ниво на защита, прието съгласно ОРЗД, и първото взаимно споразумение за адекватно ниво на защита.

<sup>(171)</sup> Доклад на Комисията относно първия преглед на функционирането на решението относно адекватното ниво на защита за Япония, 3.4.2023 г., COM(2023) 275 final (и SWD(2023) 75 final).

<sup>(172)</sup> Андора, Аржентина, Гърнзи, Джърси, Израел, Канада (за търговските оператори), Нова Зеландия, остров Ман, Уругвай, Фарьорските острови, Швейцария.



стандарта за адекватно ниво на защита доведеха до подробен обмен със съответните държави и територии относно съответните аспекти на тяхната правна рамка, както и механизмите за надзор и правоприлагане.

На 15 януари 2024 г. Комисията публикува доклада си относно тези 11 решения, заедно с подробни доклади по държави, в които се описва развитието във всяка от държавите и териториите след приемането на решенията относно адекватното ниво на защита, както и правилата, които се прилагат за достъп до данни от публичните органи, по-специално за целите на правоприлагането и националната сигурност <sup>(173)</sup>. В доклада се стига до заключението, че всичките 11 държави и територии продължават да осигуряват адекватно ниво на защита на предадените от ЕС лични данни. В него е отразено, че всички съответни държави и територии са осъвременили и укрепили по различни начини правната си рамка за неприкосновеност на личния живот. Освен това, за да се преодолеят съответните различия в нивото на защита и когато това е необходимо, за да се гарантира непрекъснатостта на решението относно адекватното ниво на защита, бяха договорени и съгласувани допълнителни гаранции за личните данни, предавани от Европа.

Тези прегледи показват и че вместо решенията относно адекватното ниво на защита да представляват „краен етап“, с тях се полагат основите за по-тясно сътрудничество и по-нататъшно регулаторно сближаване между ЕС и единомислещите партньори. Например в доклада относно първия преглед на решението относно адекватното ниво на защита за Япония се признава, че допълнителното укрепване на японската рамка за защита на данните може да покаже посоката за разширяване на обхвата на решението относно адекватното ниво на защита отвъд търговския обмен така, че да обхване предаванията, които понастоящем са изключени от неговия обхват, като например в областта на регулаторното сътрудничество и научните изследвания. Понастоящем продължават разговорите за проучване на такова разширяване на обхвата. Като цяло решенията относно адекватното ниво на защита се превърнаха в стратегически компонент на цялостните отношения на ЕС с тези чуждестранни партньори и се признават като основен фактор за задълбочаване на сътрудничеството в широк кръг от области.

Освен че предоставя стабилна основа за засилено двустранно сътрудничество, нарастващата мрежа от държави и територии, за които ЕС е приел решение относно адекватното ниво на защита, предоставя нови възможности за увеличаване в максимална степен на ползите от безопасните и свободни потоци от данни и за по-тясно сътрудничество между партньори с еднакви възгледи по отношение на прилагането на правилата за защита на данните. Поради това през март 2024 г. Комисията стана домакин на първата по рода си среща на високо равнище относно безопасните потоци от данни, като събра отговорни министри и ръководители на органите за защита на данните от 15 държави и територии, за които ЕС е приел решение относно адекватното ниво на защита, както и председателя на Европейския комитет по защита на данните <sup>(174)</sup>. На срещата бяха набелязани няколко конкретни точки за действие, по които продължава работата в рамките на тази група.

В по-общ план чрез техния „мрежов ефект“ приетите от Европейската комисия решения относно адекватното ниво на защита имат все по-голямо значение и извън ЕС, тъй като позволяват свободно движение на данни не само в 30-те икономики на ЕИП, но и в много повече юрисдикции по целия свят, в които държавите, за които

---

<sup>(173)</sup> Доклад на Комисията относно първия преглед на функционирането на решенията относно адекватното ниво на защита, приети съгласно член 25, параграф 6 от Директива 95/46/ЕО, 15.1.2024 г., COM(2024) 7 final (и SWD(2024) 3 final).

<sup>(174)</sup> [https://ec.europa.eu/commission/presscorner/detail/bg/mex\\_24\\_1307#11](https://ec.europa.eu/commission/presscorner/detail/bg/mex_24_1307#11)

има решение на ЕС относно адекватното ниво на защита, се признават за „безопасни местоназначения“ съгласно собствените им правила за защита на данните <sup>(175)</sup>.

### 7.1.2 Инструменти, осигуряващи подходящи гаранции

След доклада от 2020 г. бяха разработени допълнителни инструменти, осигуряващи подходящи гаранции, и бяха издадени практически насоки за улесняване на използването им.

Както беше обявено в доклада от 2020 г., Комисията прие осъвременени стандартни договорни клаузи (СДК) <sup>(176)</sup>, разработени като в голяма степен се разчита на обратната информация от различни заинтересовани страни <sup>(177)</sup>. С новите СДК бяха заменени трите групи СДК, които бяха приети съгласно Директивата за защита на личните данни. Основните иновации включват: i) актуализиране на гаранциите в съответствие с ОРЗД; ii) модулен подход, при който се предлага една входна точка, покриваща широк набор от сценарии за предаване на данни; iii) увеличаване на гъвкавостта за употребата на СДК от множество страни; и iv) практически инструментариум за спазване на решението по делото *Schrems II*.

Осъвременените СДК бяха приветствани от заинтересованите страни и получената обратна информация потвърждава, че СДК остават най-използваният инструмент за предаване от износители на данни от ЕС <sup>(178)</sup>. За да подпомогне износителите на данни в техните усилия за съответствие, Комисията разработи въпроси и отговори, които предоставят допълнителни насоки относно използването на клаузите <sup>(179)</sup>, които ще бъдат допълнително актуализирани, ако възникнат нови въпроси, включително с оглед на допълнителната обратна информация, получена като част от тази оценка.

Много износители на данни съобщават, че изпитват трудности при извършването на изискваните съгласно решението по делото *Schrems II* „оценки на въздействието върху предаването на данни“, като посочват по-специално тяхната сложност, както и разходите и времето, необходими за извършването им <sup>(180)</sup>. Въпреки че приветстват насоките на Комитета и СДК, те призовават за допълнителни насоки (например относно отговорностите на участващите страни и степента на детайлност, изисквана при оценките на въздействието върху предаването на данни) и допълнителни инструменти за подпомагане на извършването на такива оценки (например образци, общи оценки по държави, каталози на риска). Макар че заинтересованите страни предоставят такава обратна информация основно относно СДК, същите оценки се изискват и за други инструменти за предаване на данни (като задължителни фирмени правила). Поради това е важно Комитетът — като се използва и опитът от прилагането на изискванията от решението по делото *Schrems II* през последните години, включително като част от дейностите по правоприлагане на националните органи за защита на данните — да обмисли проучване на начини/инструменти за допълнително подпомагане на износителите на данни в техните усилия за спазване на изискванията в този контекст.

<sup>(175)</sup> Например Аржентина, Израел, Колумбия, Мароко, Уругвай и Швейцария.

<sup>(176)</sup> Решение за изпълнение (ЕС) 2021/914 на Комисията, ОВ L 199, 7.6.2021 г., стр. 31—61.

<sup>(177)</sup> Това включва например Съвместно становище 2/2021 на ЕКЗД и ЕНОЗД като част от процедурата за приемане на СДК.

<sup>(178)</sup> Позиция и констатации на Съвета, точка 37, принос на Комитета, стр. 9, обобщение на обратната информация от Многостранната група на заинтересованите страни по въпросите на ОРЗД.

<sup>(179)</sup> [https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview\\_bg](https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_bg).

<sup>(180)</sup> Вж. например обобщение на обратната информация от Многостранната група на заинтересованите страни по въпросите на ОРЗД.

За да допълни съществуващите СДК Комисията разработва допълнителни набори от клаузи, за да предостави на износителите на данни от ЕС цялостен и последователен пакет. Това ще включва СДК съгласно Регламент (ЕС) 2018/1725 относно предаване на данни от институции и органи на ЕС на търговски оператори в трети държави <sup>(181)</sup> и СДК за предаване на данни на вносители на данни от трети държави, чиито операции по обработване пряко подлежат на ОРЗД. Последните отговарят на призива на заинтересованите страни да обхващат конкретно сценарии, при които вносителят на данни попада в териториалния обхват на приложение на ОРЗД (например тъй като въпросното обработване е насочено към пазара на ЕС в съответствие с член 3, параграф 2 от ОРЗД <sup>(182)</sup>). Както беше изяснено от Комитета, инструмент за предаване на данни съгласно глава V от ОРЗД е необходим и в този случай поради повишените рискове за личните данни, обработвани извън ЕС, например поради евентуални противоречия на националните закони или непропорционален правителствен достъп в третата държава <sup>(183)</sup>. В новите СДК, които се разработват от Комисията, ще се разглежда конкретно този сценарий и ще се вземат изцяло предвид изискванията, които вече се прилагат директно по отношение на тези администратори и обработващи лични данни съгласно ОРЗД <sup>(184)</sup>.

Както се признава и от различни видове заинтересовани страни <sup>(185)</sup>, образците на клаузи играят все по-централна роля при улесняването на потоците от данни по света. Няколко юрисдикции са одобрили СДК на ЕС като механизъм за предаване на данни съгласно собствените си закони за защита на данните, с ограничени официални адаптации спрямо вътрешния си правен ред <sup>(186)</sup>. Редица други държави са приели свои собствени образци на клаузи, които споделят важни общи характеристики със СДК на ЕС <sup>(187)</sup>. Особено уместен пример е създаването на образци на клаузи от други международни/регионални организации или мрежи, като например от Консултативния комитет на Съвета на Европа по Конвенция 108, Иберо-американската мрежа за защита на данните и Асоциацията на народите от Югоизточна Азия (АСЕАН) <sup>(188)</sup>. Това отваря нови възможности за улесняване на потоците от данни между различни региони на света на основата на образци на клаузи. Конкретен пример е Ръководството ЕС—АСЕАН за СДК на ЕС и образци на клаузи на АСЕАН, което, като се основава на приноса на дружествата, ги подпомага в усилията им за спазване и на двата набора от клаузи <sup>(189)</sup>.

В допълнение към СДК задължителните фирмени правила (ЗФП) продължават да се използват широко за потоци от данни между членове на корпоративни групи или

---

<sup>(181)</sup> В съответствие с член 48, параграф 2, буква б) от Регламент (ЕС) 2018/1725.

<sup>(182)</sup> Позиция и констатации на Съвета, точка 37, принос на Комитета, стр. 9, обобщение на обратната информация от Многостранната група на заинтересованите страни по въпросите на ОРЗД.

<sup>(183)</sup> Насоки 05/2021 на ЕКЗД, т. 3.

<sup>(184)</sup> Както е посочено и в Насоки 05/2021 на ЕКЗД, раздел 4.

<sup>(185)</sup> Принос на Комитета, стр. 9, обобщение на обратната информация от Многостранната група на заинтересованите страни по въпросите на ОРЗД.

<sup>(186)</sup> Например Обединеното кралство (<https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf>) и Швейцария ([https://www.edoeb.admin.ch/edoeb/en/home/datenschutz/arbeit\\_wirtschaft/datenuebermittlung\\_ausland.html](https://www.edoeb.admin.ch/edoeb/en/home/datenschutz/arbeit_wirtschaft/datenuebermittlung_ausland.html)).

<sup>(187)</sup> Например Нова Зеландия (<https://privacy.org.nz/responsibilities/your-obligations/disclosing-personal-information-outside-new-zealand/>) и Аржентина (<https://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/267922/norma.htm>).

<sup>(188)</sup> Вж. <https://rm.coe.int/t-pd-2022-1rev10-en-final/1680abc6b4;https://www.redipd.org/sites/default/files/2023-02/anexo-modelos-clausulas-contractuales-en.pdf> и [https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows\\_Final.pdf](https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf).

<sup>(189)</sup> [https://commission.europa.eu/document/download/df5cd5a0-7387-4a2a-8058-8d2ccfec3062\\_en?filename=%28Final%29%20Joint\\_Guide\\_to\\_ASEAN\\_MCC\\_and\\_EU\\_SCC.pdf](https://commission.europa.eu/document/download/df5cd5a0-7387-4a2a-8058-8d2ccfec3062_en?filename=%28Final%29%20Joint_Guide_to_ASEAN_MCC_and_EU_SCC.pdf).

между предприятия, ангажирани в съвместна стопанска дейност. Тъй като ОРЗД се прилага, Комитетът прие 80 положителни становища относно национални решения, одобряващи ЗФП<sup>(190)</sup>. Комитетът издаде и насоки относно елементите, които трябва да бъдат включени в ЗФП за администратори (и информацията, която трябва да бъде предоставена като част от приложението на ЗФП), които са актуализирани, за да отразят изискванията на ОРЗД и решението по делото *Schrems II*<sup>(191)</sup>. Разработват се и актуализирани насоки за ЗФП за обработващи лични данни<sup>(192)</sup>. Тъй като със ЗФП се цели въвеждането в дружествата на задължителни политики/програми за защита на данните, много заинтересовани страни ги смятат за особено полезен инструмент за съответствие и надежден инструмент за предаване на данни<sup>(193)</sup>. В същото време заинтересованите страни продължават да съобщават, че по-широкото навлизане на ЗФП се възпрепятства от продължителността и сложността на процеса на одобрение от националните органи за защита на данните. Поради това е важно органите да продължат да работят за рационализиране и съкращаване на процеса на одобрение.

След доклада от 2020 г. бяха предприети също така стъпки за улесняване на използването на сертифициране и кодекси за поведение като инструменти за предаване на данни, например чрез приемането на специални насоки от Комитета за двата инструмента<sup>(194)</sup>. В същото време заинтересованите страни съобщават за същите проблеми относно графика и сложността на процеса на одобрение като горепосочените по отношение на сертифицирането и кодексите за поведение като инструменти за отчетност.

Накрая, в ОРЗД се предвиждат и специални инструменти — международни споразумения и административни договорености, одобрени от органите за защита на данните — които да се използват от публичните органи за предаване на лични данни на техни партньори в трети държави или на международни организации. Комитетът прие насоки относно гаранциите, които трябва да бъдат включени в такива инструменти<sup>(195)</sup> инструменти които могат да подпомогнат договарянето на такива споразумения и договорености.

### 7.1.3 Гарантиране на взаимно допълване с други политики

Тъй като потоците от данни станаха съществени за толкова много дейности, гарантирането на взаимното допълване между политиките за защита на данните и другите политики е от ключово значение. Включването на гаранции за защита на данните в международните инструменти често е не само предпоставка за потоци от данни, но и важен фактор за стабилно и надеждно сътрудничество.

Например международните споразумения, предвиждащи необходимите гаранции за защита на данните, включително чрез осигуряване на непрекъснатост на защитата от страна на запитващия орган, са от съществено значение за гарантиране на вежливост и улесняване на трансграничния достъп на правоприлагащите органи до съхранявани от дружествата електронни доказателства, а по този начин за по-ефективна борба с престъпността. Този подход е отразен във втория допълнителен

---

<sup>(190)</sup> Принос на Комитета, стр. 9.

<sup>(191)</sup> Препоръки 1/2022 на ЕКЗД.

<sup>(192)</sup> Принос на Комитета, стр. 9.

<sup>(193)</sup> Обобщение на обратната информация от Многостранната група на заинтересованите страни по въпросите на ОРЗД.

<sup>(194)</sup> Насоки 07/2022 и Насоки 04/2021 на ЕКЗД.

<sup>(195)</sup> Насоки 2/2020 на ЕКЗД.

протокол към Конвенцията за престъпленията в кибернетичното пространство<sup>(196)</sup>, с който се подобряват съществуващите правила за получаване на трансграничен достъп до електронни доказателства при наказателни разследвания, като същевременно се гарантират подходящи гаранции за защита на данните. Междувременно протоколът беше подписан от няколко държави — членки на ЕС. По подобен начин напредват двустранните преговори между ЕС и САЩ относно споразумение за трансграничен достъп до електронни доказателства за сътрудничество по наказателноправни въпроси<sup>(197)</sup>.

Обменът на резервационни данни на пътниците (PNR данни) е друга област от политиката за сигурност на ЕС, за която е от полза разработването на силни гаранции за защита на данните. През 2023 г. ЕС и Канада приключиха преговорите си по ново споразумение за PNR данни в съответствие с изискванията, определени от Съда в неговото Становище 1/15<sup>(198)</sup>. Подобни гаранции са въведени в главата за PNR данните от Споразумението за търговия и сътрудничество между ЕС и Обединеното кралство. Включването на подобрена защита на неприкосновеността на личния живот в тези споразумения, което може да служи като образец за бъдещи споразумения с други партньори, осигурява правна сигурност на въздушните превозвачи, като същевременно гарантира стабилността на важния обмен на информация за борбата с тероризма и други сериозни трансгранични престъпления.

Комисията е привърженик и на строги разпоредби за защита на неприкосновеността на личния живот и насърчаване на цифровата търговия в Световната търговска организация в рамките на текущите преговори по инициативата за съвместно изявление относно електронната търговия. Подобни разпоредби за борба с неоснователни пречки пред цифровата търговия, като същевременно се защитава необходимото политическо пространство на страните в областта на защитата на данните, бяха последователно включени в споразуменията за свободна търговия, сключени от ЕС след влизането в сила на ОРЗД, по-специално в Споразумение за търговия и сътрудничество между ЕС и Обединеното кралство и в споразуменията с Чили, Япония и Нова Зеландия. Разпоредбите за неприкосновеност на личния живот и потоците от данни се обсъждат и в текущите преговори относно цифровата търговия със Сингапур и Южна Корея.

## **7.2 Международно сътрудничество относно защитата на данните**

### *7.2.1 Двустранното измерение*

Комисията продължи да участва в диалог с държави и международни организации относно разработването, реформата и прилагането на правилата за неприкосновеност на личния живот, включително чрез представяне на предложения за обществени консултации относно проекти на законодателство или регулаторни мерки в областта на неприкосновеността на личния живот<sup>(199)</sup>, като свидетелства пред компетентни парламентарни органи<sup>(200)</sup> и като участва в специални срещи с

---

<sup>(196)</sup> Втори допълнителен протокол към Конвенцията за престъпления в кибернетичното пространство за засилено сътрудничество и разкриване на електронни доказателства (CETS № 224).

<sup>(197)</sup> [https://commission.europa.eu/news/eu-us-announcement-resumption-negotiations-eu-us-agreement-facilitate-access-electronic-evidence-2023-03-02\\_en?prefLang=bg](https://commission.europa.eu/news/eu-us-announcement-resumption-negotiations-eu-us-agreement-facilitate-access-electronic-evidence-2023-03-02_en?prefLang=bg).

<sup>(198)</sup> Предложение за Решение на Съвета за подписване от името на Европейския съюз на Споразумение между Канада и Европейския съюз относно предаването и обработването на резервационни данни на пътниците (PNR данни), COM(2024) 94 final.

<sup>(199)</sup> Това се отнася до консултации, организирани например от Австралия, Аржентина, Бразилия, Етиопия, Индонезия, Китай, Малайзия, Перу, Руанда и Тайланд.

<sup>(200)</sup> Например пред парламентарните органи на Еквадор, Парагвай и Чили.



представители на правителства, парламентарни делегации и регулаторни органи от много региони на света<sup>(201)</sup>. Редица от тези дейности са извършени чрез финансирането от ЕС проект „Засилена защита на личните данни и движението на данни“, с който се подкрепят държави, възнамеряващи да разработят модерни рамки за защита на данните или да укрепят капацитета на своите регулаторни органи, чрез обучение, споделяне на знания, изграждане на капацитет и обмен на най-добри практики. Комисията допринесе и за други инициативи, като например цифровия альянс между ЕС и CELAC.

Защитата на данните ще продължи да играе ключова роля и в работата на Комисията, свързана с разширяването. Законодателството на ЕС за защита на данните е важен компонент от общите усилия на държавите, обхванати от процеса на разширяване, да приведат своите правни рамки в съответствие с тези на ЕС (особено след като обработването и обменът на лични данни са в основата на толкова много политики). Нещо повече, независимостта и правилното функциониране на органа за защита на данните е ключов елемент от цялостните проверки и баланси и върховенството на закона и ще става все по-важно, тъй като ЕС постепенно интегрира държавите, обхванати от процеса на разширяване, в единния пазар (както се предвижда от инициативи като Плана за растеж на Западните Балкани).

Все по-важен аспект от диалога на ЕС с трети държави е свързан с обмена между регулаторите. Както беше обявено в доклада от 2020 г., Комисията създаде „Академия за защита на данните“, за да насърчи обмена между органите за защита на данните в ЕС и трети държави и по този начин да допринесе за изграждането на капацитет и да подобри сътрудничеството „на място“. Академията предлага специално подготвени обучения по искане на органите на трети държави и обединява експертния опит на представителите на правоприлагащата общност, академичните среди, частния сектор и европейските институции. Добавената стойност на обученията се състои в приспособяването на различните компоненти към интересите и нуждите на запитващия орган. Освен това тези обучения позволяват на органите за защита на данните в ЕС и трети държави да установяват контакти, да споделят знания, да обменят опит и най-добри практики и да установяват потенциални области за сътрудничество. До този момент академията е предоставила обучение на органите за защита на данните на Бразилия, Индонезия, Кения, Нигерия и Руанда, като в момента е в процес на подготовка на обучения за няколко други държави.

Освен че е важно да се поддържа диалог между регулаторните органи, съществува все по-голяма необходимост, както се признава и в получената от Съвета и Комитета обратна информация<sup>(202)</sup>, да се разработят подходящи правни инструменти за по-тесни форми на сътрудничество и взаимопомощ, включително като се даде възможност за необходимия обмен на информация в контекста на разследванията. В действителност, тъй като нарушенията на неприкосновеността на личния живот все повече водят до трансгранични последици, те често могат да бъдат ефективно разследвани и разглеждани само чрез сътрудничество между регулаторните органи от ЕС и от трети държави. Поради това Комисията ще поиска разрешение за започване на преговори за сключване на споразумения за сътрудничество в областта на правоприлагането със съответните трети държави (както е предвидено и в член 50 от ОРЗД). В това отношение Комисията отбелязва искането на Комитета да се вземат предвид по-специално държавите с най-много оператори, които пряко подлежат на

---

<sup>(201)</sup> Това включва и организиране на семинари и учебни посещения, например в Индонезия, Кения и Сингапур.

<sup>(202)</sup> Принос на Комитета, стр. 8; Позиция и констатации на Съвета, точка 38.



ОРЗД, като потенциални контрагенти, по-специално държавите от Г-7 и/или държавите, които се ползват от решенията относно адекватното ниво на защита<sup>(203)</sup>.

Въвеждането на такова сътрудничество в областта на правоприлагането и споразумения за взаимопомощ също би помогнало за осигуряване на спазване от страна на чуждестранни оператори, които са обект на ОРЗД, тъй като са насочени например конкретно към пазара на ЕС, като предлагат стоки или услуги. Съветът отбелязва значението на налагането на съответствие с ОРЗД в такива случаи и изразява загриженост относно еднаквите условия на конкуренция с юридическите лица в ЕС, както и ефективната защита на правата на физическите лица<sup>(204)</sup>. Комисията изразява съгласие с призива на Съвета да се проучат различни начини за улесняване на прилагането при този сценарий. Въпреки че по-официалните форми на сътрудничество с регулаторните органи на трети държави със сигурност биха могли да играят важна роля, следва да се търси по-енергично и използването на други, вече съществуващи пътища. Това включва пълно използване на инструментариума за прилагане на член 58 от ОРЗД и включване на представители на чуждестранни дружества в ЕС (назначени в съответствие с член 27 от ОРЗД).

### 7.2.2 Многостранното измерение

Комисията продължава да участва активно и в редица международни форуми за насърчаване на споделени ценности и изграждане на сближаване на регионално и глобално равнище.

Това например включва активен принос към работата на Консултативния комитет по Конвенцията за защита на лицата при автоматизираната обработка на лични данни (Конвенция 108) — единственият многостранен инструмент със задължителен характер в областта на защитата на личните данни. Досега 31 държави са ратифицирали протокола за изменение на Конвенция 108<sup>(205)</sup>, включително много държави — членки на ЕС, както и някои държави, които не са членки на Съвета на Европа (Аржентина, Мавриций и Уругвай). Сред държавите — членки на ЕС, все още не е подписала само една държава членка<sup>(206)</sup>, докато досега осем държави членки<sup>(207)</sup> са подписали, но не са ратифицирали осъвременената конвенция. Комисията настоятелно призовава единствената оставаща държава членка да подпише конвенцията за осъвременяване, а останалите бързо да пристъпят към ратифициране, за да се даде възможност Конвенцията да влезе в сила в близко бъдеще. Освен това тя ще продължи да насърчава активно присъединяването на трети държави.

На равнището на Г-20 и Г-7 обсъжданията относно неприкосновеността на личния живот и потоците от данни са съсредоточени върху въвеждането на понятието за „основано на доверие свободно движение на данни“ (DFFT), първоначално предложено от Япония, която признава, че защитата и сигурността на данните може да допринесат за доверието в цифровата икономика и за улесняване на потоците от данни<sup>(208)</sup>. ОИСР играе особено важна роля в този контекст, като предоставя форум за експертна общност за основано на доверие свободно движение на данни,

<sup>(203)</sup> Принос на Комитета, стр. 8.

<sup>(204)</sup> Позиция и констатации на Съвета, точка 39.

<sup>(205)</sup> Протокол за изменение на Конвенцията за защита на лицата при автоматизираната обработка на лични данни (CETS № 223).

<sup>(206)</sup> Дания.

<sup>(207)</sup> Белгия, Гърция, Ирландия, Латвия, Люксембург, Нидерландия, Чехия и Швеция.

<sup>(208)</sup> Вж.

например

<https://www.g7germany.de/resource/blob/974430/2062292/fbdb2c7e996205aee402386aae057c5e/2022-07-14-leaders-communicate-data.pdf?download=1>

обединяваща широк кръг от заинтересовани страни (правителства, регулаторни органи, промишленост, гражданско общество, академични среди), за да предоставят принос по конкретни проекти и въпроси, свързани с DFFT. Освен това важен резултат от инициативата за основано на доверие свободно движение на данни, за която Комисията има значителен принос, е приемането от ОИСР на Декларацията относно достъпа на правителствата до лични данни, съхранявани от субекти от частния сектор, която представлява първият международен инструмент в тази област. Тя съдържа поредица от споделени изисквания за защита на неприкосновеността на личния живот при достъп до лични данни за целите на националната сигурност и правоприлагането. На фона на нарастващото признаване в световен мащаб, че доверието в предаването на данни е повлияно отрицателно от непропорционалният правителствен достъп, тази декларация е важен принос за улесняване на надеждните потоци от данни. Комисията ще продължи да насърчава държавите да се присъединят към декларацията, която е отворена и за членове извън ОИСР.

Комисията се ангажира и с различни регионални организации и мрежи, които оформят общи гаранции за защита на данните. Това се отнася например за Асоциацията на народите от Югоизточна Азия (АСЕАН), Африканския съюз, Форум на органите за защита на неприкосновеността на личния живот в азиатско-тихоокеанския регион (АРРА), Иберо-американската мрежа за защита на данните и Мрежата на африканските органи за защита на данните (NADPA — RADPD). Разработването на посоченото по-горе Ръководство ЕС—АСЕАН за образци на клаузи е конкретен пример за такова ползотворно сътрудничество.

Накрая, Комисията поддържа диалог с различни международни организации, включително за проучване на начини за допълнително улесняване на потоците от данни между ЕС и такива организации. Тъй като много организации са модернизирани своите рамки за защита на данните през последните години или са в процес на модернизирване, възникват и нови възможности за обмен на опит и най-добри практики. В това отношение годишните работни семинари с международни организации и специалната работна група относно международните предавания на данни, организирана от Европейския надзорен орган по защита на данните, се оказаха особено полезни форуми за обмен и проучване на конкретни инструменти за сътрудничество, включително обмен на лични данни <sup>(209)</sup>.

## 8 ЗАКЛЮЧЕНИЕ

През шестте години от влизането му в сила, ОРЗД даде правомощия на хората да упражняват контрол върху своите данни. Той спомогна и за създаването на еднакви условия на конкуренция за предприятията, като положи основите за набор от инициативи, които движат цифровия преход в ЕС.

За пълно постигане на двойните цели на ОРЗД, а именно силна защита на лицата при гарантиране на свободно движение на лични данни в рамките на ЕС и безопасно движение на данни извън ЕС, е необходимо съсредоточаване върху:

- надеждно прилагане на ОРЗД, като се започне с бързото приемане на предложението на Комисията относно процедурните правила за предоставяне на бързи средства за правна защита и правна сигурност в случаи, засягащи физически лица в целия ЕС;

---

<sup>(209)</sup> [https://www.edps.europa.eu/data-protection/our-work/edps-worldwide/data-protection-and-international-organisations\\_en](https://www.edps.europa.eu/data-protection/our-work/edps-worldwide/data-protection-and-international-organisations_en)

- проактивна подкрепа от страна на органите за защита на данните за заинтересованите страни в техните усилия за спазване на изискванията, по-специално МСП и малките оператори;
- последователно тълкуване и прилагане на ОРЗД в целия ЕС;
- ефективно сътрудничество между регулаторните органи както на национално, така и на европейско равнище, за да се гарантира последователното и съгласувано прилагане на нарастващия набор от цифрови правила на ЕС;
- по-нататъшно развитие на международната стратегия на Комисията за защита на данните.

За да се подпомогне ефективното прилагане на ОРЗД и по-нататъшното осмисляне на защитата на данните, са необходими няколко действия, набелязани тук. Комисията ще подкрепя и ще наблюдава тяхното изпълнение с оглед на следващия доклад през 2028 г.

#### *Разработване на ефективни структури за сътрудничество*

Европейският парламент и Съветът се приканват да приемат бързо предложението относно процедурните правила на ОРЗД.

Комитетът и органите за защита на данните се приканват:

- да установят редовно сътрудничество с други секторни регулаторни органи по въпроси, които оказват въздействие върху защитата на данните, по-специално с органите, създадени съгласно новото цифрово законодателство на ЕС, и активно да участват в структури на равнището на ЕС, предназначени да улесняват междурегулаторното сътрудничество;
- да използват по-пълноценно инструментите за сътрудничество, предвидени в ОРЗД, така че да се стига до разрешаване на спорове само в краен случай;
- да прилагат по-ефективни и целенасочени работни договорености за насоки, становища и решения и да отдават приоритет на ключови въпроси с цел да намалят тежестта върху органите за защита на данните и да реагират по-бързо на развитието на пазара.

Държавите членки следва:

- да гарантират ефективната и пълна независимост на националните органи за защита на данните;
- да разпределят достатъчно ресурси на органите за защита на данните, за да им предоставят възможност да изпълняват своите задачи, по-специално като им предоставят технически ресурси и експертен опит, необходими за справяне с нововъзникващи технологии и за изпълнение на нови отговорности съгласно цифровото законодателство;
- да оборудват органите за защита на данните с необходимите инструменти за разследване, за да използват ефективно предоставените от ОРЗД правомощия за прилагане;
- да подкрепят диалога между органите за защита на данните и други национални регулаторни органи, по-специално създадените съгласно новото цифрово законодателство.

Комисията:

- ще подкрепя активно бързото приемане на предложението относно процедурните правила на ОРЗД от съзакондателите;
- ще продължи да следи отблизо ефективната и пълна независимост на националните органи за защита на данните;
- ще изгради полезни взаимодействия и съгласуваност между ОРЗД и цялото законодателство, засягащо обработването на лични данни въз основа на опит и, ако е необходимо, ще предприеме подходящи действия за осигуряване на правна сигурност;
- ще обмисли как по-добре да удовлетвори необходимостта от структурирано и ефективно междурегулаторно сътрудничество, за да се гарантира ефективно, последователно и съгласувано прилагане на цифровите правила на ЕС, като същевременно зачита компетентността на органите за защита на данните по всички въпроси, свързани с обработването на лични данни.

*Прилагане и допълване на правната уредба*

Държавите членки следва:

- да гарантират, че с органите за защита на данните се провеждат своевременни консултации преди приемането на законодателство относно обработването на лични данни.

Комисията:

- ще продължи да използва всички инструменти, с които разполага, включително производствата за установяване на нарушение, за да гарантира, че държавите членки спазват ОРЗД;
- ще продължи да подкрепя обмена на мнения и национални практики между държавите членки, включително чрез експертната група на държавите членки по ОРЗД;
- ще предприеме действия, за да гарантира, че децата са защитени, овластени и уважавани онлайн;
- ще обмисли възможните следващи стъпки по отношение на предложението за Регламент за неприкосновеността на личния живот в сектора на електронните съобщения, включително взаимодействието му с ОРЗД.

*Подкрепа за заинтересованите страни*

Комитетът и органите за защита на данните се приканват:

- да участват в конструктивен диалог с администратори и обработващи лични данни относно спазването на ОРЗД;
- да увеличат допълнително усилията за подпомагане на спазването на изискванията от страна на МСП чрез предоставяне на специално пригодени насоки и инструменти, за разсейване на всички неоснователни опасения относно спазването на изискванията на МСП, чиято основна дейност не е обработването на лични данни, и да оказват съдействие в усилията им за спазване на изискванията;
- да подпомагат прилагането на ефективни мерки за спазване на изискванията от страна на предприятията, като например сертифициране и кодекси за поведение (включително като инструменти за предаване на данни), като работят със

заинтересованите страни по време на процеса на одобрение, предоставят ясни срокове за одобрения и, както е обещано в стратегията на Комитета за периода 2024—2027 г., изясняват на ключови групи от заинтересовани страни начина, по който могат да се използват тези инструменти;

- да гарантират, че националните насоки и прилагането на ОРЗД на национално равнище са в съответствие с насоките на Комитета и съдебната практика на Съда;
- да разрешават въпроси, свързани с различни тълкувания на ОРЗД между органите за защита на данните, включително между органи в рамките на една и съща държава членка;
- да предоставят насоки, които са кратки, практични и достъпни за съответната аудитория в съответствие с ангажимента, поет в стратегията на Комитета за периода 2024—2027 г.;
- да осигуряват по-ранни и по-задълбочени консултации относно насоките и становищата, за да се разбират по-добре динамиката на пазара и търговските практики и да се вземат предвид получената обратна информация и конкретното прилагане на приетите тълкувания;
- да приключат приоритетно текущата работа по насоките относно личните данни на децата, научните изследвания, анонимизирането, псевдонимизацията и законния интерес;
- да засилят дейностите за повишаване на осведомеността, информацията и действията по правоприлагане, за да се гарантира, че длъжностните лица по защита на данните могат да изпълняват ролята си съгласно ОРЗД.

Комисията:

- ще продължи да предоставя финансова подкрепа за дейности на органите за защита на данните, с които се улеснява изпълнението на задълженията по ОРЗД от страна на МСП;
- ще използва всички налични средства, за да предостави своевременни разяснения по въпроси от значение за заинтересованите страни, включително МСП, по-специално чрез искане на становища от Комитета.

*По-нататъшно развитие на инструментариума за предаване на данни и международно сътрудничество*

Комитетът и органите за защита на данните се приканват:

- да приключат работата по рационализиране и съкращаване на процеса на одобрение за задължителни фирмени правила, както и по актуализиране на насоките относно елементите, които могат да бъдат намерени в задължителните фирмени правила за обработващите лични данни;
- да проучат начини/инструменти за допълнително подпомагане на износителите на данни в техните усилия за спазване на изискванията на решението по делото „Schrems II“;
- да проучат допълнителни начини за осигуряване на ефективно правоприлагане срещу оператори, установени в трети държави, попадащи в териториалния обхват на приложение на ОРЗД.

Държавите членки следва:

- да гарантират възможно най-скоро полагането на оставащите подписи и ратификациите на осъвременената Конвенция 108+ на Съвета на Европа, за да стане възможно влизането ѝ в сила.

#### Комисията:

- ще постигне допълнителен напредък в текущите разговори относно адекватното ниво на защита, ще проучи по-нататъшното развитие на съществуващите констатации относно адекватното ниво на защита и ще проведе нови диалози относно адекватното ниво на защита със заинтересованите партньори;
- ще подкрепя засиленото сътрудничество между мрежата от държави, които се ползват от решенията относно адекватното ниво на защита;
- ще приключи работата по допълнителни стандартни договорни клаузи, по-специално за предаване на данни на вносителите на данни, чието обработване пряко подлежи на ОРЗД, и предаване на данни съгласно Регламент (ЕС) 2018/1725 за предавания на данни от институции и органи на ЕС;
- ще си сътрудничи с международни партньори за улесняване на потоците от данни на основата на примерни договорни клаузи;
- ще подкрепя текущите процеси на реформи в трети държави по отношение на нови или осъвременени правила за защита на данните чрез споделяне на опит и най-добри практики;
- ще взаимодейства с международни и регионални организации, като например ОИСР и Г-7, за насърчване на сигурните потоци на данни въз основа на високи стандарти за защита на данните, включително в контекста на инициативата за свободно движение на данни, основано на доверие;
- ще улеснява и подпомага обмена между европейски и международни регулаторни органи, включително чрез своята Академия за защита на данните;
- ще допринася за улесняването на международното сътрудничество в областта на правоприлагането между надзорните органи, включително чрез договаряне на споразумения за сътрудничество и взаимопомощ.