



ЕВРОПЕЙСКА  
КОМИСИЯ

Брюксел, 24.7.2019 г.  
COM(2019) 374 final

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

**Правилата за защита на данните като катализатор на доверието в ЕС и извън него  
— преглед на постигнатите резултати**

## Съобщение на Комисията до Европейския парламент и Съвета

### Правилата за защита на данните като катализатор на доверието в ЕС и извън него — преглед на постигнатите резултати

#### I. Въведение

Общият регламент относно защитата на данните<sup>1</sup> (наричан по-нататък „Регламентът“) се прилага в целия Европейски съюз от повече от една година. Той е в центъра на съгласувана и модернизирана уредба на ЕС за защита на данните, която включва също Директивата относно правоприлагането в областта на защитата на данните<sup>2</sup> и Регламента относно защитата на данните от институциите и органите на ЕС<sup>3</sup>. Тази уредба предстои да бъде допълнена с Регламента за неприкосновеността на личния живот и електронните съобщения, който е в законодателната фаза.

За да се гарантира основното право на защита на личните данни, от основно значение е наличието на строги правила за защита на данните. Те са жизненоважни за демократичните общества<sup>4</sup> и важен елемент на основаната на все повече данни икономика. ЕС се стреми да се възползва от многобройните възможности, предлагани от цифровата трансформация по отношение на услугите, работните места и иновациите, като същевременно посреща предизвикателствата, които тези възможности поставят. Кражбата на самоличност, изтичането на чувствителни данни, дискриминацията на отделни лица, програмираната пристрастност, споделянето на незаконно съдържание и разработването на инструменти за нежелано наблюдение са само няколко примера за проблеми, които все по-често присъстват в обществените дебати, от които е ясно, че хората очакват техните данни да бъдат защитени.

---

<sup>1</sup> Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) (ОВ L 119, 4.5.2016 г., стр. 1): <https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A32016R0679>.

<sup>2</sup> Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни, и за отмяна на Рамково решение 2008/977/ПВП на Съвета (ОВ L 119, 4.5.2016 г.): <https://eur-lex.europa.eu/legal-content/BG/ALL/?uri=celex:32016L0680>. Държавите членки трябваше да я транспонират до 6 май 2018 г. В докладите относно Съюза на сигурност се представя актуалното състояние във връзка с транспонирането ѝ.

<sup>3</sup> Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета от 23 октомври 2018 г. относно защитата на физическите лица във връзка с обработването на лични данни от институциите, органите, службите и агенциите на Съюза и относно свободното движение на такива данни и за отмяна на Регламент (ЕО) № 45/2001 и Решение № 1247/2002/ЕО (ОВ L 295, 21.11.2018 г., стр. 39—98): <https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A32018R1725>. Той започна да се прилага от 11 декември 2018 г.

<sup>4</sup> В своето знаково решение от 24 август 2017 г. Върховният съд на Индия призна зачитането на неприкосновеността на личния живот за основно право — „съществен аспект на човешкото достойнство“.

Защитата на данните се превърна в истинско глобално явление, тъй като хората по света все повече отстояват и ценят защитата и сигурността на своите данни. Много държави приеха или са в процес на приемане на всеобхватни правила за защита на данните въз основа на принципи, подобни на тези от Регламента, което води до сближаване на правилата за защита на данните в световен план. Това открива нови възможности за улесняване на потоците от данни между търговски оператори или публични органи, като същевременно се повишава нивото на защита на личните данни в ЕС и в целия свят.

На защитата на данните се обръща по-сериозно внимание от всякога, тъй като тя има широкообхватно отражение върху различни заинтересовани страни и сектори. Комисията е решена да води ЕС към успешното прилагане на новия режим за защита на данните и да подкрепи всички мерки за пълноценното функциониране на този режим. С настоящото съобщение Комисията отчита постигнатите досега резултати във връзка с последователното прилагане на правилата за защита на данните в целия ЕС, функционирането на новата система за управление, отражението върху гражданите и предприятията и усилията на ЕС за насърчаване на сближаването на режимите за защита на данните в световен план. То се явява като продължение на Съобщението на Комисията относно прилагането на Регламента от януари 2018 г.<sup>5</sup> и се основава на работата на многостранната група на заинтересованите страни<sup>6</sup>, по-специално на нейния принос за едногодишния преглед на постигнатото, както и обсъжданията, проведени по време на прегледа на постигнатото, организиран от Комисията на 13 юни 2019 г.<sup>7</sup> Настоящото съобщение ще допринесе и за преразглеждането, което Комисията планира да извърши до май 2020 г.<sup>8</sup>

Законодателната уредба на ЕС за защита на данните е в основата на европейския ориентиран към човека подход към иновациите. Тя бива интегрирана в регулаторната основа на все по-широка гама от политики, включително здравеопазването и научните изследвания, изкуствения интелект, транспорта, енергетиката, конкуренцията и правоприлагането. Комисията непрестанно подчертава значението на правилното прилагане и изпълнение на новите правила за защита на данните, както се изтъква в нейното съобщение относно прилагането на Регламента, публикувано през януари 2018 г., и в Насоките относно използването на лични данни в контекста на избори, публикувани през септември 2018 г.<sup>9</sup> До изготвянето на настоящото съобщение беше отбелязан значителен напредък в постигането на тази цел, въпреки че са необходими допълнителни усилия, за да може Регламентът да започне да функционира пълноценно.

---

<sup>5</sup> Съобщение на Комисията до Европейския парламент и Съвета, озаглавено „По-силна защита, нови възможности — насоки на Комисията относно прякото прилагане, считано от 25 май 2018 г., на Общия регламент относно защитата на данните“, COM(2018) 43 final: <https://eur-lex.europa.eu/legal-content/BG/TXT/?qid=1517578296944&uri=CELEX%3A52018DC0043>.

<sup>6</sup> Многостранната група на заинтересованите страни по Регламента, създадена от Комисията, включва представители на гражданското общество, стопанските и академичните среди и практикуващи юристи: <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537&Lang=BG>.

<sup>7</sup> [http://europa.eu/rapid/press-release\\_IP-19-2956\\_bg.htm](http://europa.eu/rapid/press-release_IP-19-2956_bg.htm).

<sup>8</sup> Член 97 от Регламента.

<sup>9</sup> Насоки на Комисията относно прилагането на правото на Съюза в областта на защитата на данните в контекста на избори, COM(2018) 638: <https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:52018DC0638&qid=1564390069062&from=BG>.

## **II. Един континент, един закон: уредбата за защита на данните е въведена в държавите членки**

Една от основните цели на Регламента беше да се сложи край на разпокъсаността на законодателната уредба, съставена от 28 различни национални закона, които съществуваха съгласно предишната Директива за защита на личните данни<sup>10</sup>, и да се осигури правна сигурност за физическите лица и предприятията в целия ЕС. До голяма степен тази цел бе постигната.

### *Хармонизиране на правната уредба*

Въпреки че Регламентът се прилага пряко в държавите членки, той ги задължава да предприемат редица правни действия на национално равнище, по-специално да установят и предоставят правомощия на националните органи за защита на данните<sup>11</sup>, да определят правила по конкретни въпроси, като например съгласуването на правото на защита на личните данни със свободата на изразяване и информация, и да изменят или отменят секторното законодателство, уреждащо аспекти, свързани със защитата на данните. Към момента на изготвяне на настоящото съобщение всички държави членки, с изключение на три<sup>12</sup>, са актуализирали националното си законодателство за защитата на данните. Работата на национално равнище по адаптирането на секторните закони все още продължава. След включването му в Споразумението за Европейското икономическо пространство приложното поле на Регламента беше разширено, така че да обхване Норвегия, Исландия и Лихтенщайн, които също са приели свои национални закони за защита на данните.

Въпреки това заинтересованите страни призовават за още по-голяма хармонизация в някои области<sup>13</sup>. Регламентът позволява на държавите членки да доуточнят неговото приложение в някои области, като например възрастта за изразяване на съгласие от деца за онлайн услуги<sup>14</sup> или обработването на лични данни в области като медицината и общественото здраве. В този случай действията на държавите членки се определят от две условия:

---

<sup>10</sup> Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 г. за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни <https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=celex:31995L0046>.

<sup>11</sup> Като например правомощието да налагат административни глоби.

<sup>12</sup> Към 23 юли 2019 г. Гърция, Португалия и Словения все още са в процес на приемане на своето национално законодателство.

<sup>13</sup> Вж. доклада на Многостранната група на заинтересованите страни по Регламента, публикуван на 13 юни 2019 г.: <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670&Lang=BG>.

<sup>14</sup> 13 години за Белгия, Дания, Естония, Латвия, Малта, Обединеното кралство, Финландия и Швеция; 14 години за Австрия, България, Испания, Италия, Кипър и Литва; 15 години за Франция и Чехия; 16 години за Германия, Ирландия, Люксембург, Нидерландия, Полша, Румъния, Словакия, Унгария и Хърватия.

- i) всеки национален специален закон трябва да отговаря на изискванията на Хартата на основните права<sup>15</sup> (и да не надхвърля границите, определени с Регламента, който се основава на Хартата);
- ii) тези действия не могат да нарушават свободното движение на лични данни в рамките на ЕС<sup>16</sup>.

В някои случаи държавите членки са въвели национални изисквания, надхвърлящи тези на Регламента, по-конкретно посредством редица секторни закони, а това води до разпокъсаност и създаване на ненужна тежест. Един пример за допълнително изискване, въведено от държавите членки, което надхвърля изискванията на Регламента, е задължението съгласно германското законодателство да се определя длъжностно лице за защита на данните в дружествата с 20 или повече служители, които се занимават постоянно с автоматизираното обработване на лични данни.

### *Продължаващи усилия за по-голяма хармонизация*

Комисията участва в двустранни диалози с националните органи, по време на които обръща специално внимание на националните мерки по отношение на:

- действителната независимост на органите за защита на данните, включително предоставянето на подходящи за целта финансови, човешки и технически ресурси;
- как националните закони ограничават правата на субектите на данни;
- факта, че с националното законодателство не следва да се въведат изисквания, които надхвърлят обхвата на Регламента, когато няма поле за уточнения, като например допълнителни условия за обработването;
- изпълнението на задължението за съгласуване на правото на защита на личните данни със свободата на изразяване и информация, като се има предвид, че с това задължение не следва да се злоупотребява с цел оказване на възпиращ ефект върху журналистическата работа.

Работата на органите за защита на данните, които си сътрудничат в рамките на Европейския комитет по защита на данните („Комитетът“), е основна движеща сила за последователното прилагане на новите правила: действията по правоприлагане, които засягат няколко държави членки, преминават през механизма за сътрудничество и съгласуваност<sup>17</sup> в рамките на Комитета, като приетите от него насоки допринасят за хармонизираното тълкуване на Регламента. Въпреки това заинтересованите страни очакват от органите за защита на данните да положат допълнителни усилия в тази насока.

Работата на националните съдилища и на Съда на Европейския съюз също спомага за последователното тълкуване на правилата за защита на данните. Наскоро националните

---

<sup>15</sup> Член 8.

<sup>16</sup> В съответствие с член 16, параграф 2 от Договора за функционирането на Европейския съюз.

<sup>17</sup> В член 60 от Регламента се предвижда сътрудничество между органите за защита на данните с оглед на единното тълкуване на Регламента в конкретни случаи. В член 64 се предвижда, че в някои случаи Комитетът ще издава становища, за да се гарантира последователното прилагане на Регламента. И накрая, Комитетът има правомощието да приема решения със задължителна сила, адресирани до органите за защита на данните, в случай на несъгласие между тях.

съдилища издадоха решения за обезсилване на разпоредбите в националните закони, които се отклоняват от Регламента<sup>18</sup>.

### III. Пъзелът на новата система за управление се подрежда

С Регламента бе създадена нова структура на управление, в чийто център са независимите национални органи за защита на данните в качеството си на органи, отговарящи за прилагането на Регламента, и на първи точки за контакт за заинтересованите страни. Въпреки че през последната година ресурсите на повечето органи по защита на данните бяха увеличени, все още съществуват големи различия между държавите членки<sup>19</sup>.

#### *Органите за защита на данните използват новите си правомощия*

Регламентът предоставя на органите за защита на данните по-големи правомощия за правоприлагане. Противно на опасенията, изразени от някои заинтересовани страни преди май 2018 г., националните органи за защита на данните възприеха балансиран подход към правомощията за правоприлагане. Те се съсредоточиха по-скоро върху диалога, отколкото върху санкциите, по-специално за най-малките оператори, за които обработването на лични данни не е основна дейност. В същото време те не се поколебаха да използват ефективно новите си правомощия, когато това бе необходимо, включително чрез започването на разследвания в областта на социалните медии<sup>20</sup> и налагането на административни глоби в диапазон от няколко хиляди до няколко милиона евро в зависимост от тежестта на нарушенията на правилата за защита на данните.

Примери за глоби, наложени от органите за защита на данните<sup>21</sup>:

- 5 000 EUR на кафене за спортни залагания в Австрия за незаконно видеонаблюдение;
- 220 000 EUR на дружество посредник за данни в Полша, което не е уведомило физическите лица за това, че данните им се обработват;
- 250 000 EUR, наложени на испанската футболна лига LaLiga, поради липсата на прозрачност при изготвянето на нейното приложение за смартфон;
- 50 милиона евро на Google във Франция поради условията за получаване на съгласие от страна на потребителите.

При провеждането на разследвания е от съществено значение органите за защита на данните да събират съответните доказателства, да следват всички процедурни стъпки

---

<sup>18</sup> Такъв е бe случаят в Германия и Испания.

<sup>19</sup> [https://edpb.europa.eu/sites/edpb/files/files/file1/19\\_2019\\_edpb\\_written\\_report\\_to\\_libe\\_en.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/19_2019_edpb_written_report_to_libe_en.pdf)

<sup>20</sup> Така например ирландската комисия за защита на данните започна 15 официални разследвания във връзка със спазването на Регламента от страна на мултинационалните технологични дружества. Вж. стр. 49 от годишния доклад за 2018 г. на ирландската комисия за защита на данните: <https://www.dataprotection.ie/en/news-media/press-releases/dpc-publishes-annual-report-25-may-31-december-2018>.

<sup>21</sup> Няколко от решенията за налагане на глоби все още подлежат на съдебна проверка.

съгласно националното законодателство и да гарантират справедлив процес в често сложни преписки. Това изисква време и значителна работа, което обяснява защо повечето разследвания, започнати след влизането в сила на Регламента, все още не са приключени.

При все това успехът на Регламента не бива да се измерва с броя на наложените глоби, а с промените в културата и поведението на всички участници. В този контекст органите за защита на данните разполагат с други инструменти, като например налагането на временно или окончателно ограничаване на обработването, включително забрана или разпореждане за преустановяването на потоците от данни към получател в трета държава<sup>22</sup>.

Някои органи за защита на данните създадоха нови инструменти, като например линии за помощ и набори от инструменти за предприятията, докато други разработиха новаторски подходи, например „регулаторни лаборатории“<sup>23</sup>, които да подпомагат предприятията в усилията им за спазване на изискванията. Въпреки това редица заинтересовани страни все още смятат, че не са получили достатъчно подкрепа и информация, по-специално малките и средните предприятия в някои държави членки<sup>24</sup>. С оглед на преодоляването на тази ситуация Комисията предоставя безвъзмездни средства на органите за защита на данните, за да достигнат до заинтересованите страни, по-специално физическите лица и малките и средните предприятия<sup>25</sup>.

#### *Европейският комитет по защита на данните функционира*

Органите за защита на данните засилиха работата си в рамките на Европейския комитет по защита на данните<sup>26</sup>. Тяхната интензивна дейност позволи на Комитета да приеме около 20 насоки по ключови аспекти на Регламента<sup>27</sup>. Бъдещите области на работа на Комитета са представени в двугодишна програма<sup>28</sup> в съответствие с изискванията на Регламента.

При трансгранични случаи вече никой орган за защита на данните не е просто национален орган, а е част от един истински общоевропейски процес на всички етапи — от разследването до решението. Това тясно сътрудничество се превърна в ежедневна

---

<sup>22</sup> Член 58, параграф 2, букви е) и й).

<sup>23</sup> <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/09/ico-call-for-views-on-creating-a-regulatory-sandbox/>

<sup>24</sup> Вж. доклада на Многостранната група на заинтересованите страни по ОРЗД: <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670&Lang=BG>

<sup>25</sup> През 2018 г. бяха отпуснати 2 милиона евро на девет органа за защита на данните за дейности в периода 2018—2019 г.: Белгия, България, Дания, Латвия, Литва, Нидерландия, Словения, Унгария и Исландия: <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/rec-rdat-trai-ag-2017;>

през 2019 г. ще бъдат отпуснати 1 милион евро:

[https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/rec-rdat-trai-ag-2019.](https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/rec-rdat-trai-ag-2019)

<sup>26</sup> Комитетът е юридическо лице и се състои от ръководителите на националните надзорни органи за защита на данните и на Европейския надзорен орган по защита на данните.

<sup>27</sup> [https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices\\_bg](https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_bg)

<sup>28</sup> [https://edpb.europa.eu/our-work-tools/our-documents/publication-type/work-program\\_bg](https://edpb.europa.eu/our-work-tools/our-documents/publication-type/work-program_bg)

практика: до края на юни 2019 г. чрез механизма за сътрудничество бяха разгледани 516 трансгранични случая.

Комисията допринася активно за работата на Комитета<sup>29</sup> с оглед на утвърждаването на духа и буквата на Регламента и припомня общите принципи на правото на ЕС<sup>30</sup>.

#### *Към изграждането на култура на ЕС за защита на данните*

Новата система на управление все още трябва да реализира пълния си потенциал. Важно е Комитетът да оптимизира допълнително своя процес на вземане на решения и да изгради обща култура на ЕС за защита на данните сред своите членове. Възможността органите за защита на данните да обединяват усилията си<sup>31</sup> по въпроси, засягащи повече от една държава членка, например да провеждат съвместни разследвания и мерки за правоприлагане, може да допринесе за постигането на тази цел, като същевременно се намали натискът върху ресурсите.

Много заинтересовани страни желаят да видят още по-стабилно сътрудничество и единен подход от страна на националните органи за защита на данните<sup>32</sup>. Те също така искат по-голяма съгласуваност на съветите, предоставяни от органите за защита на данните<sup>33</sup>, и цялостно привеждане в съответствие на националните насоки с тези на Комитета. Някои от тях очакват и допълнителни пояснения на основни понятия от Регламента, например основания на риска подход, като се обърне специално внимание най-вече на опасенията на малките и средните предприятия.

В този контекст е от съществено значение да се даде възможност на заинтересованите страни да участват по-активно в работата на Комитета. Ето защо Комисията приветства системното организиране от страна на Комитета на публични консултации относно насоките. Тази практика, заедно с организирането на работни срещи със заинтересованите страни по набелязани теми на ранен етап от обсъждането, следва да бъде продължена и разширена, за да се гарантират прозрачността, приобщаването и целесъобразността на работата на Комитета.

---

<sup>29</sup> Като участник без право на глас.

<sup>30</sup> Комисията помогна също така за гладкото учредяване на Комитета и способства за неговото функциониране, като му предостави своята комуникационна система.

<sup>31</sup> Член 62 от Регламента.

<sup>32</sup> Вж. доклада на Многостранната група на заинтересованите страни по Регламента: <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670&Lang=BG>.

Така например предприятията считат, че националните списъци на видовете операции по обработване, които изискват оценка на въздействието върху защитата на данните съгласно член 35 от Регламента, биха могли да бъдат по-добре хармонизирани.

<sup>33</sup> Включително между различните органи във федералните държави.



#### **IV. Хората се ползват от правата си, но повишаването на осведомеността трябва да продължи**

Друга основна цел на Регламента беше укрепването на правата на физическите лица. Сдруженията за защита на гражданските права и организациите на потребителите считат като цяло Регламента за важна стъпка в изграждането на справедливо цифрово общество, основано на взаимно доверие.

*Повече осведоменост за правата, свързани със защитата на данните*

Физическите лица в ЕС са все по-осведомени за правилата за защита на данните и за своите права: 67 % от участниците в проучване на Евробарометър, проведено през май 2019 г.<sup>34</sup>, са чували за Регламента, а 57 % знаят, че съществува национален орган за защита на данните, към който могат да се обръщат за информация или да подават жалби. 73 % от запитаните са чували поне за едно от правата, предоставени с Регламента. Въпреки това голям брой физически лица в ЕС все още не предприемат активни действия за защита на своите лични данни, когато са онлайн. Така например 44 % от физическите лица не са променили своите настройки, гарантиращи неприкосновеността на личния живот, в социалните мрежи.

*Физическите лица все по-често упражняват правата си*

С повишаването на осведомеността за правата им физическите лица започнаха да ги упражняват по-интензивно под формата на запитвания от клиенти и да се обръщат по-често към органите за защита на данните, за да търсят информация или да подават жалби<sup>35</sup>. Предприятията също съобщават, че исканията за достъп до лични данни са се увеличили в няколко сектора, като например банковото дело и далекосъобщенията. Освен това физическите лица по-често оттеглят съгласието си и упражняват правото си на възражение срещу търговски съобщения<sup>36</sup>.

Някои оператори обаче съобщиха за неправилно разбиране от страна на физическите лица на правилата за защита на данните, като например убеждението, че те трябва да дават съгласието си за всички видове обработване или че правото на заличаване е абсолютно (в някои случаи операторите трябва да съхраняват личните данни, за да изпълнят правните си задължения)<sup>37</sup>. Организациите на гражданското общество пък се оплакват от дългото време, което отнема получаването на отговор от някои предприятия и органи за защита на данните.

Важно е да се отбележи, че неправителствени организации внесоха представителни иски, след като им бе възложен мандат за това от физически лица, използвайки

---

<sup>34</sup> [http://europa.eu/rapid/press-release\\_IP-19-2956\\_bg.htm](http://europa.eu/rapid/press-release_IP-19-2956_bg.htm)

<sup>35</sup> [https://ec.europa.eu/commission/sites/beta-political/files/infographic-gdpr\\_in\\_numbers\\_1.pdf](https://ec.europa.eu/commission/sites/beta-political/files/infographic-gdpr_in_numbers_1.pdf)

<sup>36</sup> Вж. доклада на Многостранната група на заинтересованите страни по Общия регламент относно защитата на данните.

<sup>37</sup> Вж. доклада на Многостранната група на заинтересованите страни по Общия регламент относно защитата на данните.

новите възможности съгласно Регламента<sup>38</sup>. Прибягването до представителни искове щеше да бъде по-лесно, ако повече държави членки се възползваха от възможността, предвидена в Регламента, неправителствените организации да предприемат действия без да им бъде възлаган мандат за това<sup>39</sup>.

#### *Необходимост от продължаване на усилията за повишаване на осведомеността*

Следователно усилията за диалог и повишаване на осведомеността, насочени към широката общественост, трябва да продължат на национално равнище и на равнището на ЕС. За тази цел през юли 2019 г.<sup>40</sup> Комисията стартира нова онлайн кампания, с която да се насърчат физическите лица да четат декларациите за поверителност и да оптимизират своите настройки, гарантиращи неприкосновеността на личния живот.

### **V. Предприятията адаптират своите практики**

Целта на Регламента е да се окаже подкрепа на предприятията в цифровата икономика, като се предложат ориентирани към бъдещето решения. Като цяло предприятията приветстват принципа на отчетност в Регламента, който се отдалечава от предишния обременяващ подход *ex ante* (като се премахват изискванията за уведомяване, въвежда се степенуване на задълженията и гъвкавост на принципа за защита на данните на етапа на проектирането и по подразбиране, което дава поле за конкуренция въз основа на решения, гарантиращи неприкосновеността на личния живот). Същевременно някои призовават за по-голяма правна сигурност и допълнителни или по-ясни насоки от органите за защита на данните<sup>41</sup>.

#### *Добро управление на данните*

Макар дружествата да докладват за редица предизвикателства при адаптирането към новите правила<sup>42</sup>, много от тях подчертават, че това е и възможност въпросът за защитата на данните да бъде поставен на вниманието на управителните съвети на дружествата, да въведат ред по отношение на данните, които притежават, да подобрят сигурността, да бъдат по-добре подготвени в случай на инциденти, да намалят излагането на ненужни рискове и да изградят отношения на доверие със своите клиенти и търговски партньори. По отношение на прозрачността, предприятията и организациите на гражданското общество посочват деликатното равновесие, което трябва да се постигне между предоставянето на физическите лица на цялата

---

<sup>38</sup> Член 80, параграф 1 от Регламента.

<sup>39</sup> Член 80, параграф 2 от Регламента.

<sup>40</sup> Тази кампания се явява като продължение на предишни кампании, имащи за цел разпространението на информационни материали за физическите лица и предприятията, които могат да бъдат намерени на адрес: [https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules\\_bg](https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_bg).

<sup>41</sup> Вж. доклада на Многостранната група на заинтересованите страни по Регламента.

<sup>42</sup> Актуализирането на ИТ системата често се посочва като едно от основните предизвикателства, особено по отношение на практическото прилагане на принципите за защита на данните на етапа на проектирането и по подразбиране, правото на заличаване от резервни копия и т.н.

необходима информация съгласно Регламента и същевременното използване на ясни и недвусмислени формулировки и формат, които хората могат да разберат. В тази връзка операторите разработват иновативни решения.

Като цяло предприятията посочиха, че са успели да приложат новите права на субектите на данни, въпреки че понякога е било трудно да се спазят сроковете поради нарасналия брой на исканията и по-разнообразното им естество<sup>43</sup> или да се провери самоличността на лицето, което отправя искането.

### *Въздействие върху иновациите*

Регламентът не само позволява, но и насърчава разработването на нови технологии, като същевременно се зачита основното право на защита на личните данни. Такъв е случаят в области като изкуствения интелект.

Предприятията започнаха да разработват своите предложения за нови услуги, гарантиращи в по-голяма степен неприкосновеността на личния живот. Така например търсачките, които не проследяват потребителите или не използват поведенческа реклама в интернет, постепенно увеличават пазарните си дялове в някои държави членки. Други дружества разработват услуги, които са съобразени с новите права, предоставени на физическите лица, като например преносимостта на личните им данни. Все по-голям брой предприятия наблягат на зачитането на личните данни като фактор за диференциация и продажба. Тези явления не се ограничават до ЕС, а се наблюдават и във високоинновативни чуждестранни икономики<sup>44</sup>.

### *Специфичното положение на нискорисковите микро- и малки предприятия*

Въпреки че ситуацията се различава в отделните държави членки, микропредприятията и малките предприятия<sup>45</sup>, за които обработването на лични данни не е основна дейност, са сред заинтересованите страни с най-много въпроси относно прилагането на Регламента. Макар да изглежда, че тези въпроси произтичат отчасти от липсата на осведоменост относно правилата за защита на данните, опасенията на тези предприятия понякога се изострят допълнително от кампаниите на консултантски фирми, които се стремят да им предоставят платени съвети, от разпространението на неточна информация, например относно необходимостта от систематично получаване на съгласие от физическите лица<sup>46</sup>, както и от допълнителни изисквания, наложени на национално равнище.

---

<sup>43</sup> Предприятията също призоваха Комитета да разработи насоки относно неоснователните и прекомерните искания.

<sup>44</sup> Според доклад, публикуван от израелската асоциация на предприятията в сектора на киберсигурността, през 2018 г. подсекторът „Защита на данните и неприкосновеност на личния живот“ на сектора на киберсигурността е бил най-бързо разрастващия се подсектор, отчасти в резултат на влизането в сила на ОРЗД.

<sup>45</sup> Съгласно определението за МСП, достъпно на адрес: [https://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition\\_bg](https://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_bg).

<sup>46</sup> Всъщност Регламентът не разчита единствено на съгласието, а предвижда и няколко правни основания за обработването на лични данни.

В този контекст микропредприятията и малките предприятия призовават за изготвянето на насоки, които са съобразени със специфичното им положение и предоставят съвсем практическа информация. Някои органи за защита на данните вече изготвиха такива насоки на национално равнище<sup>47</sup>. За да допълни националните инициативи, Комисията публикува информационни материали, които да помогнат на тези дружества да спазват новите правила чрез поредица от практически стъпки<sup>48</sup>.

#### *Използване на набора от инструменти, предвидени в Регламента*

В Регламента са предвидени инструменти за доказване на съответствието с неговите разпоредби, като например стандартни договорни клаузи, кодекси за поведение, както и нововъведените механизми за сертифициране.

Стандартните договорни клаузи представляват примерни клаузи, които могат да бъдат включени на доброволен принцип в даден договор, например в договор между администратор на лични данни и обработващ лични данни, и които определят задълженията на договарящите се страни съгласно Регламента. С Регламента се разширяват възможностите за използване на стандартни договорни клаузи както за международното предаване на данни, така и в рамките на ЕС<sup>49</sup>. Широката им употреба в областта на международното предаване на данни показва<sup>50</sup>, че тези клаузи са много полезни за предприятията в техните усилия за спазване на изискванията и са от особена полза за дружествата, които не разполагат с необходимите ресурси, за да договарят индивидуални договори с всеки от своите изпълнители за обработване на данни.

Редица отрасли също смятат приемането на стандартни договорни клаузи като полезен начин за насърчаване на хармонизацията, особено когато Комисията е тази, която ги приема. Комисията ще работи съвместно със заинтересованите страни, за да се възползва от възможностите, предоставени с Регламента, и за да актуализира съществуващите клаузи.

Придържането към кодекси за поведение е друг оперативен и практически инструмент, с който предприятията разполагат, за да улеснят доказването на съответствие с Регламента<sup>51</sup>. Тези кодекси следва да бъдат разработвани от търговски сдружения или органи, представляващи категории администратори и обработващи лични данни, и следва да описват как правилата за защита на данните могат да се прилагат в конкретен

---

<sup>47</sup> Например ръководството, съставено от френския орган за защита на данните: <https://www.cnil.fr/fr/la-cnil-et-bpifrance-sassocient-pour-accompagner-les-tpe-et-pme-dans-leur-appropriation-du-reglement>.

<sup>48</sup> <https://ec.europa.eu/commission/sites/beta-political/files/ds-02-18-544-bg-n.pdf>.

<sup>49</sup> Вж. член 28 от Регламента. Стандартните договорни клаузи, приети от Комисията, са валидни навсякъде в ЕС. За разлика от това, стандартните договорни клаузи, приети съгласно член 28, параграф 8 от даден орган за защита на данните, са задължителни единствено за органа, който ги е приел, и поради това могат да се използват като стандартни договорни клаузи за операциите по обработване, които попадат под юрисдикцията на този орган в съответствие с членове 55 и 56.

<sup>50</sup> Те са на практика основният инструмент, на който разчитат дружествата при износа на данни.

<sup>51</sup> Европейският комитет по защита на данните прие насоки относно кодексите за поведение на 4 юни 2019 г. В тях се изясняват процедурите и правилата, свързани с внасянето, одобряването и публикуването на тези кодекси както на национално равнище, така и на равнището на ЕС.

отрасъл. Установявайки параметрите на задълженията в зависимост от рисковете<sup>52</sup>, тези кодекси могат да се окажат много полезен и рентабилен начин за изпълнение на задълженията от страна на малките и средните предприятия.

И накрая, сертифицирането може да бъде също полезен инструмент за доказване на съответствието със специфичните изисквания на Регламента. Чрез него може да се повиши правната сигурност за предприятията и да се популяризира Регламента в световен план. Наскоро приетите от Европейския комитет по защита на данните насоки за сертифицирането и акредитацията<sup>53</sup> ще позволят разработването на схеми за сертифициране в ЕС. Комисията ще наблюдава тези разработки и, ако е целесъобразно, ще използва предоставените ѝ по силата на Регламента правомощия, за да формулира изискванията за сертифициране. Комисията може също така да отправи искане за стандартизация до органите по стандартизация на ЕС относно елементите, които са от значение за Регламента.

## **VI. Възходящото сближаването напредва на международно равнище**

Търсенето на защита на личните данни не се ограничава до ЕС. Едно неотдавнашно глобално проучване на сигурността в интернет показва, че дефицитът на доверие се увеличава по целия свят, което кара хората да променят поведението си онлайн<sup>54</sup>. Все по-голям брой дружества отговарят на тези опасения, като разширяват по собствена инициатива прилагането на правата, създадени с Регламента, към своите клиенти, които не са установени в ЕС.

Освен това, тъй като държавите по света са изправени все по-често пред сходни предизвикателства, те изготвят нови правила за защита на данните или модернизират съществуващите такива. Тези закони често имат редица общи характеристики, които се съдържат и в режима на ЕС за защита на данните, като например хоризонтално законодателство вместо секторни правила, приложими индивидуални права и независим надзорен орган. Тази тенденция е наистина глобална — от Южна Корея до Бразилия, от Чили до Тайланд, от Индия до Индонезия. Присъединяването на все

---

<sup>52</sup> Съображение 98 от Регламента.

<sup>53</sup> [https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification\\_bg](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_bg);  
[https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42018-accreditation-certification-bodies-under\\_bg](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42018-accreditation-certification-bodies-under_bg)

<sup>54</sup> Вж. „Global Survey on Internet Security and Trust“ („Глобално проучване на сигурността и доверието в интернет) от 2019 г. на Центъра за иновации в международното управление (CIGI) и консултантската фирма Ipsos. Според проучването 78 % от анкетираните са загрижени за неприкосновеността на личния си живот онлайн, като 49 % заявяват, че недоверието им е довело до разкриването на по-малко лична информация онлайн, 43 % съобщават, че са положили по-големи усилия, за да обезопасят своето устройство, а 39 % отговарят, че използват интернет по-селективно, наред с други предпазни мерки. Проучването беше проведено в 25 икономики: Австралия, Бразилия, Великобритания, Германия, Египет, Индия, Индонезия, Италия, Канада, Кения, Китай, Мексико, Нигерия, Пакистан, Полша, Република Корея, Русия, САЩ, Тунис, Турция, Франция, Хонконг, Швеция, Южна Африка и Япония.

повече страни по света към Конвенция № 108 на Съвета на Европа<sup>55</sup> — наскоро осъвременена<sup>56</sup> със значителния принос на Комисията — е друг ясен знак за тази тенденция на възходящо сближаване.

*Насърчаване на безопасното и свободно движение на данни чрез решенията относно адекватното ниво на защита и други мерки*

Все по-тясното сближаване открива нови възможности за улесняване на потоците от данни, а следователно и на търговията, както и на сътрудничеството между публичните органи, като същевременно се повишава нивото на защита на личните данни на физическите лица в ЕС, когато данните им се предават в чужбина.

В изпълнение на стратегията, изложена в съобщението ѝ от 2017 г., озаглавено „Обмен и защита на личните данни в един глобализиран свят“<sup>57</sup>, Комисията засили работата си с трети държави и други международни партньори, основавайки се на и доразвивайки елементите на сближаване между системите за опазване на неприкосновеността на личния живот. Това включваше проучване на възможността за приемане на констатации относно адекватното ниво на защита с избрани трети държави<sup>58</sup>. С тази работа бяха постигнати важни резултати, по-специално влизането в сила през февруари 2019 г. на договореност с Япония за взаимно предоставяне на адекватно ниво на защита, с която беше създадена най-голямата зона в света за свободно и безопасно движение на данни. Преговорите за адекватното ниво на защита с Южна Корея са в напреднал стадий, като проучвателната работа продължава с цел започване на преговори за адекватност с няколко държави от Латинска Америка — като Чили или Бразилия — в зависимост от приключването на текущите законодателни процеси. Обещаващи са развитията и в някои части на Азия, като например Индия, Индонезия и Тайван, както и в източните и южните съседни на ЕС държави, като те биха могли да проправят пътя за бъдещи решения относно адекватното ниво на защита.

Същевременно Комисията приветства факта, че други държави, които са въвели инструменти за предаване, сходни с адекватното ниво на защита съгласно Регламента, признаха, че ЕС и държавите, признати от ЕС като „адекватни“, гарантират

---

<sup>55</sup> Конвенция на Съвета на Европа от 28 януари 1981 г. за защита на лицата при автоматизираната обработка на лични данни (ETS № 108) и Допълнителният протокол от 2001 г. към Конвенцията за защита на лицата при автоматизирана обработка на лични данни, по отношение на надзорните органи и трансграничните информационни потоци (ETS № 181). Това е единственият многостранен инструмент със задължителна сила в областта на защитата на данните. Сред държавите, ратифицирали последно Конвенцията, са Аржентина, Мексико, Кабо Верде и Мароко.

<sup>56</sup> Протокол за изменение на Конвенцията за защита на лицата при автоматизираната обработка на лични данни (ETS № 108), договорен на 128-та сесия на Комитета на министрите в Елсинор, Дания, 17—18 май 2018 г. Консолидиращият текст на осъвременената Конвенция № 108 е на разположение на адрес: <https://rm.coe.int/16808ade9d>.

<sup>57</sup> Съобщение на Комисията до Европейския парламент и Съвета — „Обмен и защита на личните данни в един глобализиран свят“, COM(2017) 07 final.

<sup>58</sup> Регламентът създаде също така възможност за констатации относно адекватното ниво на защита и по отношение на международни организации като част от усилията на ЕС за улесняване на обмена на данни с такива структури.

необходимото ниво на защита<sup>59</sup>. По този начин има възможност да се създаде мрежа от държави, между които данните могат да се движат свободно.

Наред с това в момента се работи усилено с други трети държави, като Канада, Нова Зеландия, Аржентина и Израел, за да се гарантира приемствеността съгласно Регламента на решенията относно адекватното ниво на защита, приети въз основа на Директивата за защита на данните от 1995 г. Междувременно Щитът за личните данни в отношенията между ЕС и САЩ, в който участват над 4700 дружества<sup>60</sup>, се доказва като полезен инструмент за осигуряването на трансатлантически потоци от данни въз основа на високо ниво на защита. Годишният му преглед гарантира, че правилното функциониране на рамката се проверява редовно и че новите въпроси могат да бъдат разгледани навреме.

Тъй като не съществува универсално решение за всички видове потоци от данни, Комисията работи също така съвместно със заинтересованите страни и с Комитета, за да се използва пълният потенциал на набора от инструменти за международно предаване на данни, съдържащ се в Регламента. Тази работа засяга инструменти като стандартни договорни клаузи, разработване на схеми за сертифициране, кодекси за поведение или административни договорености за публичните органи. В това отношение Комисията проявява интерес към обмена на опит и най-добри практики с други системи, които може да имат конкретен опит с някои от тези инструменти. Комисията ще обмисли възможността да използва своите правомощия по Регламента във връзка с тези инструменти за предаване, и по-специално стандартните договорни клаузи.

Освен чисто двустранните инструменти, би било полезно и да се проучи дали държавите със сходни възгледи биха могли да създадат многонационална рамка в тази област в момент, когато потоците от данни са все по-важна част от търговията, комуникациите и социалните взаимодействия. Такъв инструмент ще даде възможност за свободно движение на данни между договарящите страни, като същевременно се гарантира необходимото ниво на защита на основата на споделени ценности и сближаване на системите. Той може да бъде разработен например въз основа на осъвременената Конвенция № 108 или да черпи вдъхновение от инициативата „свободно и надеждно движение на данни“, стартирана от Япония в началото на тази година.

#### *Разработване на нови синергии между инструментите за търговия и за защита на данните*

Комисията насърчава сближаването на стандартите за защита на данните на международно равнище и същевременно е решена да се бори с цифровия протекционизъм. За тази цел тя разработи специални разпоредби относно потоците от

---

<sup>59</sup> Това е подходът, възприет например от Аржентина, Колумбия, Израел и Швейцария.

<sup>60</sup> Това означава, че през първите три години от съществуването си в Щита за личните данни участват повече дружества, отколкото в неговия предшественик, рамката „Safe Harbour“, след 13 години функциониране.

данни и защитата на данните в търговски споразумения, които системно включва във водените от нея двустранни и многостранни преговори, като например текущите преговори в рамките на СТО за електронната търговия. Тези хоризонтални разпоредби изключват чисто протекционистки мерки, като например изисквания за задължително локализиране на данните, като същевременно запазват регулаторната независимост на страните да отстояват основното право на защита на данните.

Макар че диалозите относно защитата на данните и търговските преговори трябва да се водят по отделни направления, те могат да се допълват взаимно: договореността между ЕС и Япония за взаимно предоставяне на адекватно ниво на защита е най-добрият пример за такива синергии, които допълнително улесняват търговския обмен и по този начин засилват ползите от Споразумението за икономическо партньорство. Този вид сближаване, почиващо на споделени ценности и високи стандарти и подкрепено с ефективно правоприлагане, предоставя най-стабилна основа за обмена на лични данни, като това все по-често се признава от нашите международни партньори<sup>61</sup>. Като се има предвид, че дружествата работят все по-често през граница и предпочитат да прилагат сходни набори от правила във всички свои стопански дейности по света, това сближаване спомага за създаването на среда, която благоприятства преките инвестиции, улеснява търговията и повишава доверието между търговските партньори.

*Улесняване на обмена на информация с цел борба с престъпността и тероризма въз основа на подходящи гаранции*

По-голямата съвместимост между режимите за защита на данните може значително да улесни така необходимия обмен на информация между ЕС и чуждестранните регулаторни, полицейски и съдебни органи и по този начин да допринесе за по-ефективното и по-бързо сътрудничество в областта на правоприлагането<sup>62</sup>. За тази цел Комисията възнамерява да се възползва от възможността да приеме решения относно адекватното ниво на защита съгласно Директивата относно правоприлагането в областта на защитата на данните, за да задълбочи сътрудничеството си с ключови партньори в борбата с престъпността и тероризма. Освен това Рамковото споразумение за защита на данните между ЕС и САЩ<sup>63</sup>, което влезе в сила през февруари 2017 г.,

---

<sup>61</sup> Както е отразено, например, в позоваването на понятието „свободно и надеждно движение на данни“ в Декларацията на ръководителите на държавите от G-20 от Осака: [https://www.consilium.europa.eu/media/40124/final\\_g20\\_osaka\\_leaders\\_declaration.pdf](https://www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf).

<sup>62</sup> Съобщение на Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите — „Европейска програма за сигурност“, COM(2015) 185 final.

<sup>63</sup> Споразумение между ЕС и САЩ относно защитата на личната информация във връзка с предотвратяването, разследването, разкриването и наказателното преследване на престъпления, включително тероризъм, в рамките на полицейското сътрудничество и съдебното сътрудничество по наказателноправни въпроси: [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:22016A1210\(01\)](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:22016A1210(01)) („Рамковото споразумение“). Рамковото споразумение представлява първото двустранно международно споразумение в областта на правоприлагането, с което се установява изчерпателен списък на правата и задълженията, свързани със защитата на данните, в съответствие с достиженията на правото на ЕС. То е успешен пример за това как сътрудничеството в областта на правоприлагането с важен международен партньор може да бъде засилено чрез договарянето на солиден набор от гаранции за защита на данните.



може да се използва като модел за подобни споразумения с други важни партньори в областта на сигурността.

Други примери за значението на високите стандарти за защита на данните като основа за стабилно сътрудничество в областта на правоприлагането с трети държави са предаването на резервационни данни на пътниците (PNR данни)<sup>64</sup> и обменът на оперативна информация между Европол и важни международни партньори. Във връзка с това в момента се водят или предстоят да започнат преговори по международни споразумения с няколко държави от региона на южното съседство<sup>65</sup>.

Строгите гаранции за защита на данните също ще бъдат съществен елемент на всяко бъдещо споразумение за трансграничен достъп до електронни доказателства при наказателни разследвания на двустранно равнище (споразумение между ЕС и САЩ) или на многостранно равнище (втори допълнителен протокол към Конвенцията на Съвета на Европа за престъпления в кибернетичното пространство)<sup>66</sup>.

#### *Насърчаване на сътрудничеството между правоприлагащите органи по защитата на данните*

В момент, когато проблеми при спазването на правилата за неприкосновеност на личния живот или инциденти, свързани със сигурността, могат да засегнат едновременно голям брой физически лица в няколко юрисдикции, по-тясното сътрудничество между надзорните органи на международно равнище може да спомогне за осигуряване както на по-ефективна защита на индивидуалните права, така и на по-стабилна среда за стопанските субекти. В този контекст и в тясна връзка с Комитета Комисията ще работи върху начините за улесняване на сътрудничеството и взаимната помощ при правоприлагането между ЕС и чуждестранните надзорни органи, включително чрез използването на новите правомощия, предоставени ѝ в тази област от Регламента<sup>67</sup>. Това би могло да включва различни форми на сътрудничество — от изготвянето на общи тълкувателни или практически инструменти<sup>68</sup> до обмена на информация за текущи разследвания.

Накрая, Комисията възнамерява също така да засили диалога си с регионалните организации и мрежи, като Асоциацията на народите от Югоизточна Азия (АСЕАН), Африканския съюз, Форума на органите за защита на неприкосновеността на личния

---

<sup>64</sup> Резолюция 2396 на Съвета за сигурност на ООН от 21 декември 2017 г. призовава всички държави — членки на ООН, да развият способността да събират, обработват и анализират PNR данни при пълно зачитане на правата на човека и основните свободи. Вж. също Съобщение на Комисията „Европейска програма за сигурност“, COM(2015) 185 final: <http://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:52015DC0185&from=EN>.

<sup>65</sup> [https://ec.europa.eu/home-affairs/news/security-union-strengthening-europols-cooperation-third-countries-fight-terrorism-and-serious\\_en](https://ec.europa.eu/home-affairs/news/security-union-strengthening-europols-cooperation-third-countries-fight-terrorism-and-serious_en)

<sup>66</sup> [http://europa.eu/rapid/press-release\\_IP-19-2891\\_en.htm](http://europa.eu/rapid/press-release_IP-19-2891_en.htm)

<sup>67</sup> Вж. член 50 от Регламента относно международното сътрудничество в областта на защитата на данните. Тази разпоредба обхваща широк спектър от форми на сътрудничество — от информацията относно законодателството за защита на данните до препращането на жалби и помощта при разследвания.

<sup>68</sup> Като например общи образци за уведомления за нарушения.

живот в азиатско-тихоокеанския регион (АРРА) или Иbero-американската мрежа за защита на данните, които играят все по-важна роля при формулирането на общи стандарти за защита на данните, насърчаването на обмена на най-добри практики и установяването на сътрудничество между правоприлагащите органи. Тя ще работи и с Организацията за икономическо сътрудничество и развитие и с Азиатско-тихоокеанската организация за икономическо сътрудничество с цел постигане на сближаване към високо равнище на защита на данните.

## **VII. Законодателството в областта на защитата на данните е неразделна част от широк спектър от политики**

Защитата на личните данни е гарантирана и интегрирана в няколко политики на Съюза.

### *Далекосъобщителни и електронни съобщителни услуги*

През януари 2017 г. Комисията прие предложение за регламент за неприкосновеността на личния живот и електронните съобщения<sup>69</sup>. Целта на предложението е да се защити поверителността на съобщенията, както е предвидено в Хартата на основните права, но и да се защитят личните данни, които могат да бъдат част от съобщение, както и крайните устройства на крайните потребители.

Предложеният регламент за неприкосновеността на личния живот и електронните съобщения конкретизира и допълва Регламента, като определя конкретни правила за постигането на горепосочените цели. С него се осъвременяват действащите правила на ЕС за защита на неприкосновеността на личния живот и електронните съобщения<sup>70</sup> с цел да се вземе предвид технологичното и правното развитие. С него се подобрява неприкосновеността на личния живот на физическите лица, като се разширява обхватът на новите правила, така че да се обхванат и доставчиците на ОТТ услуги, с което се създават равни условия за всички електронни съобщителни услуги. Въпреки че Европейският парламент прие през октомври 2017 г. мандат за започването на тристранен диалог, Съветът все още не е постигнал съгласие по общ подход. Комисията продължава да поддържа безусловно Регламента за неприкосновеността на личния живот и електронните съобщения и ще подкрепи съзаконодателите в усилията им за бързо приемане на предложения регламент.

### *Здравеопазване и научни изследвания*

Улесняването на обмена между държавите членки на данни за здравословното състояние, които съгласно Регламента се определят като чувствителни данни, придобива все по-голямо значение в областта на общественото здраве по съображения

---

<sup>69</sup> <https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A52017PC0010>

<sup>70</sup> Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 г. относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронни комуникации) (ОВ L 201, 31.7.2002 г., стр. 37—47).

от обществен интерес. Тези съображения включват предоставянето на здравно обслужване или лечение, защитата срещу сериозни трансгранични заплахи за здравето и осигуряването на високи стандарти за качество и безопасност на здравните грижи и лекарствените продукти или медицинските изделия. Регламентът определя правилата, с които се гарантират законосъобразното и надеждно обработване и обмен на данни за здравословното състояние в целия ЕС. Тези правила се прилагат и за достъпа на трети страни до медицинските данни на пациентите, включително за данните, съхранявани в техните медицински досиета, електронните рецепти и в дългосрочен план за изчерпателните електронни здравни досиета, както и за използването им за научноизследователски цели. В специфичната област на клиничните изпитвания Комисията изготви специален документ с въпроси и отговори относно взаимодействието между Регламента за клиничните изпитвания<sup>71</sup> и Общия регламент относно защитата на данните<sup>72</sup>.

### *Изкуствен интелект*

Тъй като изкуственият интелект придобива стратегическа важност, от съществено значение е да се оформят правила на световно равнище за неговото развитие и използване. При насърчаването на разработването и внедряването на изкуствения интелект Комисията избра подход, ориентиран към човека, което означава, че приложенията на изкуствения интелект трябва да спазват основните права<sup>73</sup>. В този контекст установените в Регламента правила предоставят обща рамка и съдържат специални задължения и права, които са от особено значение за обработването на лични данни с изкуствен интелект. Така например в Регламента се предвижда правото физическите лица да не подлежат на изцяло автоматизирано вземане на решения, освен в определени ситуации<sup>74</sup>. Той съдържа също така специални изисквания за прозрачност относно използването на автоматизирано вземане на решения, а именно задължението да се информира за съществуването на такива решения и да се предоставят съдържателна информация и обяснения за неговото значение и очакваните последствия от обработването за физическото лице<sup>75</sup>. Тези основни принципи на Регламента бяха признати от Експертната група на високо равнище по въпросите на изкуствения интелект<sup>76</sup>, Организацията за икономическо сътрудничество и развитие<sup>77</sup> и Г-20<sup>78</sup> като

<sup>71</sup> <https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=celex%3A32014R0536>

<sup>72</sup> [https://ec.europa.eu/health/sites/health/files/documents/qa\\_clinicaltrials\\_gdpr\\_en.pdf](https://ec.europa.eu/health/sites/health/files/documents/qa_clinicaltrials_gdpr_en.pdf)

<sup>73</sup> Съобщение на Комисията от 8 април 2019 г. относно изграждането на доверие в ориентирания към човека изкуствен интелект: <https://eur-lex.europa.eu/legal-content/BG/TXT/?qid=1564565098928&uri=CELEX:52019DC0168>.

Насоки относно етичните аспекти за надежден изкуствен интелект, представени от Експертната група на високо равнище на 8 април 2019 г.: <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>. Вж. също Препоръката на Съвета на ОИСР относно изкуствения интелект: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>, принципите на изкуствения интелект на Г-20, одобрени като част от Декларацията на ръководителите на държавите от Г-20 от Осака: [https://www.g20.org/pdf/documents/en/annex\\_08.pdf](https://www.g20.org/pdf/documents/en/annex_08.pdf) и Декларацията на министрите на държавите от Г-20 относно търговията и цифровата икономика: [https://g20trade-digital.go.jp/dl/Ministerial\\_Statement\\_on\\_Trade\\_and\\_Digital\\_Economy.pdf](https://g20trade-digital.go.jp/dl/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf).

<sup>74</sup> Член 22 от Регламента.

<sup>75</sup> Член 13, параграф 2, буква е) от Регламента.

<sup>76</sup> <https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence>

особено важни за справянето с предизвикателствата и използването на възможностите, произтичащи от изкуствения интелект. Европейският комитет по защита на данните определи изкуствения интелект като една от възможните теми в работната си програма за периода 2019—2020 г.<sup>79</sup>

### *Транспорт*

Развитието на свързани автомобили и интелигентни градове разчита все повече на обработването и обмяна на големи обеми лични данни между множество страни, в това число автомобили, производители на автомобили, доставчици на телематични услуги и публични органи, отговарящи за пътната инфраструктура. Тази многолика среда създава известна сложност по отношение на разпределението на ролите и отговорностите на различните участници в обработването на личните данни, както и по отношение на начините за гарантиране на законосъобразността на обработването от всички участници. Спазването на Регламента и на законодателството в областта на неприкосновеността на личния живот и електронните съобщения е от съществено значение за успешното внедряване на интелигентни транспортни системи във всички видове транспорт и за разпространението на цифрови инструменти и услуги, позволяващи по-голяма мобилност на хора и стоки<sup>80</sup>.

### *Енергетика*

Разработването на цифрови решения за енергийния сектор все повече разчита на обработването на лични данни. Законодателството, прието като част от пакета „Чиста енергия за всички европейци“<sup>81</sup>, включва нови разпоредби, които правят възможна цифровизацията на електроенергийния сектор, и правила за достъпа до данни, управлението на данни и оперативната съвместимост, които дават възможност за работа с данните на потребителите в реално време за постигане на икономии и насърчаване на собственото производство на електроенергия и участие в енергийния пазар. Поради това спазването на правилата за защита на данните е от голямо значение за успешното прилагане на тези разпоредби.

### *Конкуренция*

Обработването на лични данни е все по-често аспект, на който следва да се обръща внимание в политиката в областта на конкуренцията<sup>82</sup>. Като се има предвид, че органите за защита на данните са единствените органи, на които е възложено да

---

<sup>77</sup> Препоръка на Съвета относно изкуствения интелект:  
<https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>.

<sup>78</sup> Декларацията на министрите на държавите от Г-20 относно търговията и цифровата икономика:  
[https://g20trade-digital.go.jp/dl/Ministerial\\_Statement\\_on\\_Trade\\_and\\_Digital\\_Economy.pdf](https://g20trade-digital.go.jp/dl/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf).

<sup>79</sup> [https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12plen-2.ledpb\\_work\\_program\\_bg.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12plen-2.ledpb_work_program_bg.pdf)

<sup>80</sup> Например чрез улесняване на планирането и използването на различни транспортни средства по време на цялото им пътуване.

<sup>81</sup> По-специално Директивата за електроенергията:  
<https://eur-lex.europa.eu/legal-content/BG/ALL/?uri=CELEX%3A32009L0072>.

<sup>82</sup> Например дело M.8788 — Apple/Shazam и дело M. M.8124 — Microsoft/LinkedIn.

оценяват нарушенията на правилата за защита на данните, органите за защита на конкуренцията, потребителите и органите за защита на данните си сътрудничат и ще продължат да си сътрудничат при необходимост в пресечната точка на съответните им области на компетентност. Комисията ще насърчава това сътрудничество и ще следи отблизо неговия развой.

### *В контекста на избори*

В своите Насоки относно защитата на данните в контекста на избори<sup>83</sup>, публикувани през септември 2018 г. като част от пакета от мерки за изборите<sup>84</sup>, Комисията обърна внимание на правилата от особено значение за участниците в изборите, включително въпросите, свързани с микротаргетирането на гласоподавателите. Тези насоки бяха повторени в изявление на Европейския комитет по защита на данните<sup>85</sup> и от редица органи по защита на данните издадоха насоки на национално равнище. Пакетът от мерки за изборите включваше и призив към всяка държава членка да създаде национална избирателна мрежа с участието на националните органи, компетентни по изборните въпроси, и органите, отговарящи за наблюдението и прилагането на правилата, като например за защитата на данните и онлайн дейностите, свързани с изборите. Бяха приети и нови мерки, въвеждащи санкции за нарушения на правилата за защита на данните от страна на европейските политически партии и фондации. Комисията препоръча на държавите членки да възприемат същия подход на национално равнище. В оценката на изборите за Европейски парламент през 2019 г., която трябва да бъде публикувана през октомври 2019 г., ще бъдат взети предвид и аспектите, свързани със защитата на данните.

### *Правоприлагане*

Ефективен и истински Съюз на сигурност може да бъде изграден единствено въз основа на пълното зачитане на основните права, залегнали в Хартата на основните права на ЕС и вторичното законодателство на ЕС, включително подходящи гаранции за защита на данните, за да се даде възможност за сигурен обмен на лични данни за целите на правоприлагането. Всички ограничения на основното право на неприкосновеност на личния живот и на защита на личните данни подлежат на строга проверка за необходимост и пропорционалност.

## **VIII. Заключение**

Въз основа на информацията, която е на разположение към момента, и на диалога със заинтересованите страни, предварителната оценка на Комисията е, че резултатите от първата година от прилагането на Регламента като цяло са положителни. Въпреки това,

---

<sup>83</sup> <https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:52018DC0638&qid=1564574699366&from=EN>

<sup>84</sup> [https://europa.eu/rapid/press-release\\_IP-18-5681\\_bg.htm](https://europa.eu/rapid/press-release_IP-18-5681_bg.htm)

<sup>85</sup> [https://edpb.europa.eu/sites/edpb/files/files/file1/201902\\_edpb\\_statementonelections\\_bg.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/201902_edpb_statementonelections_bg.pdf)

както се посочва в настоящото съобщение, в редица области е необходим допълнителен напредък.

*Изпълнение и допълване на правната уредба:*

- Трите държави членки, които все още не са актуализирали своите национални закони за защита на данните, трябва да го направят незабавно. Всички държави членки следва да завършат привеждането в съответствие на своето секторно законодателство с изискванията на Регламента.
- Комисията ще използва всички инструменти, с които разполага, включително производствата за установяване на нарушение, за да гарантира, че държавите членки спазват Регламента, и за да ограничи разпокъсаността на уредбата за защита на данните.

*Разгръщане на пълния потенциал на новата система на управление:*

- Държавите членки следва да осигурят на националните органи за защита на данните достатъчно човешки, финансови и технически ресурси.
- Органите за защита на данните следва да засилят сътрудничеството помежду си, например като провеждат съвместни разследвания. Държавите членки следва да способстват за провеждането на такива разследвания.
- Комитетът следва да продължи да развива културата на ЕС за защита на данните и да използва пълноценно инструментите, предвидени в Регламента, за да гарантира хармонизирано прилагане на правилата. Той следва да продължи работата си по изготвянето на насоки, особено за малките и средните предприятия.
- Експертният опит на секретариата на Комитета следва да се подсили, така че той да подпомага и ръководи по-ефективно работата на Комитета.
- Комисията ще продължи да оказва подкрепа на органите за защита на данните и Комитета, по-специално като участва активно в работата на Комитета и привлича неговото внимание към изискванията на правото на ЕС в хода на прилагането на Регламента.
- Комисията ще подкрепя взаимодействието между органите за защита на данните и други компетентни органи, по-специално в областта на конкуренцията, при пълно зачитане на съответните им компетентности.

*Подкрепа и участие на заинтересованите страни:*

- Комитетът следва да подобри начина, по който включва заинтересованите страни в своята работа. Комисията ще продължи своята финансова подкрепа за органите за защита на данните, за да им помогне да достигнат до заинтересованите страни.

- Комисията ще продължи своите дейности за повишаване на осведомеността и работата си със заинтересованите страни.

*Насърчаване на международното сближаване:*

- Комисията ще активизира още повече диалога относно адекватното ниво на защита с отговарящите на условията за това ключови партньори, включително в областта на правоприлагането. По-специално, тя си поставя за цел да приключи текущите преговори с Южна Корея през идните месеци. Тя ще докладва през 2020 г. относно прегледа на 11-те решения относно адекватното ниво на защита, приети съгласно Директивата за защита на данните.
- Комисията ще продължи работата си, включително чрез техническа помощ, обмен на информация и най-добри практики, с държавите, проявяващи интерес към приемането на модерни закони за неприкосновеността на личния живот, и ще насърчава сътрудничеството с надзорните органи на трети държави и регионалните организации.
- Комисията ще си сътрудничи с многостранни и регионални организации за популяризирането на високи стандарти за защита на данните като фактор, способстващ за търговията и улесняващ сътрудничеството (например в рамките на инициативата „Свободно и надеждно движение на данни“, стартирана от Япония в контекста на Г-20).

Съгласно Регламента<sup>86</sup> от Комисията се изисква да докладва за неговото изпълнение през 2020 г. Това ще даде възможност за оценка на постигнатия напредък и на това дали след две години на прилагане различните компоненти на новия режим за защита на данните функционират пълноценно. За тази цел Комисията ще работи с Европейския парламент, Съвета, държавите членки, Европейския комитет по защита на данните, съответните заинтересовани страни и гражданите.

---

<sup>86</sup> Член 97 от Регламента.