

Становище на Европейския икономически и социален комитет относно „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“

COM(2010) 609 окончателен

(2011/C 248/21)

Докладчик: **г-н MORGAN**

На 4 ноември 2010 г. Европейската комисия реши, в съответствие с член 304 от Договора за функционирането на Европейския съюз, да се консултира с Европейския икономически и социален комитет относно

„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“

COM (2010) 609 окончателен.

Специализирана секция „Заетост, социални въпроси и гражданство“, на която беше възложено да подготви работата на Комитета по този въпрос, прие своето становище на 27 май 2011 г.

На 472-ата си пленарна сесия, проведена на 15 и 16 юни 2011 г. (заседание от 16 юни 2011 г.), Европейският икономически и социален комитет прие настоящото становище с 155 гласа „за“, 9 гласа „против“ и 12 гласа „въздържал се“.

1. **Заклучения и препоръки**

1.1 Правото на ЕС в областта на защитата на личните данни се основава на Директива № 95/46/ЕО от 1995 г., която има две цели, изразени по следния начин:

- (1) *Държавите-членки защитават основните права и свободи на физическите лица и в частност правото им на личен живот при обработката на лични данни;*
- (2) *Държавите-членки не могат нито да ограничават, нито да забраняват свободното движение на лични данни между държавите-членки по съображения, свързани със защитата, предоставяна съгласно параграф 1.*

От първостепенно значение е да се постигне баланс между тези две цели, така че те да не влизат в противоречие. Главната цел на новото законодателство е създаването на правна рамка, която да спомога за постигането и на двете цели.

1.2 ЕИСК приветства настоящото съобщение, което представя подхода на Комисията към актуализирането на Директива № 95/46 ЕО за защита на личните данни. Бурното развитие на новите технологии води до експоненциален ръст на количеството данни, обработвани онлайн, което изисква съответно увеличаване на защитата на личните данни, за да се избегне мащабно нерегулирано навлизане в личния живот. Събирането, обобщаването и управлението на данни от множество източници следва да бъде внимателно и точно описано. Публичният сектор поддържа много различни данни за различни аспекти на отношенията между гражданите и държавата. Следва да се събират само минималните данни, необходими за съответната цел, и да се въведе забрана за събирането на различните данни в база данни от типа „Големия брат“.

1.3 Едновременно с това ЕИСК призовава към предпазливост. Законодателството, което регулира стопанската дейност, трябва да остава стабилно и предвидимо. Затова ЕИСК подкрепя едно целесъобразно преразглеждане на Директивата за защита на личните данни.

1.4 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. ЕИСК предлага новото законодателство да гарантира по-последователна защита на личните данни на работниците в целия ЕС, в това число Европейска рамка за засилване на правната яснота и сигурност. В този смисъл ЕИСК приветства по-конкретно намерението да стане задължително назначаването на независими служители за защита на данните в предприятията и да бъдат хармонизирани правилата относно задачите и правомощията на тези служители.

1.5 Предвид възможния конфликт между частния живот на физическите лица и използването на данните, свързани със съответното лице, за търговски цели, и на високия залог, хората трябва да осъзнаят във все по-голяма степен целите, за които се събират техните данни и възможностите, с които разполагат за упражняване на контрол върху вече събраните данни. Затова ЕИСК е убеден, че ефективното прилагане и правната защита представляват задължително условие, за да може настоящият проект да стане действително „всеобхватен“. Освен това трябва да бъде обхванато и трансграничното измерение.

1.6 Когато става дума за граждани на ЕС, приложимото право в Европейския съюз следва да бъде правото на държавата-членка на администратора на данни, там където се съхраняват данните. За уязвими лица, особено работници и потребители, в сила трябва да бъде правото на защита на личните данни според обичайното местопребиване.

1.7 Децата се споменават твърде бегло. Необходимо е да се постави специално ударение върху въпросите, свързани с неприкосновеността на личния живот на децата. Правото „да се забрави“ би могло да позволи заличаването на регистрирани данни за извършени детски пакости и провинения на подрастващи, но то може да се окаже неосъществимо на практика.

1.8 Настоящото определение за чувствителни данни има нужда от изясняване, тъй като категориите електронни данни за физическите лица продължават да се увеличават. Широко разпространеното и безразборно прилагане на камери за наблюдение тревожи ЕИСК. Важно е да се приложи законът, ограничаваш непромерното използване на тези изображения. GPRS данните, които са свързани с местонахождението на лицата, представляват друг източник на спорове. Нараства и свалянето на биометрични данни. Определението следва да включва подобни нови технологии и методологии, и следва да дава възможност за включване на по-нататъшни развития в областта на технологиите. Вероятно ще е необходимо да се установят принципи, свързани с контекста. ЕИСК се застъпва за коректното използване на тези нови технологии.

1.9 Въпреки че признава чувствителността на въпросите, свързани с полицейското сътрудничество между отделните държави, ЕИСК изразява убеждение, че е изключително важно на основните права, в това число и на защитата на лични данни, да се обръща възможно най-голямо внимание във всеки един момент.

1.10 ЕИСК подкрепя принципния стремеж на Комисията да гарантира по-последователно прилагане на правилата на ЕС за защита на данните във всички държави-членки. ЕИСК изразява безпокойство, че всичките 12 нови държави-членки вероятно все още не са постигнали цялостно и ефективно прилагане на Директива 95/46.

1.11 ЕИСК е на мнение, че националните органи за защита на личните данни са в общия случай безсилни и претоварени и независимостта им следва да бъде подсилена. Всяка нова директива следва да изисква от националните органи да разполагат със статута, правомощията и ресурсите, необходими за изпълнение на ролята им.

1.12 Въз основа на досегашния ѝ принос в областта на защитата на физическите лица по отношение на обработката на лични данни, ЕИСК е убеден, че Работната група по член 29 може да продължи да изпълнява ценна роля.

1.13 Във връзка с Програмата в областта на цифровите технологии за Европа ЕИСК отправя искане към Комисията да обмисли създаването на орган, който да анализира по-широките последици за обществото от интернет за период от 10 до 20 години. Сегашните разпоредби за сигурност на личните данни и обща киберсигурност стават все по-неадекватни и обществото се озовава в догонваща позиция. Що се отнася до защитата на личните данни, ЕИСК препоръчва създаването на надзорен орган по защита на данните за целия Европейски съюз. Настоящият Европейски надзорен орган по защита на данните се занимава само с институциите на ЕС. Необходим е орган, който да отговаря за координирането и оперативните стандарти на държавите-членки. Създаването му обаче би представлявало само част от върховния орган, който Комитетът има предвид.

2. Въведение

2.1 ЕИСК продължава да подкрепя принципите, на които се основава директивата от 1995 г. По-долу са представени в опростен и синтезиран вид извадки от текста на директивата. Те ясно изразяват принципите, за които става дума:

— Член 6

Държавите-членки предвиждат, че личните данни трябва:

- a) да се обработват справедливо и законно;
- b) да се събират за конкретни, ясно формулирани и законни цели;
- v) да бъдат адекватни, релевантни, и да не са прекомерни по отношение на целите, за които се събират и/или обработват допълнително;
- g) да бъдат точни и при необходимост да се актуализират;
- d) да се поддържат във форма, която позволява идентифицирането на съответните физически лица за срок не по-дълъг от необходимия за целите, за които са събрани тези данни.

— Член 7

Държавите-членки предвиждат, че обработката на лични данни може да се извършва, само ако:

- a) съответното физическо лице е дало недвусмислено своето съгласие за това; или
- b) обработването е необходимо за изпълнението на договор, по който съответното физическо лице е страна; или
- v) обработването е необходимо за спазването на правно задължение, чийто субект е администраторът; или
- g) обработването е необходимо, за да бъдат защитени жизнено важни интереси на съответното физическо лице; или
- d) обработването е необходимо за изпълнението на задача, която се осъществява в обществен интерес; или
- e) обработването е необходимо за целите на законните интереси, преследвани от администратора.

— Член 8

Държавите-членки забраняват обработването на лични данни, разкриващи расов или религиозен произход, политически идеи, религиозни или философски убеждения, членство в професионални съюзи, като и обработването на данни, свързани със здравословното състояние и полови живот.

2.2 През последното десетилетие обстоятелствата се промениха значително с нови разпоредби в член 16 от Договора от Лисабон и член 8 от Хартата за основните права.

2.3 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.

2.4 В днешно време обменът на информация в глобален мащаб е по-лесен и по-бърз. Личните данни на хората – електронен адрес, снимки и електронни бележници, могат да бъдат създавани в Обединеното кралство, като се ползва софтуер, хостван в Германия, да се обработват в Индия, да се съхраняват в Полша и да са достъпни в Испания за гражданин на Италия. Това бързо нарастване на информационните потоци в целия свят представлява голямо предизвикателство пред правата на лицата за защита на неприкосновеността на личните им данни. Въпросите, свързани със защитата на личните данни, в това число и трансграничното измерение, оказват ежедневно влияние върху хората – на работното им място, при взаимодействието им с държавните органи, когато закупуват стоки или услуги, когато пътуват или сърфират в интернет.

2.5 През 2011 г. Комисията ще предложи законодателство, чиято цел е да се преразгледа правната рамка за защита на данните и да се укрепи позицията на ЕС по отношение защитата на личните данни на физическите лица в контекста на всички политики на ЕС, в това число правоприлагане и предотвратяване на престъпления, като се отчетат спецификите 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.

2.6 Освен това Комисията ще продължи да осигурява подходящо наблюдение върху правилното прилагане на правото на Съюза в тази област, като провежда активна политика спрямо нарушенията, в случаите когато правилата на ЕС за защита на данните не се въвеждат и прилагат правилно.

2.7 Всеобхватният подход към защитата на данните има следните пет основни цели:

- засилване на правата на физическите лица;
- засилване на измерението, свързано с вътрешния пазар;
- преразглеждане на правилата за защита на данните в областта на полицейското и съдебното сътрудничество по наказателноправни въпроси;
- глобалното измерение на защитата на данните;
- засилена институционална организация за по-добро прилагане на правилата за защита на личните данни.

В параграфи от 3 до 7 по-долу тези цели се обобщават и се представя гледната точка на ЕИСК по предложенията. Заглавията в **получер шрифт** следват структурата на съобщението. Текстът в *курсив* представлява резюме на текста.

3. Засилване на правата на физическите лица

3.1 Осигуряване на подходяща защита на физическите лица при всички обстоятелства

Хартата на основните права включва правото на защита на личните данни. Определението за „лични данни“ цели да обхване всички сведения, свързани пряко или непряко с физическо лице, чиято самотичност е установена или може да бъде установена. Ще бъдат разгледани средствата за осигуряване на съгласувано прилагане на правилата за защита на данните предвид въздействието на новите технологии върху правата и свободите на физическите лица и целта за гарантиране на свободното движение на лични данни в рамките на вътрешния пазар.

3.1.1 Свободното движение на лични данни в рамките на вътрешния пазар е необходимо за пълноценното функциониране на пазара, но представлява и потенциална заплаха за неприкосновеността на личните данни на работниците, които се съхраняват от дружествата. Необходими са специфични защитни мерки, като отчетност на администраторите на данни за многонационален обмен на данни и използване на криптиране за по-чувствителните данни.

3.1.2 ЕИСК желае да подчертае, че секторът на заетостта е малко или много изключен не само от настоящото съобщение, но също така и от целия дебат за защита на данните в Европа. Извършената вече на европейско ниво работа следва да послужи за отправна точка и по-конкретно предложенията, направени от Работната група по член 29.

3.2 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. Ще бъдат разгледани общ принцип за прозрачна обработка, вменяване на конкретни задължения за администраторите на данни, особено по отношение на децата, стандартни съобщения за поверителност на личните данни и задължително уведомяване при нарушаване на сигурността на личните данни.

3.2.1 Стандартните съобщения са за предпочитане, тъй като така се избягва конфликт на интереси. Те следва да се използват на доброволна основа.

3.2.2 Прозрачността не се отнася непременно до въпроса за едностранните договорни условия. Важно е да се разработят по-строги правила, осигуряващи по-голяма защита срещу несправедливите условия.

3.2.3 Децата се споменават твърде повърхностно. Необходимо е да се постави специално ударение върху въпросите, свързани с неприкосновеността на личния живот на децата. Правото „да се забрави“ би могло да позволи заличаването на регистрирани данни за извършени детски пакости и провинения на подрастващи, но то може да се окаже неосъществимо на практика (3.3.2 по-долу).

3.2.4 Новото законодателство трябва да изясни ролята на лицата, отговарящи за обработката на данните и на лицата, отговарящи за записването им, за да няма объркване относно тяхната самоличност и задълженията и правата на всеки от тях.

3.2.5 ЕИСК подкрепя предложението за задължително уведомяване в случай на нарушаване на сигурността на данните, но смята, че то няма да бъде приложимо във всички случаи за всички сектори и при всички обстоятелства.

3.3 Засилване на контрола върху собствените лични данни

Важни предпоставки представляват ограниченията по отношение на обработката на данни във връзка с конкретните цели (принцип за свеждане до минимум на данните) и ефективния контрол от страна на субектите на данни върху техните собствени данни. Ще бъдат разгледани укрепването на принципа за свеждане до минимум на данните, усъвършенстването на начините за упражняване на правото на достъп, поправяне, заличаване или блокиране на данни, изясняването на „правото да се забрави“ и гарантирането на изричното право на преносимост на данните.

3.3.1 По принцип ЕИСК подкрепя всяко действие, което е насочено към засилване на неприкосновеността на личния живот. Физическите лица следва да имат право на свободен достъп до всички данни, които се набират за тях. Можем да дадем пример със свободния достъп до данни за кредитния рейтинг. Оттеглянето на съгласието без причина и ефективното „право да се забрави“ са основни права, но неприкосновеността на личния живот може допълнително да бъде укрепена, ако по принцип се събират по-малко данни. Затова ЕИСК настоятелно приканва Комисията да приложи предложението за укрепване на принципа на ограничаването до минимум на събираните данни.

3.3.2 Въпреки че „правото да се забрави“ е привлекателно понятие, прилагането му ще се постигне трудно поради вирусния характер на данните в интернет и технологиите, които изтриват, но не забравят.

3.4 Повишаване на осведомеността

Дейностите за повишаване на осведомеността следва да бъдат насърчавани, в това число предоставянето на информация на уебсайтовете, като по ясен начин се описват правата на субектите на данни и отговорностите на администраторите на данни. Особена тревога буди липсата на информираност сред младите хора.

3.4.1 Постигането на необходимите промени в поведението ще бъде трудно, особено предвид факта, че бързото развитие на социалните мрежи не е съпроводено от повишаване на осведомеността на ползвателите относно последствията от големия брой данни, които те предоставят. Макар че по принцип би било добре да има задължителни информационни съобщения за всяка интернет услуга, те може да се окажат проблем за бизнеса. Следва да се обърне внимание на информационните протоколи по категории услуги – интернет търговия, доставчици на интернет услуги, интернет търсачки, социални мрежи и др.

3.4.2 ЕИСК приветства намерението на Комисията да остави европейско финансиране в подкрепа на дейностите за повишаване на осведомеността. ЕИСК би желал то да бъде разширено, така че да обхване и съфинансиране на дейности за повишаване на осведомеността, осъществявани от социалните партньори и организациите на гражданското общество на европейско и национално равнище.

3.5 Осигуряване на информирано и доброволно съгласие

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

3.5.1 Видовете съгласие, които се изискват, следва да продължат да бъдат обвързани с вида данни, които се обработват, а не с използваната технология. Но ЕИСК изразява загриженост поради факта, че в повечето случаи, когато се дава съгласие в интернет среда, приложението не предоставя никакво потвърждение относно съответното съгласие, нито пък има ефективни механизми за регистриране на оттеглянето на съгласие. Освен това съгласието може да включва натискане на бутон за изразяване на съгласие с многобройни условия, от които съгласието може да бъде само малък елемент. По-логично би било съгласието, свързано с администриране на данни, да представлява отделен опростен документ, който да бъде изпълнен със съдържание, да показва познаване на материята и да отговаря на конкретния случай.

3.5.2 За организациите и предприятията, които извършват своите дейности по интернет, обработката на лична информация е от жизненоважно значение. Опцията по подразбиране очевидно е изгодна за оператора, но ако не се прилага коректно, може да бъде в ущърб на клиента. Използването ѝ следва да бъде точно дефинирано, така че всички оператори да са задължени да предлагат на клиентите си зачитане на неприкосновеността на личния живот по подразбиране, ако клиентите им желаят това.

3.5.3 За да може съгласието да бъде свободно изразено, договърът също трябва да бъде справедлив. Необходимо е да бъдат установени принципи за избягване на неполярни търговски практики.

3.6 Защита на чувствителни данни

Ще бъдат разгледани разширяването на обхвата на определението за „чувствителни данни“, за да бъдат включени, например, генетични данни, както и по-нататъшното хармонизиране на условията за обработка на чувствителни данни.

3.6.1 Настоящото определение за чувствителни данни има нужда от изясняване, тъй като категориите електронни данни за физическите лица продължават да се увеличават. Широко разпространеното и безразборно прилагане на камери за наблюдение тревожи ЕИСК. Важно е да се приложи законът, ограничаващ неправомерното използване на тези изображения. GPRS данните, които са свързани с местонахождението на лицата, представляват друг източник на спорове. Нараства и свалянето на биометрични данни. Определението следва да включва подобни нови технологии и методологии, и следва да дава възможност за отразяване на по-нататъшни развития в областта на технологиите. Вероятно ще е необходимо да се установят принципи, свързани с контекста. ЕИСК се застъпва за коректното използване на тези нови технологии.

3.6.2 Следва също да се осигури повишена защита на чувствителните данни. Криптирането също следва да бъде задължително за определени чувствителни данни. Трябва да бъдат приложени най-добрите възможни технологии. Администраторите следва да носят отговорност за нарушаване на сигурността.

3.7 По-ефективни средства за правна защита и санкции

Ще бъдат разгледани разширяването на правомощията за предявяване на иск пред националните съдилища и евентуалното включване на наказателни санкции при сериозни нарушения.

3.7.1 Предвид възможния конфликт между личния живот на физическите лица и използването на данните, свързани със съответното лице, с търговски цели, и на високия залог, хората трябва да осъзнаят във все по-голяма степен целите, за които се събират техните данни и възможностите, с които разполагат за упражняване на контрол върху вече събраните данни. Затова ЕИСК е убеден, че ефективното прилагане и правната защита представляват задължително условие, за да може настоящият проект да стане действително „всеобхватен“. Освен това трябва да бъде обхванато и трансграничното измерение.

3.7.2 Възможността за предявяване на колективен иск следва да бъде разгледана като мярка в случай на сериозен провал по отношение на защитата. Следва да бъде обмислена възможността професионалните и браншовите организации и синдикатите да представляват физическите лица и да завеждат дела в съдилищата.

4. Укрепване на измерението, свързано с вътрешния пазар

4.1 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. Ще бъдат разгледани начините за постигане на по-нататъшна хармонизация на правилата за защита на данните на равнище ЕС.

4.1.1 ЕИСК изразява загриженост във връзка с факта, че обхватът на решенията, вземани от държавите-членки според разпоредбите на Директива 95/46, създава проблем по отношение на изпълнението. В този контекст регламентът вероятно би гарантирал по-голяма сигурност. Хармонизацията следва да бъде осъществена посредством набор от стандарти, достатъчни за удовлетворяване на изискванията, поставени от директивата.

4.1.2 Никъде в съобщението не се споменават работниците и достъпът до техните лични данни, които са на разположение на работодателите. В мултинационалните фирми, които могат да централизират архива си в рамките на ЕС или дори извън него, работниците имат нужда от ясно разписани правила за достъп, които следва да бъдат въведени с новото законодателство.

4.2 Намаляване на административната тежест за администраторите

Ще бъдат проучени различни възможности за опростяване и хармонизиране на действащата система за уведомяване, в това число евентуалното изготвяне на единен регистрационен формуляр за целия ЕС. Уведомленията биха могли да бъдат публикувани в интернет.

4.2.1 ЕИСК определено би подкрепил тези инициативи.

4.3 Изясняване на правилата относно приложимото право и отговорността на държавите-членки

Когато става въпрос за няколко държави-членки, за администраторите на данни и надзорните органи за защита на данните не винаги е ясно коя държава-членка носи отговорност и кое е приложимото право. Глобализацията и технологичният напредък още повече влошават този проблем. Ще бъдат проучени преразглеждането и уточняването на съществуващите разпоредби по отношение на приложимото право с цел да се увеличи правната сигурност и да се изяснят отговорностите на държавите-членки.

4.3.1 Когато става дума за граждани на ЕС, приложимото право в Европейския съюз следва да бъде правото на държавата-членка на администратора на данни, там където се съхраняват данните. За уязвими лица, особено работници и потребители, в сила трябва да бъде правото на защита на личните данни според обичайното местопребиваване.

4.4 Повишаване на отговорността на администраторите на лични данни

Комисията ще проучи начини, които да гарантират, че администраторите на данни ще приложат ефективни политики и механизми, гарантиращи спазване на правилата за защита на данните. Ще бъдат разгледани въвеждането на задължение за назначаване на независим служител за защита на данните и хармонизирането на правилата, свързани с неговите задължения, както и въвеждането на задължение за оценка на въздействието върху защитата на данните. В допълнение, Комисията ще насърчава по-нататъшното използване на технологии за подобряване на защитата на личния живот (PETs) и прилагане на концепцията за „защита на личния живот още при проектирането“.

4.4.1 PETs и концепцията за „защита на личния живот още при проектирането“ имат потенциала да освободят администраторите на данните от необходимостта от лична преценка, тъй като в противен случай те могат да бъдат изправени пред конфликт заради търговските приоритети на своите организации. ЕИСК настоява Комисията да инициира по-нататъшно проучване и разработване на тези инструменти, тъй като те имат потенциала да подсилят защитата на данните, като елиминират конфликта на интереси. В идеалния случай тези инструменти биха могли да станат задължителни.

4.4.2 С цел избягване на съмненията, администраторите на данните следва да подлежат на отчетност за всички аспекти, свързани с обработката на данни, за която отговарят. В този смисъл, когато са включени подизпълнители и/или предприятия в други държави, задълженията за поверителност на личните данни следва да бъдат ясно определени в съответния договор.

4.4.3 ЕИСК смята, че всяка държава-членка следва да създаде професионален орган, който да отговаря за уменията и сертифицирането на служителите за защита на данните.

4.4.4 Прилагането на разпоредбите по това заглавие следва да бъде в съзвучие с целта за намаляване на административната тежест за администраторите на данни, разгледана в параграф 4.2.

4.5 *Настърчаване на инициативи за саморегулиране и проучване на схемите на ЕС за сертифициране*

Комисията ще проучи начините за по-нататъшно настърчаване на инициативите за саморегулиране, напр. кодекси за поведение, както и за въвеждане на схемите на ЕС за сертифициране.

4.5.1 Вж. 3.7.1. по-горе: прилагането и правната защита са основен повод за тревога за ЕИСК. Това са привлекателни предложения, доколкото могат да допринесат за намаляване на огромната регулаторна тежест, понасяна от бизнеса. Всяка държава-членка следва да финансира сборник или наръчник на най-добрите практики.

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

Инструментът на ЕС за защита на личните данни в областта на полицейското и съдебното сътрудничество по наказателноправни въпроси е Рамково решение 2008/977/ПВР. То има множество недостатъци, които могат да повлияят върху възможността на физическите лица да упражняват своите права за защита на данните в такива области като знание за това какви техни лични данни се обработват и обменят, от кого и с каква цел, и как да упражняват правата си, като например правото на достъп до техните собствени данни.

Ще бъдат обмислени разширяване на обхвата на приложение на общите правила за защита на данните и към областите на полицейското и съдебното сътрудничество по наказателноправни въпроси, въвеждане на нови разпоредби в области като обработката на генетични данни, провеждане на консултация относно преразглеждането на системите за надзор в тази област и оценка на необходимостта в дългосрочен план различните специфични секторни правила да бъдат приведени в съответствие с новата обща правна рамка за защита на данните.

5.1 Въпреки че признава чувствителното естество на междудържавното полицейско сътрудничество, ЕИСК изразява убеждение, че е изключително важно на основните права, в това число и на защитата на личните данни, да се обръща възможно най-голямо внимание във всеки един момент. ЕИСК се опасява, че загрижеността за сигурността, понякога изопачена, често води до незачитане на основни права. Хората следва да бъдат по-добре информирани относно методите и целите, чрез които и в името на които различни органи събират лични данни от телефонни сметки, банкови сметки, проверки по летищата и др.

6. **Глобално измерение на защитата на данните**

6.1 *Разясняване и опростяване на правилата относно международния трансфер на лични данни*

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 критериите и изискванията за оценка на равнището на защита на данните в трети държави или международни организации;

— определяне на основни елементи на ЕС за защита на данните, които да се ползват във всички видове международни споразумения.

6.1.1 ЕИСК подкрепя тези похвални инициативи и изразява надежда, че Комисията ще стъпее да постигне широкото международно съгласие, без което тези предложения няма да имат ефект.

6.2 *Настърчаване на универсални принципи*

Европейският съюз трябва да продължи да бъде движеща сила за разработването и популяризирането на международни правни и технически стандарти за защита на личните данни. За тази цел Комисията ще работи активно в областта на международните стандарти, както и в областта на сътрудничеството с трети държави и международни организации като ОИСР.

6.2.1 ЕИСК отново изразява своята подкрепа. Като се има предвид глобалният характер на интернет, от първостепенно значение е правилата и насоките в различните части на света да бъдат съвместими. Личните данни трябва да имат трансгранична защита. Следва да се отбележат насоките на ОИСР, а също и Конвенция № 108 на Съвета на Европа. Конвенцията е в процес на преразглеждане. Комисията следва да осигури съвместимост между Конвенцията и новата директива.

7. **По-засилена институционална организация за по-добро прилагане на правилата за защита на личните данни**

Комисията ще разгледа начини за:

— засилване, изясняване и хармонизиране на статута и правомощията на националните органи за защита на данните;

— 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. Мерките биха могли да включват:

— укрепване на ролята на националните надзорни органи за защита на данните;

— по-добра координация на тяхната работа посредством Работната група по член 29;

— създаване на механизъм, който да гарантира последователността под ръководството на Европейската комисия.

7.1 С оглед на тревогата на ЕИСК относно прилагането и правната защита, Комитетът счита тези предложения за ключови. Ние подкрепяме изразите „укрепване, изясняване и хармонизиране“ и „сътрудничество и координация“, както и принципния стремеж на Комисията да гарантира по-последователно прилагане на правилата на ЕС за защита на данните във всички държави-членки. ЕИСК изразява тревога, че всичките 12 нови държави-членки вероятно все още не са постигнали цялостно и ефективно прилагане на Директива 95/46.

7.2 ЕИСК е на мнение, че националните органи за защита на личните данни са в общия случай безсилни и претоварени и

независимостта им следва да бъде подсилена. Всяка нова директива следва да изисква от националните органи да разполагат със статута, правомощията и ресурсите, необходими за изпълнение на ролята им. Задачите и ресурсите им следва да се определят в общоевропейски план. Следва да се обмисли създаването на Европейски надзорен орган за защита на данните.

7.3 Въз основа на досегашния ѝ принос в областта на защитата на физическите лица по отношение на обработката на лични данни, ЕИСК е убеден, че Работната група по член 29 може да продължи да изпълнява ценна роля.

Брюксел, 16 юни 2011 г.

Председател
на Европейския икономически и социален комитет
Staffan NILSSON

ПРИЛОЖЕНИЕ

към становището на Европейския икономически и социален комитет

Следните текстове от становището на специализираната секция бяха отхвърлени в полза на приетите от Пленарната асамблея предложения за изменение, въпреки че бяха подкрепени от най-малко от една четвърт от подадените гласове:

Параграф 1.6

Когато става дума за граждани и работници на ЕС, приложимото право в Европейския съюз следва да бъде правото на държавата-членка на администратора на данни там, където се съхраняват данните.

Параграф 4.3.1

Когато става дума за граждани и работници на ЕС, приложимото право в Европейския съюз следва да бъде правото на държавата-членка на администратора на данни, там където се съхраняват данните.

Резултат

86 гласа за изменение на тези параграфи,

72 гласа „против“,

19 гласа „въздържал се“.
