ЕВРОПЕЙСКА КОМИСИЯ

Брюксел, 25.1.2012 г.
COM(2012) 9 final

СЪОБЩЕНИЕ ОТ КОМИСИЯТА ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ, ДО СЪВЕТА, ДО ЕВРОПЕЙСКИЯ ИКОНОМИЧЕСКИ И СОЦИАЛЕН КОМИТЕТ И ДО КОМИТЕТА НА РЕГИОНИТЕ

Защитата на правото на личен живот във взаимосвързания свят
Европейска рамка за защита на данните за 21-ви век(Текст от значение за ЕИП)

[…]

СЪОБЩЕНИЕ ОТ КОМИСИЯТА ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ, ДО СЪВЕТА, ДО ЕВРОПЕЙСКИЯ ИКОНОМИЧЕСКИ И СОЦИАЛЕН КОМИТЕТ И ДО КОМИТЕТА НА РЕГИОНИТЕ

Защитата на правото на личен живот във взаимосвързания свят
Европейска рамка за защита на данните за 21-ви век

(Текст от значение за ЕИП)

1. ДНЕШНИТЕ ПРЕДИЗВИКАТЕЛСТВА ЗА ЗАЩИТАТА НА ДАННИТЕ

Бързите темпове на технологичните промени и глобализацията коренно промениха начина, по който се събират, правят достъпни, използват и предават все по-голям обем от лични данни. Новите начини за обмен на информация чрез социални мрежи и за съхраняване на големи количества данни от разстояние са част от живота на много от 250-те милиона души, ползващи интернет в Европа. Същевременно личните данни се превърнаха в ценна придобивка за много предприятия. Събирането, организирането и анализирането на данни на потенциални клиенти често е важна част от икономическата им дейност[1].

В тази нова цифрова среда **физическите лица имат правото да упражняват ефективен контрол върху своята лична информация.** Защитата на личните данни е основно право в Европа, залегнало в член 8 от Хартата на основните права на Европейския съюз, както и в член 16, параграф 1 от Договора за функционирането на Европейския съюз (ДФЕС), и трябва да бъде защитавано по-съответния начин.

Липсата на доверие кара потребителите да се колебаят дали да пазаруват онлайн и дали да ползват нови услуги. Ето защо високото ниво на защита на данните е жизненоважна за повишаване на доверието в онлайн услугите и за реализиране на потенциала на цифровата икономика, с което ще се насърчат **икономическият растеж и конкурентоспособността на предприятията в ЕС**.

Необходими са съвременни съгласувани норми в целия ЕС, за да могат данните да се преминават безпрепятствено от една държава-членка в друга. Предприятията се нуждаят от ясни и уеднаквени правила, които предоставят правна сигурност и свеждат до минимум административната тежест. Това е от съществено значение за функционирането на единния пазар и за **стимулирането на икономическия растеж, създаването на нови работни**

[1] Пазарът за анализ на много големи набори от данни се увеличава с 40 % годишно в световен мащаб: http://www.mckinsey.com/mgi/publications/big_data/.

места и поощряването на иновациите[2]. Осъвременяването на правилата на ЕС за защита на данните, с което се засилва тяхното измерение, свързано с вътрешния пазар, гарантира високо ниво на защита на личните данни на физическите лица и увеличава правната сигурност, яснотата и съгласуваността, и следователно заема важно място в Плана за действие на Европейската комисия за изпълнение на Стокхолмската програма[3], в Програмата в областта на цифровите технологии за Европа[4] и, в по-широк план, за стратегията на ЕС за растеж „Европа 2020“[5].

Директивата на ЕС от 1995 г.[6], която е основният законодателен инструмент за защитата на личните данни в Европа, представлява важен етап в историята на защитата на данните. Целта на директивата — да се гарантират функционирането на единния пазар и ефективната защита на основните права и свободи на физическите лица, остава актуална. Директивата обаче беше приета преди 17 години, когато интернет все още беше съвсем в началото на своето развитие. В днешната нова, изпълнена с предизвикателства цифрова среда съществуващите норми не предвиждат нито необходимата степен на хармонизиране, нито нужната ефикасност, за да се подсигури правото на защита на личните данни. Ето защо Европейската комисия предлага фундаментална реформа на правната рамка на ЕС за защита на данните.

Освен това с Договора от Лисабон, и по-специално с член 16 от ДФЕС, се създаде ново правно основание за осъвременен и комплексен подход към защитата на данните и свободното движение на лични данни, включително в областта на полицейското и съдебното сътрудничество по наказателноправни въпроси[7]. Този подход е отразен в съобщенията на Европейската комисия относно Стокхолмската програма и Плана за действие по нея[8], в които се подчертава необходимостта Съюзът да „разполага с цялостен режим на защита на личните данни, който обхваща всички области на компетентност на Съюза“ и „да гарантира, че основното право на защита на данните се прилага по последователен начин“.

За да подготви по прозрачен начин реформата на правната рамка на ЕС за защита на данните, Комисията проведе обществени консултации по въпросите на защитата на данните[9] и участва в интензивен диалог със заинтересованите

---

2 Вж. също заключенията на Европейския съвет от 23 октомври 2011 г., в които се подчертават „ключовата роля“ на единния пазар „за осигуряване на растеж и трудова заетост“, както и нуждата да се завърши изграждането на цифровия единен пазар до 2015 г.

3 COM(2010) 171 final.

4 COM(2010) 245 final.

5 COM(2010) 2020 final.

6 Директива 95/46/ЕО за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни, ОВ L 281, 23.11.1995 г., стр. 31.

7 С решение на Съвета на основание член 39 от ДЕС ще бъдат установени специфични норми за обработването на данни от държавите-членки в областта на общата външна политика и политиката на сигурност.

8 COM (2009) 262 и COM (2010) 171 съответно.

9 Две обществени консултации бяха проведени във връзка с реформата на защитата на данните: една в периода от юли до декември 2009 г., (http://ec.europa.eu/justice/news/consulting_public/news_consulting_0003_en.htm) и втора в периода от ноември 2010 г. до януари 2011 г. (http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm).

страни[10]. На 4 ноември 2010 г. Комисията публикува съобщение, озаглавено „Всеобхватен подход за защита на личните данни в Европейския съюз“[11], в което се посочват основните теми на реформата. В периода между септември и декември 2011 г. Комисията участва в засилен диалог с европейските национални органи по защита на данните и Европейския надзорен орган по защита на данните с цел да проучи варианти за по-съгласувано прилагане на правилата на ЕС за защита на данните във всички държави-членки на ЕС[12].

Тези дискусии ясно показаха, че гражданите и предприятията желаят Европейската комисия да проведе цялостна реформа на правилата на ЕС за защита на данните. След като оцени въздействието на различните варианти за политика[13], Европейската комисия понастоящем предлага **стабилна и съгласувана законодателна рамка за политики на Съюза, с която се усъвършенстват правата на физическите лица и свързаното с единния пазар измерение на защитата на данните и се намалява драстично бюрокрацията за предприятията**[14]**.** Комисията предлага новата рамка да се състои от:

– **регламент** (заменящ Директива 95/46/ЕО), с който се установява общата правна рамка на ЕС за защита на данните[15];

– и **директива** (заменяща Рамково решение 2008/977/ПВР[16]), с която се установяват нормите относно защитата на личните данни, обработвани за целите на **предотвратяването, разкриването, разследването или наказателното преследване на престъпления и свързани съдебни дейности**.

---

10 През 2010 г. бяха организирани целенасочени консултации с органите на държавите-членки и със заинтересовани страни от частния сектор. През ноември 2010 г. комисарят по правосъдието Вивиан Рединг организирани кръгла маса относно реформата на защитата на данните. През 2011 г. бяха проведени и допълнителни специализирани работни срещи и семинари по конкретни въпроси (напр. уведомленията за нарушения на сигурността на данните).

11 COM(2010)609.

12 Вж. писмото на комисаря по правосъдието на ЕС Вивиан Рединг от 19 септември 2011 г. до членовете на работната група по член 29, публикувано на адрес: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/index_en.htm.

13 Вж. оценката на въздействието SEC(2012)72.

14 Това ще включва на по-късен етап изменения за привеждане в съответствие на специфични и секторни инструменти, по-специално Регламент (ЕО) № 45/2001 (ОВ L 8, 12.1.2001 г., стр. 1.).

15 С регламента се правят също така ограничен брой технически промени в Директивата за правото на неприкосновеност на личния живот и електронни комуникации (Директива 2002/58/ЕО, последно изменена с Директива 2009/136/ЕО, ОВ L 337, 18.12.2009 г., стр. 11), с които да се отчете превръщането на Директива 95/46/ЕО в регламент. Комисията ще направи своевременен преглед на материалноправните последици от новия регламент и новата директива за Директивата за правото на неприкосновеност на личния живот и електронни комуникации, при който ще бъде отчетен резултатът от обсъжданията на представените понастоящем предложения в Европейския парламент и в Съвета.

16 Рамково решение 2008/977/ПВР на Съвета от 27 ноември 2008 година относно защитата на личните данни, обработвани в рамките на полицейското и съдебното сътрудничество по наказателноправни въпроси, OJ L 350, 30.12.2008 г., стр. 60. Като част от пакета от реформи на защитата на данните е приет доклад за прилагането на рамковото решение от държавите-членки (COM(2012)12).

Настоящото съобщение представя основните елементи на реформата на правната рамка на ЕС за защита на данните.

2. ПРЕДОСТАВЯНЕ НА ФИЗИЧЕСКИТЕ ЛИЦА НА КОНТРОЛ ВЪРХУ ЛИЧНИТЕ ИМ ДАННИ

Съгласно Директива 95/46/ЕО — основният законодателен акт на ЕС в областта на защитата на данните към днешна дата — начините, по които физическите лица могат да упражняват правото си на защита на данните, не са достатъчно хармонизирани в различните държави-членки. Правомощията на националните органи, отговорни за защитата на личните данни, също не са хармонизирани достатъчно, за да се гарантира съгласуваното и ефективно прилагане на нормите. Това означава, че действителното упражняване на тези права е по-трудно в някои държави-членки в сравнение с други, особено онлайн.

Тези трудности се дължат също и на огромния обем от данни, които се събират ежедневно, както и на факта, че потребителите често не са съвсем наясно, че техните данни се събират. Въпреки че много европейци считат, че разкриването на лични данни е във все по-голяма степен част от съвременния живот[17], 72 % от ползващите интернет в Европа все още се притесняват, че им се искат твърде много лични данни онлайн[18]. Те имат усещането, че нямат контрол върху своите данни. Те не са информирани по подходящ начин за това какво се случва с личните им данни, на кого се предават и за какви цели. Често те не знаят как да упражняват правата си онлайн.

„Правото да бъдеш забравен“

Европейски студент, който е член на социална мрежа онлайн, решава да поиска достъп до всички лични данни, с които мрежата разполага за него. Правейки това, той открива, че мрежата събира много повече данни, отколкото той си е мислел, и че някои лични данни, които според него са били заличени, все още се съхраняват.

С реформата на правилата на ЕС за защита на данните ще се гарантира, че това няма да се случва повече, посредством въвеждането на:

- изрично изискване, което задължава социалните мрежи онлайн (и всички други администратори на данни) да свеждат до минимум обема на личните данни на ползвателите, които те събират и обработват;

- изискване стандартните настройки да гарантират, че данните не са обществено достъпни;

- изрично задължение за администраторите на данни да заличават личните данни на дадено физическо лице, ако това лице изрично поиска заличаването им и ако не съществуват други легитимни причини те да бъдат запазени.

В този конкретен случай това ще задължи доставчика на социалната мрежа да заличи незабавно и изцяло личните данни на студента.

---

17 Вж. Специално проучване на Евробарометър 359 — „*Нагласи относно защитата на данните и електронната самоличност в Европейския съюз*“, юни 2011 г., стр. 23.

18 Пак там, стр. 54.

Както се подчертава в Програмата в областта на цифровите технологии за Европа, опасенията за неприкосновеността на личния живот са сред най-честите причини хората да не купуват стоки и услуги онлайн. Като се има предвид приносът на сектора на информационните и комуникационните технологии (ИКТ) за общия растеж на производителността в Европа — 20 % пряко от сектора на ИКТ и 30 % от инвестиции в ИКТ[19] — доверието в тези услуги е жизненоважно, за да се стимулират растежът на икономиката на ЕС и конкурентоспособността на европейската промишленост.

Уведомления за нарушения на сигурността на личните данни

Хакери атакуват услуга за хазартни игри, насочена към ползватели в ЕС. Нарушението на сигурността засяга бази данни, съдържащи личните данни (включително имена, адреси и вероятно информация за кредитни карти) на десетки милиони ползватели от целия свят. Дружеството изчаква цяла седмица, преди да уведоми заинтересованите ползватели.

С реформата на правилата на ЕС за защита на данните ще се гарантира, че това повече няма да се случва. Новите правила ще задължат дружествата:

- да засилят своите мерки за сигурност за предотвратяване и избягване на нарушения на сигурността;

- да уведомяват за нарушения на сигурността както националния орган за защита на данните — в срок от 24 от установяване на нарушението на сигурността, когато това е възможно — така и засегнатите физически лица без ненужно забавяне.

Целта на новите законодателни актове, предложени от Комисията, е да се укрепят правата, да се предоставят ефикасни и оперативни средства на хората, с които да се гарантира, че те са изчерпателно информирани за това, което се случва с личните им данни, и да им се предостави възможност да упражняват по-ефективно правата си.

С цел да се утвърди правото на физическите лица на защита на данните, Комисията предлага нови правила, които ще:

подобрят способността на физическите лица да осъществяват контрол над своите данни, като:

- се гарантира, че когато **съгласието** им се изисква, то се **дава изрично, т.е. то се основава на изявление или на потвърждаващо действие от страна на засегнатото лице** и е свободно изразено;

- се предостави на ползващите интернет действително **право да бъдат забравяни** в онлайн средата: правото техните данни да се заличат, ако те оттеглят своето съгласие и ако няма законни основания за задържане на данните;

- се гарантира **лесен достъп до собствените данни** и **право на преносимост на данните**: право на получаване на копие на съхраняваните данни от администратора на лични данни и свободата да се прехвърлят безпрепятствено от един доставчик на услуги към друг;

[19] Вж. Програма в областта на цифровите технологии за Европа, пак там., стр. 4.

- се утвърди **правото на информация**, така че физическите лица напълно да разбират как се обработват техните лични данни, особено когато дейностите по обработването засягат **деца**.

Подобрят средствата, с които физическите лица да упражняват своите права, като:

- се увеличат **независимостта и правомощията на националните органи по защита на данните**, така че те да са добре оборудвани за ефективно разглеждане на жалби, да имат правомощия да провеждат ефективни разследвания, да вземат решения със задължителен характер и да налагат ефективни и възпиращи санкции;

- се подобрят **административните и съдебните средства за защита** при нарушения на правата на защита на личните данни. По-специално, квалифицирани сдружения ще могат да предявяват искове в съда от името на засегнатото физическо лице.

Засилят сигурността на данните, като:

- се насърчат **технологиите за подобряване на защитата на личния живот** *(технологии, които защитават личния живот чрез свеждане до минимум на съхранението на лични данни*), **стандартните настройки, гарантиращи неприкосновеността на личния живот, и схемите за сертифициране за неприкосновеност на личния живот;**

- се въведе **общо задължение**[20] за администраторите на лични данни да **уведомяват за нарушения на сигурността на данните** както засегнатите физически лица, така и органите за защита на данните **без излишно забавяне** (което, когато е осъществимо, се прави в срок от 24 часа).

Подобрят отчетността на обработващите лични данни, по-специално като:

- се изиска от администраторите на лични данни да определят **длъжностно лице за защита на данните** в дружествата с повече от 250 служители и във фирми, които се занимават с операции по обработване, които създават конкретни рискове за правата и свободите на субектите на данни поради своето естество, обхват или цели („рисково обработване“);

- се въведе **принципът на защита на личните данни още при проектирането**, за да се гарантира, че предпазните мерки за защита на данните се вземат предвид още на етапа на планиране на процедурите и системите;

- се задължат организациите, занимаващи се рисково обработване, да извършват **оценки на въздействието върху защитата на данните**.

[20] Това понастоящем е задължително само в сектора на далекосъобщенията съгласно Директивата за правото на неприкосновеност на личния живот и електронни комуникации.

3. ПРАВИЛА ЗА ЗАЩИТАТА НА ДАННИТЕ, ПРИСПОСОБЕНИ ЗА ЦИФРОВИЯ ЕДИНЕН ПАЗАР

Въпреки че целта на съществуваща директива е да се гарантира еднакво ниво на защита на данните в ЕС, правилата в държавите-членки все още се различават значително. Поради това на администраторите на лични данни се налага да се съобразяват с 27 различни национални закона и изисквания. Резултатът е **фрагментарна правна среда**, която създава **правна несигурност** и неравностойна защита за физическите лица. Това причинява **ненужни разходи и административна тежест** за стопанските субекти и представлява пречка за предприятията, функциониращи в рамките на единния пазар, които може да пожелаят да разширят дейността си зад граница.

Ресурсите и правомощията на националните органи, отговорни за защитата на данните, се различават значително сред държавите-членки[21]. В някои случаи те не са в състояние да изпълняват своите задачи по правоприлагане по задоволителен начин. Сътрудничеството между тези органи на европейско равнище — чрез съществуващата консултативна група (т. нар. „работна група по член 29“)[22] — не винаги води до съгласувано правоприлагане и поради това то също трябва да бъде подобрено.

Последователно прилагане на правилата за защита на личните данни в цяла Европа

Мултинационална компания с няколко клона в ЕС използва система за картографиране онлайн в цяла Европа, която събира изображения на всички частни и обществени сгради и може също така да прави снимки на хората по улиците. В една държава-членка включването на незамъглени снимки на хора, които не знаят, че са били фотографирани, бе счетено за неправомерно, докато в други държави-членки такова нарушение на законите за защита на данните няма. В резултат на това нямаше съгласувана реакция сред националните органи по защита на данните, за да се коригира тази ситуация.

С реформата на правилата на ЕС за защита на данните ще се гарантира, че това няма да се повтори в бъдеще, тъй като:

- изискванията и предпазните мерки за защита на данните ще бъдат установени с регламент на ЕС с пряко прилагане в целия Съюз;

- само органът по защита на данните на мястото, където се намира основното седалище на дружеството, ще отговаря за решението дали дружеството действа в рамките на закона или не;

- своевременната и ефективна координация между националните органи по защита на данните — при условие че услугата е предназначена за физически лица в няколко държави-членки — ще спомогне да се гарантира, че новите норми на ЕС за защита на данните ще се прилагат и изпълняват съгласувано във всички държави-членки.

---

21 За повече подробности по този въпрос вж. оценката на въздействието, придружаваща правните предложения, SEC(2012)72.

22 Работната група по член 29 бе създадена през 1996 г. (съгласно член 29 на Директива 95/46/ЕО) със статут на консултативен орган и е съставена от представители на националните надзорните органи по защита на данните (ОЗД), Европейския надзорен орган по защита на данните (ЕНОЗД) и Комисията. За повече информация относно нейните дейности, вж. http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm.

Националните органи трябва да бъдат подсилени, а сътрудничеството между тях — укрепено, за да се гарантират съгласуваното правоприлагане и, в крайна сметка, еднаквото прилагане на правилата в целия ЕС.

Една солидна, ясна и уеднаквена законодателна рамка на равнище ЕС ще спомогне за разгръщането на потенциала на цифровия единен пазар и за увеличаването на икономическия растеж, иновациите и създаването на работни места. С регламента ще се сложи край на фрагментарността на правните режими във всичките 27 държави-членки и ще се отстранят пречките при навлизане на пазара — фактор от особено значение за микропредприятията и за малките и средните предприятия.

Новите правила ще дадат освен това предимство на дружествата от ЕС в световната конкуренция. Съгласно реформираната регулаторна рамка те ще могат да гарантират на своите клиенти, че ценната лична информация ще бъде третирана с необходимата грижа и добросъвестност. Доверието в съгласувания регулаторен режим на ЕС ще бъде от съществено значение за доставчиците на услуги и стимул за инвеститорите, които търсят оптимални условия, когато избират къде да предоставят услугите си.

За да се подобри **свързаното с единния пазар измерение на защитата на данните**, Комисията предлага:

- да се установят правила за защита на данните на равнище ЕС чрез **пряко приложим във всички държави-членки регламент**[23], с който ще се сложи край на кумулативното и едновременно прилагане на различните национални закони за защита на данните. Това ще доведе до нетни **икономии за дружествата в размер на близо 2,3 млрд. EUR годишно само що се отнася до административната тежест;**

- **да се опрости регулаторната среда, като се намали драстично бюрокрацията** и се премахнат такива **формалности** като общите изисквания за уведомяване (което ще доведе до нетни икономии от 130 млн. EUR годишно само що се отнася до административната тежест); Като се има предвид тяхното значение за конкурентоспособността на европейската икономика, особено внимание се отделя на специфичните нужди на микропредприятията и на малките и средните предприятия;

- **да се засилят допълнително независимостта и правомощията на националните органи по защита на данните (ОЗД)**, за да им се даде възможност да провеждат разследвания, да вземат решения със задължителен характер и да налагат ефективни и възпиращи санкции, както и да се задължат държавите-членки да им предоставят **необходимите ресурси** за това;

- **да се създаде система от типа „едно гише“ за защитата на данните в ЕС:** администраторите на данни в ЕС ще трябва да работят само с **един ОЗД**, а

[23] Предлага се чрез директива да се установят нормите, приложими в областта на полицейското и съдебното сътрудничество по наказателноправни въпроси (вж. раздел 4 по-долу), което ще даде възможност за повече гъвкавост за държавите-членки в тази специфична област.

именно органа по защита на данните на държавата-членка, в която се намира основното седалище на дружеството;

- да се създадат условия за **бързо и ефикасно сътрудничество между органите по защита на данните**, включително задължението даден ОЗД да провежда разследвания и проверки при поискване от друг ОЗД, и за взаимно признаване на решенията на различните ОЗД;

- **да се създаде механизъм за съгласуваност** на равнище ЕС, да се гарантира, че в решенията на даден ОЗД с голямо отражение на европейско равнище са взети изцяло предвид становищата на другите засегнати ОЗД и че те са изцяло в съответствие с правото на ЕС;

- да се превърне работната група по член 29 в независим Европейски комитет по защита на данните, за да се подобри приносът ѝ към съгласуваното прилагане на правото за защита на данните и да се предостави стабилна основа за сътрудничество между органите по защита на данните, включително Европейския надзорен орган по защита на данните; да се засилят синергиите и ефективността, като се предвиди Европейският надзорен орган по защита на данните да осигурява секретариата на Европейския комитет по защита на данните.

Новият регламент на ЕС ще осигури силна защита на основното право на защита на личните данни в целия Европейски съюз и ще подобри функционирането на вътрешния пазар. Същевременно, с оглед на това, че — както бе подчертано от Съда на Европейския съюз[24] — правото на защита на личните данни не е абсолютно право, а трябва да бъде разглеждано във връзка с неговата функция в обществото[25] и да бъде балансирано с други основни права, в съответствие с принципа на пропорционалност [26]— в настоящия регламент ще бъдат включени изрични разпоредби, с които да се гарантира зачитането на други основни права като свободата на изразяване и на информация, правото на защита, както и професионалната тайна (напр. за юридическите професии), без да се нарушава статутът на църквите по силата на законите на държавите-членки.

---

[24] Съд на Европейския съюз, решение от 9.11.2010 г. по съединени дела Volker und Markus Schecke (C-92/09) и Eifert (C-93/09), което все още не е официално съобщено.

[25] В съответствие с член 52, параграф 1 от Хартата ограничения могат да бъдат налагани върху упражняването на правото на защита на данните, доколкото такива ограничения са предвидени по закон, зачитат основното съдържание на същите права и свободи и, при спазване на принципа на пропорционалност, са необходими и действително отговарят на признати от Европейския съюз цели от общ интерес или на необходимостта да се защитят правата и свободите на други хора.

[26] Съд на Европейския съюз, решение от 6.11.2003 г. по дело C-101/01, Lindqvist [2003] ECR I-12971, параграфи 82—90; Решение от 16.12.2008 г. по дело C-73/07, Satamedia [2008], ECR I-9831, параграфи 50—62.

4. ИЗПОЛЗВАНЕТО НА ДАННИ В ОБЛАСТТА НА ПОЛИЦЕЙСКОТО И СЪДЕБНОТО СЪТРУДНИЧЕСТВО ПО НАКАЗАТЕЛНОПРАВНИ ВЪПРОСИ

Влизането в сила на Договора от Лисабон и най-вече въвеждането на ново правно основание (член 16 от ДФЕС) позволяват установяването на цялостна рамка за защита на данните, с която да се гарантира високо ниво на защита на данните на физическите лица, съобразено със специфичното естество на областта на полицейското и съдебното сътрудничество по наказателноправни въпроси. По-специално, това дава възможност за преработена рамка на ЕС за защита на личните данни, за да се обхванат трансграничното и националното обработване на лични данни. Това ще намали различията между законодателството в държавите-членки в полза на защитата на личните данни като цяло. Това би могло да доведе също така до по-безпрепятствен обмен на информация между полицейските и съдебните органи на държавите-членки, като по този начин ще се подобри сътрудничеството в борбата с тежката престъпност в Европа. Обработването на данни от страна на полицейските и съдебните органи по наказателноправни въпроси понастоящем се урежда главно с Рамково решение 2008/977/ПВР, което предшества влизането в сила на Договора от Лисабон. Тъй като то е рамково решение, Комисията не разполага с правомощия да привежда в действие неговите разпоредби, а това допринася за непоследователното му прилагане. Освен това приложното поле на рамковото решение се ограничава до трансгранични дейности по обработване на данни[27]. Това означава, че обработването на лични данни, които не са били предмет на обмен, в момента не е уредено с правилата на ЕС, регулиращи обработването и гарантиращи основното право на защита на данните. Това създава също така практически затруднения за полицията и другите органи, които може да не са в състояние да определят дали обработването на данни следва да бъде изцяло вътрешно или трансгранично; или да предвидят дали „вътрешните“ данни биха могли да бъдат обект на последващ трансграничен обмен[28].

Ето защо с новата реформирана правна рамка на ЕС за защита на данните се цели да се гарантира съгласувано високо ниво на защита на данните, **за да се повиши взаимното доверие между полицейските и съдебните органи на различните държави-членки, с което да се улеснят свободното движение на данни и ефективното сътрудничество между полицейските и съдебните органи**.

С цел гарантиране на високо ниво на защита на личните данни в областта на полицейското и съдебното сътрудничество по наказателноправни въпроси и улесняване на обмена на лични данни между полицейските и съдебните органи на държавите-членки Комисията предлага като част от пакета за реформа на защитата на данните директива, която ще:

[27] По-точно, рамковото решение се прилага за лични данни, които са предадени или предоставени между държавите-членки или са обменени между държавите-членки и институциите или органите на ЕС (вж. член 1, параграф 2).

[28] Това беше потвърдено от няколко държави-членки в отговорите им на въпросника на Комисията във връзка с доклада за прилагането на рамковото решение (COM(2012)12).

- **прилага общите принципи за защита на данните** за полицейското и съдебното сътрудничество по наказателноправни въпроси, като се зачита спецификата на тези области[29];

- предвижда **минимални хармонизирани критерии и условия относно възможните ограничения** на общите правила. Това засяга, по-специално, правото на физическите лица да бъдат информирани, когато полицейските и съдебните органи обработват техните данни или имат достъп до тях. Такива ограничения са необходими за ефективното предотвратяване, разследване, разкриване или съдебно преследване на престъпления;

- **установи специални правила, с които да се уреди специфичното естество на дейностите по правоприлагане, като се включи разграничаване между различните категории субекти на данни**, чиито права може да се различават (например свидетели и заподозрени лица).

5. ЗАЩИТАТА НА ДАННИТЕ ВЪВ ВЗАИМОСВЪРЗАНИЯ СВЯТ

Правата на физическите лица трябва да продължат да бъдат гарантирани, когато лични данни се предоставят от ЕС на трети държави и когато физически лица в държавите-членки са набелязани и техните данни се използват или анализират от доставчици на услуги в трети държави. Това означава, че стандартите на ЕС за защита на данните трябва да се прилагат независимо от географското местоположение на дружеството или неговото звено за обработване на данни.

В днешния глобализиран свят личните данни се предават през все по-голям брой виртуални и географски граници и се съхраняват на сървъри в множество държави. Все повече дружества предлагат услуги за изчисления в облак, което позволява на клиентите да осъществяват достъп и да съхраняват данни на отдалечени сървъри. Тези фактори налагат да се подобрят съществуващите механизми за предаване на данни на трети държави. Това включва решения относно адекватността — т.е. решения, които удостоверяват „адекватността“ на стандартите за защита на данните в трети държави — и подходящи гаранции като стандартни договорни клаузи или задължителни фирмени правила[30], така че да се осигури високо ниво на защита на данните при международни операции по обработване, както и да се улесни движението на данни през границите.

Задължителни фирмени правила

[29] Вж. Декларация № 21 относно защитата на личните данни в областта на съдебното сътрудничество по наказателноправни въпроси и полицейското сътрудничество, приложена към Заключителния акт на междуправителствената конференция, която прие Договора от Лисабон.

[30] Задължителните фирмени правила (ЗФП) са основани на европейските стандарти за защита на данните практически правилници, които са одобрени от поне един орган по защита на данните и които организациите изготвят доброволно и следват, за да осигуряват адекватни гаранции за категориите предавания на лични данни между дружествата, които са част от една и съща корпоративна група и които са обвързани от тези правила. Те не са изрично уредени с Директива 95/46/ЕО, но бяха разработени като част от практиката между ОЗД с подкрепата на работната група по член 29.

Корпоративна група редовно трябва да предава лични данни от своите филиали в ЕС към своите филиали, разположени в трети държави. Групата иска да въведе набор от задължителни фирмени правила (ЗФП), за да се съобрази със законодателството на ЕС, като същевременно ограничи административните изисквания за всяко отделно предаване на данни. На практика чрез ЗФП се гарантира, че в цялата група се прилага един единствен набор от правила, вместо различни вътрешни договори.

Въз основа на съществуващите практики, договорени на равнището на работната група по член 29, за да се признае, че ЗФП на дадено дружество предоставят адекватни гаранции, е необходим задълбочен преглед от страна на три органа по защита на данните (един „водещ“ОЗД и два „проверяващи“ ОЗД), но няколко други ОЗД също могат да дадат своите становища по тях. Освен това много от законите на държавите-членки изискват допълнителни национални разрешения за предаванията на данни, които се уреждат със ЗФП, а това прави процеса по приемането им твърде тромав, скъп, продължителен и сложен.

След реформата на защитата на данните:

- този процес ще бъде опростен и рационализиран;

- ЗФП ще бъдат одобрявани само от един ОЗД при наличието на механизми за гарантиране на бързото включване на други заинтересовани ОЗД;

- когато един ОЗД добри дадени ЗФП, те стават валидни за целия ЕС, без да е необходимо каквото и да било допълнително разрешение на национално равнище.

За да се **посрещнат предизвикателствата на глобализацията**, са необходими гъвкави инструменти и механизми, особено за предприятията, развиващи дейност в целия свят, като същевременно се гарантира защитата на данните на физическите лица без пропуски. Комисията предлага следните мерки:

- **ясни правила**, с които се определя кога **правото на ЕС се прилага за администраторите на данни, установени в трети държави**, по-специално като се посочва, че когато на физически лица в ЕС се предлагат стоки и услуги, или когато се следи тяхното поведение, **се прилагат европейските правила**;

- **решенията относно адекватността** ще бъдат вземани от Европейската комисия въз основа на изрични и ясни критерии, включително в областта на полицейското сътрудничество и наказателното правосъдие;

- законното движение на данни към трети държави ще бъде улеснено, като се усъвършенстват и опростят **правилата за международно предаване на данни** към държави, които не са обхванати от решение относно адекватността, по-специално като се рационализира и увеличи употребата на инструменти като **задължителните фирмени правила**, така че те да могат да се използват за обезпечаване на **обработващите данни** и в рамките на **групи от дружества**, отразявайки по този начин нарастващия брой дружества, които се занимават с дейности по обработване на данни, особено в изчислителни облаци;

- откриване на **диалог** и, когато е уместно, **преговори** с трети държави — в частност стратегическите партньори на ЕС и страните партньори в рамките на Европейската политика на съседство — и съответните международни организации (напр. Съвета на Европа, Организацията за икономическо сътрудничество и развитие, Обединените нации), за да се **насърчат високите и оперативно съвместими стандарти за защита на данните** в целия свят.

6. ЗАКЛЮЧЕНИЕ

С реформата на ЕС на защитата на данните се цели изграждането на **съвременна, стабилна, съгласувана и цялостна правна рамка за защита на данните за Европейския съюз**. Укрепва се основното право на физическите лица на защита на личните данни. Ще се зачитат и други права като свободата на изразяване на мнение и свободата на информация, правата на детето, правото на стопанска дейност, правото на справедлив съдебен процес и професионална тайна (напр. за юридическите професии), както и статутът на църквите по силата на законите на държавите-членки.

Реформата ще бъде от полза преди всичко за физическите лица, тъй като чрез нея техните права на защита на личните данни ще бъдат утвърдени, а доверието им в цифровата среда — засилено. Освен това с реформата ще се опрости значително правната среда за предприятията и публичния сектор. Очаква се това да стимулира развитието на цифровата икономика в целия единен пазар на ЕС и извън него в съответствие с целите на стратегията „Европа 2020“ и Програмата в областта на цифровите технологии за Европа. Накрая, с реформата ще се засили доверието между правоприлагащите органи и ще се улесни обменът на данни между тях и сътрудничество в борбата с тежката престъпност, като същевременно ще гарантира високо ниво на защита за физическите лица.

Комисията ще работи в тясно сътрудничество с Европейския парламент и Съвета, за да гарантира постигането на споразумение относно новата правна рамка на ЕС за защита на данните до края на 2012 г. По време на процеса на приемане и след това, особено в контекста на прилагането на новите правни инструменти, Комисията ще води **тесен и прозрачен диалог с всички заинтересовани страни**, включително представители на частния и публичния сектор. Това ще включва представители на полицията и съдебната система, регулаторите на електронни комуникации, организациите на гражданското общество, органите по защита на данните и университетските среди, както и на специализираните агенции на ЕС като Евроюст, Европол, Агенцията за основните права и Европейската агенция за мрежова и информационна сигурност.

Предвид постоянното развитие на информационните технологиите и променящото се социално поведение такъв диалог е от първостепенно значение, за да се ползва получената информация, необходима за осигуряването на високо ниво на защита на данните на физическите лица, растежа и конкурентоспособността за предприятията от ЕС, оперативната ефективност на публичния сектор (включително полицията и съдебната система) и малка административна тежест.