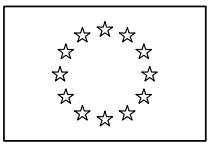

ЕВРОПЕЙСКА КОМИСИЯ

Брюксел, 4.11.2010
COM(2010) 609 окончателен

# СЪОБЩЕНИЕ НА КОМИСИЯТА ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ, СЪВЕТА, ИКОНОМИЧЕСКИЯ И СОЦИАЛЕН КОМИТЕТ И КОМИТЕТА НА РЕГИОНИТЕ

## „Всеобхватен подход за защита на личните данни в Европейския съюз“

**СЪОБЩЕНИЕ НА КОМИСИЯТА ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ, СЪВЕТА, ИКОНОМИЧЕСКИЯ И СОЦИАЛЕН КОМИТЕТ И КОМИТЕТА НА РЕГИОНИТЕ**

**„Всеобхватен подход за защита на личните данни в Европейския съюз“**

## 1. НОВИ ПРЕДИЗВИКАТЕЛСТВА ПРЕД ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ

Директивата от 1995 г. за защита на личните данни[1] бележи важен исторически етап в развитието на защитата на личните данни в Европейския съюз. Директивата утвърждава две от най-старите и еднакво важни цели на процеса на европейска интеграция: от една страна, защитата на основните права и свободи на физическите лица, и по-специално на основното право на защита на личните данни, а от друга — изграждането на вътрешния пазар, в този случай свободното движение на лични данни.

Петнадесет години по-късно тази двойна цел е все още в сила, а принципите, заложени в директивата, все така валидни. **Бързото развитие на технологиите и глобализацията обаче коренно промениха обкръжаващия ни свят и доведоха до нови предизвикателства пред защитата на личните данни.**

Днес технологиите позволяват на хората лесно да споделят информация за своето поведение и предпочитания, като тази информация е публично достъпна в невиждан досега световен мащаб. Сайтовете за социални контакти със стотици милиони членове по целия свят са може би най-очевидният, но не и единствен пример за това явление. „Изчислителните облаци“ — т.е. използването на изчислителни системи, базирани в Интернет, при което софтуерът, споделените ресурси и информацията са на отдалечени сървъри („в облака“) — също могат да представляват предизвикателства пред защитата на личните данни, тъй като могат да доведат до загубата на контрол от страна на лицата над потенциално чувствителна информация, когато съхраняват техните данни с програми, хоствани на чужд хардуер. Неотдавнашно проучване потвърждава, че е налице близост във възгледите (на органите за защита на данните, на стопанските сдружения и организациите на потребителите), че рисковете за неприкосновеността на личния живот и защитата на личните данни, свързани с дейности в Интернет, се увеличават[2].

В същото време, **начините за събиране на лични данни стават все по-усъвършенствани и по-трудно откриваеми.** Така например, използването на сложни технологии позволява на икономическите оператори да персонализират своята дейност спрямо физическите лица, като проследяват поведението им в Интернет. Нарастващото използване на процедури, позволяващи автоматичното събиране на данни, като например електронни транспортни билети, събиране на пътна такса или устройства за

---

[1] Директива 95/46/ЕО на Европейския парламент и на Съвета от 24.10.1995 г. за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни (ОВ L 281, 23.11.1995, стр. 31).

[2] Вж. *Проучване на икономическите ползи от технологиите за подобряване на защитата на личния живот,* London Economics, юли 2010 г. (http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf), стр. 14.

гео-локализиране, улесняват определянето на местоположението на лицата само поради факта, че те използват мобилни устройства. Държавните органи също използват все повече лични данни за различни цели, като например проследяването на лица при епидемия от заразна болест, за по-ефективното предотвратяване и борба срещу тероризма и престъпността, при управлението на схеми за социална сигурност или за целите на данъчното облагане, като част от своите приложения за електронно правителство и т.н.

Всичко това неминуемо поставя въпроса дали действащото законодателство на ЕС за защита на данните все още е в състояние да даде пълноценен и ефективен отговор на тези предизвикателства.

За да отговори на този въпрос, Комисията започна преразглеждане на сега действащата правна рамка — този процес бе открит с конференция на високо равнище през май 2009 г., последвана от обществена консултация, проведена до края на 2009 г.[3] Бе даден ход на редица проучвания[4].

Резултатите от този процес потвърдиха, че основните принципи на директивата са все още валидни, а нейният технологично неутрален характер следва да се запази. Бяха идентифицирани обаче няколко въпроса, които са проблемни и поставят специфични предизвикателства. Те включват:

- *Разглеждане на въздействието на новите технологии*

В отговорите, получени по време на консултациите както от частни лица, така и от организации, бе потвърдена необходимостта от поясняване и уточняване на прилагането спрямо новите технологии на принципите за защита на данните, за да се гарантира, че личните данни на физическите лица действително са ефективно защитени, независимо от използваната технология за обработка на тези данни, и че администраторите на лични данни напълно съзнават последиците от новите технологии за защитата на данните. Тези въпроси са частично разгледани в Директива 2002/58/ЕО (т.нар. Директива за правото на неприкосновеност на личния живот и електронни

---

[3] Вж. отговорите на обществената консултация, проведена от Комисията: http://ec.europa.eu/justice/news/consulting_public/news_consulting_0003_en.htm. През 2010 г. бяха проведени още целенасочени консултации със заинтересованите страни. Заместник-председателят Вивиан Рединг председателства също така среща на високо равнище със заинтересованите страни, провела се на 5 октомври в Брюксел. Комисията се допита и до Работната група по член 29, която допринесе значително за консултациите през 2009 г. (WP 168), а през юли 2010 г. прие специално становище относно концепцията за отчетност(WP 173).

[4] Освен *Проучването на икономическите ползи от технологиите за подобряване на защитата на личния живот* (цитирано в бележка под линия 2), вж. също *„Сравнително проучване на различни подходи към новите предизвикателства пред неприкосновеността на личния живот, по-специално с оглед на технологичното развитие“* от януари 2010 г. (http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf). В процес на подготовка е и проучване за оценка на въздействието на бъдещата правна рамка на ЕС върху защитата на личните данни.

комуникации)[5], с която се доуточнява и допълва за сектора на електронните комуникации общата Директива за защита на данните[6].

- *Засилване на измерението, свързано с вътрешния пазар, на защитата на данните*

Едно от основните и най-често изразявани опасения на заинтересованите страни, особено на многонационалните компании, е липсата на достатъчно хармонизиране между законодателствата на държавите-членки в областта на защитата на данните, въпреки наличието на обща правна рамка на ЕС. Заинтересованите страни подчертаха необходимостта от по-голяма правна сигурност, по-малка административна тежест и от гарантиране на равни условия за икономическите оператори и за другите администратори на лични данни.

- *Разглеждане на въпросите, свързани с глобализацията, и подобряване на международния трансфер на данни*

Няколко заинтересовани страни подчертаха, че нарастващото възлагане на обработката на данни на външни изпълнители, много често извън ЕС, поставя редица проблеми по отношение на правото, приложимо към обработката, както и по отношение на разпределението на свързаната с това отговорност. Що се отнася до международните трансфери на данни, много организации изразиха становище, че настоящите схеми не са напълно задоволителни и трябва да бъдат преразгледани и рационализирани за постигането на по-опростени и по-лесни трансфери.

- *Осигуряване на по-засилена институционална организация за ефективно прилагане на правилата за защита на личните данни*

Налице е консенсус между заинтересованите страни за необходимостта от засилване на ролята на органите за защита на личните данни с цел да се гарантира по-добро прилагане на правилата за защита на данните. Някои организации поискаха и по-голяма прозрачност в работата на Работната група по член 29 (*вж. точка 2.5 по-долу*), както и разясняване на нейните задачи и правомощия.

- *Подобряване на съгласуваността на правната рамка за защита на личните данни*

По време на обществената консултация всички заинтересовани страни подчертаха необходимостта от всеобхватен инструмент, приложим към операциите за обработка на

---

[5] 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).

[6] С Директива 95/46/ЕО за защита на данните се определят стандартите за защита на данните за всички законодателни актове на ЕС, включително Директива 2002/58/ЕО за правото на неприкосновеност на личния живот и електронни комуникации (изменена с Директива 2009/136/ЕО, ОВ L 337, 18.12.2009 г., стр. 11). Директивата за правото на неприкосновеност на личния живот и електронни комуникации се прилага за обработката на лични данни във връзка с предоставянето на обществено достъпни електронни съобщителни услуги в обществени съобщителни мрежи. Тя трансформира принципите, заложени в Директивата за защита на данните, в специфични правила за сектора на електронните комуникации. Директива 95/46/ЕО се прилага наред с другото и за съобщителни услуги, които не са обществено достъпни.

данни във всички сектори и политики на Съюза, който да осигурява интегриран подход и непрекъсната, последователна и ефективна защита[7].

Тези предизвикателства **изискват ЕС да разработи всеобхватен и съгласуван подход**, който гарантира **пълното съблюдаване на основното право на защита на личните данни на физическите лица във и извън рамките на ЕС**. Договорът от Лисабон предостави на ЕС допълнителни средства за постигането на тази цел: Хартата на основните права — в чийто член 8 правото на защита на личните данни се признава като самостоятелно право — стана правно обвързващ инструмент, и бе въведено ново правно основание[8], което позволява установяването на всеобхватно и съгласувано законодателство на ЕС за защитата на физическите лица по отношение на обработката на личните им данни и за свободното движение на тези данни. По-конкретно, новото правно основание позволява на ЕС да урежда в рамките на един правен инструмент защитата на лични данни, включително в областта на полицейското и съдебното сътрудничество по наказателноправни въпроси. Член 16 от ДФЕС само частично обхваща областта на общата външна политика и политиката на сигурност, тъй като с решение на Съвета и въз основа на друго правно основание трябва да бъдат определени специфични правила за обработката на лични данни от държавите-членки[9].

Като се възползва от тези нови правни възможности, Комисията ще даде възможно най-голям приоритет на усилията за гарантиране на съблюдаването на основното право на защита на личните данни в целия Европейски съюз и в неговите политики, като в същото време засилва измерението, свързано с вътрешния пазар, на защитата на данните и улеснява свободното движение на лични данни. В този контекст при гарантирането на основното право за защита на личните данни трябва да бъдат взети изцяло предвид другите свързани основни права, залегнали в Хартата, както и другите цели на Договорите.

Целта на настоящото съобщение е да представи подхода на Комисията за модернизиране на правната система на ЕС за защита на личните данни във всички области на дейност на Съюза, като се отчитат по-специално предизвикателствата, произтичащи от глобализацията и новите технологии, за да се гарантира и в бъдеще високо равнище на защита на физическите лица при обработката на личните им данни във всички области на дейност на Съюза. Това ще позволи на ЕС да запази водещата си роля в насърчаването на високи стандарти за защита на данните в световен план.

---

[7] В отделни становища, представени след края на обществената консултация, Европол и Евроюст помолиха въпреки всичко да се отчетат особеностите на тяхната работа по отношение на координацията на дейностите за правоприлагане и предотвратяване на престъпността.

[8] Вж. член 16 от Договора за функционирането на Европейския съюз (ДФЕС).

[9] Вж. член 16, параграф 2, последно изречение от ДФЕС и член 39 от Договора за Европейския съюз (ДЕС).

## 2. ОСНОВНИ ЦЕЛИ НА ВСЕОБХВАТНИЯ ПОДХОД ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

### 2.1. Засилване на правата на физическите лица

#### *2.1.1. Осигуряване на подходяща защита на физическите лица при всички обстоятелства*

Целта на правилата в понастоящем действащите инструменти на ЕС за защита на данните е **опазването на основните права на физическите лица, и по-специално на правото им на защита на личните данни**, в съответствие с Хартата на основните права на ЕС[10].

Понятието за „лични данни“ е едно от основните понятия в защитата на физическите лица, осигурена от действащите инструменти на ЕС за защита на данните, и води до прилагане на задълженията, наложени на администраторите на лични данни и лицата, обработващи данни[11]. Определението за „лични данни“ цели да обхване всички сведения, свързани пряко или непряко с физическо лице, чиято самоличност е установена или може да бъде установена. За да се определи дали може да се установи самоличността на дадено лице, следва да се вземат предвид „всички средства, които биха могли да бъдат използвани разумно от администратора или от друго лице с цел идентифицирането на даденото лице“[12]. Законодателят умишлено е избрал този подход, чиято гъвкавост позволява неговото прилагане към различни ситуации и промени, които засягат основните права, включително такива, които не са били предвидими при приемане на директивата. Въпреки това, в резултат на такъв широк и гъвкав подход, в много случаи при прилагане на директивата не винаги е ясно кой подход трябва да се следва, дали лицата се ползват от правото на защита на данните и дали администраторите на лични данни трябва да спазват задълженията, наложени им с директивата[13].

Съществуват ситуации, които включват обработка на специфични сведения, за които са необходими допълнителни мерки в правото на Съюза. Такива мерки вече съществуват в някои случаи. Така например съхраняването на данни в крайното далекосъобщително оборудване (например мобилни телефони) е разрешено единствено при условие, че лицето е дало своето съгласие. Това може да бъде необходимо да се разгледа на равнище ЕС по отношение, например, на данни, кодирани с ключ, данни за локализиране, технологии за „извличане на данни“, които позволяват комбинирането на данни от различни източници, или в случаите, когато трябва да се осигури поверителността и целостта на системи за информационни технологии[14].

---

10 Вж. Съд на Европейския съюз, Дело № C-101/01, „Bodil Lindqvist“, ECR [2003], I-1297, 96, 97 и Дело № C-275/06, Productores de Música de España (Promusicae) срещу Telefónica de España SAU, ECR [2008] I-271. Вж. също съдебната практика на Европейския съд за правата на човека, например в дела: S. и Marper срещу Обединеното кралство, 4.12. 2008 г. (Жалби с номера 30562/04 и 30566/04) и Rotaru срещу Румъния, 4.5. 2000 г.; № 28341/95, § 55, ECHR 2000-V.

11 Вж. определенията за „администратор“ и „обработващ лични данни“ в член 2, букви г) и д) от Директива 95/46/ЕО.

12 Вж. съображение 26 от Директива 95/46/ЕО.

13 Вж. например случая с IP адресите, разгледан в Становище 4/2007 на Работната група по член 29 относно понятието лични данни (WP 136).

14 Вж. например решение на Германския федерален конституционен съд (*Bundesverfassungsgericht*) от 27 февруари 2008 г., 1 BvR 370/07.

Ето защо се налага внимателно разглеждане на всички тези въпроси.

Комисията ще обмисли **как да се осигури съгласувано прилагане на правилата за защита на данните предвид въздействието на новите технологии върху правата и свободите на физическите лица и целта да се осигури свободното движение на лични данни в рамките на вътрешния пазар**.

*2.1.2. Повишаване на прозрачността за субектите на данни*

Прозрачността е съществено условие, което дава възможност на хората да упражняват контрол върху собствените си данни и което осигурява ефективна защита на личните данни. Ето защо е от изключителна важност администраторите на данни да **информират** хората по **ясен, пълен и прозрачен начин** за това как и от кого се събират и обработват техните данни, поради какви причини, за колко време и какви са техните права, ако те желаят достъп, коригиране или заличаване на тези данни. Съответните разпоредби относно информацията, която трябва да бъде предоставена на субектите на данни[15], не са достатъчни.

Сред основните елементи на прозрачността са изискванията за **лесно достъпна и лесна за разбиране информация и използването на ясни и недвусмислени формулировки**. Това важи в особена степен за интернет средата, където доста често съобщенията за защита на личните данни са неясни, трудно достъпни, непрозрачни[16] и не винаги в пълно съответствие с действащите правила. Пример за това могат да бъдат поведенческите реклами в интернет, където както увеличеният брой участници в предоставянето на поведенчески реклами, така и технологичната сложност на тази практика трудно позволяват на отделния човек да знае и да разбира дали се събират лични данни, от кого и с каква цел.

В този контекст е необходима специална защита за **децата**, тъй като те не съзнават така добре рисковете, последиците, защитните мерки и правата, свързани с обработката на лични данни[17].

Комисията ще разгледа възможността за:

- въвеждане в правната рамка на **общ принцип за прозрачна обработка** на личните данни;

- въвеждане на **конкретни задължения** за администраторите на данни относно вида информация, която следва да бъде предоставяна, и **начините** за нейното предоставяне, включително по отношение на **децата**;

---

15 Вж. членове 10 и 11 от Директива 95/46/ЕО.

16 Проучване на Евробарометър, проведено през 2009 г., показа, че около половината от запитаните намират съобщенията за защита на личните данни в уебсайтовете за „много“ или „твърде неясни“ (вж. Flash Eurobarometer № 282: http://ec.europa.eu/public_opinion/flash/fl_282_en.pdf).

17 Вж. изследването „По-безопасен интернет за децата“, което обхваща деца на възраст 9—10 г. и 12—14 г. и което показва, че децата са склонни да подценяват рисковете, свързани с използването на Интернет и омаловажават последиците от своето рисково поведение (на адрес: http://ec.europa.eu/information_society/activities/sip/surveys/qualitative/index_en.htm).

- създаване на един или повече **стандартни формуляри на ЕС** („**съобщения за защитата на личните данни**“), които да бъдат използвани от администраторите на данни.

Също така е важно хората да бъдат информирани, когато техните данни са били случайно или неправомерно унищожени, загубени, променени или когато са били разкрити, или до тях са имали достъп неоторизирани лица. При последния преглед на Директивата за правото на неприкосновеност на личния живот и електронни комуникации бе въведено **задължително уведомяване при нарушаване на сигурността на личните данни**, което обаче обхваща единствено сектора на телекомуникациите. Като се има предвид, че рисковете от нарушаване на сигурността на данните съществуват и в други сектори (напр. финансовия сектор), Комисията ще разгледа възможността за въвеждане и в други сектори на задължението за уведомяване при нарушаване на сигурността на данните в съответствие с декларацията на Комисията от 2009 г. пред Европейския парламент относно уведомяването при нарушаване на сигурността на личните данни, направена в контекста на реформата на регулаторната рамка за електронните комуникации[18]. Това няма да засегне разпоредбите на Директивата за правото на неприкосновеност на личния живот и електронни комуникации, която трябва да бъде транспонирана в национални закони до 25 май 2011 г.[19] Следва да се гарантира последователен и съгласуван подход по този въпрос.

Комисията ще:

- проучи начините за въвеждане в общата правна рамка на **общо уведомяване при нарушаване на сигурността на личните данни**, като ще бъдат обсъдени и адресатите на такова уведомяване и критериите за прилагане на задължението за уведомяване.

*2.1.3. Засилване на контрола върху собствените лични данни*

Две важни предпоставки за гарантиране на висока степен на защита на данните са **ограничаването на обработката на данни от администратора единствено до необходимото за целите на обработката (принцип за свеждане до минимум на данните)** и запазването от страна на субектите на данни на **ефективен контрол върху техните собствени данни**. В член 8, параграф 2 от Хартата се посочва, че „всеки има право на достъп до събраните данни, отнасящи се до него, както и правото да изиска поправянето им“. Лицата винаги следва да разполагат с възможност за достъп, поправка, заличаване или блокиране на своите данни, освен ако няма основателни

[18] „Комисията взема под внимание желанието на Европейския парламент задължението за уведомяване за нарушения по отношение на личните данни да не бъде ограничено до сектора на електронните комуникации, но също така да се прилага за организации, като например доставчици на услуги на информационното общество […]. Затова Комисията незабавно ще инициира съответната подготвителната работа, включително консултации със заинтересованите страни, така че да бъдат представени до 2011 г. необходимите предложения в тази област […]“, декларацията се намира на адрес: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2009-0360+0+DOC+XML+V0//BG. Вж. също съображение 59 от Директива 2009/136/ЕО за изменение на Директива 2002/58/ЕС за правото на неприкосновеност на личния живот и електронни комуникации: „Интересът на ползвателите да бъдат уведомявани очевидно не се ограничава в рамките на сектора на електронните съобщения и следователно изрични, задължителни изисквания за уведомяване, приложими към всички сектори, следва да бъдат приоритетно въведени на общностно равнище.“

[19] Вж. член 4 от Директива 2009/136/ЕО.

причини, предвидени в закона, които не позволяват това. Тези права вече съществуват в действащата правна рамка. Въпреки това начинът, по който те могат да бъдат упражнявани, не е хармонизиран и в резултат на това на практика тяхното упражняване е по-лесно в някои държави-членки, отколкото в други. Нещо повече, това е особено трудно в интернет средата, където данните често се съхраняват без въпросното лице да е било уведомено и/или да е дало своето съгласие за това.

Особено уместен пример в това отношение са социалните мрежи в Интернет, тъй като те поставят значително предизвикателство пред ефективния контрол на лицето върху собствените му данни. Комисията получи различни запитвания от лица, които не винаги са били в състояние да си възвърнат от онлайн доставчици на услуги свои лични данни, като например снимки, и които по този начин са били възпрепятствани да упражнят своите права за достъп, поправка и заличаване.

Следователно тези права трябва да намерят по-категоричен израз, да бъдат пояснени и евентуално засилени.

Ето защо Комисията ще проучи възможности за:

- укрепване на **принципа за свеждане до минимум на данните**;

- **усъвършенстване на начините** за действителното **упражняване на правата на достъп, поправяне, заличаване или блокиране на данни** (например като се въведат срокове за отговор на искания от лицата, като се позволи упражняването на правата по електронен път или като се предвиди, че предоставянето на право за достъп следва по принцип да бъде безплатно);

- пояснyване на т. нар. „**право да бъдеш забравен**“, т.е. правото данните на лицата да бъдат заличени или да не бъдат допълнително обработвани, след като вече не са необходими за законосъобразни цели. Това, например, се отнася за случаите, когато обработката на данни се основава на съгласието на лицето и когато то оттегли своето съгласие или когато периодът на съхранение, за който е било дадено съгласие, е изтекъл;

- допълване на правата на субектите на данни чрез гарантиране на „**преносимост на данните**“, т.е. предоставяне на изричното право на лицето да оттегля своите лични данни (например свои снимки или списък с приятели) от дадено приложение или услуга, така че оттеглените данни да могат да бъдат прехвърлени към друго приложение или услуга, доколкото това е технически възможно, без създаването на пречки от страна на администраторите на лични данни.

### *2.1.4. Повишаване на осведомеността*

Въпреки че прозрачността е от съществено значение, необходимо е широката общественост, и особено младите хора, да са запознати по-добре с рисковете, свързани с обработката на лични данни, и със своите права. Според проучване на Евробарометър от 2008 г. голяма част от хората в държавите-членки на ЕС смятат, че информираността за защитата на личните данни в тяхната държава е ниска[20]. Ето защо дейностите за повишаване на осведомеността следва да се насърчават и подкрепят от широк кръг участници, т.е. от органите на държавите-членки и по-специално от органите за защита

[20] Вж. Flash Eurobarometer № 225 – Защита на личните данни в Европейския съюз: http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf.

на данните и от образователните институции, както и от администраторите на данни и сдруженията на гражданското общество. Тези дейности следва да включват незаконодателни мерки като кампании за повишаване на осведомеността в печатните и електронните медии и предоставяне на ясна информация на уебсайтове, като по разбираем начин се излагат правата на субектите на данни и отговорностите на администраторите на данни.

Комисията ще проучи:

- възможността за **съфинансиране** от бюджета на Съюза **на дейности за повишаване на осведомеността относно защитата на данните**;

- необходимостта и възможността за включване в правната рамка на **задължение за провеждане на дейности за повишаване на осведомеността** в тази област.

*2.1.5. Осигуряване на информирано и доброволно съгласие*

Когато се изисква информирано съгласие, настоящите правила предвиждат, че съгласието на физическото лице за обработването на неговите лични данни трябва да бъде „свободно изразено, конкретно и информирано указание за волята“, с което лицето изразява своето съгласие за обработка на данните[21]. Понастоящем обаче тези условия се тълкуват по различен начин в държавите-членки, като варират от общо изискване за писмено съгласие до приемане на мълчаливо съгласие.

Освен това в интернет средата, поради непрозрачността на политиките за защита на личните данни, често е по-трудно за хората да бъдат запознати със своите права и да дадат информирано съгласие. Това се усложнява още повече от факта, че в някои случаи дори не е ясно какво представлява свободно изразено, конкретно и информирано съгласие за обработка на лични данни, какъвто е случаят при поведенческите реклами, където настройките на интернет браузъра се считат от някои, но не от други, за израз на съгласието на потребителя.

Следователно е необходимо пояснявӑне на условията за получаване на съгласие от субекта на данните, така че винаги да се гарантира информирано съгласие и да се осигури, че лицето напълно осъзнава, че дава своето съгласие и напълно разбира за каква обработка на данни го дава, в съответствие с член 8 от Хартата на основните права на ЕС. Яснотата по ключовите понятия би могла да благоприятства и развитието на инициативи за саморегулиране за разработването на практически решения, които са в унисон с правото на ЕС.

Комисията ще проучи възможности за **разясняване и засилване на правилата относно съгласието**.

*2.1.6. Защита на чувствителни данни*

Понастоящем вече е забранена обработката на чувствителни данни, т.е. данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения, членство в синдикални организации и обработката на данни, отнасящи се до здравето или сексуалния живот, като съществуват ограничени

[21] Вж. член 2, буква з) от Директива 95/46/ЕО.

изключения при определени условия и при наличието на защитни мерки[22]. Необходимо е обаче, с оглед на технологичното развитие и другите промени в обществото, съществуващите разпоредби относно чувствителните данни да бъдат преразгледани, да се обмисли евентуалното добавяне на други категории данни и да се изяснят допълнително условията за тяхната обработка. Това се отнася, например, за генетичните данни, които понастоящем не са изрично посочени като категория чувствителни данни.

Комисията ще разгледа възможността:

- дали други категории данни следва да се считат за „чувствителни **данни**“, например **генетични** данни;

- за по-нататъшно пояснявane и **хармонизиране на условията**, позволяващи обработката на категории чувствителни данни.

*2.1.7. По-ефективни средства за правна защита и санкции*

За да се гарантира прилагането на правилата за защита на данните, от ключово значение е наличието на **ефективни разпоредби за средства за правна защита и санкции**. В много случаи, когато дадено лице е засегнато от нарушаване на правилата за защита на данните, са засегнати и значителен брой други лица в подобна ситуация.

Поради това Комисията ще:

- разгледа възможността за **разширяване на правомощието за предявяване на иск пред националните съдилища**, като такова право бъде дадено на органите за защита на данните и на сдруженията на гражданското общество, както и да **други сдружения, които представляват интересите на субектите на данни**;

- оцени необходимостта от **засилване на съществуващите разпоредби за санкции**, например чрез изрично включване на наказателни санкции в случай на сериозни нарушения на защитата на данните, с цел да засили тяхната ефективност.

## 2.2. Засилване на измерението, свързано с вътрешния пазар

*2.2.1. Повишаване на правната сигурност и осигуряване на равни условия за администраторите на лични данни*

Защитата на данните в ЕС има **ясно изразено измерение, свързано с вътрешния пазар**, т.е. необходимостта да се гарантира свободното движение на лични данни между държавите-членки в рамките на вътрешния пазар. В резултат на това хармонизирането на националните закони за защита на данните с директивата не се ограничава до минимално хармонизиране, а достига до хармонизиране, което в по-голямата си част е пълно[23].

Същевременно директивата предоставя на държавите-членки свобода на действие в определени области и им дават право да запазят или да въведат специални правила за специфични случаи[24]. Това, заедно с факта, че в някои случаи държавите-членки са

---

22 Вж. член 8 от Директива 95/46/ЕО.

23 Съд на Европейския съюз, Дело № C-101/01, „Bodil Lindqvist“, ECR [2003], I-1297, 96, 97.

24 Пак там, 97. Вж. също съображение 9 от Директива 95/46/ЕО.

приложили директивата неправилно, води до **различия между националните закони за прилагане на директивата, което е в противоречие с една от нейните основни цели, а именно гарантирането на свободното движение на лични данни в рамките на вътрешния пазар**. Това важи за голям брой сектори и ситуации, например при обработката на лични данни в сферата на заетостта или за целите на общественото здраве. Липсата на хармонизация е един от основните и най-често изтъквани проблеми от частните заинтересовани страни, особено от икономическите оператори, тъй като води до допълнителни разходи и административна тежест за тях. Това важи в особена степен за администраторите на лични данни, установени в няколко държави-членки и задължени да се съобразяват с изискванията и практиките във всяка от тези държави. Освен това различията в прилагането на директивата от държавите-членки създават правна несигурност не само за администраторите на лични данни, но и за субектите на данни, създавайки риск от нарушаване на еднаквото ниво на защита, което директивата би трябвало да постигне и да гарантира.

Комисията ще разгледа начините за постигане на **по-нататъшна хармонизация на правилата за защита на данните на равнище ЕС**.

*2.2.2. Намаляване на административната тежест*

Осигуряването на равни условия ще намали необходимостта от съобразяване с различаващи се национални изисквания и по този начин значително ще намали административната тежест за администраторите на данни. Друг конкретен елемент за намаляване на административната тежест и съкращаване на разходите за администраторите на данни е **преразглеждането и опростяването на действащата система за уведомяване**[25]. По общо мнение на администраторите на данни настоящото общо задължение за уведомяване на органите за защита на данните относно всички операции за обработка на данни е доста обременително задължение, което само по себе си не предоставя реална добавена стойност за защитата на личните данни. Нещо повече, това е един от случаите, в които директивата оставя на държавите-членки известна свобода на действие, като те са свободни да определят възможните изключения и опростяване, както и процедурите, които да бъдат следвани.

Една хармонизирана и опростена система ще намали разходите и административната тежест, особено за многонационалните компании, установени в няколко държави-членки.

Комисията ще проучи различни възможности за **опростяването и хармонизирането на съществуващата система за уведомяване**, включително и възможността за изготвянето на **единен за целия ЕС регистрационен формуляр**.

*2.2.3. Изясняване на правилата относно приложимото право и отговорността на държавите-членки*

В първия доклад на Комисията относно прилагането на Директивата за защита на личните данни от 2003 г.[26] вече бе изтъкнат фактът, че разпоредбите относно

[25] Вж. член 18 от Директива 95/46/ЕО.

[26] Доклад на Комисията – Първи доклад относно прилагането на Директивата за защита на личните данни (95/46/ЕО) (COM (2003) 265 окончателен).

приложимото право[27] „в няколко случая са недостатъчни, в резултат на което биха могли да възникнат стълкновения на правни норми от вида, който този член има за цел да избегне“. Оттогава ситуацията не се е подобрила, като в резултат на това не винаги е ясно за администраторите на лични данни и за надзорните органи за защита на данните коя държава-членка носи отговорност и чий закон се прилага в случаите, когато са засегнати няколко държави-членки. Това важи особено за случаите, когато даден администратор на лични данни трябва да спазва различни изисквания от различни държави-членки, когато многонационално предприятие е установено в повече от една държава-членка или когато администраторът на данните не е установен в ЕС, но предлага своите услуги на пребиваващи в ЕС лица.

**Сложността се увеличава също и в резултат на глобализацията и технологичните промени**: администраторите на лични данни все по-често осъществяват дейност в няколко държави-членки и юрисдикции, като предоставят услуги и помощ денонощно. С помощта на Интернет е много по-лесно за администраторите на лични данни, установени извън Европейското икономическо пространство (ЕИП)[28], да предоставят услуги от разстояние и да обработват лични данни в интернет средата и често е трудно да се определи местоположението на личните данни и на оборудването, използвано в даден момент (например при приложения и услуги в „изчислителни облаци“).

Въпреки това Комисията счита, че фактът, че обработката на лични данни се извършва от администратор на данни, установен в трета държава, не следва да лишава лицата от защитата, която им се полага по силата на Хартата на основните права на ЕС и законодателството на ЕС за защита на данните.

Комисията ще проучи начините за **преразглеждане и изясняване на съществуващите разпоредби относно приложимото право**, включително настоящите критерии за определяне на приложимото право, за да се повиши правната сигурност, да се изясни отговорността на държавите-членки за прилагане на правилата за защита на данните и в крайна сметка да се предостави еднакво ниво на защита на субектите на данни от ЕС, независимо от географското местоположение на администратора на лични данни.

*2.2.4. Засилване на отговорността на администраторите на лични данни*

Административното опростяване **не трябва да води до общо намаляване на отговорността на администраторите на лични данни за осигуряване на ефективна защита на личните данни**. Напротив, Комисията счита, че техните задължения трябва да бъдат по-ясно разписани в правната рамка, включително по отношение на механизмите за вътрешен контрол и сътрудничеството с надзорните органи за защита на данните. Освен това следва да се гарантира, че тази отговорност се прилага и за администраторите, които са предмет на задължения за професионална тайна (например юристи), както и за все по-често срещаните случаи, когато администраторите на лични данни делегират обработката на данни на други организми (например лица, обработващи данни).

Ето защо Комисията ще проучи начините **да се гарантира, че администраторите на лични данни въвеждат ефективни политики и механизми за гарантиране на**

[27] Вж. член 4 от Директива 95/46/ЕО.

[28] Европейското икономическо пространство включва Норвегия, Лихтенщайн и Исландия.

**спазването на правилата за защита на данните**. В този процес Комисията ще вземе предвид текущия дебат за евентуалното въвеждане на принципа за „accountability“ (отчетност)[29]. Това няма да доведе до увеличаване на административната тежест за администраторите на лични данни, тъй като тези мерки се фокусират върху създаването на защитни мерки и механизми, чрез които спазването на правилата за защита на данните става по-ефективно, като същевременно се намаляват и опростяват някои административни формалности, като например уведомяването (*вж. точка 2.2.2 по-горе*).

Насърчаването на използването на технологии за подобряване на защитата на личния живот (PETs), както вече бе посочено в съобщението на Комисията от 2007 г. по този въпрос, както и на принципа за „защита на личния живот още при проектирането“ може да играе важна роля в това отношение, включително и за гарантиране на сигурността на данните[30].

Комисията ще разгледа следните елементи за засилване на отговорността на администраторите на лични данни:

– въвеждане на задължението за назначаване на независим **служител за защита на данните** и хармонизиране на правилата, свързани с неговите задачи и компетентност[31], като същевременно се обмисли подходящ праг, за да се избегне ненужната административна тежест, особено за малките предприятия и микропредприятията.

– включване в правната рамка на задължение за администраторите на данни да извършват **оценка на въздействието върху защитата на данните** в специфични случаи, например при обработката на чувствителни данни, или когато обработката по друг начин включва специфични рискове, по-специално при използването на специфични технологии, механизми или процедури, включително профилиране или видео наблюдение;

– по-нататъшно насърчаване на използването на PETs и на възможностите за конкретното прилагане на идеята за „**защита на личния живот още при проектирането**“.

### *2.2.5. Насърчаване на инициативи за саморегулиране и проучване на схеми на ЕС за сертифициране*

Комисията продължава да счита, че **инициативите за саморегулиране** на администраторите на лични данни могат да **допринесат за по-доброто прилагане на правилата за защита на данните**. Сега действащите разпоредби относно

---

29 Вж. по-специално становището, прието от Работната група по член 29 на 13 юли, 3/2010.

30 Принципът „защита на личния живот още при проектирането“ означава, че неприкосновеността на личния живот и защитата на данните са включени в целия жизнен цикъл на технологиите, от най-ранния стадий на тяхното проектиране, до тяхното внедряване, използване и окончателно изваждане от употреба. Този принцип е включен също и в Съобщението на Комисията „Програма в областта на цифровите технологии за Европа “, COM (2010) 245.

31 В няколко държави-членки вече се прилага настоящата възможност администраторът на лични данни да назначи служител за защита на данните, за да се гарантира по независим начин съответствието с европейските и националните правила за защита на данните и за подпомагане на физическите лица (вж. например „*Beauftragter für den Datenschutz*“ в Германия и „*correspondant informatique et libertés (CIL)*“ във Франция).

саморегулирането в Директивата за защита на личните данни, а именно възможността за изработване на кодекси на поведение[32], до този момент са рядко използвани и частните заинтересовани лица не ги считат за задоволителни.

Освен това Комисията ще проучи възможното създаване на **схеми** на ЕС **за сертифициране (напр. „печати за неприкосновеност на личния живот“)** за процеси, технологии, продукти и услуги, които отговарят на изискванията за защита на неприкосновеността на личния живот[33]. Това не само ще служи за ориентир на потребителите на такива технологии, продукти и услуги, но и ще бъде от значение във връзка с отговорността на администраторите на лични данни: изборът на сертифицирани технологии, продукти или услуги може да помогне да се докаже, че администраторът е изпълнил задълженията си (*вж. точка 2.2.4 по-горе)*. Разбира се, от съществено значение ще бъде да се **гарантира надеждността на тези печати за неприкосновеност на личния живот** и да се види как те се вписват в правните задължения и международните технически стандарти.

Комисията ще:

- проучи средствата за **допълнително насърчаване на инициативи за саморегулиране**, включително активното поощряване на използването на кодекси за поведение;

- разгледа възможността за създаване на **схеми на ЕС за сертифициране** в областта на неприкосновеността на личния живот и защитата на данните.

### 2.3. Преразглеждане на правилата за защита на данните в областта на полицейското и съдебното сътрудничество по наказателноправни въпроси

Директивата за защита на данните се прилага за всички дейности за обработка на лични данни в държавите-членки, както в обществения, така и в частния сектор. Въпреки това тя не се прилага за обработването на лични данни „при извършване на дейности извън приложното поле на правото на Общността“, каквито са дейностите в рамките на полицейското и съдебното сътрудничество по наказателноправни въпроси[34]. С Договора от Лисабон обаче предходната „структурата по стълбове“ на ЕС беше премахната и беше въведена ново и широкообхватно правно основание за защитата на личните данни във всички политики на Съюза[35]. В този контекст и с оглед на Хартата на основните права на ЕС в своите съобщения относно Стокхолмската програма и Стокхолмския план за действие[36] Комисията подчерта нуждата да се въведе „широкообхватна схема за защита“ и да „ се укрепи позицията на ЕС относно защитата на личните данни на отделния човек в контекста на всички политики на ЕС, включително правоприлагането и предотвратяването на престъпления“.

Инструментът на ЕС за защита на личните данни в областта на полицейското и съдебното сътрудничество по наказателноправни въпроси е **Рамково решение**

---

32 Вж. член 27 от Директива 95/46/ЕО.

33 По този аспект вж. също съобщението относно PETs, цитирано в бележка под линия 30.

34 Вж. член 3, параграф 2, първо тире от Директива 95/46/ЕО.

35 Вж. член 16 от ДФЕС.

36 Вж. COM(2009) 262, 10.6.2009 г. и COM(2010) 171, 20.4.2010 г.

**2008/977/ПВР** [37]. Рамковото решение представлява важна стъпка напред в сфера, където определянето на общи стандарти за защита на данните бе изключително необходимо. Необходима е обаче по-нататъшна работа.

**Рамковото решение се прилага единствено за трансграничния обмен на лични данни в рамките на ЕС**, но не и за вътрешните операции по обработка на данни в държавите-членки. Това разграничение е много трудно да бъде постигнато на практика и може да затрудни реалното изпълнение и прилагане на рамковото решение[38].

Освен това в **рамковото решение се съдържа твърде широко изключение от принципа за ограничаване на обработката до необходимото за постигане на целите**. Друг недостатък е липсата на разпоредби за това, че различните категории данни следва да се разграничават според тяхната степен на точност и надеждност, че данните, основани на факти, следва да се разграничават от данните, основани на мнения или лични оценки[39], и че следва да се прави разграничение между различни категории субекти на данни (престъпници, заподозрени, жертви, свидетели и т.н.), като се определят специални гаранции за данните, свързани с лицата, които не са заподозрени[40].

Освен това **рамковото решение не заменя различните секторно-специфични законодателни актове за полицейско и съдебно сътрудничество по наказателноправни въпроси, приети на равнище ЕС**[41], и по-специално тези, които уреждат функционирането на Европол, Евроюст, Шенгенската информационна система (ШИС) и Митническата информационна система (МИС)[42], които или съдържат специални режими за защита на данните и/или обикновено се позовават на инструментите за защита на данните на Съвета на Европа. За дейностите в областта на полицейското и съдебното сътрудничество всички държави-членки се присъединяват към Препоръка № R (87) 15 на Съвета на Европа, която излага принципите на Конвенция № 108 по отношение на полицейския сектор. Тази препоръка обаче не е правно обвързващ инструмент.

**Тази ситуация би могла пряко да засегне възможността на физическите лица да упражняват правата си за защита на данните в тази област** (например да знаят

---

37 Рамково решение 2008/977/ПВР на Съвета от 27 ноември 2008 г. относно защитата на личните данни, обработвани в рамките на полицейското и съдебното сътрудничество по наказателноправни въпроси, (ОВ L 350, 30.12.2008 г., стр. 60). В рамковото решение се предвижда само минимална хармонизация на стандартите за защита на данните.

38 Такова разграничение не съществува в съответните инструменти на Съвета на Европа като например Конвенцията за защита на лицата при автоматизираната обработка на лични данни (CETS № 108), нейния Допълнителен протокол относно контролните органи и трансграничните потоци от данни ((ETS № 181) ) и Препоръка № R (87) 15 на Комитета на министрите към държавите-членки, с която се урежда използването на лични данни в сектора на полицията, приета на 17 септември 1987 г.

39 Както се изисква от принцип 3.2 от Препоръка № R (87) 15.

40 В разрез с принцип 2 от Препоръка № R (87) 15 и докладите за оценка към нея.

41 Вж. обобщение на тези инструменти в съобщението на Комисията, озаглавено „Преглед на управлението на информацията в областта на свободата, сигурността и правосъдието“, COM (2010) 385.

42 За да се гарантира надзор над защитата на данните, по силата на съответните инструменти са създадени съвместни надзорни органи, в допълнение към общите надзорни правомощия, които Европейският надзорен орган за защита на данните упражнява върху институциите, органите, службите и агенциите на ЕС в съответствие с Регламент (ЕО) № 45/2001.

какви техни лични данни се обработват и обменят, от кого и с каква цел, и как да упражняват своите права, като например правото на достъп до своите данни).

От целта да се създаде всеобхватна и съгласувана система в ЕС и по отношение на трети държави произтича **необходимостта да се обмисли възможността за преразглеждане на действащите правила за защита на данните в областта на полицейското и съдебното сътрудничество по наказателноправни въпроси**. Комисията подчертава, че идеята за всеобхватна схема за защита на данните не изключва прилагането на специфични правила към защитата на данните за полицията и съдебната система в контекста на общата рамка, като се отчита подобаващо спецификата на тези сфери, както е посочено в Декларация 21 към Договора от Лисабон. Това включва, например, необходимостта да се разгледа степента, в която в даден конкретен случай упражняването на правата за защита на данните от дадено лице може да застраши предотвратяването, разследването, разкриването или преследването на престъпления или изпълнението на наказания.

Комисията, по-специално, ще:

- обмисли **разширяване на обхвата на приложение на общите правила за защита на данните и към областите на полицейското и съдебното сътрудничество по наказателноправни въпроси**, включително към обработката на данни на национално равнище, при същевременното предоставяне, когато това е необходимо, на хармонизирани **ограничения** на правата на физическите лица за защита на данните, например по отношение на правото на достъп или на принципа на прозрачност;

- разгледа необходимостта от въвеждане в новата обща рамка за защита на данните на **специфични и хармонизирани разпоредби**, например относно защитата на данните при обработка на **генетични данни** за целите на наказателното право или относно разграничаването на различните категории физически лица (свидетели, заподозрени и т.н.) в областта на полицейското и съдебното сътрудничество по наказателноправни въпроси;

- даде ход през 2011 г. на **консултация** с всички заинтересовани страни относно най-добрия начин за **преразглеждане на съществуващите системи за надзор в областта на полицейското и съдебното сътрудничество по наказателноправни въпроси**, за да се гарантира ефективен и последователен надзор на защитата на данните върху всички институции, органи, служби и агенции на Съюза;

- оцени необходимостта в дългосрочен план **съществуващите различни секторни правила, приети в специфични инструменти на равнище ЕС за полицейско и съдебно сътрудничество по наказателноправни въпроси, да бъдат приведени в съответствие** с новата обща правна рамка за защита на данните.

### 2.4. Глобално измерение на защитата на данните

#### *2.4.1. Разясняване и опростяване на правилата относно международния трансфер на лични данни*

Един от начините да се даде възможност за трансфер на лични данни извън ЕС и ЕИП е т. нар. „**оценка на адекватността**“. Понастоящем адекватността на предоставената от трета държава защита, т.е. дали ЕС счита за адекватно равнището на защита в тази държава, може да се определи от Комисията и от държавите-членки.

Ако Комисията заключи, че равнището на защита е адекватно, 27-те държави-членки на ЕС и трите държави от ЕИП могат свободно да предават лични данни към тази трета държава, без да бъдат необходими допълнителни предпазни мерки. Въпреки това понастоящем Директивата за защита на данните не определя в достатъчни подробности точните изисквания за признаване на адекватност от страна на Комисията. Освен това в рамковото решение не се предвижда Комисията да взема такова решение.

В някои държави-членки адекватността се оценява на първо място от администратора на данни, който предава личните данни на дадена трета държава, като понякога надзорният орган за защита на данните извършва последващ контрол. Тази ситуация може да доведе до различни подходи към оценката на степента на адекватност на защитата в трети държави или международни организации, и **води до риска държавите-членки да оценят по различен начин равнището на защита на субектите на данни, осигурено в дадена трета държава**. Освен това действащите правни инструменти не съдържат подробни, хармонизирани указания за това кои трансфери могат да се считат за законни. Това води до различни практики в различните държави-членки.

Също така за трансфера на данни към трети държави, които не гарантират адекватно равнище на защита, настоящите общи договорни клаузи на Комисията за трансфер на лични данни към администратори[43] и лица, обработващи данни[44], не са предназначени да бъдат използвани в ситуации, които не са обхванати от договор, и не могат да бъдат използвани, например, при трансфера на данни между публичните администрации.

Също така често в международните споразумения, сключени от ЕС или неговите държави-членки, се изисква включване на принципите за защита на данните и на специални разпоредби. Това може да доведе до различаващи се текстове с несъответстващи разпоредби и права, като по този начин се дава възможност за различни тълкувания в ущърб на субекта на данните. В резултат на това Комисията обяви, че ще работи за включването в споразуменията между Съюза и трети държави на основни елементи за защита на личните данни за целите на правоприлагането[45].

Някои други средства, разработени като форма на саморегулация, например вътрешните кодекси за поведение на дружествата, познати като „задължителни фирмени правила“ (BCRs)[46], също могат да бъдат полезен инструмент за законен

---

43 Решение 2001/497/ЕО на Комисията от 15 юни 2001 г. относно общите договорни клаузи за трансфера на лични данни към трети страни съгласно Директива 95/46/ЕО (ОВ L 181, 4.7.2001 г., стр. 19); Решение № 2002/16/ЕО на Комисията от 27 декември 2001 г. относно общите договорни клаузи за трансфера на лични данни към лицата, които ги обработват, установени в трети страни, съгласно Директива 95/46/ЕО (ОВ L 6, 10.1.2002 г., стр. 52); Решение № 2004/915/ЕО на Комисията от 27 декември 2004 г. за изменение на Решение № 2001/497/ЕО за въвеждане на алтернативен комплект общи договорни клаузи за прехвърляне на лични данни в трети страни (ОВ L 385, 29.12.2004 г., стр. 74).

44 Решение на Комисията от 5 февруари 2010 г. относно стандартните договорни клаузи при предаването на лични данни към лицата, които ги обработват, установени в трети страни, съгласно Директива 95/46/ЕО на Европейския парламент и на Съвета (ОВ L 39, 12.2.2010 г., стр. 5).

45 План за действие от Стокхолм, цитиран по-горе (бележка под линия 36).

46 „Задължителните фирмени правила“ са кодекси на поведение, основани на европейските стандарти за защита на данните, които многонационалните организации изготвят и следват доброволно, за да осигурят адекватни защитни мерки при трансферите или категориите трансфери на лични данни между дружествата, които са част от една и съща корпоративна група

трансфер на лични данни между дружества от една и съща корпоративна група. Заинтересованите страни обаче изказват мнение, че този механизъм може да бъде допълнително подобрен, а неговото прилагане – облекчено.

За да се отговори на така поставените въпроси **е необходимо като цяло да се усъвършенстват действащите механизми за международни трансфери на лични данни**, като същевременно се осигури адекватна защита на личните данни, когато те се прехвърлят и обработват извън ЕС и ЕИП.

Комисията възнамерява да проучи начини за:

- **подобряване и рационализиране на действащите процедури** за международен трансфер на данни, за да се осигури **по-еднообразен и последователен подход на ЕС** по отношение на трети държави и международни организации;

- **изясняване на процедурата на Комисията за оценка на адекватността** и по-добро определяне на **критериите и изискванията** за оценяване на равнището на защита на данните в трета държава или международна организация;

- определяне на **основни елементи на ЕС за защита на данните**, които биха могли да се използват във всички видове международни споразумения.

*2.4.2. Насърчаване на универсални принципи*

Обработката на лични данни е глобализиран процес и изисква разработването на универсални принципи за защитата на физическите лица по отношение на обработката на техните лични данни.

Правната рамка на ЕС за защита на личните данни често служи за **ориентир на третите държави при въвеждането на разпоредби за защита на данните**. Нейната сила и въздействие, в рамките на Съюза и извън него, са от изключително значение. Ето защо **Европейският съюз трябва да продължи да бъде движеща сила за разработването и популяризирането на международни правни и технически стандарти за защита на личните данни**, въз основа на съответните актове на ЕС и други европейски инструменти за защита на данните. Това важи в особена степен за политиката на ЕС за разширяване.

По отношение на международните технически стандарти, разработени от организации за стандартизация, Комисията счита, че съгласуваността между бъдещата правна рамка и тези стандарти е от особена важност за осигуряването на последователно и практическо прилагане на правилата за защита на данните от администраторите на данни.

---

и които са обвързани от тези корпоративни правила. Вж.: http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf.

Комисията ще:

- продължи да **насърчава разработването на високи правни и технически стандарти за защита на данните** в трети държави и на международно равнище;

- се стреми към **принципа за реципрочност на защитата в международните действия на Съюза,** и по-специално по отношение на лицата, чиито данни се изнасят от ЕС към трети държави;

- **засили своето сътрудничество с трети държави и международни организации** като ОИСР, Съвета на Европа, Организацията на обединените нации и други регионални организации за постигането на тази цел;

- **следи отблизо разработването на международни технически стандарти от организациите за стандартизация** като CEN и ISO, за да гарантира, че тези стандарти успешно допълват правните норми и за да гарантира оперативното и ефективното изпълнение на основните изисквания за защита на данните.

### 2.5. По-засилена институционална организация за по-добро прилагане на правилата за защита на личните данни

Изпълнението и прилагането на принципите и правилата за защита на данните е ключов елемент за гарантиране на зачитането на правата на личността.

В този контекст **ролята на органите за защита на данните (ОЗД) е от съществено значение** за прилагането на правилата за защита на данните. Те са независими гаранти на основните права и свободи по отношение на защитата на личните данни, като физическите лица разчитат на тях за защитата на своите лични данни и законосъобразността на операциите по обработката им. Поради тази причина Комисията счита, че ролята на ОЗД следва да бъде укрепена, особено като се отчита неотдавнашната съдебна практика на Съда на ЕС по отношение на тяхната независимост[47], и те следва да разполагат с необходимите правомощия и ресурси за правилното изпълнение на своите задачи както на национално равнище, така и при взаимното си сътрудничество.

В същото време Комисията счита, че **органите за защита на данните следва да засилят сътрудничеството помежду си и да координират своите действия по-добре**, особено когато са изправени пред въпроси, които по своя характер имат трансгранично измерение. Това важи в особена степен за случаите, когато многонационални предприятия са установени в няколко държави-членки и извършват дейност във всяка от тези държави, или когато е необходим надзор, координиран с Европейския надзорен орган за защита на данните[48].

---

47 Решение на Съда на ЕС от 9.3.2010 г., Комисията срещу Германия, Дело № C-518/07.

48 Понастоящем това важи за големите информационни системи, например ШИС II (вж. член 46 от Регламент (ЕО) № 1987/2006, ОВ L 318, 28.12.2006 г., стр. 4) и ВИС (вж. член 43 от Регламент (ЕО) № 767/2008, ОВ L 218, 13.8.2008 г., стр. 60).

**Важна роля** в това отношение **може да играе Работната група по член 29**[49], която, освен консултативната си функция[50], вече има за задача да допринася за еднаквото прилагане на национално равнище на правилата на ЕС за защита на данните. Все пак съществуващите различия в прилагането и тълкуването на правилата на ЕС от органите за защита на данните, дори когато предизвикателствата пред защитата на личните данни са едни и същи в целия ЕС, изискват засилване на ролята на Работната група при координирането на позициите на ОЗД, за да се осигури по този начин по-еднообразно прилагане на национално равнище, а съответно и равностойно равнище на защита на личните данни.

Комисията ще разгледа начини за:

- **засилване, изясняване и хармонизиране на статута и правомощията на националните органи за защита на данните** в новата правна рамка, включително пълното прилагане на понятието за „пълна независимост“[51];

- постигане на **по-добро сътрудничество и координация между органите за защита на данните**;

- **осигуряване** на по-последователно прилагане на правилата на ЕС за защита на данните в рамките на вътрешния пазар. Това може да включва **укрепване на ролята на националните надзорни органи за защита на данните, по-добра координация на тяхната работа посредством Работната група по член 29 (която следва да се превърне в по-прозрачна структура) и/или създаване на механизъм, който да гарантира последователността на вътрешния пазар под ръководството на Европейската комисия.**

## 3. ЗАКЛЮЧЕНИЕ: ПЪТЯТ НАПРЕД

Също както и технологиите начинът, по който нашите лични данни се използват и се споделят в нашето общество се променя непрекъснато. Това изправя законодателите пред предизвикателството да се изгради законодателна рамка, която ще устои на изпитанието на времето. След приключване на процеса на реформи европейските правила за защита на данните следва да продължат да гарантират високо равнище на защита и да осигуряват правна сигурност за физическите лица, държавните администрации и стопанските субекти на вътрешния пазар в продължение на няколко поколения. Независимо от трудността на ситуацията или сложността на технологиите, трябва да има яснота относно приложимите правила и стандарти, които националните органи следва да прилагат, а стопанските субекти и разработващите нови технологии ─ да съблюдават. Хората трябва да са наясно и с правата, с които разполагат.

**Всеобхватният подход на Комисията** за решаване на проблемите и за постигане на основните цели, подчертани в настоящото съобщение, ще послужи за основа на по-

---

[49] Работната група по член 29 е консултативен орган, съставен от по един представител на държавите-членки, на органите за защита на данните, на Европейския надзорен орган за защита на данните и на Комисията (без право на глас), като Комисията също така предоставя секретариата на Работната група. Вж.: http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm .

[50] Работната група по член 29 има за задача да съветва Комисията относно равнището на защита в ЕС и в трети държави и относно всяка друга мярка, свързана с обработката на лични данни.

[51] Вж. Решение на Съда на ЕС от 9.3.2010 г., Комисията срещу Германия, Дело № C-518/07.

нататъшните дискусии с другите европейски институции и с други заинтересовани страни, а на по-късен етап ще бъдат изработени конкретни предложения и мерки от законодателен и незаконодателен характер. За тази цел Комисията приветства всички мнения по въпросите, повдигнати в настоящото съобщение.

На тази основа и след провеждането на оценка на въздействие, като вземе предвид Хартата на основните права на ЕС Комисията ще направи **законодателни предложения през 2011 г.**, които ще имат за цел да се преразгледа правната рамка за защита на данните, за да се укрепи позицията на ЕС относно защитата на личните данни на отделния човек в контекста на всички политики на ЕС, включително правоприлагането и предотвратяването на престъпления, като се отчетат особеностите на тези области. Успоредно с това ще се работи по незаконодателни мерки като насърчаване на саморегулирането и разглеждане на възможността за създаване на печати на ЕС за неприкосновеност на личния живот.

Като втора стъпка Комисията ще **оцени необходимостта от адаптиране на други правни инструменти** към новата обща рамка за защита на личните данни. Това се отнася преди всичко за Регламент (ЕО) № 45/2001, чиито разпоредби ще трябва да бъдат адаптирани към новата обща правна рамка. На по-късен етап ще трябва да се направи също така внимателна оценка на въздействието върху други секторни инструменти.

Комисията ще продължи също така да осигурява подходящ мониторинг на правилното прилагане на правото на Съюза в тази област, като провежда **активна политика спрямо нарушенията**, когато правилата на ЕС за защита на данните не са правилно въведени и прилагани. На практика настоящото преразглеждане на инструментите за защита на данните не засяга задължението на държавите-членки да изпълняват съществуващите правни инструменти за защита на личните данни и да гарантират тяхното правилно прилагане[52].

Най-добрият начин за насърчаване и популяризиране в световен мащаб на стандартите на ЕС за защита на данните е осигуряването на високо и еднакво равнище на защита на данните в рамките на самия ЕС.

[52] Това включва и Рамково решение № 2008/977/ПВР на Съвета: държавите-членки трябва да предприемат до 27 ноември 2010 г. необходимите мерки, за да се съобразят с разпоредбите на това рамково решение.