ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 6.11.2015 г.
COM(2015) 566 final

СЪОБЩЕНИЕ НА КОМИСИЯТА ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И СЪВЕТА

относно предаването на лични данни от ЕС на Съединените американски щати съгласно Директива 95/46/ЕО след решението на Съда по дело C-362/14 (Schrems)

СЪОБЩЕНИЕ НА КОМИСИЯТА ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И СЪВЕТА

относно предаването на лични данни от ЕС на Съединените американски щати съгласно Директива 95/46/ЕО след решението на Съда по дело C-362/14 (Schrems)

1. ВЪВЕДЕНИЕ: ОТМЯНАТА НА РЕШЕНИЕТО ОТНОСНО „СФЕРАТА НА НЕПРИКОСНОВЕНОСТ НА ЛИЧНИЯ ЖИВОТ“ (SAFE HARBOUR)

Решението на Съда на Европейския съюз (наричан по-нататък: „Съдът на ЕС“ или „Съдът“) от 6 октомври 2015 г. по дело Schrems, C-362/14[1], потвърждава важното значение на основното право на защита на личните данни, залегнало в Хартата на основните права на ЕС, включително когато тези данни се предават извън ЕС.

Предаването на лични данни е съществен елемент на трансатлантическите отношения. ЕС и САЩ са най-важните търговски партньори един за друг и предаването на данни представлява все по-съществена част от търговския им обмен.

За да улесни движението на тези потоци от данни и същевременно да гарантира висока степен на защита на личните данни, Комисията призна адекватността на рамката относно „сферата на неприкосновеност на личния живот“ чрез приемането на Решение 2000/520/ЕО на Комисията от 20 юли 2000 г. (наричано по-нататък „Решението за „сфера на неприкосновеност на личния живот“). В това решение, прието на основание член 25, параграф 6 от Директива 95/46/ЕО[2], Комисията призна, че принципите за сфера на неприкосновеност на личния живот и придружаващите ги често задавани въпроси, публикувани от Департамента по търговия на САЩ, предоставят адекватна защита за целите на предаването на лични данни от ЕС[3]. В резултат на това беше възможно лични данни да се прехвърлят свободно от държавите — членки на ЕС, на дружествата в САЩ, които са приели въпросните принципи, въпреки липсата на общ закон за защита на данните в САЩ. Функционирането на договорността за „сфера на неприкосновеност на личния живот“ се основаваше на самосертифицирането и поемането на ангажимент за изпълнение от дружествата, присъединили се към тази договорност. Присъединяването към принципите за сфера на неприкосновеност на личния живот и придружаващите ги често задавани въпроси е доброволно, но тези правила стават задължителни съгласно правото на САЩ за

[1] Решение от 6 октомври 2015 г. по дело Maximilian Schrems/Data Protection Commissioner, C-362/14, EU:C:2015:650 (наричано по-нататък също: „решението“ или „решението Schrems“).

[2] Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 г. за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни, ОВ L 281, 23.11.1995 г., стр. 31 (по-нататък: „Директива 95/46/ЕО“ или „Директивата“).

[3] За целите на настоящото съобщение терминът „ЕС“ обхваща и ЕИП. Поради това позоваванията на „държави членки“ се разбират така, че да обхващат и държавите — членки на ЕИП.

дружествата, които са се присъединили към тях и изпълнението им се следи от Федералната търговска комисия на САЩ[4].

В своето решение от 6 октомври 2015 г. Съдът обяви Решението за „сфера на неприкосновеност на личния живот“ за невалидно. В този контекст настоящото съобщение има за цел да направи общ преглед на алтернативните инструменти за трансатлантическо предаване на данни съгласно Директива 95/46/ЕО в отсъствието на решение относно адекватността. В него накратко се описват и последствията от съдебното решение върху други решения на Комисията относно адекватността. В решението си Съдът пояснява, че за да се приеме решение относно адекватността съгласно член 25, параграф 6 от Директива 95/46/ЕО, Комисията трябва да констатира, че в съответната трета страна съществува степен на защита на личните данни, която, макар и да не е непременно идентична, „по същество е равностойна“ на гарантираната в ЕС по силата на Директивата, разглеждана във връзка с Хартата на основните права. Що се отнася конкретно до Решението за „сфера на неприкосновеност на личния живот“, Съдът е приел, че в него не се съдържат достатъчно констатации на Комисията относно ограниченията върху достъпа на публичните органи на САЩ до данни, предавани съгласно това решение, и относно наличието на ефективна правна защита срещу подобна намеса в личния живот. По-специално Съдът е пояснил, че законодателство, което дава възможност на публични органи да имат всеобхватен достъп до съдържанието на електронните съобщения, трябва да се разглежда като възпрепятстващо същността на основното право на зачитане на личния живот. Освен това Съдът е потвърдил, че дори при наличие на решение относно адекватността по член 25, параграф 6 от Директива 95/46/ЕО, органите за защита на данните (ОЗД) на държавите членки продължават да имат правото и задължението да проучат, напълно независимо, дали предаването на данни на трета държава се извършва в съответствие с изискванията, определени от Директива 95/46/ЕО, разглеждана в светлината на членове 7, 8 и 47 от Хартата на основните права. При все това Съдът е постановил също така, че само той може да обяви акт на Съюза, като например решение за адекватност на Комисията, за невалиден.

Решението на Съда се основава на Съобщението на Комисията от 2013 г. относно функционирането на „сферата на неприкосновеност на личния живот“ („Safe Harbour“) от гледна точка на гражданите на ЕС и дружествата, установени в ЕС[5], в което Комисията посочи редица недостатъци и направи 13 препоръки. Въз основа на тези

---

[4] За по-задълбочен преглед на договорността за „сфера на неприкосновеност на личния живот“, вж. Съобщение на Комисията до Европейския парламент и Съвета относно функционирането на „сферата на неприкосновеност на личния живот“ („Safe Harbour“) от гледна точка на гражданите на ЕС и дружествата, установени в ЕС, COM(2013) 847 final.

[5] Съобщение на Комисията до Европейския парламент и Съвета относно функционирането на „сферата на неприкосновеност на личния живот“ („Safe Harbour“) от гледна точка на гражданите на ЕС и дружествата, установени в ЕС, COM(2013) 847 final, 27 ноември 2013 г. Вж. също Съобщение на Комисията до Европейския парламент и Съвета „Възстановяване на доверието в обмена на данни между ЕС и САЩ“, COM(2013) 846 final, 27 ноември 2013 г., и свързания с него Меморандум „Възстановяване на доверието в обмена на данни между ЕС и САЩ — често задавани въпроси“, MEMO/13/1059, 27 ноември 2013 г.

препоръки от януари 2014 г. насам Комисията води разговори с органите на САЩ с цел да се постигне обновена и по-стабилна договореност за трансатлантически обмен на данни.

След решението на Съда Комисията продължи да преследва целта си за въвеждане на обновена и сигурна рамка за трансатлантическото предаване на лични данни. В тази връзка Комисията незабавно поднови и ускори темпа на разговори с правителството на САЩ, за да гарантира, че всяко ново споразумение за трансатлантическо предаване на лични данни е изцяло в съответствие със стандартите, установени от Съда. От това следва, че в тази рамка трябва да са включени достатъчно ограничения, гаранции и механизми за съдебен контрол, които да гарантират непрекъснатата защита на личните данни на гражданите на ЕС, включително що се отнася до евентуалния достъп до тях на публичните органи за целите на правоприлагането и националната сигурност. Междувременно от страна на представители на промишлеността бяха изразени притеснения по отношение на възможностите за продължаване на предаването на данни[6]. Поради това е необходимо да се уточнят условията, при които предаването може да продължи. Това накара Работната група по член 29 — независим консултативен орган, обединяващ представители на всички ОЗД на държавите членки и Европейския надзорен орган по защита на данните — да направи на 16 октомври изявление[7] относно първите изводи, които могат да бъдат извлечени от съдебното решение. Наред с другото, в изявлението се съдържат следните насоки относно предаването на данни:

- предаването на данни не може повече да се основава на обявеното за невалидно Решение за „сфера на неприкосновеност на личния живот“ на Комисията;

- стандартните договорни клаузи (наричани по-нататък също „СДК“) и задължителните фирмени правила (наричани по-нататък също „ЗФП“) могат междувременно да се използват като основа за предаването на данни, въпреки че Работната група по член 29 заяви още, че ще продължи да проучва последиците от решението върху тези алтернативни инструменти.

В изявлението освен това държавите членки и институциите на ЕС са призовани да започнат разговори с американските органи за намирането на правни и технически решения за предаването на данни. Преговорите за нова договореност за „сфера на

---

[6] Представители на промишлени асоциации изразиха тези опасения, *inter alia*, на среща, организирана скоро след издаването на решението Schrems от заместник-председателя Ансип и комисарите Йоурова и Йотингер на 14 октомври. Вж. Новините (Daily News) от 14.10.2015 г. (MEX/15/5840). Вж. също: „Open letter on the implementation of the CJEU Judgement on Case C-362/14 Maximillian Schrems v Data Protection Commissioner“ от 13 октомври 2015 г., адресирано до председателя на Комисията Жан-Клод Юнкер, и подписано от различни европейски и американски промишлени асоциации и дружества: http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=1045&PortalId=0&TabId=353

[7] Изявление на Работната група по член 29, достъпно на следния интернет адрес: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf

неприкосновеност на личния живот“ могат, според Работната група по член 29, да бъдат част от това решение.

Работната група по член 29 обяви, че ако до края на януари 2016 г. не бъде намерено подходящо решение с органите на САЩ, и в зависимост от оценката на алтернативните инструменти за предаване на данни, органите за защита на данните на държавите членки ще предприемат всички необходими и подходящи действия, включително координирани действия в областта на правоприлагането.

На последно място, Работната група по член 29 подчерта, че националните органи за защита на данните, институциите на ЕС, държавите членки и бизнесът носят споделена отговорност за намирането на устойчиви решения в изпълнение на решението на Съда. По-специално Работната група призова бизнеса да обмисли въвеждането на правни и технически решения за намаляване на възможните рискове, пред които дружествата са изправени при предаването на данни.

Настоящото съобщение не засяга правомощията и задълженията на националните органи за защита на данните да проверяват законосъобразността на предаването на данни в условията на пълна независимост[8]. В него не се установяват задължителни правила и се зачитат изцяло правомощията на националните съдилища да тълкуват приложимото право и, когато е необходимо, да отправят преюдициално запитване до Съда на Европейския съюз. Настоящото съобщение също така не може да представлява основание за предявяване на каквото и да било индивидуално или колективно право или правна претенция.

2. АЛТЕРНАТИВНИ ОСНОВАНИЯ ЗА ПРЕДАВАНЕ НА ЛИЧНИ ДАННИ КЪМ САЩ

Правилата за международното предаване на данни, определени в Директива 95/46/ЕО, се основават на ясно разграничение между, от една страна, предаването към трети държави, които предоставят достатъчна степен на защита (член 25 от Директивата), и от друга страна, предаване към трети държави, които не предоставят достатъчна степен на защита (член 26 от Директивата).

Решението Schrems разглежда условията, при които, съобразно член 25, параграф 6 от Директива 95/46/ЕО, Комисията може да определи дали трета държава осигурява достатъчна степен на защита.

Когато се установи, че третата държава, към която трябва да се предадат лични данни от ЕС, не предоставя достатъчна степен на защита, член 26 от Директива 95/46/ЕО предвижда редица алтернативни основания, по които предаването може въпреки всичко се осъществи. Предаване може да се осъществи по-специално, когато субектът,

[8] Вж. член 8, параграф 3 от Хартата на основните права и член 16, параграф 2 от ДФЕС. Тази независимост е подчертана и от Съда в Решението Schrems.

отговарящ за определянето на целите и средствата на обработка на лични данни („администраторът“):

– представя достатъчни гаранции по смисъла на член 26, параграф 2 от Директива 95/46/ЕО, по отношение на защитата на личния живот и основните права и свободи на лицата и по отношение на упражняването на тези права. Тези гаранции може по-специално да бъдат предоставени посредством договорни клаузи, обвързващи износителя и вносителя на данни (вж. раздели 2.1 и 2.2 по-долу). Това могат да бъдат и стандартни договорни клаузи, изготвени от Комисията, или — по отношение на предаване на данни между различните субекти в рамките на мултинационална корпоративна група — задължителните фирмени правила, одобрени от органите за защита на данните; или

– ползва като основание една от дерогациите, изрично изброени в член 26, параграф 1, букви а) — е) от Директива 95/46/ЕО (вж. раздел 2.3 по-долу).

В сравнение с решенията относно адекватността, изготвяни в резултат от цялостната оценка на системата на дадена трета държава, и които може по принцип да се отнасят за всяко предаване на данни към тази система, тези алтернативни основания за предаване са едновременно с по-ограничен обхват (тъй като се прилагат само за определени потоци от данни) и с по-широк обсег (тъй като не са непременно ограничени до конкретна държава). Те се прилагат за пренос на данни, извършван от определени субекти, които са решили да използват една от възможностите, предоставени от член 26 на Директива 95/46/ЕО. Освен това, когато извършват предаването на данни на такова основание, и тъй като не могат да се позоват на констатация за достатъчна степен на защита в третата държава, съдържаща се в решение за адекватност на Комисията, износителите и вносителите на данни носят отговорността да гарантират, че предаването отговаря на изискванията на Директивата.

2.1. Договорни решения

Както бе подчертано от Работната група по член 29, за да предоставят достатъчни гаранции по смисъла на член 26, параграф 2 от Директива 95/46/ЕО, договорните клаузи „трябва успешно да компенсират липсата на общо равнище на достатъчна защита чрез включването на съществените елементи на защита, които липсват в конкретната ситуация“[9]. За да улесни използването на такива инструменти при международното предаване на данни, Комисията одобри в съответствие с член 26, параграф 4 от Директивата четири набора от стандартни договорни клаузи, за които се счита, че изпълняват изискванията на член 26, параграф 2 от Директивата. Два набора от стандартни клаузи се отнасят до предаването на данни между администратори[10], а

[9] Вж. Работна група по член 29, „Предаване на лични данни към трети държави: прилагане на членове 25 и 26 от Директивата на ЕС за защита на данните“, (WP 12), 24 юли 1998 г., стр. 16.

[10] 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, и Решение 2004/915/ЕО на Комисията от 27 декември 2004 г. за изменение на Решение

другите два касаят предаването между администратора и обработващия лични данни, действащ по негови указания[11]. Във всеки от тези набори от стандартни клаузи се определят съответните задължения на износителите и вносителите на данни. Те включват задължения, свързани наред с другото с мерките за сигурност, информацията за субекта на данните в случай на предаване на чувствителни данни, уведомяването на износителя на данни за искания за достъп от страна на правоприлагащите органи на трети държави или за всеки случай на неволен или неразрешен достъп, и правата на субектите на данни във връзка с достъпа, поправката и заличаването на техните лични данни, както и правилата за обезщетяване на субекта на данни, в случай на претърпени вреди, произтичащи от нарушение, извършено от някоя от страните по договорните клаузи. Стандартните клаузи съдържат също така изискване субектите на данни от ЕС да имат възможност да се позоват пред орган за защита на личните данни и/или съд на държавата членка, в която е установен износителят на данни, на своите права, произтичащи от договорните клаузи, в качеството си на трета страна бенефициер[12]. Тези права и задължения са необходими в договорните клаузи, тъй като за разлика от ситуацията, при която Комисията е направила констатация за адекватност, не може да се предполага, че вносителят на данни в третата държава е обхванат от адекватна система за надзор и прилагане на правилата за защита на данните.

Тъй като решенията на Комисията са задължителни в своята цялост в държавите членки, включването на стандартните договорни клаузи в договор води до това, че националните органи, по принцип, са задължени да ги приемат. Следователно органите не могат да откажат предаването на данни към трета държава единствено на основание, че тези стандартни договорни клаузи не предоставят достатъчни гаранции. Това обаче не засяга правомощията им да направят проверка на тези клаузи с оглед на изискванията, изложени от Съда в решението Schrems. В случай на съмнения, органите следва да внесат иск пред национален съд, който на свой ред може да отправи преюдициално запитване до Съда на Европейския съюз. Въпреки че в законодателството на повечето държави членки, транспониращо Директива 95/46/ЕО, не съществува изискване за предварително национално разрешение за осъществяването на предаването на данни, някои държави членки поддържат система за нотифициране и/или предварително разрешение за използването на стандартните договорни клаузи. В тези случаи националните ОЗД трябва да сравнят клаузите, които действително се съдържат в разглеждания договор, със стандартните договорни клаузи и да потвърдят,

---

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.

[11] 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, и Решение 2010/87/ЕС 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. Първото решение, което бе отменено с второто, се прилага само за договори, сключени преди 15 май 2010 г.

[12] Вж. например съображение 6 от Решение 2004/915/ЕО на Комисията и клауза V от приложението към него; клауза 7 от приложението към Решение 2010/87/ЕС на Комисията.

че не е извършена промяна[13]. Ако клаузите са били използвани без изменение[14], по принцип разрешението[15] се предоставя автоматично[16]. Както се пояснява по-долу (вж. раздел 2.4), това не засяга допълнителните мерки, които износителят на данни може да се наложи да предприеме, по-специално вследствие на предоставена от вносителя на данни информация относно промени в правната система на третата държава, които могат да попречат на вносителя на данни да изпълнява задълженията си по договора. При изпълнението на стандартните договорни клаузи износителите на данни, а чрез приемането на клаузите на договора — и вносителите на данни, попадат под контрола на органите за защита на данните.

Приемането на СДК не възпрепятства дружествата да разчитат и на други инструменти, като например договорни споразумения *ad hoc*, за да докажат, че предаването на данни се извършва с достатъчни гаранции по смисъла на член 26, параграф 2 от Директива 95/46/ЕО. Съгласно член 26, параграф 2 от Директивата, тези разпоредби трябва да бъдат одобрявани за всеки отделен случай от националните органи. Някои органи за защита на данните са разработили насоки в тази област, включително под формата на стандартизирани договори или подробни правила, които следва да се спазват при изготвянето на клаузите за предаване на данни. Повечето договори обаче, които понастоящем се използват от дружествата, за да извършват международно предаване на данни, се основават на одобрените от Комисията СДК[17].

2.2. Предаване на данни в рамките на една група

За предаването на лични данни от ЕС на свързани предприятия, разположени извън ЕС, в съответствие с изискванията по член 26, параграф 2 от Директива 95/46/ЕО, многонационалните дружества могат да приемат задължителни фирмени правила

---

[13] Следва да се отбележи, че предложението за Общ регламент относно защитата на данните (COM(2012) 11 final) предвижда, че за предаването на данни въз основа на СДК или ЗФП, доколкото те са били приети от Комисията или в съответствие с предвидения механизъм за съгласуваност, не се изисква допълнително разрешение.

[14] Използването на СДК обаче не възпрепятства страните да се споразумеят да добавят други клаузи, доколкото същите не противоречат пряко или косвено на клаузи, одобрени от Комисията, нито засягат основните права или свободи на субектите на данни. Вж. Европейска комисия, „Често задавани въпроси във връзка с предаването на лични данни от ЕС/ЕИП към трети държави“ (ЧЗВ Б.1.9), стр. 28 (достъпни на адрес: http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf).

[15] Ако орган за защита на данните има съмнения относно съвместимостта на СДК с изискванията на Директивата, той следва да отнесе въпроса до национален съд, който може след това да отправи преюдициално запитване към Съда на Европейския съюз (вж. точки 51, 52, 64 и 65 от решението Schrems).

[16] Работната група по член 29 е въвела специална процедура на сътрудничество между ОЗД за одобряване на договорни клаузи, които дадено дружество възнамерява да използва в различни държави членки. Вж. Работна група по член 29, *Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on 'Contractual clauses' Considered as compliant with the EC Model Clause* (Работен документ за създаване на процедура за сътрудничество за изготвяне на общи становища относно „договорни клаузи“, считани за съответстващи на стандартните договорни клаузи на ЕО) (WP 226), 26 ноември 2014 г. Вж. също клауза VII от приложението към Решение 2004/915/ЕО на Комисията и клауза 10 от приложението към Решение 2010/87/ЕС на Комисията.

[17] Вж. Работна група по член 29, *Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on 'Contractual clauses' Considered as compliant with the EC Model Clause* (WP 226), 26 ноември 2014 г., стр. 2.

(ЗФП). Този вид установена практика предоставя основание за предаване на данни само в рамките на дадена корпоративна група.

Използването на ЗФП позволява следователно личните данни да се движат свободно между различните субекти, които са част от дадена корпоративна група на световно равнище — без да е необходимо да има договорни отношения между отделните корпоративни субекти, — като същевременно се гарантира същата висока степен на защита на личните данни в рамките на цялата корпоративна група посредством единен набор от задължителни и подлежащи на принудително изпълнение правила. Наличието на единен набор от правила създава по-опростена и по-ефикасна система, която е по-лесна за прилагане от персонала и по-лесна за разбиране от субектите на данни. С цел да подпомогне дружествата при изготвянето на ЗФП Работната група по член 29 формулира материалните (напр. ограничаване в рамките на целта, сигурност на обработката, прозрачна информация за субектите на данни, ограничения за последващо предаване извън групата, индивидуални права на достъп, коригиране и възражение) и процесуалните (напр. одити, наблюдаване на съответствието, разглеждането на жалбите, сътрудничество с ОЗД, отговорност и юрисдикция) изисквания за ЗФП, въз основа на стандартите на ЕС за защита на данните[18]. Тези правила са не само задължителни за членовете на корпоративната група, но подобно на СДК тяхното изпълнение в ЕС е правно обезпечено: лица, чиито данни се обработват от субект в корпоративна група, имат право като трета страна бенефициер да изискат спазването на ЗФП, като подадат жалба пред ОЗД или иск пред съд на държава членка. Освен това в ЗФП трябва да се определи кой е субектът в рамките на ЕС, който поема отговорност за нарушения на правилата, допуснати от член на корпоративната група, обвързана от тези правила, намиращ се извън ЕС.

Съгласно законите на повечето държави членки за транспониране на директивата предаването на данни въз основа на ЗФП трябва да бъде разрешено от органа за защита на личните данни във всяка държава членка, от която мултинационалното дружество възнамерява да предава данни. За улесняване и ускоряване на процеса, както и за намаляване на административната тежест за заявителите, Работната група по член 29 е въвела стандартизиран формуляр[19] и специална процедура за сътрудничество между

[18] Вж. Работна група по член 29, *Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules* (Работен документ за съставянето на таблица с елементите и принципите, които трябва да бъдат заложени в задължителните фирмени правила) (WP 153), 24 юни 2008 г.; *Working Document setting up a framework for the structure of Binding Corporate Rules* (Работен документ за създаването на рамка за структурата на задължителните фирмени правила) (WP 154), 24 юни 2008 г.; и *Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules* (Работен документ относно често задаваните въпроси (ЧЗВ), свързани със задължителните фирмени правила) (WP155), 24 юни 2008 г.

[19] Работна група по член 29, *Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data* (Стандартно заявление за одобряване на задължителни фирмени правила за прехвърляне на лични данни) (WP133), 10 януари 2007 г.

съответните ОЗД[20], предвиждаща определянето на един „водещ орган“, който да отговаря за процедурата по одобрение.

2.3. Дерогации

Когато няма решение относно адекватността по член 25, параграф 6 от Директива 95/46/ЕО и независимо от това дали се прилагат СДК и/или ЗФП, личните данни могат все пак да бъдат предадени на субекти, установени в трета държава, доколкото се прилага някоя от предложените дерогации, посочени в член 26, параграф 1 от Директива 95/46/ЕО[21] :

- субектът на данните недвусмислено е дал своето съгласие за предлаганото предаване на данни;

- предаването е необходимо за изпълнението на договор между съответното физическо лице и администратора или за изпълнението на мерки по предварителен договор, предприети по искане на съответното физическо лице;

- предаването е необходимо за сключването или изпълнението на договор, сключен в интерес на съответното физическо лице между администратора и трета страна;

- предаването е необходимо или изисквано от закона по съображения от важен обществен интерес[22] или за установяването, упражняването или защитата на правото на иск;

- предаването е необходимо за защита на жизнените интереси на съответното физическо лице;

---

[20] Работна група по член 29, *Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From 'Binding Corporate Rules* (Работен документ за определяне на процедура за сътрудничество за изготвяне на общи становища относно достатъчните гаранции в резултат от „задължителните фирмени правила), (WP 107), 14 април 2005 г.

[21] Както е подчертала Работната група по член 29, доколкото други разпоредби от Директива 95/46/ЕО съдържат допълнителни изисквания във връзка с използването на тези дерогации (например ограниченията по член 8 за обработката на чувствителни данни), тези изисквания трябва да бъдат спазени. Вж. Работна група по член 29, *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995* (Работен документ относно общо тълкуване на член 26, параграф 1 от Директива 95/46/ЕО от 24 октомври 1995 г.) (WP 114), 25 ноември 2005 г., стр. 8. Вж. също Европейска комисия, *Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries* (FAQ D.2) (Често задавани въпроси във връзка с предаването на лични данни от ЕС/ЕИП към трети държави, стр. 50.

[22] Това може да включва, например, предаване на данни между данъчни или митнически власти или между служби, компетентни в областта на общественото осигуряване (вж. съображение 58 от Директива 95/46/ЕО). Предаването между надзорните органи в сектора на финансовите услуги също може да е предмет на дерогация. Вж. Работна група по член 29, „Работен документ: предаване на лични данни към трети държави: прилагане на членове 25 и 26 от Директивата на ЕС за защита на данните“, (WP 12), 24 юли 1998 г., стр. 25.

– предаването се извършва от регистър, който съгласно законови или подзаконови разпоредби, е предназначен да предоставя информация на обществеността и е достъпен за справка от обществеността по принцип или от всяко лице, което може да докаже, че има законен интерес за това, доколкото условията за справка, посочени в закона, са изпълнени в конкретния случай.

Тези основания предоставят дерогация от общата забрана за предаване на лични данни към субекти, установени в трета държава, където не съществува достатъчна степен на защита. В действителност, износителят на данни не трябва да гарантира, че вносителят на данни ще предостави достатъчна степен на защита и обикновено не е необходимо да получи предварително разрешение за предаването на данните от компетентните национални органи. При все това Работната група по член 29 счита, че поради извънредния им характер, тези дерогации трябва да се тълкуват стриктно[23].

Работната група по член 29 е публикувала няколко незадължителни документи с насоки относно прилагането на член 26, параграф 1 от Директива 95/46/ЕО[24]. Те включват редица правила за „най-добри практики“, които са предназначени да насочат действията по правоприлагане на националните органи по защита на данните[25]. По-специално, Работната група препоръчва предаването на лични данни, което може да се квалифицира като многократно, масово или структурно, да се извършва при осигуряване на достатъчно гаранции и, когато е възможно, в рамките на специфична правна рамка, като СДК или ЗФП[26].

В настоящото съобщение Комисията разглежда само тези дерогации, които са от особено значение за предаването на данни в търговски контекст след обявяването на Решението за „сфера на неприкосновеност на личния живот“ за невалидно.

2.3.1. Предаване, необходимо за изпълнението на договор или мерки по предварителен договор, предприети по искане на субекта на данните (член 26, параграф 1, буква б)

Тази дерогация може да се приложи например в контекста на хотелска резервация, или когато информация за плащане се предава на трета страна за извършването на банков превод. Въпреки това във всеки от тези случаи Работната група по член 29 счита, че

---

[23] Работна група по член 29, *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995* (WP 114), 25 ноември 2005 г., стр. 17.

[24] Работна група по член 29, *Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive* (WP 12), 24 юли 1998 г.; *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995* (WP 114), 25 ноември 2005 г. Вж. също Европейска комисия, *Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries" (FAQ D.1 до D.9)*, стр. 48-54.

[25] Работна група по член 29, *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995* (WP 114), 25 ноември 2005 г., стр. 8-10.

[26] Работна група по член 29, *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995* (WP 114), 25 ноември 2005 г., стр. 9. Според Работната група масовото или многократното предаване може да се извършва само въз основа на дерогация, ако прибягването до СДК или ЗФП е невъзможно на практика и когато рисковете за субектите на данни са малки (напр. международни парични преводи). Вж. също Европейска комисия, *Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries (FAQ D.1)*, стр. 49.

трябва да е налице „тясна и съществена връзка“ и „пряка и обективна връзка“ между субекта на данните и целите на договорната или преддоговорната мярка (тест за необходимост)[27]. Освен това дерогацията не може да се прилага за предаване на допълнителна информация, която не е необходима за целите на предаването, или предаване на данни с цел, различна от изпълнението на договора (например последващи маркетингови действия)[28]. По отношение на преддоговорните мерки Работната група по член 29 смята, че са обхванати само контакти по инициатива на субекта на данните (например, искане за информация относно дадена услуга), но не и контакти в резултат от маркетингови операции на администратора на данни[29].

2.3.2. Предаване, необходимо за сключването или изпълнението на договор, сключен в интерес на субекта на данни, между администратора на данните и трета страна (член 26, параграф 1, буква в)

Тази дерогация може да се прилага например, когато субектът на данни получава международен банков превод или когато туристически агент препраща данните за полетна резервация на въздушния превозвач. В този случай също се прилага тест за необходимост, при който се изисква тясна и съществена връзка между интереса на субекта на данните и целите, преследвани с договора.

2.3.3. Предаване, необходимо или изисквано от закона за установяването или упражняването на право на иск или защитата срещу предявен иск (член 26, параграф 1, буква г)

Тази дерогация може да се прилага например, когато дадено дружество трябва да предаде данни, за да се защити срещу съдебен иск, или да предяви такъв иск в съд или пред публичен орган. Както и в предходните два случая, настоящата дерогация трябва да бъде подложена на теста за необходимост[30]: трябва да има тясна връзка със съдебния спор или производството (включително и административно).

Според Работната група по член 29, дерогацията може да се прилага само ако всички международни правила за сътрудничеството по граждански или наказателни

---

[27] Работна група по член 29, *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995* (WP 114), 25 ноември 2005 г., стр. 13. Вж. също *Opinion 6/2002 on transmission of passenger manifest information and other data from airlines to the United States* (Становище 6/2002 относно предаването на информация от списъка на пътниците и други данни от авиокомпаниите на органите на САЩ) (WP 66), 24 октомври 2002 г.

[28] Работна група по член 29, *Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive* (WP 12), 24 юли 1998 г., стр. 24; *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995* (WP 114), 25 ноември 2005 г., стр. 13.

[29] Работна група по член 29, *Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive*, (WP № 12), 24 юли 1998 г., стр. 24.

[30] Работна група по член 29, *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995* (WP 114), 25 ноември 2005 г., стр. 15. Например, в контекста на трудови правоотношения дерогацията не може да се използва за предаване на всички досиета на служителите на дружеството майка на групата, установено в трета държава, с мотива за възможно бъдещо съдебно производство.

производства, уреждащи този тип предаване, са били спазени, по-специално тъй като те произтичат от разпоредбите на Хагската конвенция от 18 март 1970 г. („Конвенцията за събиране на доказателства“)[31].

2.3.4. Недвусмислено предварително съгласие от субекта на данните за предлаганото предаване на данни (член 26, параграф 1, буква а)

Въпреки че съгласието може да бъде използвано като основание за предаване на данни, следва да бъдат взети под внимание редица съображения. Тъй като съгласието трябва да се даде за „предложеното“ предаване, се изисква получаването на предварително съгласие за конкретното предаване (или за определена категория предаване). Когато искането е направено онлайн, Работната група по член 29 препоръчва използването на полета, в които да се постави отметка (а не предварително отбелязани с отметка полета)[32]. Тъй като съгласието трябва да бъде недвусмислено, всяко съмнение дали то действително е било предоставено ще направи дерогацията неприложима. Това вероятно ще означава, че в много ситуации, в които съгласието в най-добрия случай се предполага (например защото дадено лице е било информирано за предаване и не е възразило), дерогацията не би могла да се прилага. Обратно, дерогацията може да се използва в случаите, когато предаващият субект е в пряка връзка със субекта на данните и необходимата информация може лесно да се предостави и да се получи недвусмислено съгласие[33].

Наред с това съгласно член 2, буква з) от Директива 95/46/ЕО, съгласието трябва да бъде свободно изразено, конкретно и информирано. Според Работната група по член 29 първото изискване означава, че всеки „натиск“ може да доведе до изключване на съгласието. Това е особено приложимо в контекста на трудовите правоотношения, където подчинеността и присъщата зависимост на служителите обикновено биха поставили под въпрос надеждността на предоставено съгласие[34]. В по-общ план,

---

[31] Хагска конвенция за събиране на доказателства в чужбина по граждански и търговски дела, *открита за подписване* на 18 март 1970 г., 23 U.S.T. 2555, 847 U.N.T.S. 241. Тази конвенция обхваща, например, досъдебните процедури за представяне на доказателства („pre-trial discovery“) или исканията от страна на съдебен орган на една държава до компетентния орган на друга държава за събиране на доказателства, предназначени за използване в съдебно производство на молещата държава.

[32] Работна група по член 29, *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995* (WP 114), 25 ноември 2005 г., стр. 10, във връзка със „Становище 5/2004 относно съобщенията от нежелан директен маркетинг по член 13 от Директива 2002/58/ЕО“ (*Opinion 5/2004 on unsolicited direct marketing communications under Article 13 of Directive 2002/58/EC*) (WP 90), 27 февруари 2004 г., точка 3.2.

[33] Работна група по член 29, *Working Document: Transfers of personal data to third countries:* Applying Articles 25 and 26 of the EU data protection directive, (WP12), 24 юли 1998 г., стр. 24.

[34] Работна група по член 29, *Opinion 8/2001 on the processing of personal data in the employment context* (Становище 8/2001 относно обработването на лични данни в областта на трудовите взаимоотношения) (WP 48), 13 септември 2001 г., стр. 3, 23 и 26. Според Работната група, използването на получено съгласие следва да се ограничи до случаите, в които служителят е имал реален свободен избор и впоследствие може да оттегли съгласието си, без това да доведе до негативни последици за него. Вж. също Работна група по член 29, *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995* (WP 114), 25 ноември 2005 г., стр. 11.

съгласието на субект на данни, който не е имал възможност да направи реален избор или е бил поставен пред свършен факт, не може да се счита за валидно[35].

От съществено значение е субектите на данни да бъдат добре информирани предварително, че данните могат да се предават извън ЕС, до коя трета държава и при какви условия (целта на предаването, кой е получателят(ите) и подробности за него(тях) и др.). От тази информация трябва да става ясен конкретният риск, че данните може да бъдат предадени на трета държава, която не предоставя достатъчна защита[36]. Освен това, както бе посочено от Работната група по член 29, оттеглянето на съгласието на субекта на данни, макар и да не е с ретроактивно действие, следва по принцип да спре всяко по-нататъшно обработване на личните данни[37]. С оглед на тези ограничения, Работната група по член 29 счита, че е малко вероятно даването на съгласие да предостави подходяща дългосрочна рамка за администраторите на лични данни в случаите на структурно предаване на данни[38].

2.4. Обобщение на алтернативните основания за предаване на лични данни

От гореизложеното следва, че дружествата могат да използват редица различни алтернативни инструменти за осъществяването на международно предаване на данни към трети държави, за които се счита, че не предоставят достатъчна степен на защита по смисъла на член 25, параграф 2 от Директива 95/46/ЕО. Вследствие на решението Schrems Работната група по член 29 поясни по-специално, че СДК и ЗФП могат да се използват за предаване на данни на САЩ, докато тя извършва оценката си и без да се засягат правомощията на ОЗД да разследват отделни случаи[39]. От своя страна, представителите на промишлеността реагираха по различни начини на решението, включително и чрез основаване на извършваното от тях предаване на данни на тези алтернативни инструменти[40].

---

35 Работна група по член 29, *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995* (WP 114), 25 ноември 2005 г., стр. 11. Вж. също *Opinion 6/2002 on transmission of passenger manifest information and other data from airlines to the United States* (Становище 6/2002 относно предаването на информация от списъка на пътниците и други данни от авиокомпаниите на органите на САЩ) (WP 66), 24 октомври 2002 г.

36 Работна група по член 29, „*Working Document: Transfers of personal data to third countries:* Applying Articles 25 and 26 of the EU data protection directive, (WP 12), 24 юли 1998 г., стр. 24.

37 Работна група по член 29, *Opinion 15/2011 on the definition of consent* (Становище 15/2011 относно определението за съгласие) (WP 187), 13 юли 2011 г., стр. 9.

38 Работна група по член 29, *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995* (WP 114), 25 ноември 2005 г., стр. 11.

39 Вж. изявление на Работната група по член 29 от 16 октомври 2015 г. (бележка под линия № 8 по-горе).

40 Редица мултинационални дружества са заявили, че основават своите предавания на данни към САЩ на алтернативни инструменти. Вж. например изявленията на Microsoft (http://blogs.microsoft.com/on-the-issues/2015/10/06/a-message-to-our-customers-about-eu-us-safe-harbor/) или Salesforce (http://www.salesforce.com/company/privacy/data-processing-addendum-faq.jsp). Други американски дружества, като Oracle, са заявили, че предлагат на потребителите на услуги „в облак“ възможността да съхраняват своите данни в Европа, така че да не се изпращат за съхранение на друго място: http://www.irishtimes.com/business/technology/oracle-keeps-european-data-within-its-eu-based-data-centres-1.2408505?mode=print&ot=example.AjaxPageLayout.ot

Въпреки това трябва да се обърне внимание на две важни условия. На първо място следва да се припомни, че независимо от правното основание, на което се базира, предаването на данни към трета държава може да е законно само ако данните първоначално са били събрани и обработени от администратор на лични данни, установен в Европейския съюз, в съответствие с приложимото национално законодателство, с което се транспонира Директива 95/46/ЕО. В директивата изрично се посочва, че дейността по обработването, която се извършва преди предаването, както и самото предаване, трябва изцяло да спазват правилата, приети от държавите членки в изпълнение на други разпоредби на директивата[41]. На второ място, при липсата на решение за адекватност на Комисията, администраторите на данни носят отговорност за това, че извършваното от тях предаване на данни се осъществява с достатъчни гаранции за защита в съответствие с член 26, параграф 2 от директивата. Тази оценка трябва да бъде извършена като се вземат предвид всички обстоятелства, свързани с конкретното предаване. В частност, както СДК, така и ЗФП предвиждат, че ако вносителят на данни има причини да смята, че приложимото законодателство в държавата получател може да му попречи да изпълни задълженията си, той своевременно информира износителя на данни в ЕС. В такъв случай износителят на данни е отговорен за предприемането на съответните мерки, необходими, за да се гарантира защитата на личните данни[42]. Те могат да включват технически, организационни и правни мерки или такива, свързани с бизнес модела[43] и да се стигне до възможността за спиране на предаването на данни или за прекратяване на договора. Следователно, след като са взели предвид всички обстоятелства по предаването, износителите на данни може да се наложи да предложат допълнителни гаранции, които да допълнят тези, предвидени в съответното правно основание за предаване, така че да се изпълнят изискванията на член 26, параграф 2 от директивата.

Спазването на тези изисквания в крайна сметка се преценява от органите за защита на данните във всеки отделен случай, в рамките на упражняването на техните надзорни и правоприлагащи функции, включително в контекста на одобряването на договорни споразумения и ЗФП или въз основа на индивидуални жалби. Докато някои ОЗД изразиха съмнения относно възможността за използване на инструменти като СДК и ЗФП за трансатлантическите потоци от данни[44], в изявлението си, направено след

---

41 Виж съображение 60 и член 25, параграф 1 от Директива 95/46/ЕО.

42 Вж. например клауза 5 от приложението към Решение 2010/87/ЕС на Комисията, и работният документ на Работната група по член 29, *Working Document setting up a framework for the structure of Binding Corporate Rules* (Работен документ за установяването на рамка за структурата на задължителните фирмени правила) (WP 154), 24 юни 2008 г., стр. 8.

43 Вж. например насоките, издадени от Европейската агенция за мрежова и информационна сигурност (ENISA): https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf.

44 Вж. напр. становището, издадено на 26.10.2015 г., от Конференцията за защита на данните на германските органи по защита на личните данни на федерално и национално равнище: https://www.datenschutz.hessen.de/ft-europa.htm#entry4521. Като се изтъква, че в решението Schrems се съдържат „строги изисквания по същество“, които както Комисията, така и националните надзорни органи за защита на данните трябва да спазват, в становището се посочва, че германските ОЗД ще преценяват законосъобразността на предаването на данни, извършвано въз основа на алтернативни инструменти (СДК, ЗФП), и повече няма да предоставят нови разрешения за използването на тези средства. Успоредно с това отделни германски ОЗД ясно предупредиха, че алтернативните средства

решението Schrems, Работната група по член 29 обяви, че ще продължи своя анализ на въздействието на решението върху другите инструменти за предаване[45]. Това не засяга правомощията на ОЗД да разследват отделни случаи и да упражняват своите правомощия в защита на отделните лица.

3. ПОСЛЕДИЦИТЕ ОТ РЕШЕНИЕТО SCHREMS ВЪРХУ РЕШЕНИЯТА ОТНОСНО АДЕКВАТНОСТТА

В решението си Съдът не поставя под въпрос правомощията на Комисията съгласно член 25, параграф 6 от Директива 95/46/ЕО да установи, че третата държава осигурява достатъчна степен на защита, щом изискванията, посочени от Съда, са спазени. В съответствие с тези изисквания, предложението от 2012 г. за Общ регламент относно защитата на данните[46], който да замени Директива 95/46/ЕО, допълнително изяснява и подробно описва условията, при които могат да бъдат приемани решения относно адекватността. В решението Schrems Съдът също така е пояснил, че когато Комисията приеме решение относно адекватността, то е обвързващо за всички държави членки и техните органи, включително органите за защита на данните, докато не бъде оттеглено, отменено или обявено за невалидно от Съда, който единствен е компетентен в това отношение. ОЗД продължават да са компетентни да разглеждат жалби по смисъла на член 28, параграф 4 от Директива 95/46/ЕО, относно това дали предаването на данни е в съответствие с изискванията, определени от Директивата (съгласно тълкуването на Съда), но не могат да правят категорични констатации. По-скоро държавите членки трябва да предвидят възможността да се заведе дело пред национален съд, който от своя страна може да сезира Съда на ЕС посредством преюдициално запитване по силата на член 267 от Договора за функционирането на Европейския съюз (ДФЕС).

Освен това Съдът изрично потвърди, че използването от трета държава на система за самосертифициране (както при принципите за сфера на неприкосновеност на личния живот (Safe Harbour) не изключва констатация за адекватност съгласно член 25, параграф 6 от Директива 95/46/ЕО, доколкото са налице ефективни механизми за

за предаване подлежат на правен контрол. Вж. например становищата, издадени от ОЗД на Schleswig-Holstein: https://www.datenschutzzentrum.de/artikel/981-ULD-Position-Paper-on-the-Judgment-of-the-Court-of-Justice-of-the-European-Union-of-6-October-2015,-C-36214.html и на Rheinland-Pfalz: https://www.datenschutz.rlp.de/de/aktuell/2015/images/20151026_Folgerungen_des_LfDI_RLP_zum_EuGH-Urteil_Safe_Harbor.pdf.

45 Вж. изявление на Работната група по член 29 от 16 октомври 2015 г. (бележка под линия 8 по-горе).

46 Европейска комисия, Предложение за Регламент на Европейския парламент и на Съвета относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни (Общ регламент относно защитата на данните). Вж. също Европейски парламент, Законодателна резолюция от 12 март 2014 г. относно предложението за регламент на Европейския парламент и на Съвета относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни (Общ регламент относно защитата на данните), (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)); Съвет, Предложение за регламент на Европейския парламент и на Съвета относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни (Общ регламент относно защитата на данните), подготовка за общ подход, 9565/15. Предложението в момента е на последния етап от законодателния процес.

откриване и контрол, които правят възможно на практика да се открие и санкционира всяко нарушение на правилата за защита на данните.

Като се има предвид, че Решението за „сфера на неприкосновеност на личния живот“ не съдържа достатъчно констатации в това отношение, Съдът обяви решението за невалидно. Следователно е ясно, че предаването на данни между ЕС и САЩ вече не може да се извършва на това основание, т.е. единствено чрез позоваване на придържането към принципите за сфера на неприкосновеност на личния живот. Тъй като предаването на данни към трети държави, които не гарантират достатъчна степен на защита (или поне когато това не е установено в решение на Комисията съгласно член 25, параграф 6 от Директива 95/46/ЕО), е по принцип забранено[47], то предаването ще бъде законосъобразно единствено ако износителят на данни може да използва един от алтернативните инструменти, описани по-горе в раздел 2. При липсата на решение относно адекватността, износителят на данни носи отговорност — под надзора на националните органи за защита на данните — да гарантира, че условията за използването на (един от) тези инструменти са изпълнени по отношение на съответното предаване на данни.

Обхватът на съдебното решение е ограничен до Решението за „сфера на неприкосновеност на личния живот“ на Комисията. Въпреки това, всяко от другите решения относно адекватността[48] съдържа ограничение на правомощията на ОЗД, което е идентично с член 3 от Решението за „сфера на неприкосновеност на личния живот“, обявено от Съда за невалидно[49]. Понастоящем Комисията ще изведе налагащите се от съдебното решение изводи и скоро ще изготви решение, което ще се приеме съгласно приложимата процедура по комитология и ще замени тази разпоредба във всички съществуващи решения относно адекватността. Също така, Комисията ще започне да извършва редовна оценка на действащите и бъдещите решения относно адекватността, включително чрез периодичен съвместен преглед на тяхното функциониране, заедно с компетентните органи на съответната трета държава.

4. ЗАКЛЮЧЕНИЕ

Както бе потвърдено от Работната група по член 29, алтернативните инструменти, които разрешават протичането на потоците данни, все още могат да бъдат използвани от дружествата като средство за законно предаване на данни към трети държави като САЩ. Комисията обаче счита, че договарянето на обновена и сигурна рамка за предаване на лични данни към САЩ продължава да бъде основен приоритет. Такава рамка е най-цялостното решение за осигуряване на действителна непрекъснатост на защитата на личните данни на европейските граждани, когато те се предават към САЩ.

---

47 Виж съображение 57 от Директива 95/46/ЕО.

48 Понастоящем решения относно адекватността са приети по отношение на следните държави: Андора, Аржентина, Канада, Фарьорските острови, остров Гърнзи, остров Ман, Израел, остров Джърси, Нова Зеландия, Швейцария и Уругвай. Вж.: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

49 Вж. точки 99-104 от решението Schrems.

Тя също така представлява най-доброто решение за трансатлантическата търговия, тъй като осигурява по-опростен, по-лек и следователно по-евтин механизъм за предаване на данни, особено що се отнася до МСП.

Още през 2013 г. Комисията започна преговори с правителството на САЩ за ново споразумение за трансатлантическо предаване на данни въз основа на нейните 13 препоръки[50]. Постигнат бе значителен напредък в сближаването на гледните точки на двете страни, например по отношение на засилването на надзора и прилагането на принципите за сфера на неприкосновеност на личния живот, съответно от Департамента по търговия на САЩ и Федералната комисия по търговия на САЩ, осигуряването на по-голяма прозрачност за потребителите относно техните права на защита на данните, по-лесни и евтини възможности за правна защита в случай на жалби и по-ясни правила за последващо предаване на данни от дружествата, които спазват принципите за сфера на неприкосновеност на личния живот, към такива, които не са се присъединили към тези принципи (например за целите на обработка или обработка от подизпълнители). След като Решението за „сфера на неприкосновеност на личния живот“ бе обявено за невалидно, Комисията засили темпото на разговорите с американското правителство, за да гарантира, че се спазват правните изисквания, формулирани от Съда. Целта на Комисията е тези дискусии да бъдат приключени успешно и то в рамките на три месеца.

Докато обновената трансатлантическа рамка не стане реалност, дружествата трябва да разчитат на алтернативните инструменти за предаване, които са на разположение. Този вариант обаче води до отговорности за износителите на данни, под надзора на националните органи за защита на данните.

За разлика от положението, при което Комисията е установила, че дадена трета държава осигурява достатъчна степен на защита на данните, на която износителите на данни могат да разчитат за целите на предаването на данни от ЕС, когато използват алтернативни инструменти, износителите носят отговорността да проверят, че личните данни са действително защитени. Това може да включва предприемането на подходящи мерки, когато е необходимо.

В този контекст органите за защита на данните имат централна роля. Като основни органи, осигуряващи зачитането на основните права на субектите на данни, националните органи за защита на данните са отговорни и оправомощени да упражняват надзор върху предаването на данни от ЕС към трети държави, в условията на пълна независимост. Комисията приканва администраторите на данни да си сътрудничат с ОЗД, като по този начин им помогнат в ефективното изпълнение на надзорните им функции. Комисията ще продължи да работи в близко сътрудничество с Работната група по член 29, за да гарантира еднаквото прилагане на правото на ЕС в областта на защитата на личните данни.

[50] Вж. по-горе бележка под линия 4.