

РЕШЕНИЕ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2023/1795 НА КОМИСИЯТА**от 10 юли 2023 година****съгласно Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета относно адекватното ниво на защита на личните данни в Рамката за защита на личните данни в отношенията между ЕС и САЩ**

(нотифицирано под номер C(2023) 4745)

(текст от значение за ЕИП)

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския Съюз,

като взе предвид Регламент (ЕС) 2016/679 на Европейския Парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) ⁽¹⁾, и по специално член 45, параграф 3 от него,

като има предвид, че:

1. ВЪВЕДЕНИЕ

- (1) С Регламент (ЕС) 2016/679 ⁽²⁾ се определят правилата за предаването на лични данни от администратори или обработващи лични данни в Съюза на трети държави и международни организации, доколкото това предаване попада в неговото приложно поле. Правилата относно международното предаване на данни са установени в глава V от този регламент. Въпреки че потоците от лични данни към и от държави извън Европейския съюз са от съществено значение за разширяването на трансграничната търговия и на международното сътрудничество, нивото на защита, което се предоставя за личните данни в Съюза, не трябва да бъде излагано на риск при предаването им на трети държави или международни организации ⁽³⁾.
- (2) Съгласно член 45, параграф 3 от Регламент (ЕС) 2016/679 Комисията може чрез акт за изпълнение да реши, че дадена трета държава, територия или един или повече конкретни сектори в тази трета държава осигурява(т) адекватно ниво на защита. При това условие предаването на лични данни на трета държава може да се извършва, без да е необходимо допълнително разрешение, както е предвидено в член 45, параграф 1 и в съображение 103 от Регламент (ЕС) 2016/679.
- (3) Както е посочено в член 45, параграф 2 от Регламент (ЕС) 2016/679, приемането на решение относно адекватното ниво на защита трябва да се основава на цялостен анализ на правния ред на третата държава, който обхваща както правилата, приложими към вносителите на данни, така и ограниченията и гаранциите по отношение на достъпа до лични данни от страна на публичните органи. В своята оценка Комисията трябва да определи дали въпросната трета държава гарантира ниво на защита, „по същество“ равностойно на нивото, гарантирано в рамките на Съюза (съображение 104 от Регламент (ЕС) 2016/679). Стандартът, спрямо който се оценява равностойността по същество, е определеният от законодателството на ЕС, по-специално от Регламент (ЕС) 2016/679, както и от съдебната практика на Съда на Европейския съюз (Съда) ⁽⁴⁾.

⁽¹⁾ ОВ L 119, 4.5.2016 г., стр. 1.

⁽²⁾ Със справочна цел в приложение VIII е включен списък на съкращенията, използвани в настоящото решение.

⁽³⁾ Вж. съображение 101 от Регламент (ЕС) 2016/679.

⁽⁴⁾ Вж. като най-скорошна практика решението на Съда по дело C-311/18, *Facebook Ireland* и *Schrems* (решение по делото *Schrems II*), ECLI:EU:C:2020:559.

- (4) Както бе уточнено от Съда в решението му от 6 октомври 2015 г. по дело C-362/14, *Maximilian Schrems/Data Protection Commissioner* ⁽⁵⁾ (*Schrems*), за тази цел не се изисква установяване на идентично ниво на защита. По-специално средствата, до които въпросната трета държава прибегва за защита на личните данни, може да са различни от прилаганите вътре в Съюза, стига на практика те да се окажат ефективни за гарантирането на достатъчна степен на защита ⁽⁶⁾. Поради това стандартът за адекватно ниво на защита не включва изискване за буквално възпроизвеждане на правилата на Съюза. Критерият се състои по-скоро в това дали чрез същността на правата на неприкосновеност на личния живот и тяхното ефективно прилагане, надзор и изпълнение чуждестранната система като цяло осигурява необходимото ниво на защита ⁽⁷⁾. Освен това, съобразно това решение, когато прилага този стандарт, Комисията следва по-специално да прецени дали в правната рамка на въпросната трета държава са предвидени правила, предназначени за ограничаване на намесата, засягаща основните права на лицата, чиито данни се прехвърлят от Съюза, която намеса държавните структури на тази държава имат право да извършват, ако преследват законосъобразни цели, като например осигуряването на националната сигурност, и дали въпросната правна рамка осигурява ефективна правна защита срещу този вид намеса ⁽⁸⁾. В референтния документ за адекватното ниво на защита на Европейския комитет по защита на данните, който се стреми да изясни допълнително този стандарт, също са предоставени насоки в това отношение ⁽⁹⁾.
- (5) Приложимият стандарт по отношение на подобна намеса, засягаща основните права на неприкосновеност на личния живот и на защита на личните данни, беше допълнително разяснен от Съда в решението му от 16 юли 2020 г. по дело C-311/18, *Data Protection Commissioner/Facebook Ireland Limited u Maximilian Schrems* (*Schrems II*), с което беше обявено за невалидно Решение за изпълнение (ЕС) 2016/1250 на Комисията ⁽¹⁰⁾ относно предходна рамка за трансатлантическите потоци от данни, Щита за личните данни в отношенията между ЕС и САЩ („Рамка на Щита за личните данни“). Съдът счита, че ограниченията на защитата на личните данни, които произтичат от вътрешноправната уредба на Съединените щати относно достъпа и използването от американските публични органи на такива данни, предадени от Съюза на Съединените щати за целите на националната сигурност, не са определени по начин, който да отговаря на изисквания, които по същество са равностойни на предвидените съгласно правото на Съюза, що се отнася до необходимостта и пропорционалността на такава намеса в правото на защита на данните ⁽¹¹⁾. Съдът също така счита, че не е налице способ за защита пред орган, който предоставя на лицата, чиито данни са предадени на Съединените щати, гаранции, които по същество са равностойни на изискваните от член 47 от Хартата относно правото на ефективни правни средства за защита ⁽¹²⁾.
- (6) След решението по делото *Schrems II* Комисията започна разговори с правителството на САЩ с оглед на евентуално ново решение относно адекватното ниво на защита, което да отговаря на изискванията на член 45, параграф 2 от Регламент (ЕС) 2016/679, както е тълкуван от Съда. В резултат на тези разговори на 7 октомври 2022 г. Съединените щати приеха Изпълнителен указ № 14086 „Засилване на защитните мерки за дейностите по радиоелектронно разузнаване на САЩ“ (Указ 14086), който е допълнен от Наредба относно Апелативния съд в областта на защитата на личните данни, издадена от министъра на правосъдието на САЩ (Наредба на МП) ⁽¹³⁾. Освен това рамката, която се прилага по отношение на търговските субекти, обработващи данни, предавани от Съюза съгласно настоящото решение — Рамката за личните данни в отношенията между ЕС и САЩ (РЗЛД в отношенията между ЕС и САЩ или РЗЛД) — беше актуализирана.
- (7) Комисията внимателно анализира законодателството и практиката на САЩ, включително Указ 14086 и Наредбата на МП. Въз основа на констатациите, развити в съображения 9—200, Комисията стигна до заключението, че Съединените американски щати гарантират адекватна степен на защита на личните данни, които се предават съгласно Рамката между ЕС и САЩ от администратор, или обработващ данни в Съюза ⁽¹⁴⁾, към сертифицирани организации в САЩ.

⁽⁵⁾ Дело C-362/14, *Maximilian Schrems/Data Protection Commissioner* (*Schrems*), ECLI:EU:C:2015:650, т. 73.

⁽⁶⁾ Решение по дело *Schrems*, т. 74.

⁽⁷⁾ Вж. Съобщение на Комисията до Европейския парламент и Съвета „Обмен и защита на личните данни в един глобализиран свят“ (COM (2017) 7, 10.1.2017 г., раздел 3.1, стр. 6—7).

⁽⁸⁾ Делото *Schrems*, т. 88—89.

⁽⁹⁾ Референтният документ на Европейския комитет по защита на данните за адекватното ниво на защита, WP 254 rev. 01., е достъпен на следния адрес: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

⁽¹⁰⁾ Решение за изпълнение (ЕС) 2016/1250 на Комисията от 12 юли 2016 г. съгласно Директива 95/46/ЕО на Европейския парламент и на Съвета относно адекватността на защитата, осигурявана от Щита за личните данни в отношенията между ЕС и САЩ (ОВ L 207, 1.8.2016 г., стр. 1).

⁽¹¹⁾ Решение по делото *Schrems II*, т. 185.

⁽¹²⁾ Решение по делото *Schrems II*, т. 197.

⁽¹³⁾ 28 CFR Част 302.

⁽¹⁴⁾ Настоящото решение е от значение за ЕИП. В Споразумението за Европейското икономическо пространство (Споразумението за ЕИП) се предвижда разширяването на вътрешния пазар на Европейския съюз, за да включи трите държави от ЕИП — Исландия, Лихтенщайн и Норвегия. Решението на Съвместния комитет за включване на Регламент (ЕС) 2016/679 в приложение XI към Споразумението за ЕИП бе прието от Съвместния комитет на ЕИП на 6 юли 2018 г. и влезе в сила на 20 юли 2018 г. Регламентът следователно попада в обхвата на това споразумение. За целите на решението позоваванията на ЕС и държавите членки на ЕС следва да се считат като обхващащи и държавите, участващи в ЕИП.

- (8) Решението води до това, че предаването на лични данни от администратори и обработващи лични данни в Съюза ⁽¹⁵⁾ на сертифицирани организации в Съединените щати може да се извърши, без да е необходимо получаването на допълнително разрешение. То не засяга прякото приложение на Регламент (ЕС) 2016/679 спрямо такива организации, когато условията относно териториалния обхват на посочения регламент, изложени в член 3 от него, са изпълнени.

2. РАМКА ЗА ЛИЧНИТЕ ДАННИ В ОТНОШЕНИЯТА МЕЖДУ ЕС И САЩ

2.1 Персонално и материално приложно поле

2.1.1 Сертифицирани организации

- (9) Рамката за личните данни в отношенията между ЕС и САЩ се базира на система за сертифициране, чрез която организациите в САЩ се ангажират да спазват един набор от принципи за неприкосновеност на личния живот — рамковите принципи на Рамката за личните данни в отношенията между ЕС и САЩ, включително допълнителните принципи (наричани по-долу общо „Принципите“), — публикувани от Министерството на търговията на САЩ и посочени в приложение I към настоящото решение ⁽¹⁶⁾. За да отговаря на условията за сертифициране по РЗЛД в отношенията между ЕС и САЩ, дадена организация трябва да е обект на правомощията за разследване и правоприлагане на Федералната търговска комисия (ФТК) на САЩ или Министерството на транспорта („МТ“) ⁽¹⁷⁾. Принципите се прилагат незабавно след сертифицирането. Както е обяснено по-подробно в съображения 48—52, от организациите, попадащи в обхвата на РЗЛД в отношенията между ЕС и САЩ, се изисква ежегодно да подновяват сертифицирането за спазване на принципите ⁽¹⁸⁾.

2.1.2 Определение за понятията „лични данни“, „администратор на лични данни“ и „представител“

- (10) Защитата, предоставяна по силата на РЗЛД в отношенията между ЕС и САЩ, се прилага за всички лични данни, предавани от Съюза на организации в САЩ, които са удостоверили спазването на принципите пред Министерството на търговията, с изключение на данните, които се събират с цел публикуване, излъчване или други форми на публично разпространение на журналистически материали и информация в публикувани преди това материали, разпространявани от медийни архиви ⁽¹⁹⁾. Следователно такава информация не може да бъде предавана въз основа на РЗЛД.
- (11) В принципите понятията „лични данни“/„лична информация“ са определени по същия начин, както в Регламент (ЕС) 2016/679, т.е. като „данни относно идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано, които са в обхвата на ОРЗД, предадени са от Европейския съюз на организация в Съединените щати и са записани под каквато и да е форма“ ⁽²⁰⁾. Съответно те обхващат и псевдонимизирани (или „кодирани с ключ“) данни от научни изследвания (включително когато ключът не се споделя с получаващата организация в САЩ) ⁽²¹⁾. По подобен начин понятието за обработване се определя като „всяка операция или съвкупност от операции, извършвана с лични данни чрез автоматични или други средства, като събиране, записване, организиране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване или разпространяване и изтриване или унищожаване“ ⁽²²⁾.
- (12) РЗЛД в отношенията между ЕС и САЩ се прилага спрямо организации в САЩ, които са квалифицирани като администратори (т.е. като физическо лице или организация, което/която само(а) или съвместно с други определя целите и средствата за обработването на лични данни) ⁽²³⁾ или като обработващи лични данни (т.е. представители, извършващи дейности от името на администратор) ⁽²⁴⁾. Обработващите лични данни от САЩ трябва да бъдат

⁽¹⁵⁾ Решението не засяга изискванията на Регламент (ЕС) 2016/679, които се прилагат спрямо субектите (администратори и обработващи лични данни) в Съюза, които предават данните, по отношение например на ограничаването в рамките на целта, свеждането на данните до минимум, прозрачността и сигурността на данните (вж. също член 44 от Регламент (ЕС) 2016/679).

⁽¹⁶⁾ Вж. във връзка с това точка 81 от делото *Schrems*, в което Съдът потвърди, че чрез система за самосертифициране може да се осигури адекватно ниво на защита.

⁽¹⁷⁾ Приложение I, раздел I, точка 2. ФТК разполага с широки компетенции в областта на търговските дейности с някои изключения, например по отношение на банките, въздушните превозвачи, застрахователната дейност и дейностите на доставчиците на далекосъобщителни услуги в качеството им на общи преносители (въпреки че с решението на Апелативния съд на Съединените американски щати за девети район от 26 февруари 2018 г. по дело ФТК/AT&T беше потвърдено, че ФТК е компетентна по отношение на дейностите на такива субекти в качеството им на различни от общи преносители). Вж. също приложение IV, бележка под линия 2. Министерството на транспорта е компетентно да налага спазването на изискванията от страна на въздушните превозвачи и билетните агенции (за въздушния транспорт), вж. приложение V съгласно раздел A.

⁽¹⁸⁾ Приложение I, раздел III, точка 6.

⁽¹⁹⁾ Приложение I, раздел III.2.

⁽²⁰⁾ Приложение I, раздел I, точка 8, буква а).

⁽²¹⁾ Приложение I, раздел III, точка 14, буква ж).

⁽²²⁾ Приложение I, раздел I, точка 8, буква б).

⁽²³⁾ Приложение I, раздел I, точка 8, буква в).

⁽²⁴⁾ Вж. например приложение I, раздел II, точка 2, буква б), и раздел II, точка 3, буква б) и точка 7, буква г), в които се пояснява, че представителите действат от името на администратор, в зависимост от инструкциите на администратора и съгласно конкретни договорни задължения.

договорно обвързани да извършват действия само въз основа на указания от администратора от ЕС и да го подпомагат при изготвянето на отговори на лицата, упражняващи своите права по силата на принципите ⁽²⁵⁾. Освен това, когато обработването се извършва от подизпълнител, обработващият лични данни трябва да сключи договор с него, който да гарантира същото ниво на защита, което се осигурява от принципите, и да предприеме мерки да гарантира, че договърът се изпълнява правилно ⁽²⁶⁾.

2.2 Принципи на Рамката за защита на личните данни между ЕС и САЩ

2.2.1 Ограничаване в рамките на целта и избор

- (13) Личните данни следва да се обработват законосъобразно и добросъвестно. Те следва да се събират с конкретна цел и впоследствие да се използват само дотолкова, доколкото употребата им не е несъвместима с целта на обработването.
- (14) По РЗЛД това се гарантира чрез различни принципи. На първо място, съгласно *принципа „Пълнота на данните и ограничаване в рамките на целта“*, подобно на посоченото в член 5, параграф 1, буква б) от Регламент (ЕС) 2016/679, никоя организация не може да обработва лични данни по начин, несъвместим с целите, за които те са били събрани първоначално или за които по-късно е получено разрешение от субекта на данните ⁽²⁷⁾.
- (15) На второ място, преди да използва лични данни за нова (променена) цел, която се различава съществено, но все пак е съвместима с първоначалната цел, или да ги разкрие на трета страна, организацията трябва да предостави на субектите на данни правото на възражение (клауза за неучастие „opt out“) в съответствие с *принципа „Избор“* ⁽²⁸⁾ чрез ясен, разбираем и леснодостъпен механизъм. Важно е да се отбележи, че този принцип не отменя изричната забрана за несъвместимо обработване ⁽²⁹⁾.

⁽²⁵⁾ Приложение I, раздел III, точка 10, буква а). Вж. също насоките, изготвени от Министерството на търговията след консултации с Европейския комитет по защита на данните в рамките на Щита за личните данни, в които се разясняват задълженията на обработващи лични данни от САЩ, които получават лични данни от Съюза съгласно рамката. Тъй като тези правила не са променени, настоящите насоки/ЧЗВ продължават да са уместни съгласно РЗЛД в отношенията между ЕС и САЩ (<https://www.privacyshield.gov/article?id=Processing-FAQs>)

⁽²⁶⁾ Приложение I, раздел II, точка 3, буква б).

⁽²⁷⁾ Приложение I, раздел II, точка 5, буква а). Съвместимите цели може да включват одитиране, предотвратяване на измами или други цели, съответстващи на очакванията на разумно лице предвид контекста на събирането (вж. приложение I, бележка под линия б).

⁽²⁸⁾ Приложение I, раздел II, точка 2, буква а). Това не се прилага, когато дадена организация предоставя лични данни на обработващ лични данни, който извършва дейност от нейно име и по нейни указания (приложение I, раздел II, точка 2, буква б). Въпреки това в този случай организацията трябва да има сключен договор и да гарантира спазването на *принципа на отчетност за последващо предаване*, както е описано по-подробно в съображение 43. Освен това принципът *Избор* (както и принципът за *уведомяване*) може да бъде ограничен при обработването на лични данни в контекста на комплексна проверка (като част от потенциално сливане или поглъщане) или при одити до степента и за срока, необходими за изпълнение на законови изисквания или изисквания от обществен интерес, или до степента и срока, до които прилагането на тези принципи би накърнило законните интереси на организацията в конкретния контекст на проучванията за целите на комплексна проверка или одитите (приложение I, раздел III, точка 4). Допълнителен принцип 15 (приложение I, раздел III, точка 15, букви а) и б) предвижда също така изключения по отношение на *принципа „Избор“* (както и на *принципа за уведомяване* и *принципа на отчетност за последващото предаване*), що се отнася до лични данни от обществено достъпни източници (освен когато износителят на данни от ЕС покаже, че информацията подлежи на ограничения, които изискват прилагането на тези принципи) или до лични данни, събрани от регистри, отворени за справки от широката общественост (стига да не са съчетани с информация от непублични регистри и да са спазени всички условия за справките). По същия начин допълнителният принцип 14 (приложение I, раздел III, точка 14, буква е) предвижда изключения по отношение на *принципа „Избор“* (както и на *принципа за уведомяване* и *принципа на отчетност за последващото предаване*), що се отнася до обработването на лични данни от фармацевтично дружество или дружество за медицински изделия за целите на дейности по наблюдение на безопасността и ефикасността на продуктите, доколкото спазването на принципите пречи на спазването на регулаторните изисквания.

⁽²⁹⁾ Това се отнася до всяко предаване на данни съгласно РЗЛД, включително когато те се отнасят до данни, събрани в контекста на трудово правоотношение. Въпреки че следователно сертифицираните организации в САЩ може по принцип да използват данните, свързани с човешки ресурси, за цели, различни от целите, свързани с трудовоправните отношения (например за определени маркетингови съобщения), те трябва да спазват забраната за несъвместимо обработване, като освен това могат да правят това само в съответствие с *принципа за уведомяване* и *принципа „Избор“*. По изключение организация може да използва лични данни за допълнителна съвместима цел, без да предоставя *уведомяване* и *избор*, но само в рамките на нужното и за срока, необходим, за да се избегне накърняването на законните права на организацията да извършва повишаване в длъжност, назначения или вземането на други подобни решения в областта на трудовите правоотношения (вж. приложение I, раздел III, точка 9, буква б), подточка iv). Забраната на американската организация да предприема наказателни действия срещу даден служител при упражняването на такъв избор, включително всяко ограничаване на възможностите за заетост, ще гарантира, че въпреки връзката на подчиненост и свързаната с нея зависимост служителът няма да бъде подлаган на натиск и по този начин може да упражнява истински свободен избор. Вж. приложение I, раздел III, точка 9, буква б), подточка i).

2.2.2 Обработване на специални категории лични данни

- (16) Когато става въпрос за „специални категории данни“, трябва да има специфични гаранции.
- (17) В съответствие с принципа „Избор“ специфичните гаранции се прилагат при обработването на „чувствителна информация“, т.е. лични данни, свързани с медицинското или здравословното състояние, данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, информация за сексуалния живот на физическото лице или каквато и да е друга информация, получена от трета страна, която се определя и третира от тази страна като чувствителна ⁽³⁰⁾. Това означава, че всички данни, които се считат за чувствителни по смисъла на законодателството на ЕС в областта на защитата на личните данни (включително данните относно сексуалната ориентация, генетични и биометрични данни), ще бъдат третирани като чувствителни от РЗЛД от сертифицирани организации.
- (18) Като общо правило организациите трябва да получат изрично съгласие (т.е. opt-in) от физическите лица, за да използват чувствителна информация за цели, различни от тези, за които тя е била първоначално събрана или впоследствие разрешена от физическото лице (чрез opt-in), или за да я разкриват на трети страни ⁽³¹⁾.
- (19) Получаването на такова съгласие не е необходимо в ограничени случаи, сходни на близки до тях изключения, предвидени в законодателството на ЕС в областта на защитата на личните данни, например когато обработването на чувствителни данни е от жизненоважен интерес за дадено лице; когато е необходимо, за да се установи право на иск; или когато е необходимо, за да се окажат медицински грижи, или за определяне на диагноза ⁽³²⁾.

2.2.3 Степен на точност, свеждане до минимум и сигурност на данните

- (20) Данните следва да бъдат точни и при необходимост редовно да се актуализират. Те следва също така да са подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват, и по принцип да се съхраняват не по-дълго от необходимото за целите, за които се обработват.
- (21) Съгласно принципа „Пълнота на данните и ограничаване в рамките на целта“ ⁽³³⁾ личните данни трябва да бъдат ограничени до необходимото за целите, за които се обработват. Освен това организациите трябва да предприемат разумни стъпки, доколкото това е необходимо за целите на обработването, за да гарантират, че личните данни са надеждни за предвиденото им използване и че са точни, пълни и актуални.
- (22) Освен това личната информация може да се съхранява под форма, която идентифицира или позволява идентифицирането на физическите лица (и по този начин — под формата на лични данни) ⁽³⁴⁾, само доколкото това служи на целта(ите), за която(които) е била събрана първоначално или за която(които) по-късно е дадено разрешение от физическото лице съгласно принципа „Избор“. Това задължение не възпрепятства организациите да продължават да обработват лична информация за по-дълги периоди, но само в рамките на срок и до степента, в която това обработване обосновано служи за една от следните конкретни цели, сходни на близки до тях изключения, предвидени в законодателството на ЕС в областта на защитата на личните данни: архивиране от обществен интерес, журналистика, литература и изкуства, научни и исторически изследвания или статистически анализ ⁽³⁵⁾. В случаите, в които личните данни са задържани за една от тези цели, тяхното обработване подлежи на гаранциите, предвидени в принципите ⁽³⁶⁾.
- (23) Личните данни следва също така да се обработват по начин, който гарантира тяхната сигурност, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане. За тази цел администраторите и обработващите лични данни следва да предприемат подходящи технически или организационни мерки за защита на личните данни от възможни заплахи. Тези мерки следва да се оценяват, като се вземат предвид достиженията на техническия прогрес, съответните разходи и естеството, обхватът, контекстът и целите на обработването, както и рисковете за правата на физическите лица.

⁽³⁰⁾ Приложение I, раздел II, точка 2, буква в).

⁽³¹⁾ Приложение I, раздел II, точка 2, буква в).

⁽³²⁾ Приложение I, раздел III, точка 1.

⁽³³⁾ Приложение I, раздел II, точка 5.

⁽³⁴⁾ Вж. приложение I, бележка под линия 7, в която се пояснява, че за дадено физическо лице се счита, че „може да бъде идентифицирано“, при условие че дадена организация или трета страна може в достатъчна степен да идентифицира това физическо лице, като вземе предвид средствата за идентификация, които е вероятно да бъдат използвани (като се отчетат, наред с други неща, разходите и времето, необходими за идентифицирането му, и наличната технология към момента на обработването).

⁽³⁵⁾ Приложение I, раздел II, точка 5, буква б).

⁽³⁶⁾ Пак там.

- (24) По РЗЛД това се осигурява чрез *принципа „Сигурност“*, според който се изисква, подобно на член 32 от Регламент (ЕС) 2016/679, да бъдат приложени разумни и подходящи мерки за сигурност, като се вземат предвид рисковете, свързани с обработването и естеството на данните ⁽³⁷⁾.

2.2.4 Прозрачност

- (25) Субектите на данни следва да бъдат информирани за основните характеристики на обработването на техните лични данни.
- (26) Това се осигурява чрез *принципа за уведомяване* ⁽³⁸⁾, който, подобно на изискванията за прозрачност съгласно Регламент (ЕС) 2016/679, задължава организациите да информират субектите на данни, *inter alia*, относно i) участието на организацията в РЗЛД, ii) вида на събираните данни, iii) целта на обработването, iv) вида или самоличността на третите страни, на които тези данни биха могли да бъдат разкривани, и целите, свързани с това, v) техните лични права, vi) как да се свържат с организацията и vii) наличните средства за правна защита.
- (27) Уведомяването трябва да бъде направено на ясен и разбираем език, когато физическите лица бъдат поканени за първи път да предоставят личната информация или веднага след като стане възможно, но във всеки случай преди тези данни да бъдат използвани за цел, съществено различна от (но съвместима с) тази, за която са били първоначално събрани, или преди разкриването им за първи път на трета страна ⁽³⁹⁾.
- (28) Освен това организациите трябва да направят своите политики относно принципите публично достъпни (или в случая на данните относно човешките ресурси, да ги предоставят на разположение на засегнатите физически лица) и да предоставят линкове към уебсайта на Министерството на търговията (с допълнителни подробности относно сертифицирането, правата на субектите на данни и наличните механизми за защита), към списъка във връзка с рамката за защита на личните данни (списъка към РЗЛД), съдържащ всички участващи организации, и към уебсайта на подходящ доставчик на услуги за алтернативно уреждане на спорове ⁽⁴⁰⁾.

2.2.5 Лични права

- (29) Субектите на данни следва да имат конкретни права, които може да бъде противопоставени на обработващия лични данни или на администратора, по-специално правото на достъп до данните, правото на възражение срещу тяхното обработване, правото на коригиране или изтриване на данните.
- (30) *Принципът „Достъп“* ⁽⁴¹⁾, залегнал в РЗЛД между ЕС и САЩ, предоставя на физическите лица такива права. По-специално субектите на данни имат правото, без да е необходимо да предоставят обосновка, да получат потвърждение от страна на организацията дали тя обработва лични данни, свързани с тях; да им бъдат съобщени данните; и да получават информация относно целта на обработването, категориите лични данни, които се обработват, и (категиорите) получатели(те), на които тези данни биват разкривани ⁽⁴²⁾. От организациите се изисква да отговорят на исканията за достъп в разумен срок ⁽⁴³⁾. Организацията може да определи разумни ограничения по

⁽³⁷⁾ Приложение I, раздел II, точка 4, буква а). Освен това, що се отнася до данните относно човешките ресурси, съгласно РЗЛД в отношенията между ЕС и САЩ от работодателите се изисква да вземат предвид предпочитанията на заетите лица, като ограничават достъпа до личните данни, анонимизират някои от тях или ги кодират или псевдонимизират (приложение I, раздел III, точка 9, буква б), подточка iii).

⁽³⁸⁾ Приложение I, раздел II, точка 1.

⁽³⁹⁾ Приложение I, раздел II, точка 1, буква б). Допълнителния принцип 14 (приложение I, раздел III, точка 14, букви б) и с) съдържа конкретни разпоредби за обработването на лични данни в контекста на здравните изследвания и клиничните изпитвания. По-специално този принцип дава възможност на организациите да обработват данните от клиничните изпитвания дори след като лицето се оттегли от изпитването, ако това е било ясно посочено в уведомлението, предоставено при съгласието на лицето да участва. По подобен начин, когато дадена организация, попадаща в обхвата на РЗЛД в отношенията между ЕС и САЩ, получи достъп до лични данни, тя може да ги използва единствено за нова научноизследователска дейност в съответствие с *принципа за уведомяване* и *принципа „Избор“*. В този случай уведомлението до физическото лице по принцип следва да съдържа информация за всякакви бъдещи специфични употреби на данните (например свързани проучвания). Когато не е възможно всички бъдещи употреби на данните да бъдат включени от самото начало (тъй като съществува вероятност нови открития или медицински/изследователски разработки да доведат до нова научноизследователска употреба), трябва да се включи обяснение, че данните може да бъдат използвани при бъдещи непредвидени медицински и фармацевтични научноизследователски дейности. Ако такова по-нататъшно използване не е в съответствие с общите научноизследователски цели, за които са събрани данните (т.е. ако новите цели са съществено различни, но все пак са съвместими с първоначалната цел, вж. съображения 14—15), е необходимо да се получи ново съгласие (т.е. изрично съгласие, или клауза за участие (opt-in). Вж. в допълнение към това специфичните ограничения/изключения по отношение на *принципа за уведомяване*, описани в бележка под линия 28.

⁽⁴⁰⁾ Приложение I, раздел III, точка 6, буква г).

⁽⁴¹⁾ Вж. също допълнителния принцип по отношение на достъпа (приложение I, раздел III, точка 8).

⁽⁴²⁾ Приложение I, раздел III, точка 8, буква а), подточки i)—ii).

⁽⁴³⁾ Приложение I, раздел III, точка 8, подточка i).

отношение на броя на случаите, в които в рамките на даден период ще бъдат удовлетворявани искания за достъп от дадено физическо лице, и може да наложи такса, която не е прекомерна, например когато исканията са явно прекомерни, по-специално поради техния повтарящ се характер ⁽⁴⁴⁾.

- (31) Правото на достъп може да бъде ограничено само при изключителни обстоятелства, сходни с предвидените в законодателството на ЕС в областта на защитата на личните данни, по-специално, когато биха били нарушени законните права на други лица; когато тежестта или разходите, свързани с предоставянето на достъп, биха били непропорционални на рисковете за неприкосновеността на личния живот на лицето при конкретните обстоятелства (въпреки че разходите и тежестта не са решаващи фактори при определянето на това дали предоставянето на достъп е разумно); до степеня, до която разкриването има вероятност да засегне опазването на важни обществени интереси като националната сигурност, обществената сигурност или отбраната; данните съдържат поверителна търговска информация; или информацията се обработва единствено за изследователски или статистически цели ⁽⁴⁵⁾. всеки отказ или всяко ограничаване на правото на достъп трябва да бъдат необходими и надлежно обосновани, като организацията, която носи тежестта на доказване, че тези изисквания са спазени ⁽⁴⁶⁾. При извършването на тази оценка организацията трябва да обърне особено внимание на интересите на лицето ⁽⁴⁷⁾. Когато има възможност информация да се отдели от други данни, за които се прилага ограничение, организацията трябва да редактира защитената информация и да разкрие останалата информация ⁽⁴⁸⁾.
- (32) Освен това субектите на данни имат право да поискат коригиране или изменение на неточни данни, както и да поискат заличаване на данни, които са били обработени в нарушение на принципите ⁽⁴⁹⁾. Освен това, както е обяснено в съображение 15, физическите лица имат право на възражение/клауза за неучастие „opt out“ срещу обработването на техните данни за цели, съществено различни от (но съвместими с) тези, за които са били събрани данните, и срещу разкриването на техните данни на трети страни. Когато личните данни се използват за целите на директния маркетинг, физическите лица имат право на общо основание да се откажат от обработването по всяко време ⁽⁵⁰⁾.
- (33) В принципите не е изрично разгледан въпросът за решенията, засягащи субекта на данните, които се основават единствено на автоматизирано обработване на лични данни. Във всеки случай, що се отнася до лични данни, събрани в Съюза, всяко решение, което се основава на автоматизирано обработване, обикновено се взема от администратора на данни в Съюза (който е в пряка връзка със засегнатия субект на данни) и по този начин се подчинява непосредствено на разпоредбите на Регламент (ЕС) 2016/679 ⁽⁵¹⁾. Това включва сценарии за предаване, в които обработването се извършва от чужд стопански субект (например от САЩ), действащ като представител (обработващ лични данни) на администратора на данни в Съюза (или като подизпълнител, действащ от името на обработващ лични данни от Съюза, който е получил данните от администратора на данни от Съюза, който ги е събрал), който на това основание впоследствие взема решението.
- (34) Това беше потвърдено от проучване, поръчано от Комисията през 2018 г. в контекста на втория годишен преглед на функционирането на Щита за личните данни ⁽⁵²⁾, в което се стигна до заключението, че към онзи момент няма доказателства, които да сочат, че организациите в рамките на Щита за личните данни обикновено извършват автоматизирано вземане на решения въз основа на лични данни, предадени в рамките на Щита за личните данни.

⁽⁴⁴⁾ Приложение I, раздел III, точка 8, буква е., подточки i)–ii) и буква ж).

⁽⁴⁵⁾ Приложение I, раздел III, точка 4; точка 8, букви б), в), д); точка 14, букви д), е) и точка 15, буква г).

⁽⁴⁶⁾ Приложение I, раздел III, точка 8, буква д), подточка ii). Организацията трябва да информира физическото лице за причините за отказа/ограничението и да предостави лице за контакт за всякакви допълнителни запитвания, раздел III, точка 8, буква а, подточка iii).

⁽⁴⁷⁾ Приложение I, раздел III, точка 8, буква а), подточки ii)–iii).

⁽⁴⁸⁾ Приложение I, раздел III, точка 8, буква а), подточка i).

⁽⁴⁹⁾ Приложение I, раздел II, точка 6 и раздел III, точка 8, буква а), подточка i).

⁽⁵⁰⁾ Приложение I, раздел III, точка 8., подточка 12.

⁽⁵¹⁾ И обратно, в изключителния случай, в който организацията от САЩ има пряка връзка със субекта на данни от Съюза, това обикновено ще е в резултат от това, че стопанският субект е насочил дейността си към лицето в Съюза, предлагайки му стоки или услуги или наблюдавайки неговото поведение. При този сценарий самата организация от САЩ ще попадне в приложното поле на Регламент (ЕС) 2016/679 (член 3, параграф 2) и следователно трябва да спазва непосредствено правото на Съюза в областта на защитата на данните.

⁽⁵²⁾ SWD(2018)497 final, раздел 4.1.5. Проучването беше съсредоточено върху i) степеня, в която организациите в рамките на Щита за личните данни в САЩ вземат решения, засягащи физически лица, въз основа на автоматизирано обработване на лични данни, предадени от дружества в ЕС в рамките на Щита за личните данни; и ii) гаранциите за физическите лица, които федералното законодателство на САЩ предвижда за този вид ситуации, и условията за прилагане на тези гаранции.

- (35) Във всеки случай в правото на САЩ са предвидени специални средства за защита срещу неблагоприятни решения в областите, в които е най-вероятно дружествата да прибегват до автоматизирано обработване на личните данни с цел вземане на решения, засягащи физическите лица (например при предоставяне на заеми, оферти за ипотечни кредити, в сферата на заетостта, жилищното настаняване и застраховане) ⁽⁵³⁾. В тези актове обикновено се предвижда правото на физическите лица да бъдат информирани за конкретните причини в основата на дадено решение (например при отказ на заем), да оспорват непълна или неточна информация (както и използването на неправомерни фактори), както и да потърсят правна защита. В сферата на потребителските заеми в Закона за оповестяване на информация за кредити (Fair Credit Reporting Act — FCRA) и в Закона за равните възможности за кредитиране (Equal Credit Opportunity Act — ECOA) присъстват гаранции, които предоставят на потребителите някаква форма на право на обяснение и право на оспорване на решението. Тези закони се отнасят до широк кръг области, включително кредитиране, заетост, жилищно настаняване и застраховане. Освен това някои антидискриминационни закони, като например дял VII от Закона за гражданските права и Закона за справедливото жилищно настаняване, предоставят на лицата защита по отношение на модели, използвани при автоматизираното вземане на решения, които биха могли да доведат до дискриминация въз основа на определени характеристики, и предоставят на лицата права да оспорват такива решения, включително автоматизирани. По отношение на информацията за здравословното състояние със Закона за преносимост и отчетност при здравното застраховане (Health Insurance Portability and Accountability Act — HIPAA) с Акта за изпълнение за защита на неприкосновеността на личния живот се създават определени права, които са сходни с тези по Регламент (ЕС) 2016/679 по отношение на достъпа до лична информация за здравословното състояние. Освен това съгласно указанията на органите на САЩ доставчиците на медицински услуги трябва да получават информация, която им позволява да информират лицата за автоматизираните системи за вземане на решения, използвани в медицинския сектор ⁽⁵⁴⁾.
- (36) Следователно тези правила предлагат защита, подобна на тази, предвидена в правото на Съюза за защита на личните данните, в малко вероятната ситуация, в която автоматизираните решения се вземат от самата организация, попадаща в обхвата на РЗЛД в отношенията между ЕС и САЩ

2.2.6 Ограничения на последващото предаване на данни

- (37) Нивото на защита на личните данни, което се осигурява за данните, предавани от Съюза на организации в Съединените щати, не трябва да бъде подкопавано от по-нататъшното предаване на тези данни на получател в Съединените щати или друга трета държава.
- (38) Съгласно *принципа на отчетност за последващо предаване* ⁽⁵⁵⁾ се прилагат специални правила за така наречените „последващи предавания“, т.е. предавания на лични данни по РЗЛД от организация към трета страна администратор или обработващ данни, независимо дали те се намират в Съединените американски щати или в трета държава извън Съединените американски щати (и Съюза). Последващо предаване може да се осъществи само i) за ограничени и конкретни цели ii) въз основа на договор между организациите, попадащи в обхвата на РЗЛД между ЕС и САЩ, и третата страна ⁽⁵⁶⁾ (или съпоставима договореност в рамките на корпоративна група ⁽⁵⁷⁾) и iii) само ако този договор изисква от третата страна да осигури същото ниво на защита като гарантираното от принципите.
- (39) Задължението да се осигурява същата степен на защита, която се гарантира от принципите, разглеждано в комбинация с *принципа „Пълнота на данните и ограничаване в рамките на целта“*, предполага по-специално, че третата страна може да обработва предадената ѝ лична информация само за цели, които не са несъвместими с целите, за които тази информация е била събрана или за които по-късно е дадено разрешение от физическото лице (в съответствие с *принципа „Избор“*).

⁽⁵³⁾ Вж. напр. Закон за равните възможности за кредитиране (Equal Credit Opportunity Act (ECOA), 15 U.S.C. 1691 и следв.), Закон за оповестяване на информация за кредити (Fair Credit Reporting Act (FCRA), 15 USC § 1681 и следв.) или Закон за справедливото жилищно настаняване (Fair Housing Act (FHA), 42 U.S.C. 3601 и следв.). Освен това Съединените щати са се присъединили към принципите на Организацията за икономическо сътрудничество и развитие по отношение на изкуствения интелект, които, наред с другото, включват принципи за прозрачност, способност за обяснение, сигурност и отчетност.

⁽⁵⁴⁾ Вж. например насоките, достъпни на адрес 2042-What personal health information do individuals have a right under HIPAA to access from their health care providers and health plans? | NHS.gov.

⁽⁵⁵⁾ Вж. приложение I, раздел II, точка 3 и допълнителния принцип „Задължителни договори за последващите предавания“ (приложение I, раздел III, точка 10).

⁽⁵⁶⁾ Като изключение от този общ принцип дадена организация може да предава по-нататък лични данни на малък свои служители, без да сключва договор с получателя, за свързани с трудовоправните отношения оперативни нужди, например резервация на полет, на стая в хотел или сключване на застраховка. Въпреки това и в този случай организацията все пак трябва да спазва *принципа за уведомяване и принципа „Избор“* (вж. приложение I, раздел III, точка 9, буква д).

⁽⁵⁷⁾ Вж. допълнителния принцип „Задължителни договори за последващите предавания“ (приложение I, раздел III, точка 10, буква б). Въпреки че този принцип дава възможност предаванията да се основават също на извъндоговорни инструменти (например вътрешногрупови програми за спазване на изискванията и контрол), в текста се пояснява, че тези инструменти винаги трябва да „гарантират непрекъснатост на защитата на личната информация съгласно принципите на Щита за личните данни“. Освен това предвид това, че сертифицираните организации в САЩ ще продължат да бъдат отговорни за спазването на принципите, ще има силен стимул да се използват инструменти, които наистина са ефективни на практика.

- (40) *Принципът на отчетност за последващо предаване* следва да се разглежда също така във връзка с *принципа за уведомяване* и, в случай на последващо предаване на трета страна администратор ⁽⁵⁸⁾, с *принципа „Избор“*, съгласно който субектите на данни трябва да бъдат информирани (наред с другото) за вида/самоличността на всеки получател — трета страна, целта на последващото предаване и предлагания избор, и имат право да възразят (изрично да се откажат — opt out) или, в случай на чувствителни данни, трябва да дадат „изрично утвърдително съгласие“ (opt in) за последващото предаване.
- (41) Задължението да се осигурява същата степен на защита, която се изисква от принципите, се прилага за всяка една и за всички трети страни, участващи в обработването на данните, прехвърляни независимо от тяхното местоположение (в САЩ или в друга трета държава), както и в случая, когато първоначалният получател на третата страна предава тези данни на друг получател на третата страна, например за целите на обработване от подизпълнител.
- (42) Във всички случаи в договора с получателя на третата страна трябва да се предвижда последният да уведоми организацията — участник в РЗЛД, ако организацията констатира, че вече не е в състояние да изпълнява посоченото задължение. Когато тази констатация е направена, третата страна администратор трябва да прекрати обработването и трябва да се предприемат други обосновани и съответни мерки за справяне с положението ⁽⁵⁹⁾.
- (43) В случай на последващо предаване към трета страна посредник (т.е. обработващ лични данни) се прилага допълнителна защита. В такъв случай организацията в САЩ трябва при уведомяване да предприеме обосновани и съответни мерки, i) за да гарантира, че представителят работи единствено както е инструктиран и ефективно обработва предадената лична информация по начин, който съответства на задълженията на организацията съгласно принципите; и ii) при уведомяване да преустанови и отстрани последиците от неразрешено обработване ⁽⁶⁰⁾. Министерството на търговията може да задължи организацията да предостави обобщение или представително копие на разпоредбите от договора, свързани с неприкосновеността на личния живот ⁽⁶¹⁾. При възникване на проблеми със спазването на този принцип по веригата (и подверигите) на обработване организацията, изпълняваща ролята на администратор на личните данни, по принцип носи отговорност, както е посочено в *принципа „Защита, прилагане и отговорност за причинени вреди“*, освен ако докаже, че не е отговорна за събитието, довело до вредата ⁽⁶²⁾.

2.2.7 *Отчетност*

- (44) Съгласно *принципа на отчетност* образуванията, които обработват данни, са длъжни да въведат подходящи технически и организационни мерки за ефективно спазване на своите задължения за защита на данните, както и да могат да докажат това спазване, по-специално пред компетентния надзорен орган.
- (45) След като една организация е решила доброволно да се самосертифицира ⁽⁶³⁾ съгласно Рамката за личните данни в отношенията между ЕС и САЩ, ефективното спазване на *Принципите на неприкосновеност на личния живот* е задължително за нея. Съгласно *принципа „Защита, прилагане и отговорност за причинени вреди“* ⁽⁶⁴⁾ организациите, попадащи в обхвата на РЗЛД между ЕС и САЩ трябва да предоставят ефективни механизми, които да гарантират спазването на принципите. Организациите трябва също така да предприемат мерки за извършване на проверка ⁽⁶⁵⁾ дали политиките им в областта на неприкосновеността на личния живот съответстват на принципите на неприкосновеност на личния живот и дали се спазват на практика. Това може да става или посредством система за самооценка, която трябва да включва вътрешни процедури, чрез които да се гарантира, че служителите получават подготовка за прилагането на политиките на организацията в областта на неприкосновеността на личния живот и че периодично се извършва обективен преглед на спазването, или посредством външни проверки за спазването, сред чиито методи може да се включат методите на одитиране, случайни проверки или използване на технологични инструменти.

⁽⁵⁸⁾ Физическите лица няма да имат право на клаузата „opt out“ в случаите, когато личните данни се предават на трета страна, изпълняваща функциите на представител за осъществяване на задачи от името на и съгласно указанията на организацията в САЩ. За това обаче е необходим договор с представителя и организацията в САЩ ще поеме отговорността да гарантира защитата, предоставена по силата на *Принципите*, като упражни правомощията си за даване на указания.

⁽⁵⁹⁾ Положението е различно в зависимост от това дали третата страна е администратор, или обработващ данни (представител). При първия сценарий в договора с третата страна трябва да е предвидено тя да прекрати обработването и да предприеме други обосновани и съответни мерки за справяне с положението. При втория сценарий посочените мерки се вземат от организацията — участник в РЗЛД, като администратор на обработването, под чиито указания действа представителят. Вж. приложение I, раздел II, точка 3.

⁽⁶⁰⁾ Приложение I, раздел II, точка 3, буква б).

⁽⁶¹⁾ *Пак там*.

⁽⁶²⁾ Приложение I, раздел II, точка 7, буква г).

⁽⁶³⁾ Вж. също така допълнителния принцип „Самосертифициране“ (приложение I, раздел III, точка 6).

⁽⁶⁴⁾ Вж. също така допълнителния принцип „Разрешаване на спорове и прилагане“ (приложение I, раздел III, точка 11).

⁽⁶⁵⁾ Вж. също така допълнителния принцип „Проверка“ (приложение I, раздел III, точка 7).

- (46) Освен това организациите трябва да съхраняват документация за прилагането на своите практики в областта на неприкосновеността на личния живот съгласно РЗЛД в отношенията между ЕС и САЩ и да ги предоставят при поискване в контекста на разследване или жалба за несъответствие на независим орган за разрешаване на спорове или компетентен правоприлагащ орган ⁽⁶⁶⁾.

2.3 Управление, надзор и привеждане в изпълнение

- (47) РЗЛД ще бъде управлявана и наблюдавана от Министерството на търговията. Рамката предвижда механизми за надзор и за прилагане, за да се проверява и гарантира, че самосертифицираните организации в САЩ спазват Принципите и че се отстранява всяко неспазване. Тези механизми са изложени в принципите (приложение I) и в ангажиментите, поети от Министерството на търговията (приложение III), ФТК (приложение IV) и Министерството на транспорта (приложение V).

2.3.1 (Повторно) сертифициране

- (48) За да се сертифицират съгласно РЗЛД в отношенията между ЕС и САЩ (или ежегодно да се сертифицират повторно), от организациите се изисква да декларират публично своя поет ангажимент да спазват принципите, да предоставят на разположение своите политики за защита на личните данни и да ги прилагат изцяло ⁽⁶⁷⁾. Като част от повторното си сертифициране организациите трябва да предоставят на Министерството на търговията информация, *inter alia*, за наименованието на съответната организация, описание на целите, за които организацията ще обработва лични данни, личните данни, които ще бъдат обхванати от сертифицирането, както и за избрания метод за проверка, съответния независим механизъм за обжалване и законоустановения орган, който е компетентен да налага спазването на принципите ⁽⁶⁸⁾.
- (49) Организациите могат да получават лични данни въз основа на РЗЛД в отношенията между ЕС и САЩ от датата на тяхното вписване в списъка към РЗЛД от Министерството на търговията. За да се гарантира правната сигурност и да се избегнат „неверни твърдения“, на организациите, които се сертифицират за пръв път, не се разрешава да се позовават публично на спазването на принципите, преди Министерството на търговията да е установило, че подадената от организацията документация за сертифициране е пълна, и да е добавило организацията в списъка към РЗЛД ⁽⁶⁹⁾. За да ѝ бъде позволено да продължи да се ползва от Рамката за личните данни за получаване на лични данни от Съюза, тази организация трябва ежегодно да пресертифицира своето участие в очертаната рамка. Когато дадена организация напусне РЗЛД в отношенията между ЕС и САЩ поради каквато и да е причина, тя трябва да премахне всички изявления, които предполагат, че организацията продължава да участва в рамката ⁽⁷⁰⁾.
- (50) Както е отразено в ангажиментите, изложени в приложение III, Министерството на търговията ще проверява дали организациите отговарят на всички изисквания за сертифициране и дали са въвели (публично оповестена) политика за защита на личните данни, съдържаща информацията, изисквана съгласно *принципа за уведомяване* ⁽⁷¹⁾. Стъпвайки на вече придобития опит от процеса на (повторно) сертифициране в рамките на Щита за личните данни, Министерството на търговията ще извърши редица проверки, включително, за да провери дали политиките за защита на личните данни на организациите съдържат хипервръзка към правилния формуляр за подаване на жалби на уебсайта на съответния механизъм за разрешаване на спорове и, когато в подадената документация за сертифициране са включени няколко структури и дъщерни дружества на една организация, дали политиките за защита на личните данни на всяка от тези структури отговарят на изискванията за сертифициране и са лесно достъпни за субектите на данни ⁽⁷²⁾. Освен това, когато е необходимо, Министерството на търговията ще извършва кръстосани проверки заедно с ФТК и Министерството на транспорта, за да проверява дали организациите подлежат на надзор от надзорния орган, посочен в тяхната документация за сертифициране, и ще работи с органите за алтернативно решаване на спорове, за да проверява дали организациите са регистрирани към независимия механизъм за обжалване, посочен в тяхната документация за (повторно) сертифициране ⁽⁷³⁾.

⁽⁶⁶⁾ Приложение I, раздел III, точка 7.

⁽⁶⁷⁾ Приложение I, раздел I, точка 2.

⁽⁶⁸⁾ Приложение I, раздел III, точка 6, буква б) и приложение III, вж. раздел „Проверява[не на] изискванията за самосертифициране“.

⁽⁶⁹⁾ Приложение I, бележка под линия 1.2.

⁽⁷⁰⁾ Приложение I, раздел III, точка 6, буква з).

⁽⁷¹⁾ Приложение I, раздел III, точка 6 и бележка под линия 1.2, както и приложение III, вж. раздел „Проверява[не на] изискванията за самосертифициране“.

⁽⁷²⁾ Приложение III, раздел „Проверява[не на] изискванията за самосертифициране“.

⁽⁷³⁾ По подобен начин Министерството на търговията ще работи съвместно с третата страна, която ще служи като попечител на средствата, събрани чрез таксата за групата на органите по защита на данните (група на ОЗД) (вж. съображение 73), за да провери дали организациите, избрали ОЗД като своя независим механизъм за защита, са платили таксата за съответната година. Вж. приложение III, раздел „Проверяване на изискванията за самосертифициране“.

- (51) Министерството на търговията ще информира организациите, че за да завършат (повторното) сертифициране, те трябва да решат всички проблеми, установени по време на прегледа. В случай че дадена организация не успее да даде отговори в рамките на срока, определен от Министерството на търговията (например по отношение на повторното сертифициране се счита, че процесът трябва да приключи в рамките на 45 дни) ⁽⁷⁴⁾, или по друг начин не успее да завърши своето сертифициране, подадената документация ще се счита за изоставена. В такъв случай всяко невярно твърдение по отношение на участието във или спазването на РЗЛД в отношенията между ЕС и САЩ или спазването ѝ може да подлежи на действия по правоприлагане от страна на ФТК или Министерството на транспорта ⁽⁷⁵⁾.
- (52) За да се гарантира правилното прилагане на Рамката за личните данни в отношенията между ЕС и САЩ, заинтересованите страни, като например субектите на данни, износителите на данни и националните органи по защита на данните (ОЗД), трябва да бъдат в състояние да идентифицират организациите, които се придържат към Принципиите. За да се гарантира такава прозрачност в „точката за подаване на лични данни“, Министерството на търговията се ангажира да поддържа и предоставя на обществеността списъка на организациите, които са удостоверили придържането си към принципите и попадат в компетентността на поне един от правоприлагащите органи, посочени в приложения IV и V към настоящото решение ⁽⁷⁶⁾. Министерството на търговията ще актуализира списъка въз основа на ежегодното подаване на документация за повторно сертифициране от организациите и случаите, когато дадена организация се оттегли или бъде отстранена от Рамката. Освен това, за да гарантира прозрачност също и при „точката за извеждане на лични данни“, Министерството на търговията ще направи общодостъпен регистър на организациите, които са били премахнати от списъка, посочвайки във всеки отделен случай причината за премахването им ⁽⁷⁷⁾. И накрая, то ще предостави връзка към уебстраницата на ФТК относно РЗЛД в отношенията между ЕС и САЩ, на която ще бъдат изброени действията на ФТК по правоприлагане съгласно рамката ⁽⁷⁸⁾.

2.3.2 Наблюдение на съответствието

- (53) Министерството на търговията ще следи постоянно за ефективното спазване на принципите от страна на организациите, попадащи в обхвата на РЗЛД между ЕС и САЩ чрез различни механизми ⁽⁷⁹⁾. По-специално то ще извършва „проверки на място“ на произволно избрани организации, както и *ad hoc* проверки на място на конкретни организации, когато бъдат установени потенциални проблеми със спазването на изискванията (например такива, докладвани на Министерството на търговията от трети страни), за да проверява дали i) звено(ата) за връзка за разглеждане на жалби и искания от субекти на данни е (са) на разположение и реагира(т); ii) политиката на организацията в областта на неприкосновеността на личния живот е лесно достъпна както на нейния уебсайт, така и чрез хипервръзка на уебсайта на Министерството на търговията; iii) политиката на организацията в областта на неприкосновеността на личния живот е съобразена с изисквания за сертифициране и iv) избраният от организацията независим механизъм за разрешаване на спорове е достъпен за целите на разглеждането на жалби ⁽⁸⁰⁾.
- (54) Ако има достоверни доказателства, че дадена организация не изпълнява ангажиментите си съгласно РЗЛД в отношенията между ЕС и САЩ (включително ако Министерството на търговията получи жалби или организацията не отговаря задоволително на запитванията от страна на Министерството на търговията), Министерството на търговията ще изисква от организацията да попълни и представи подробен въпросник ⁽⁸¹⁾. Организация, която не успее да отговори задоволително и своевременно на въпросника, ще бъде сезирана от съответния орган (ФТК или Министерството на транспорта) за предприемане на евентуални действия по правоприлагане ⁽⁸²⁾. Като част от дейностите си по наблюдение на спазването на изискванията в рамките на Щита за личните данни Министерството

⁽⁷⁴⁾ Приложение III, бележка под линия 2.

⁽⁷⁵⁾ Вж. приложение III, раздел „Проверява[не на] изискванията за самосертифициране“.

⁽⁷⁶⁾ Информация за управлението на списъка към РЗЛД може да бъде намерена в приложение III (вж. въведението в част „Управление и надзор на Програмата на Щита за личните данни от Министерството на търговията“) и в приложение I (раздел I, точки 3 и 4, раздел III, точка 6, буква г) и раздел III, точка 11, буква ж).

⁽⁷⁷⁾ Приложение III, вж. въведението в част „Управление и надзор на Програмата на Щита за личните данни от Министерството на търговията“.

⁽⁷⁸⁾ Вж. приложение III, раздел „Адаптира[не на] уебсайта на рамката за защита на личните данни според целевите групи“.

⁽⁷⁹⁾ Вж. приложение III, раздел „Извършва[не на] периодични служебни прегледи и оценки на спазването на програмата за рамката за защита на личните данни“.

⁽⁸⁰⁾ Като част от дейностите по наблюдение Министерството на търговията може да използва различни инструменти, включително да проверява за неработещи хипервръзки към политиките за поверителност, или да следи активно новините за съобщения, които предоставят достоверни доказателства за неспазване на правилата.

⁽⁸¹⁾ Вж. приложение III, раздел „Извършва[не на] периодични служебни прегледи и оценки на спазването на програмата за рамката за защита на личните данни“.

⁽⁸²⁾ Вж. приложение III, раздел „Извършва[не на] периодични служебни прегледи и оценки на спазването на програмата за рамката за защита на личните данни“.

на търговията извършва редовно проверките на място, посочени в съображение 53, и непрекъснато проследява докладването пред обществеността, което му позволи да идентифицира, разглежда и разрешава проблеми, свързани със спазването на изискванията ⁽⁸³⁾. Организации, които трайно не се съобразяват с принципите, се заличават от списъка към РЗЛД и трябва да върнат или заличат личните данни, които са получили съгласно рамката ⁽⁸⁴⁾.

- (55) В други случаи на заличаване от списъка, като например доброволно оттегляне от участие или неподаване на заявление за повторно сертифициране, организациите трябва да изтрият или да върнат данните, или да ги задържат, при условие че ежегодно уверяват Министерството на търговията относно ангажираността си да продължат да прилагат принципите или да предоставят адекватна защита на личните данни посредством други разрешени средства (например като използват договор, в който изцяло са отразени изискванията на съответните одобрени от Комисията стандартни договорни клаузи) ⁽⁸⁵⁾. В този случай организацията посочва и лице за връзка с нея по всички въпроси в областта на РЗЛД в отношенията между ЕС и САЩ.

2.3.3 Идентифициране на неверни твърдения за участие и намиране на решения

- (56) Министерството на търговията ще следи за всякакви неверни твърдения за участие в РЗЛД в отношенията между ЕС и САЩ или за неправомерно използване на сертификационния знак на РЗЛД, както служебно, така и въз основа на жалби (например получени от ОЗД) ⁽⁸⁶⁾. По-конкретно Министерството на търговията ще проверява дали организациите, които i) се оттеглят от участие в РЗЛД в отношенията между ЕС и САЩ, които ii) не успяват да завършат ежегодното повторно сертифициране (т.е. които са започнали, но не са успели да завършат напълно процеса по ежегодно повторно сертифициране своевременно, или дори не са започнали процеса по повторно сертифициране), които iii) са отстранени като участници поради „трайно неспазване на принципите“ или които iv) не успяват да завършат първоначалното сертифициране (т.е. започнали са, но не са успели да завършат процеса по първоначално сертифициране своевременно), премахват от всички съответни публикувани политики за защита на личните данни препратки към РЗЛД между ЕС и САЩ, които предполагат, че организацията активно участва в рамката ⁽⁸⁷⁾. Министерството на търговията също така ще извършва проучвания в интернет, за да открива препратки към РЗЛД в отношенията между ЕС и САЩ в политиките за защита на личните данни на организациите, включително, за да установи фалшиви твърдения от организации, които никога не са участвали в РЗЛД ⁽⁸⁸⁾.
- (57) В случаите, в които Министерството на търговията установи, че препратките към РЗЛД в отношенията между ЕС и САЩ все още не са отстранени или са некоректно използвани, то ще информира организацията за евентуално сезиране на ФТК/Министерството на транспорта ⁽⁸⁹⁾. Ако дадената организация не отговори по задоволителен начин, Министерството на търговията ще отнесе въпроса до съответната агенция за предприемане на евентуални действия по правоприлагане ⁽⁹⁰⁾. Всяко невярно твърдение пред широката общественост от страна на организацията относно нейното придържане към принципите под формата на подвеждащи изявления или практики подлежи на принудителни действия по правоприлагане от страна на ФТК, Министерството на транспорта или други съответни правоприлагащи органи на САЩ. Неверни твърдения пред Министерството на търговията подлежат на санкциониране по Закона за неверните твърдения (18 U.S.C. § 1001).

⁽⁸³⁾ По време на втория годишен преглед на Щита за личните данни Министерството на търговията представи информация, че е извършило проверки на място на 100 организации и е изпратило въпросници относно съответствието в 21 случая (след което откритите проблеми са били отстранени) вж. Работен документ на службите на Комисията SWD(2018) 497 final, стр 9. Подобно на това по време на третия годишен преглед на Щита за личните данни Министерството на търговията съобщи, че е открило три инцидента чрез наблюдението си на докладването пред обществеността и е започнало практиката да извършва проверки на място на 30 дружества всеки месец, което е довело до последващи действия с въпросници относно съответствието в 28 % от случаите (след което откритите проблеми са били незабавно отстранени или, в три случая, са били разрешени след предупредително писмо), вж. Работен документ на службите на Комисията SWD(2019) 495 final, стр 8.

⁽⁸⁴⁾ Приложение I, раздел III, точка 11, буква ж). Трайно неспазване е налице по-специално, когато организацията отказва да се съобрази с окончателно решение на орган за саморегулиране във връзка с неприкосновеността на личния живот, независим орган за разрешаване на спорове или правоприлагащ орган.

⁽⁸⁵⁾ Приложение I, раздел III, точка 6, буква е).

⁽⁸⁶⁾ Приложение III, раздел „Търси[не на] неверни твърдения за участие и намира[не на] решения“.

⁽⁸⁷⁾ *Пак там*.

⁽⁸⁸⁾ *Пак там*.

⁽⁸⁹⁾ *Пак там*.

⁽⁹⁰⁾ В рамките на Щита за личните данни Министерството на търговията по време на третия ежегоден преглед на рамката докладва, че е установило 669 случая на неверни твърдения за участие (между октомври 2018 г. и октомври 2019 г.), повечето от които са били разрешени след предупредителното писмо на Министерството на търговията, а 143 случая са били отнесени до ФТК (вж. съображение 62 по-долу). Вж. Работен документ на службите на Комисията SWD(2019) 495 final, стр. 10.

2.3.4 Правоприлагане

- (58) С цел да се гарантира, че адекватното ниво на защита на данните се осигурява и на практика, следва да има независим надзорен орган с правомощия за наблюдение и осигуряване на спазването на правилата за защита на данните.
- (59) Организациите, попадащи в обхвата на РЗЛД между ЕС и САЩ, трябва да подлежат на юрисдикцията на компетентните органи на САЩ — ФТК и Министерството на транспорта, които разполагат с необходимите правомощия за разследване и правоприлагане, за да гарантират ефективно спазването на принципите ⁽⁹¹⁾.
- (60) ФТК е независим орган, съставен от петима комисари, които се назначават от президента с препоръката и съгласието на Сената ⁽⁹²⁾. Комисарите се назначават за мандат от седем години и могат да бъдат отстранени от длъжност само от президента поради неефективност, пренебрегване на служебните задължения или злоупотреба със служебно положение. ФТК не може да има повече от трима комисари от една и съща политическа партия, а по време на назначението си комисарите не могат да се занимават с друга стопанска дейност, професия или работа.
- (61) ФТК може да разследва спазването на принципите, както и неверни твърдения за придържане към тях или за участие в РЗЛД в отношенията между ЕС и САЩ от организации, които вече не са в списъка към РЗЛД или никога не са се сертифицирали ⁽⁹³⁾. ФТК може да наложи спазването на изискванията, като поиска административна заповед или разпореждане на федералния съд (включително „заповеди за съгласие“, постигнато чрез споразумения) ⁽⁹⁴⁾ за предварителни или постоянни съдебни забрани или други средства за защита, и систематично ще следи за спазването на тези заповеди ⁽⁹⁵⁾. Когато организациите не изпълняват такива заповеди, ФТК може да поиска налагане на граждански санкции и други средства за правна защита, включително за всяка вреда, причинена в резултат на неправомерно поведение. Всяка заповед за съгласие с адресат организация — участник в Рамката за личните данни, ще включва разпоредби за доброволно докладване ⁽⁹⁶⁾, а от организациите ще се изисква да обявяват публично всички релевантни и свързани с Рамката за личните данни части от евентуален доклад или оценка за спазването, представени на ФТК. И накрая, ФТК ще поддържа онлайн списък на организациите, по отношение на които са били издадени заповеди от ФТК или съдебни разпореждания по казуси, свързани с РЗЛД в отношенията между ЕС и САЩ ⁽⁹⁷⁾.
- (62) По отношение на Щита за личните данни ФТК е предприела действия по правоприлагане в около 22 от случаите, както по отношение на нарушения на конкретни изисквания на рамката (например липса на потвърждение пред Министерството на търговията, че организацията продължава да прилага защитата на Щита за личните данни, след като е напуснала рамката, липса на потвърждение чрез самооценка или външен преглед на съответствието, че организацията спазва рамката) ⁽⁹⁸⁾, така и по отношение на неверни твърдения за участие в рамката (например от организации, които не са изпълнили необходимите стъпки за получаване на сертификат или са допуснали сертифицирането им да изтече, но са представили невярна информация за продължаващото си участие) ⁽⁹⁹⁾. Това действие по правоприлагане, наред с другото, е резултат от проактивната употреба на административните призовки за получаване на материали от определени участници в Щита за личните данни с цел проверка за съществени нарушения на задълженията по Щита за личните данни ⁽¹⁰⁰⁾.

⁽⁹¹⁾ Организация, попадаща в обхвата на РЗЛД между ЕС и САЩ, трябва да обяви публично поемането на ангажимент да спазва принципите, да оповестява политиките си в областта на неприкосновеността на личния живот и да ги прилага изцяло. Неспазването подлежи на принудително изпълнение съгласно раздел 5 от Закона за Федералната комисия по търговия, който забранява неоялните и измамни практики в търговията или засягащи търговията (15 U.S.C., § 45 и 49 U.S.C., § 41712), с който се забранява на превозвач или билетна агенция всяка неоялна или измамна практика при въздушните транспортни услуги или при продажбата на въздушни транспортни услуги.

⁽⁹²⁾ 15 U.S.C. § 41.

⁽⁹³⁾ Приложение IV.

⁽⁹⁴⁾ Според информация от ФТК тя няма правомощия да извършва проверки на място в областта на защитата на неприкосновеността на личния живот. Той обаче има правомощието да задължи организациите да представят документи и да предоставят свидетелски показания (вж. член 20 от Закона за ФТК), и може да използва съдебната система за принудително изпълнение на такива заповеди в случай на неспазване.

⁽⁹⁵⁾ Вж. приложение IV, раздел „Изискване на заповеди и контрол по тях“.

⁽⁹⁶⁾ Със заповеди на ФТК или съдебни разпореждания може да се изиска от дружествата да прилагат програми за неприкосновеността на личния живот и редовно да предоставят на ФТК доклади за спазването на тези програми или оценки от независима трета страна.

⁽⁹⁷⁾ Приложение IV, раздел „Изискване на заповеди и контрол по тях“.

⁽⁹⁸⁾ Работен документ на службите на Комисията SWD(2019) 495 final, стр. 11.

⁽⁹⁹⁾ Вж. делата, изброени на уебсайта на ФТК, достъпни чрез <https://www.ftc.gov/business-guidance/privacy-security/privacy-shield>. Вж. също и Работен документ на службите на Комисията SWD (2017) 344 final, стр. 17; Работен документ на службите на Комисията SWD(2018) 497 final, стр. 12 и Работен документ на службите на Комисията SWD(2019) 495 final, стр. 11.

⁽¹⁰⁰⁾ Вж. например Prepared Remarks of Chairman Joseph Simons at the Second Privacy Shield Annual Review (Коментари на председателя Joseph Simons, подготвени за втория годишен преглед на Щита за личните данни) (ftc.gov).

- (63) В по-общ план през последните години ФТК е предприела действия по правоприлагане в редица случаи относно спазването на конкретни изисквания за защита на личните данни, които са предвидени и в РЗЛД, като например по отношение на ограничаването в рамките на целта и съхраняване на данните ⁽¹⁰¹⁾, свеждането на данните до минимум ⁽¹⁰²⁾, сигурността на данните ⁽¹⁰³⁾ и точността на данните ⁽¹⁰⁴⁾.
- (64) Министерството на транспорта има изключителни правомощия да регулира практиките за защита на личните данни на авиокомпаниите и споделя юрисдикция с ФТК по отношение на практиките за защита на личните данни на билетните агенции при продажбата на въздушен транспорт. Служителите на Министерството на транспорта се стремят първо към постигане на споразумение, а ако това не е възможно, могат да започнат процедура по правоприлагане, включваща изслушване на доказателства пред съдия по административно право на Министерството на транспорта, който е упълномощен да издава разпореждания за преустановяване и възпиране на нарушаващите действия и гражданскоправни санкции ⁽¹⁰⁵⁾. Съдиите по административно право се ползват от редица мерки за защита по Закона за административното производство (АРА), за да се гарантират тяхната независимост и безпристрастност. Например те могат да бъдат уволнени само по основателна причина; те се разпределят по дела на ротационен принцип; те не могат да изпълняват задължения, несъвместими със задълженията и отговорностите си като съдии по административно право; те не подлежат на надзор от страна на разследващия екип на органа, от който са наети (в този случай Министерството на транспорта); и те трябва да изпълняват безпристрастно функцията си по правораздаване/правоприлагане ⁽¹⁰⁶⁾. Министерството на транспорта се ангажира да наблюдава заповедите за правоприлагане и да гарантира, че заповедите, издадени в резултат на РЗЛД в отношенията между ЕС и САЩ, са достъпни на неговия уебсайт ⁽¹⁰⁷⁾.

2.4 Средства за правна защита

- (65) С цел да се осигури адекватна защита, и по-специално упражняване на индивидуалните права, на субекта на данни следва да се предоставят ефективни административни и съдебни средства за правна защита.
- (66) В принципа „Защита, прилагане и отговорност за причинени вреди“ на Рамката за личните данни в отношенията между ЕС и САЩ се съдържа изискването организациите да осигуряват защита за физическите лица, които са засегнати от неспазване, и по този начин се дава възможност на субектите на данни от ЕС да подават жалби относно неспазване от страна на организациите, попадащи в обхвата на РЗЛД между ЕС и САЩ, и тези жалби да бъдат разрешени, ако е необходимо чрез решение за предоставяне на ефективна правна защита ⁽¹⁰⁸⁾. Като част от процеса на сертифициране организациите трябва да отговорят на изискванията на този принцип, като предоставят ефективни и леснодостъпни независими механизми за подаване на жалби, чрез които жалбите и споровете на всяко физическо лице да могат да се разследват и разрешават бързо без разходи за лицето ⁽¹⁰⁹⁾.

⁽¹⁰¹⁾ Вж. например разпореждане на ФТК по делото *Drizly, LLC.*, в което от дружеството, наред с другото, се изисква 1) да заличи всички събрани от него данни, които не са необходими за предоставяне на продукти или услуги на потребителите, 2) да се въздържа от събирането или съхранението на лична информация, освен когато това е необходимо за конкретни цели, посочени в графика за съхранение.

⁽¹⁰²⁾ Вж. например разпореждане на ФТК по делото *CafePress* (24 март 2022 г.), в което, наред с другото, се изисква свеждането до минимум на обема на събираните данни.

⁽¹⁰³⁾ Вж. например действия по правоприлагане на ФТК по делата *Drizzly, LLC* и *CafePress*, при които от съответните дружества се изисква да въведат специална програма за сигурност или специфични мерки за сигурност. Освен това, що се отнася до нарушенията на сигурността на данните, вж. също разпореждане на ФТК от 27 януари 2023 г. по делото *Chegg*, постигнатото споразумение с Equifax през 2019 г. (<https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach>).

⁽¹⁰⁴⁾ Вж. също делото *RealPage, Inc* (16 октомври 2018 г.), по което ФТК предприе действия по правоприлагане съгласно FCRA срещу дружество за проверка на наематели, което е предоставяло информационни доклади за физически лица на собственици на имоти и дружества за управление на имоти, въз основа на информация от предишни данни за наеми, публична информация (включително съдебни досиета и предишни случаи на съдебно отстранение) и кредитна информация, които са били използвани като фактор при определяне на допустимостта за настаняване. ФТК е установила, че дружеството не е предприело разумни мерки, за да гарантира точността на информацията, която е предоставило въз основа на своя инструмент за автоматично вземане на решения.

⁽¹⁰⁵⁾ Вж. приложение V, раздел „Практики по принудително изпълнение“.

⁽¹⁰⁶⁾ Вж. 5 U.S.C. §§ 3105, 7521(a), 554(d) и 556(b)(3).

⁽¹⁰⁷⁾ Приложение V, вж. раздел „Контрол по изпълнението и публично оповестяване на заповеди по принудително изпълнение във връзка с нарушения на РЗЛД в отношенията между ЕС и САЩ“.

⁽¹⁰⁸⁾ Приложение I, раздел II, точка 7.

⁽¹⁰⁹⁾ Приложение I, раздел III, точка 11.

- (67) Организацията могат да изберат независими механизми за защита в Съюза или в Съединените американски щати. Както е обяснено по-подробно в съображение 73, това включва възможността доброволно да се ангажират да си сътрудничат с ОЗД в ЕС. Когато организацията обработват данни за човешките ресурси, този ангажимент за сътрудничество с органите на ЕС за защита на данните е задължителен. Другите алтернативи включват независимо извънсъдебно разрешаване на спорове или разработени от частния сектор програми за неприкосновеност на личния живот, в чиито правила са залегнали принципите. Последните трябва да включват ефективни механизми за прилагането им в съответствие с изискванията на принципа „Защита, прилагане и отговорност за причинени вреди“.
- (68) Вследствие на това РЗЛД между ЕС и САЩ предвижда редица възможности за субектите на данните да упражняват правата си, да подават жалби относно неспазване от страна на организацията в ЕС и САЩ и за разрешаване на техните жалби, ако е необходимо, чрез решение за предоставяне на ефективна правна защита. Физическите лица могат да предявят жалба директно пред организацията, независим орган за решаване на спорове, посочен от организацията, националните ОЗД, Министерството на транспорта или ФТК. В случаите, когато техните жалби не са били разрешени чрез нито един от тези механизми за защита и правоприлагане, физическите лица имат също така право да поискат въпросът да бъде решен чрез правно обвързващ арбитраж (приложение I към приложение I към настоящото решение). С изключение на арбитражния панел, при който има изискването някои средства за правна защита да бъдат изчерпани, преди да бъде използван, физическите лица имат право да упражняват някои или всички механизми за правна защита по свой избор и не са задължени да избират определен механизъм или да спазват определена последователност.
- (69) На първо място, субектите на данни от Съюза могат да преследват нарушения на спазването на принципите чрез преки контакти с РЗЛД в отношенията между ЕС и САЩ ⁽¹¹⁰⁾. За да се улесни решаването на споровете, организацията трябва да създаде ефективен механизъм за правна защита, чрез който да се разглеждат жалбите. Това означава в политиката ѝ в областта на неприкосновеността на личния живот да се предоставя ясна информация на физическите лица за звеното за връзка, независимо дали в рамките на организацията или извън нея, което отговаря за разглеждането на жалбите (включително съответна организация в Съюза, която може да отговаря на запитвания или оплаквания), както и за определения независим орган за разрешаване на спорове (вж. съображение 70). При получаване на жалба на физическо лице, директно от него или чрез Министерството на търговията след сезиране от ОЗД, организацията трябва да предостави отговор на субекта на данни от Съюза в срок от 45 дни ⁽¹¹¹⁾. Освен това от организацията се изисква да реагират своевременно на запитвания и други искания за информация от Министерството на търговията или от ОЗД ⁽¹¹²⁾ (когато организацията е ангажирана да си сътрудничи с органа за защита на личните данни) във връзка с придържането им към принципите.
- (70) На второ място организацията трябва да определят независим орган за разрешаване на спорове (в Съединените американски щати или в Съюза), който да разследва и разрешава отделните жалби (освен ако те са очевидно необосновани или нямат сериозен характер) и да предоставя безплатно подходяща защита за физическите лица ⁽¹¹³⁾. Санкциите и средствата за правна защита, налагани от този орган, трябва да са достатъчно строги, за да гарантират спазването от организацията на принципите и да осигуряват отстраняване или поправка от страна на организацията на последиците от неспазването на принципите, а в зависимост от обстоятелствата — и преустановяване на последващото обработване на въпросните лични данни и/или тяхното заличаване, както и публично оповестяване на констатациите за неспазването ⁽¹¹⁴⁾. От определените от организацията независими органи за разрешаване на спорове се изисква да включват на своите публични уебсайтове съответна информация относно Рамката за личните данни в отношенията между ЕС и САЩ и услугите, които извършват съгласно нея ⁽¹¹⁵⁾. Те трябва да публикуват ежегодно годишен доклад с обобщена статистическа информация относно тези услуги ⁽¹¹⁶⁾.

⁽¹¹⁰⁾ Приложение I, раздел III, точка 11, буква г), подточка i).

⁽¹¹¹⁾ Приложение I, раздел III, точка 11, буква г), подточка i).

⁽¹¹²⁾ Това е органът, разглеждащ жалбите, определен от неформална група на ОЗД, предвиден в допълнителния принцип „Ролята на органите по защита на данните“ (приложение I, раздел III, точка 5).

⁽¹¹³⁾ Приложение I, раздел III, точка 11, буква г).

⁽¹¹⁴⁾ Приложение I, раздел II, точка 7, и раздел III, точка 11, буква д).

⁽¹¹⁵⁾ Приложение I, раздел III, точка 11, буква г), подточка ii).

⁽¹¹⁶⁾ В годишния доклад трябва да бъдат включени: 1) общият брой на получените през отчетната година жалби във връзка с Рамката за личните данни в отношенията между ЕС и САЩ; 2) видът на получените жалби; 3) качествени показатели за решаването на спора, например времето за обработването на жалбите; и 4) резултатите от получените жалби, а именно броят и видовете средства за правна защита или санкции, които са били наложени.

- (71) Министерството на търговията ще проверява също и дали организациите, попадащи в обхвата на РЗЛД между ЕС и САЩ действително са регистрирани към независимите механизми за защита, към които са заявили, че са регистрирани ⁽¹¹⁷⁾. От организациите и от отговорните независими механизми за защита се изисква да отговарят в кратки срокове на запитвания и искания за информация от страна на Министерството на търговията във връзка с РЗЛД. Министерството на търговията ще работи съвместно с независимите механизми за защита, за да потвърди, че те включват в своите уебсайтове информация относно принципите и услугите, които предоставят съгласно РЗЛД в отношенията между ЕС и САЩ, и че публикуват годишни доклади ⁽¹¹⁸⁾.
- (72) В случай че организацията не спази решението на орган по разрешаване на спорове или на саморегулиращ се орган, последният трябва да уведоми за това Министерството на търговията и ФТК (или друг орган на САЩ, компетентен да разследва неспазване от страна на организацията) или компетентния съд ⁽¹¹⁹⁾. Ако дадена организация отказва да изпълнява окончателното решение на орган за саморегулиране във връзка с неприкосновеността на личния живот, независим орган за разрешаване на спорове или правителствен орган, или когато такъв орган констатира, че организация често нарушава принципите, това може да се счита за трайно неспазване. Вследствие на това, след като първо е изпратило на организацията нарушител тридесетдневно предизвестие и е дало възможност за отговор, Министерството на търговията ще заличи организацията от списъка към РЗЛД ⁽¹²⁰⁾. Ако след заличаването от списъка организацията продължава да твърди, че е сертифицирана съгласно Рамката за личните данни, Министерството на търговията ще отнесе въпроса пред ФТК или друга правопрелагаща агенция ⁽¹²¹⁾.
- (73) На трето място, физическите лица могат да отнесат жалбите си до национален ОЗД в Съюза, който може да използва своите правомощия за разследване и за защита съгласно Регламент (ЕС) 2016/679. Организациите са длъжни да сътрудничат при разследването и разрешаването на жалба от ОЗД или когато става въпрос за обработването на данни за човешките ресурси, събрани в рамките на трудово правоотношение, или когато съответната организация доброволно се е подложила на надзор от страна на органите за защита на данните ⁽¹²²⁾. По-специално организациите трябва да отговарят на запитвания, да спазват препоръките на ОЗД, включително за корективни или компенсаторни мерки, и да предоставят на ОЗД писмено потвърждение, че са взели такива мерки ⁽¹²³⁾. В случаи на неспазване на препоръките, издадени от органите за защита на данните, ОЗД ще отнася тези случаи до Министерството на търговията (което може да заличи организациите от списъка към РЗЛД в отношенията между ЕС и САЩ) или, за евентуално предприемане на действия по принудително изпълнение, до ФТК или до Министерството на транспорта (неоказването на съдействие на ОЗД или неспазването на принципите могат да бъдат санкционирани съгласно правото на САЩ) ⁽¹²⁴⁾.
- (74) С цел улесняване на сътрудничеството за ефективно разглеждане на жалби, както Министерството на търговията, така и ФТК са създали специално звено за връзка, което отговаря за пряката връзка с ОЗД ⁽¹²⁵⁾. Тези звена за връзка помагат при запитвания от страна на ОЗД относно спазването на принципите от дадена организация.
- (75) Препоръките, предоставяни от ОЗД ⁽¹²⁶⁾, се издават след като и двете страни по спора са имали подходяща възможност да представят своите забележки и евентуално своите доказателства. Съответната група на ОЗД може да предоставя препоръките си в най-кратки срокове, доколкото го позволява изискването за справедлив процес, и по принцип най-късно в срок от 60 дни, считано от получаването на жалбата ⁽¹²⁷⁾. Ако някоя организация не изпълни препоръката в срок от 25 дни след предоставянето ѝ, без да посочи убедително обяснение за закъснението, групата на ОЗД може да оповести намерението си да отнесе въпроса до ФТК (или друг орган на САЩ, компетентен да предприема действия за принудително изпълнение) или да заключи, че е допуснато сериозно нарушение на ангажмента за сътрудничество.

⁽¹¹⁷⁾ Приложение I, раздел II „Проверява[не на] изискванията за самосертифициране“.

⁽¹¹⁸⁾ Вж. приложение III, раздел „Улеснява[не на] сътрудничеството с органите за алтернативно решаване на спорове, които предоставят услуги, свързани с принципите“. Вж. също приложение I, раздел III, точка 11, буква г), подточки ii) и iii).

⁽¹¹⁹⁾ Вж. приложение I, раздел III, точка 11, буква д).

⁽¹²⁰⁾ Вж. приложение I, раздел III, точка 11, буква ж), по-специално подточки ii) и iii).

⁽¹²¹⁾ Вж. приложение III, раздел „Търсене на неверни твърдения за участие и намиране на решения“.

⁽¹²²⁾ Приложение I, раздел II, точка 7, буква б).

⁽¹²³⁾ Приложение I, раздел III, точка 5.

⁽¹²⁴⁾ Приложение I, раздел III, точка 5, буква в), подточка ii).

⁽¹²⁵⁾ Приложение III (вж. раздел „Улесняване на сътрудничеството с ОЗД“ и приложение IV (вж. раздел „Отдаване на приоритет на сезирания и разследване“ и раздел „Сътрудничество при правопрелагането с ОЗД на ЕС“).

⁽¹²⁶⁾ Правилникът за дейността на неформалната група на ОЗД следва да бъде определен от ОЗД въз основа на правомощието им да организират работата си и да си сътрудничат помежду си.

⁽¹²⁷⁾ Приложение I, раздел III, точка 5, буква в), подточка i).

При първия вариант това може да доведе до предприемане на действие по принудително изпълнение съгласно раздел 5 от Закона за Федералната търговска комисия (или други сходни закони) ⁽¹²⁸⁾. При втория вариант групата ще информира Министерството на търговията, което ще счете отказа на организацията да изпълни препоръките на групата на ОЗД за трайно неспазване на принципите, в резултат на което тази организация ще бъде заличена от списъка към РЗЛД.

- (76) Във всички разгледани случаи, ако ОЗД, до който е адресирана жалбата, не предприеме никакви действия или действията са недостатъчни за разрешаване на жалбата, жалбоподателят има възможността да заведе иск срещу това (без)действие в националните съдилища на съответната държава — членка на ЕС.
- (77) Освен това физическите лица могат да подават жалби до ОЗД дори когато за решаване на спорове не е била определена група на ОЗД. В тези случаи ОЗД може да отнася такива жалби до Министерството на търговията или ФТК. За да улесни съвместната работа, Министерството на търговията ще създаде специализирано звено за контакт, което да служи за връзка и да съдейства при запитвания от ОЗД относно спазването от страна на дадена организация на Принципиите на неприкосновеност на личния живот ⁽¹²⁹⁾. По същия начин ФТК се ангажира да създаде специално звено за контакт ⁽¹³⁰⁾.
- (78) На четвърто място, Министерството на търговията се е ангажирало да получава и разглежда жалби относно неспазването на принципите от дадена организация, както и да полага всички възможни усилия да ги разрешава ⁽¹³¹⁾. За тази цел Министерството на търговията предвижда специални процедури за отнасянето на жалбите от страна на ОЗД до определеното звено за контакт и за проследяването им, както и последващи действия съвместно с организациите за улесняване на разрешаването ⁽¹³²⁾. За да се ускори обработването на отделните жалби, звеното за връзка може да си сътрудничи директно със съответния ОЗД по въпросите относно спазването на принципите, и по специално да го уведомява за етапа на разглеждане на жалбите в срок до 90 дни след сезирането му ⁽¹³³⁾. Това позволява на субектите на данни да подават жалби относно неспазването на Принципиите от организациите, попадащи в обхвата на РЗЛД между ЕС и САЩ директно до своя национален ОЗД, след което тези жалби ще бъдат насочвани към Министерството на търговията, като органът в САЩ, управляващ Рамката за личните данни в отношенията между ЕС и САЩ.
- (79) Когато въз основа на служебните си проверки, жалби или друга информация, Министерството на търговията стигне до заключението, че дадена организация трайно не спазва принципите, то може да я заличи от списъка към РЗЛД ⁽¹³⁴⁾. Отказът да се съобрази с окончателно решение на който и да е орган за саморегулиране във връзка с неприкосновеността на личния живот, независим орган за разрешаване на спорове или правителствен орган с компетентност в областта на неприкосновеността на личния живот, включително ОЗД, ще бъде считан за трайно неспазване на принципите ⁽¹³⁵⁾.
- (80) Освен това, организация, попадаща в обхвата на РЗЛД в отношенията между ЕС и САЩ, трябва да подлежи на юрисдикцията на органите на САЩ, и по-специално ФТК ⁽¹³⁶⁾, които разполагат с необходимите правомощия за разследване и правоприлагане, за да гарантират ефективно спазването на принципите. ФТК ще разглежда с предимство случаи на неспазване на принципите, за които е била сезирана от независими инстанции за разрешаване на спорове или от органи за саморегулиране, от Министерството на търговията и от ОЗД (по тяхна собствена инициатива или след получени жалби), за да определи дали са нарушени изискванията на раздел 5 от Закона за Федералната търговска комисия (FTC Act) ⁽¹³⁷⁾. ФТК се е ангажира да създаде стандартен процес на сезиране, да определи звено за връзка в нея за сезираните от страна на ОЗД и да обменя информация относно случаите, за които е била сезирана. В допълнение тя може да приема жалби директно от физически лица и ще предприема разследвания във връзка с Рамката за личните данни по своя собствена инициатива, по-специално като част от по-мощни нейни разследвания по въпроси относно неприкосновеността на личния живот.

⁽¹²⁸⁾ Приложение I, раздел III, точка 5, буква в), подточка ii).

⁽¹²⁹⁾ Вж. приложение III, раздел „Улесняване на сътрудничеството с ОЗД“.

⁽¹³⁰⁾ Вж. приложение IV, раздел „Отдаване на приоритет на сезирания и разследване“ и „Сътрудничество при правоприлагането с ОЗД на ЕС“.

⁽¹³¹⁾ Приложение III, вж. раздел „Улесняване на сътрудничеството с ОЗД“.

⁽¹³²⁾ Приложение I, раздел II, точка 7, буква д) и приложение III, раздел „Улесняване на сътрудничеството с ОЗД“.

⁽¹³³⁾ *Пак там*.

⁽¹³⁴⁾ Приложение I, раздел III, точка 11, буква ж).

⁽¹³⁵⁾ Приложение I, раздел III, точка 11, буква ж).

⁽¹³⁶⁾ Организация, попадаща в обхвата на РЗЛД между ЕС и САЩ, трябва да обяви публично поемането на ангажимент да спазва принципите, да оповестява политиките си в областта на неприкосновеността на личния живот и да ги прилага изцяло. Неспазването подлежи на принудително изпълнение съгласно раздел 5 от Закона за Федералната търговска комисия, който забранява нечестните и измамни практики в търговията или засягащи търговията.

⁽¹³⁷⁾ Вж. също подобни ангажименти, поети от Министерството на транспорта, приложение V.

- (81) На шесто място, като механизъм за защита, който е последна възможност, в случай че жалбата на лицето не е получила удовлетворително решение посредством останалите налични средства за правна защита, субектът на данни от Съюза може да поиска въпросът да бъде решен чрез правно обвързващ арбитраж от панела по Рамката за защита на личните данни в отношенията между ЕС и САЩ ⁽¹³⁸⁾. Организацията трябва да информира физическите лица за възможността им да използват правно обвързващ арбитраж, както и са длъжни да реагират, след като дадено физическо лице е използвало тази възможност, като е изпратило уведомление на съответната организация ⁽¹³⁹⁾.
- (82) Панелът включва група от най-малко 20 арбитражи, които ще бъдат определени от Министерството на търговията и от Комисията въз основа на тяхната независимост, почтеност и опита им със законодателството на САЩ в областта на неприкосновеността на личния живот и законодателството на ЕС в областта на защитата на данните. За всеки индивидуален спор страните избират от тази група състав от един или трима ⁽¹⁴⁰⁾ арбитражи.
- (83) Международния център за разрешаване на спорове (ICDR) — международното подразделение на Американската асоциация за арбитраж (AAA), беше избран от Министерството на търговията да прилага арбитраж. Производствата пред панела по РЗЛД между ЕС и САЩ ще се уреждат от набор от договорени правила за арбитраж и кодекс за поведение на назначените арбитражи. В уебсайта на ICDR-AAA за физическите лица е предоставена ясна и кратка информация относно механизма за арбитраж и процедурата за подаване на молба за арбитраж.
- (84) Правилата за арбитраж, договорени между Министерството на търговията и Комисията, допълват РЗЛД в отношенията между ЕС и САЩ, която съдържа няколко характеристики, подобряващи степента на достъпност на този механизъм за субектите на данни от Съюза: i) при подготвянето на иск пред панела субектът на данни може да получи съдействие от своя национален ОЗД; ii) тъй като арбитражът ще се провежда в Съединените американски щати, субектите на данни от Съюза могат да изберат да участват чрез видео- или телефонна конферентна връзка, която ще се осигурява безплатно; iii) въпреки че езикът, използван в хода на арбитража, е по правило английски, устният превод в хода на арбитражното изслушване по принцип ще бъде осигурен въз основа на мотивирано искане от страна на субекта на данните без разходи за него; iv) и накрая, при все че всяка от страните трябва да поеме за своя сметка разходите за хонорара на своя адвокат, ако се представлява от такъв пред арбитражния състав, Министерството на търговията ще създаде фонд, който ще се захранва от годишни вноски на организацията — участници в РЗЛД в отношенията между ЕС и САЩ, от който ще бъдат покривани допустимите разходи по арбитражната процедура до един максимален размер, който ще бъде определен от органите на САЩ в консултация с Комисията ⁽¹⁴¹⁾.
- (85) Панелът по РЗЛД между ЕС и САЩ има правомощия да предписва специфични за конкретния случай непарични компенсации по съображения за справедливост ⁽¹⁴²⁾, необходими като корективно действие срещу неспазването на принципите. Макар че панелът взема предвид други средства за правна защита, които вече са използвани от други механизми в рамките на РЗЛД в отношенията между ЕС и САЩ, при вземането на решение лицата все пак могат да прибегнат до арбитраж, ако считат, че тези други средства за защита са недостатъчни. Това позволява на субектите на данни от Съюза да се позовават на арбитраж във всички случаи, когато действието или бездействието от страна на организацията, попадащи в обхвата на РЗЛД между ЕС и САЩ, независимите механизми за защита или компетентните органи на САЩ (например ФТК) не са разрешили по задоволителен начин техните жалби. Арбитражната инстанция не може да бъде сезирана, ако ОЗД има правните правомощия да разреши спорния иск по отношение на организацията, попадаща в обхвата на РЗЛД в отношенията между ЕС и САЩ, по-специално в случаите, когато организацията е задължена да съдейства и да спазва препоръките на ОЗД във връзка с обработването на данни за човешки ресурси, събрани в контекста на трудово правоотношение, или доброволно се е ангажирала да направи това. Физическите лица могат да приведат в изпълнение арбитражното решение в съдилищата на САЩ съгласно Федералния арбитражен закон (Federal Arbitration Act), като по този начин осигурят правно средство за защита, в случай че организацията не се съобрази с него.

⁽¹³⁸⁾ Вж. приложение I, приложение I „Модел за арбитраж“.

⁽¹³⁹⁾ Приложение I, раздел II, точка 1, буква а), подточка xi) и раздел II, точка 7, буква в).

⁽¹⁴⁰⁾ Броят на арбитражите в този панел ще се договаря между страните.

⁽¹⁴¹⁾ Приложение I от приложение I, раздел G, точка 6.

⁽¹⁴²⁾ Физическите лица не могат да предявяват иск за вреди в арбитражно дело, но иницирането на арбитражно дело не изключва възможността да се поиска обезщетение за вреди в обикновените съдилища на САЩ.

- (86) На седмо място, когато дадена организация не спазва ангажимента си да съблюдава принципите и публикуваната политика за защита на личните данни, в законодателството на САЩ са предвидени допълнителни възможности за съдебна защита, включително за получаване на обезщетение за вреди. Например при определени условия физическите лица могат да получат съдебна защита (включително обезщетение за вреди) по силата на държавните закони за защита на потребителите в случаи на въвеждане в заблуда с цел измама, неоялни или измамни действия или практики ⁽¹⁴³⁾, и по силата на деликтното право (по-специално във връзка с нахвърляване на личната сфера ⁽¹⁴⁴⁾, присвояване на името или приликата с друго лице ⁽¹⁴⁵⁾ и публикуването на факти от частния живот ⁽¹⁴⁶⁾).
- (87) Заедно посочените по-горе различни средства за правна защита гарантират, че по всяка жалба относно неспазването на РЗЛД в отношенията между ЕС и САЩ от страна на сертифицирани организации ще бъде произнесено ефективно решение и неспазването ще бъде отстранено.

3. ДОСТЪП И ИЗПОЛЗВАНЕ ОТ ПУБЛИЧНИ ОРГАНИ В СЪЕДИНЕНИТЕ ЩАТИ НА ЛИЧНИ ДАННИ, ПРЕДАДЕНИ ОТ ЕВРОПЕЙСКИЯ СЪЮЗ

- (88) Комисията извърши също така оценка на ограниченията и гаранциите, включително на предвидените от законодателство на Съединените щати механизми за надзор и индивидуална правна защита във връзка със събирането и последващото използване от публични органи на САЩ на лични данни, предадени на администратори и обработващи лични данни в САЩ в обществен интерес, по-специално за целите на прилагането на наказателното право и националната сигурност („достъп на държавните органи“) ⁽¹⁴⁷⁾. При оценката дали условията, при които достъпът на държавните органи до данни, предавани на Съединените щати съгласно настоящото решение, отговарят на критерия за „равностойност по същество“ съгласно член 45, параграф 1 от Регламент (ЕС) 2016/679, както се тълкува от Съда в светлината на Хартата на основните права, Комисията взе предвид няколко критерия.
- (89) По-специално всяко ограничаване на упражняването на правото на защита на личните данни трябва да бъде предвидено в закон, а самото правно основание, позволяващо намеса в това право, трябва да определя обхвата на ограничението при упражняване на съответното право ⁽¹⁴⁸⁾. Освен това, за да удовлетвори изискването за пропорционалност, съгласно което дерогациите и ограниченията на защитата на личните данни трябва да се въвеждат само доколкото са строго необходими в едно демократично общество, за да се постигнат конкретни цели от общ интерес, равностойни на тези, признати от Съюза, това правно основание трябва да предвижда ясни и точни правила, които да уреждат обхвата и прилагането на разглежданите мерки и да налагат минимални изисквания, така че лицата, чиито данни са били предадени, да разполагат с достатъчно гаранции, позволяващи ефективна защита на техните лични данни срещу рискове от злоупотреби ⁽¹⁴⁹⁾. Освен това тези правила и гаранции трябва да са правно

⁽¹⁴³⁾ Вж. например щатските закони за защита на потребителя в Калифорния (Civ. Code §§ 1750 - 1785 (West) Consumers Legal Remedies Act); District of Columbia (D.C. Code §§ 28-3901); Флорида (Fla. Stat. §§ 501.201 - 501.213, Deceptive and Unfair Trade Practices Act); Илинойс (815 Ill. Comp. Stat. 505/1 - 505/12, Consumer Fraud and Deceptive Business Practices Act); Пенсилвания (73 Pa. Stat. Ann. §§ 201-1 - 201-9.3 (West) Unfair Trade Practices and Consumer Protection Law).

⁽¹⁴⁴⁾ Т.е. в случай на умишлена намеса в личните дела или интереси на дадено лице по начин, който би бил силно оскърбителен за разумно лице (Restatement (2nd) of Torts, §652(b)).

⁽¹⁴⁵⁾ Това правонарушение обикновено се прилага в случай на присвояване и използване на името или на приликата с дадено лице за рекламиране на дружество или продукт, или за друга подобна търговска цел (вж. Restatement (2nd) of Torts, § 652C).

⁽¹⁴⁶⁾ Т.е. когато информация, засягаща личния живот на дадено лице, се оповестява публично, когато това е силно оскърбително за разумно лице и информацията и не се отнася за елемент от законов обществен интерес (Restatement (2nd) of Torts, §652D).

⁽¹⁴⁷⁾ Това е уместно и с оглед на раздел I.5 от приложение I. Съгласно този раздел и подобно на Общия регламент относно защитата на данните спазването на изискванията за защита на данните и правата, които са част от принципите за защита на личните данни, може да бъде предмет на ограничения. Такива ограничения обаче не са абсолютни, а могат да се налагат само при няколко условия, например до степента, необходима за спазване на съдебна заповед или удовлетворяване на изискванията на обществения интерес, правоприлагането или националната сигурност. Във връзка с това и от съображения за по-голяма яснота настоящият раздел се отнася и до условията, определени в Указ 14086, които са оценени, наред с другото, в съображения 127—141.

⁽¹⁴⁸⁾ Вж. решението по дело *Schrems II*, т. 174—175 и цитираната съдебна практика. По отношение на достъпа от страна на публични органи на държави членки вж. също решението по дело C-623/17 *Privacy International*, ECLI:EU:C:2020:790, т. 65; и решението по съединени дела C-511/18, C-512/18 и C-520/18 *La Quadrature du Net и др.* ECLI:EU:C:2020:791, т. 175.

⁽¹⁴⁹⁾ Вж. решението по дело *Schrems II*, т. 176 и 181, както и цитираната съдебна практика. По отношение на достъпа от страна на публични органи на държави членки вж. също решението по дело *Privacy International*, т. 68; и решението по дело *La Quadrature du Net и др.*, т. 132.

обвързващи и да могат да бъдат прилагани от лицата ⁽¹⁵⁰⁾. По-специално субектите на данни трябва да имат възможността да заведат дело пред независим и безпристрастен правораздавателен орган, за да получат достъп до отнасящи се до тях лични данни или да коригират или изтриват такива данни ⁽¹⁵¹⁾.

3.1 Достъп и използване от публични органи на САЩ за целите на прилагането на наказателното право

- (90) Що се отнася до намесата в лични данни, предадени съгласно РЗЛД в отношенията между ЕС и САЩ за целите на прилагането на наказателното право, законодателството на Съединените щати налага редица ограничения върху достъпа и използването на лични данни и предвижда механизми за надзор и правна защита, които са в съответствие с изискванията, посочени в съображение 89 от настоящото решение. Условието, при които може да се осъществи такъв достъп, и гаранциите, приложими за упражняването на тези правомощия, са разгледани подробно в следващите раздели. В тази връзка правителството на САЩ (чрез Министерството на правосъдието, DoJ) предостави също така уверения по отношение на приложимите ограничения и гаранции (приложение VI към настоящото решение).

3.1.1 Правни основания, ограничения и гаранции

3.1.1.1 Ограничения и гаранции по отношение на събирането на лични данни за целите на наказателното правоприлагане

- (91) До лични данни, обработвани от сертифицирани организации от САЩ, които ще бъдат предавани от Съюза въз основа на РЗЛД в отношенията между ЕС и САЩ, може да се осъществява достъп за целите на наказателното правоприлагане от федерални прокурори и федерални разследващи агенти на САЩ по различни процедури, както е обяснено по-подробно в съображения 92—99. Тези процедури се прилагат по един и същи начин, когато информацията се получава от която и да е организация от САЩ, независимо от гражданството или мястото на пребиваване на съответните субекти на данни ⁽¹⁵²⁾.
- (92) На първо място, по искане на федерално длъжностно лице в сферата на правоприлагането или на адвокат на държавата, съдия може да издаде заповед за обиск или изземване (включително на електронно съхранявана информация) ⁽¹⁵³⁾. Такава заповед може да бъде издадена само ако е налице „обосновано предположение“ ⁽¹⁵⁴⁾, че на посоченото в заповедта място има вероятност да бъдат намерени „подлежащи на изземване вещи“ (доказателства за престъпление, незаконно притежавани вещи или имущество, предназначено или използвано за извършване на престъпление). В заповедта трябва да се посочи имуществото или предметът, които трябва да бъдат иззети, и да се посочи съдията, на когото трябва да бъде върната заповедта. Физическо лице, което е обект на претърсване или чието

⁽¹⁵⁰⁾ Вж. решението по делото *Schrems II*, т. 181—182.

⁽¹⁵¹⁾ Вж. решение по дело *Schrems I*, точка 95 и решение по дело *Schrems II*, точка 194. В това отношение Съдът на Европейския съюз специално подчертава, че спазването на член 47 от Хартата на основните права, гарантиращо правото на ефективни правни средства за защита пред независим и безпристрастен съд, „също е част от изискваното ниво на защита в Съюза и [...] Комисията трябва да го констатира, преди да приеме решение относно адекватното ниво на защита съгласно член 45, параграф 1 от [Регламент (ЕС) 2016/679]“ (решение по дело *Schrems II*, т. 186).

⁽¹⁵²⁾ Вж. приложение VI. Вж. например по отношение на Закона за телефонното подслушване (*Wiretap Act*), Закона за съхраняваните съобщения (*Stored Communications Act*) и Закона за устройствата за регистриране (*Pen Register Act*) (споменати по-подробно в съображения 95—98), *Suzlon Energy Ltd/Microsoft Corp.*, 671 F.3d 726, 729 (9th Cir. 2011).

⁽¹⁵³⁾ Федерални правила относно наказателното производство, 41. През 2018 г. решението на Върховния съд потвърди също така, че се изисква правоприлагащите органи да разполагат със заповед за обиск или с извънредна заповед, за да имат достъп до хронологични записи на местоположения от базова станция, които предоставят цялостен преглед на движението на даден потребител, и че потребителят може разумно да очаква неприкосновеност на личния живот по отношение на такава информация (*Timothy Ivory Carpenter/Съединени американски щати*, № 16-402, 585 U.S. (2018)). В резултат на това такива данни по принцип не могат да бъдат получени от клетъчна компания въз основа на съдебно разпореждане при наличие на разумни основания да се счита, че информацията е важна и съществена за текущо наказателно разследване, а е необходимо, когато се използва съдебна заповед, да се докаже наличието на обосновано предположение.

⁽¹⁵⁴⁾ Според Върховния съд „обоснованото предположение“ съставлява „практически, а не технически“ стандарт, който се основава на „фактическите и практическите съображения от ежедневието, въз основа на които действат разумните и предпазливи хора [...]“ (*Illinois/Gates*, 462 U.S. 213, 232 (1983)). Що се отнася до заповедите за обиск, обосновано предположение е налице, когато има голяма вероятност претърсването да доведе до откриване на доказателства за престъпление (*id.*).

имущество е обект на претърсване, може да предприеме действия за спиране разглеждането на доказателства, получени чрез неправилен обиск, ако тези доказателства са представени срещу това физическо лице по време на наказателно производство ⁽¹⁵⁵⁾. Когато от притежател на данни (например дружество) се изисква да разкрие данни съгласно заповед, той може по-специално да оспори изискването за разкриване като неоправдано обременително ⁽¹⁵⁶⁾.

- (93) На второ място, призовка може да бъде издадена от големия състав съдебни заседатели (разследващо звено на съда, съставено от съдия или магистрат) в контекста на разследвания на определени тежки престъпления ⁽¹⁵⁷⁾, обикновено по искане на федерален прокурор, за да се изиска от някого да представи или предостави търговска информация, данни, съхранявани в електронна форма, или други материали. Освен това различни закони предоставят правомощия за използването на административни призовки за извличане или предоставяне на разположение на търговска информация, данни, съхранявани в електронна форма, или други материали по разследвания за измами в здравеопазването, малтретиране на деца, защита на тайните служби, по дела за контролирани вещества и в разследвания на главни инспектори ⁽¹⁵⁸⁾. И в двата случая информацията трябва да е от значение за разследването и призовката не може да бъде необоснована, т.е. прекомерна, налагаща принуда или обременяваща (и може да бъде оспорена от получателя на призовката на тези основания) ⁽¹⁵⁹⁾.
- (94) Много сходни условия се прилагат за административните призовки, издавани с цел получаване на граждански или регулаторен („правоприлагане в обществен интерес“) достъп до данни, с които разполагат дружествата в САЩ. Правомощията на институциите, които имат гражданскоправни и регулаторни отговорности да издават такива административни призовки, трябва да бъдат установени в закон. Използването на административна призовка подлежи на „тест за разумност“, съгласно който се изисква провеждането на разследването да е в съответствие със законна цел, поисканата с призовката информация да е уместна за тази цел, търсената с призовката информация все още да не е на разположение на институцията и да се следват необходимите административни стъпки за издаване на призовката ⁽¹⁶⁰⁾. В съдебната практика на Върховния съд се разяснява също така необходимостта от постигането на баланс между значението на обществения интерес към поисканата информация и значението на личните и организационните интереси към неприкосновеността на личния живот ⁽¹⁶¹⁾. Макар че използването на административна призовка не подлежи на предварително съдебно одобрение, тя е предмет на съдебен контрол в случай на оспорване от страна на получателя на горепосочените основания или ако издаващата институция иска да изпълни призовката в съда ⁽¹⁶²⁾. В допълнение към тези общи главни ограничения, съгласно отделните закони могат да се налагат по-специфични (по-строги) изисквания ⁽¹⁶³⁾.

⁽¹⁵⁵⁾ Вж. дело *Mapp/Ohayo*, 367 U.S. 643 (1961).

⁽¹⁵⁶⁾ Вж. *In re Application of United States*, 610 F.2d 1148, 1157 (3d Cir.1979 г.) (в което се постановява, че „належащото провеждане на съдебния процес изисква изслушване по въпроса за тежестта, преди да се принуди телефонната компания да предостави“ съдействие за издаване на заповед за обиск) и *In re Application of United States*, 616 F.2d 1122 (9th Cir. 1980).

⁽¹⁵⁷⁾ Петата поправка на Конституцията на САЩ изисква големият състав съдебни заседатели да повдигне обвинение за всяко „углавно или друго позорно престъпление“. Големият състав съдебни заседатели се състои от 16 до 23 члена и определя дали е налице обосновано предположение да се смята, че е извършено престъпление. За да стигнат до това заключение, големите състави от съдебни заседатели разполагат с разследващи правомощия, които им позволяват да издават призовки.

⁽¹⁵⁸⁾ Вж. приложение VI.

⁽¹⁵⁹⁾ Федерални правила относно наказателното производство, 17.

⁽¹⁶⁰⁾ *United States/Powell*, 379 U.S. 48 (1964).

⁽¹⁶¹⁾ *Oklahoma Press Publishing Co./Walling*, 327 U.S. 186 (1946).

⁽¹⁶²⁾ Върховният съд поясни, че в случай на оспорване на административна призовка, съдът трябва да прецени дали 1) разследването касае законно разрешена цел, 2) въпросният орган, който трябва да издаде призовката, попада в обхвата на управленските правомощия на Конгрес и 3) „търсените документи са от значение за разследването“. Съдът отбелязва също така, че искането за административна призовка трябва да е „разумно“, т.е. да се изисква „адекватно, но не прекомерно уточняване на документите, които трябва да бъдат представени за целите на съответното разследване“, включително „особености при „описване на мястото, което ще бъде претърсено, и лицата или вещите, които ще бъдат иззети“.

⁽¹⁶³⁾ Например със Закона за правото на неприкосновеност на личните финанси на държавен орган се предоставя правомощието да получава финансови документи, които са на разположение на финансова институция по силата на административна призовка, само ако 1) е налице основание да се счита, че исканите документи са от значение за законово разследване във връзка с правоприлагането и 2) копия от призовката или призовките е предоставено на потребителя заедно с известие, в което в разумна степен се посочва спецификата на естеството на разследването (12 U.S.C., §3405). Друг пример е Законът за оповестяване на информация за кредити, с който на агенциите за събиране на информация за потребителите се забранява да оповестяват документи на потребителите в отговор на искания за административна призовка (като единствено им се позволява да отговорят на искания за призовка на големия състав съдебни заседатели или съдебни разпореждания, 15 U.S.C., §1681 и следв.). По отношение на достъпа до комуникационна информация се прилагат специфичните изисквания на Закона за съхраняваните съобщения, включително по отношение на възможността за използване на административни призовки (за по-подробен преглед вж. съображения 96—97).

- (95) На трето място, няколко правни основания дават възможност на органите по наказателно правоприлагане да получат достъп до далекосъобщителни данни. Съдът може да издаде заповед, с която се разрешава събирането в реално време на информация без съществено съдържание във връзка с избиране, направление, адресиране и радиоелектронна информация относно даден телефонен номер или електронна поща (чрез използване на устройства за регистриране и проследяване), ако установи, че органът е удостоверил, че информацията, която може да бъде получена, е от значение за висящо наказателно разследване ⁽¹⁶⁴⁾. В заповедта трябва, *inter alia*, да се посочат самоличността на заподозрения, ако тя е известна; атрибутите на съобщенията, за които се прилага, и описание на престъплението, за което се отнася информацията, която ще се събира. Използването на електронни устройства за регистриране или проследяване може да бъде разрешено за максимален срок от шестдесет дни, който може да бъде удължен само с ново съдебно разпореждане.
- (96) Освен това достъп за целите на наказателното правоприлагане до информация за абонатите, данни за трафика и съхранено съдържание на разговори и съобщения, с които разполагат доставчиците на интернет услуги, телефонните дружества и други доставчици на услуги — трети страни, може да бъде получен въз основа на Закона за съхраняваните съобщения ⁽¹⁶⁵⁾. За да се сподият със съхраненото съдържание на електронни съобщения, органите по наказателно правоприлагане трябва по принцип да получат разпореждане от съдия на основание обосновано предположение, поради което се счита, че въпросният профил съдържа доказателства за извършено престъпление ⁽¹⁶⁶⁾. За целите на наказателното правоприлагане органите могат да използват призовка, за да се сподият с информация за регистрация на потребители, IP адреси и съответните удостоверения за време, както и информация за разплащането. За повечето друга съхранявана информация, която не се отнася за съдържание, като например заглавията на имейли без реда на темата, органът по наказателно правоприлагане трябва да получи съдебно разпореждане, което се издава, ако съдията е убеден, че има разумни основания да се счита, че исканата информация е важна и съществена за текущо наказателно разследване.
- (97) Доставчиците, които получават искания по Закона за съхраняваните съобщения, могат доброволно да уведомят клиента или абоната, чиято информация се изисква, освен в случаите, когато съответният орган по наказателно правоприлагане получи обезпечителна заповед, забраняваща подобно уведомяване ⁽¹⁶⁷⁾. Тази обезпечителна заповед представлява съдебно разпореждане, с което се изисква доставчикът на електронни съобщителни услуги или отдалечени изчислителни услуги, към когото е насочена заповед, призовка или съдебно разпореждане, да не уведомява никое друго лице за съществуването на заповедта, призовката или съдебното разпореждане толкова дълго, колкото съдът счете за необходимо. Обезпечителни заповеди се издават, ако съдът прецени, че има основание да се счита, че уведомяването би застрашило сериозно разследването или неоправдано би забавило съдебния процес, например защото би могло да доведе до застрашаване на живота или физическата безопасност на дадено физическо лице, бягство от наказателно преследване, сплашване на потенциални свидетели и др. С меморандум на заместник-министъра на правосъдието (който е задължителен за всички прокурори и представители на Министерството на правосъдието) от прокурорите се изисква да направят подробна преценка по отношение на необходимостта от издаване на обезпечителна заповед и да представят пред съда обосновка за това как в конкретния случай са изпълнени законовите критерии за получаване на обезпечителна заповед ⁽¹⁶⁸⁾. В меморандума се изисква също така в молбите за издаване на обезпечителни заповеди по принцип да не се иска отлагане на уведомяването за повече от една година. Когато при изключителни обстоятелства може да се наложи издаването на заповеди с по-дълъг срок, такива заповеди могат да бъдат заявявани само с писменото съгласие на надзорния орган, определен от министъра на правосъдието на САЩ или съответния заместник-министър на правосъдието. Освен това при приключване на разследването прокурорът трябва незабавно да прецени дали е налице основание за запазване на действието на неизтеклите обезпечителни заповеди и ако това не е така, да прекрати обезпечителната заповед и да гарантира, че доставчикът на услуги е уведомен за това ⁽¹⁶⁹⁾.

⁽¹⁶⁴⁾ 18 U.S.C. § 3123.

⁽¹⁶⁵⁾ 18 U.S.C. §§ 2701-2713.

⁽¹⁶⁶⁾ 18 U.S.C. §§ 2701(a)-(b)(1)(A). Ако съответният абонат или клиент е уведомен (предварително или, при определени обстоятелства, чрез забавено уведомяване), информацията за съдържанието, съхранявана за повече от 180 дни, може да бъде получена и въз основа на административна призовка или призовка от големия състав съдебни заседатели (18 U.S.C. §§ 2701(b)(1)(B) или въз основа на съдебно разпореждане (при наличие на разумни основания да се счита, че информацията е от значение и е съществена за текущо наказателно разследване (18 U.S.C. §§ 2701(d)). В съответствие с решение на федерален апелативен съд обаче правителствените следователи обикновено получават заповед за обиск от съдии, за да съберат информация за съдържанието на частни съобщения или съхранени данни от търговски доставчик на далекосъобщителни услуги. *United States срещу Warshak*, 631 F.3d 266 (6th Cir. 2010).

⁽¹⁶⁷⁾ 18 U.S.C. § 2705(b).

⁽¹⁶⁸⁾ Вж. меморандума, издаден от заместник-министъра на правосъдието Род Розеншайн на 19 октомври 2017 г. относно по-рестриктивната политика по отношение на молбите за издаване на обезпечителни заповеди (или разпореждания за неразкриване на информация), достъпен на адрес <https://www.justice.gov/criminal-ccips/page/file/1005791/download>.

⁽¹⁶⁹⁾ Меморандум, издаден от заместник-министъра на правосъдието Lisa Monaco на 27 май 2022 г., относно допълнителна политика по отношение на молбите за издаване на обезпечителни заповеди съгласно 18 U.S.C., §2705(b).

- (98) Органите по наказателно правоприлагане могат също така да прихващат в реално време кабелни, устни или електронни комуникации въз основа на съдебно разпореждане, в което съдията установява, *inter alia*, че има обосновано предположение да се смята, че подслушването или прихващането на електронни съобщения ще осигурят доказателства за престъпление срещу федералните закони или информация за местонахождението на лице, укриващо се с цел избягване на наказателна отговорност ⁽¹⁷⁰⁾.
- (99) Допълнителна защита се осигурява от различни политики и насоки на Министерството на правосъдието, включително Насоките на министъра на правосъдието за вътрешните операции на ФБР (AGG-DOM), в които, наред с другото, се изисква Федералното бюро за разследвания (ФБР) да използва методи за разследване с най-ниска възможна степен на вмешателство, като взема предвид въздействието върху неприкосновеността на личния живот и гражданските свободи ⁽¹⁷¹⁾.
- (100) Съгласно писмените изявления на правителството на САЩ за разследванията за целите на правоприлагането на държавно равнище (по отношение на разследванията, които се извършват в съответствие с федералните закони) се прилага същата или по-висока степен на защита, като описаната по-горе ⁽¹⁷²⁾. По-конкретно, конституционните разпоредби, както и законите и съдебната практика на държавно равнище потвърждават горепосочените защити срещу необосновани претърсвания и изземвания, като изискват издаването на заповед за обиск ⁽¹⁷³⁾. Подобно на защитите, предоставени на федерално равнище, заповедите за обиск могат да бъдат издадени само при доказване на обосновано предположение и трябва да описват мястото, което ще бъде претърсено, и лицето или предмета, който трябва да бъде иззет ⁽¹⁷⁴⁾.

⁽¹⁷⁰⁾ 18 U.S.C. §§ 2510-2522.

⁽¹⁷¹⁾ Насоки на министъра на правосъдието за вътрешните операции на Федералното бюро за разследвания (ФБР) (Attorney General's Guidelines for Domestic Federal Bureau of Investigation (FBI) Operations) (септември 2008 г.), достъпни на адрес: <http://www.justice.gov/archive/opa/docs/guidelines.pdf>. Допълнителни правила и политики, с които се предвиждат ограничения за разследващите дейности на федералните прокурори, са определени в Наръчника на прокурорите в Съединените щати (United States Attorneys' Manual), на разположение на адрес <http://www.justice.gov/usam/united-states-attorneys-manual>. За да се допусне отклоняване от тези насоки, трябва да се получи предварително одобрение от директора, или заместник-директора на ФБР или изпълнителния помощник-директор на ФБР, определен от директора, освен ако такова одобрение не може да бъде получено поради непосредствеността или сериозността на заплахата за безопасността на хората или имуществото или за националната сигурност (в този случай директорът или друго упълномощено лице трябва да бъде уведомено възможно най-скоро). Когато насоките не се спазват, ФБР трябва да уведоми за това Министерството на правосъдието, което от своя страна трябва да информира министъра на правосъдието и заместник-министъра на правосъдието.

⁽¹⁷²⁾ Приложение VI, бележка под линия 2. Вж. също например *Arnold/City of Cleveland*, 67 Ohio St.3d 35, 616 N.E.2d 163, 169 (1993 г.) („По отношение на областите на индивидуалните права и гражданските свободи, в Конституцията на Съединените щати, когато е приложима за отделните щати, се предвижда праг, който трябва да се спазва в решенията на щатските съдилища“); *Cooper/California*, 386 U.S. 58, 62, 87 S.Ct. 788, 17 L.Ed.2d 730 (1967 г.) („Нашето участие, разбира се, не засяга правомощията на държавата да налага по-високи стандарти за претърсвания и изземвания от изискваните от федералната конституция, в случай че реши да го направи“); *Petersen/City of Mesa*, 63 P.3d 309, 312 (Ariz. Ct. App. 2003 г.) („Въпреки че с конституцията на Аризона може да се налагат по-строги стандарти за претърсвания и изземвания, отколкото с федералната конституция, съдилищата на Аризона не могат да предоставят по-малка степен на защита от предоставяната с Четвъртата поправка“).

⁽¹⁷³⁾ Повечето щати са възприели предоставяната съгласно Четвъртата поправка защита в своите конституции. Вж. конституция на Алабама, член I, § 5; конституция на Аляска, член I, § 14; 1; конституция на Арканзас, член II, § 15; конституция на Калифорния, член I, § 13; конституция на Колорадо, член II, § 7; конституция на Конектикут, член I, § 7; конституция на Делауеър, член I, § 6; конституция на Флорида, член I, § 12; конституция на Джорджия, член I, § I, параг. XIII; конституция на Хавай, член I, § 7; конституция на Айдахо, член I, § 17; конституция на Илинойс, член I, § 6; конституция на Индиана, член I, § 11; конституция на Айова, член I, § 8; конституция на Канзас Bill of Rights (Декларация за правата), § 15; конституция на Кентъки § 10; конституция на Луизиана, член I, § 5; конституция на Мейн, член I, § 5; конституция на Масачузетс, Декларация за правата, член 14; конституция на Мичиган, член I, § 11; конституция на Минесота, член I, § 10; конституция на Мисисипи, член III, § 23; конституция на Мисури, член I, § 15; конституция на Монтана, член II, § 11; конституция на Небраска, член I, § 7; конституция на Невада, член I, § 18; конституция на Ню Хампшър, част 1, член 19; конституция на Ню Джърси, член II, § 7; конституция на Ню Мексико, член II, § 10; конституция на Ню Йорк, член I, § 12; конституция на Северна Дакота, член I, § 8; конституция на Охайо, член I, § 14; конституция на Оклахома, член II, § 30; конституция на Орегон, член I, § 9; конституция на Пенсилвания, член I, § 8; конституция на Роуд Айлънд, член I, § 6; конституция на Южна Каролина, член I, § 10; конституция на Южна Дакота, член VI, § 11; конституция на Тенеси, член I, § 7; конституция на Тексас, член I, § 9; конституция на Юта, член I, § 14; конституция на Вермонт, част I, член 11; конституция на Западна Вирджиния, член III, § 6; конституция на Уисконсин, член I, § 11; конституция на Уайоминг, член I, § 4. Други (например Мериленд, Северна Каролина и Вирджиния) са заложили в своите конституции конкретен текст относно заповедите, който е тълкуван от съда с цел да се предостави защита, която е подобна или по-висока от предоставяната с Четвъртата поправка (вж. Декларация за правата на Мериленд член 26; конституция на Северна Каролина, член I, § 20; конституция на Вирджиния, член I, § 10, и съответната съдебна практика, например *Hamel/State*, 943 A.2d 686, 701 (Md. Ct. Spec. App. 2008; *State/Johnson*, 861 S.E.2d 474, 483 (N.C. 2021 г.) и *Lowe/Commonwealth*, 337 S.E.2d 273, 274 (Va. 1985 г.) Накрая, Аризона и Вашингтон разполагат с конституционни разпоредби, с които се осигурява по-обща защита на неприкосновеността на личния живот (конституция на Аризона, член 2, § 8; конституция на Вашингтон, член I, § 7), които са тълкувани от съда с цел да се предостави по-висока степен на защита от предоставяната с Четвъртата поправка (вж. например *State/Bolt*, 689 P.2d 519, 523 (Ariz. 1984), *State/Ault*, 759 P.2d 1320, 1324 (Ariz. 1988), *State/Myrick*, 102 Wn.2d 506, 511, 688 P.2d 151, 155 (1984), *State/Young*, 123 Wn.2d 173, 178, 867 P.2d 593, 598 (1994)).

⁽¹⁷⁴⁾ Вж. например Наказателен кодекс на Калифорния (California Penal Code, § 1524,3(b); правило 3.6-3.13 от наказателнопроцесуални норми на Алабама; член 10.79.035; Измененият кодекс на Вашингтон; член 19.2-59 от глава 5, дял 19.2 от Наказателно-процесуалния кодекс на Вирджиния.

3.1.1.2 По-нататъшно използване на събраната информация

- (101) Що се отнася до по-нататъшното използване на данните, събирани от федералните органи по наказателно правоприлагане, с различни закони, насоки и стандарти се налагат специфични предпазни мерки. С изключение на специфичните инструменти, приложими по отношение на дейностите на ФБР (AGG-DOM и Ръководство за национални оперативни дейности и разследвания на ФБР), описаните в настоящия раздел изисквания обикновено се прилагат за по-нататъшното използване на данни от всеки федерален орган, включително на данните, до които се предоставя достъп за гражданскоправни или регулаторни цели. Това включва изискванията, произтичащи от меморандумите/разпоредбите на Службата за управление и бюджет, Федералният закон за модернизация на управлението на информационната сигурност, Законът за електронното правителство и Законът за федералните архиви.
- (102) В съответствие с правомощията, предоставени от Закона Clinger-Cohen (P.L. 104—106, раздел E) и Закона за компютърната сигурност от 1987 г. (P.L. 100—235), Службата за управление и бюджет (OMB) издаде Циркулярно писмо № A-130, за да установи общи задължителни насоки, които се прилагат за всички федерални агенции (включително правоприлагащите органи), когато боравят с информация за самоличността⁽¹⁷⁵⁾. По-специално, циркулярното писмо изисква от всички федерални агенции да „ограничат създаването, събирането, използването, обработването, съхранението, поддържането, разпространението и разкриването на информация за самоличността до тази, която е законно разрешена, релевантна и разумно считана за необходима за правилното изпълнение на разрешените функции на агенцията“⁽¹⁷⁶⁾. Освен това, доколкото това е разумно осъществимо, федералните агенции трябва да гарантират, че информацията за самоличността е точна, релевантна, навременна и пълна и е сведена до минимума, необходим за правилното изпълнение на функциите на агенцията. В по-общ план федералните агенции трябва да създадат цялостна програма за защита на личните данни, за да гарантират спазването на приложимите изисквания за защита на личните данни, да разработват и оценяват политики за защита на личните данни и да управляват рисковете, свързани със защитата на личните данни; да поддържат процедури за откриване, документиране и докладване на инциденти, свързани със спазването на поверителността; да разработват програми за повишаване на осведомеността относно неприкосновеността на личния живот и програми за обучение на служителите и изпълнителите; и да въвеждат политики и процедури, за да гарантират, че персоналът носи отговорност за спазването на изискванията и политиките в областта на неприкосновеността на личния живот⁽¹⁷⁷⁾.
- (103) Освен това съгласно Закона за електронното правителство⁽¹⁷⁸⁾ от всички федерални агенции (включително от органите по наказателно правоприлагане) се изисква да въведат защити за сигурността на информацията, които са съизмерими с риска и размера на вредите, които биха възникнали в резултат на непозволен достъп, използване, разкриване, прекъсване, промяна или унищожаване; да имат главен служител по въпросите на информацията, който да гарантира спазването на изискванията за информационна сигурност, и да извършват годишна независима оценка (например от генерален инспектор, вж. съображение 109) на програмата и практиките си за информационна сигурност⁽¹⁷⁹⁾. По подобен начин съгласно Закона за федералните архиви (Federal Records Act — FRA)⁽¹⁸⁰⁾ и допълнителните разпоредби⁽¹⁸¹⁾ се изисква информацията, съхранявана от федералните агенции, да подлежи на предпазни мерки, гарантиращи физическата цялост на информацията и защитата ѝ от непозволен достъп.
- (104) Съгласно федералните законови правомощия, включително Закона за модернизиране на федералната информационна сигурност от 2014 г., OMB и Националният институт по стандарти и технологии (NIST) са разработили стандарти, които са задължителни за федералните агенции (включително за органите по наказателно правоприлагане) и които допълнително уточняват минималните изисквания за информационна сигурност, които трябва да бъдат въведени, включително контрол на достъпа, осигуряване на осведоменост и обучение, планиране на действия при извънредни ситуации, реагиране на инциденти, инструменти за одит и отчетност, осигуряване на целостта на системата и информацията, извършване на оценки на риска за неприкосновеността на личния живот и сигурността и т.н.⁽¹⁸²⁾.

⁽¹⁷⁵⁾ Т.е. „информация, която може да бъде използвана за разграничаване или проследяване на самоличността на дадено лице, самостоятелно или в комбинация с друга информация, която е свързана или може да бъде свързана с конкретно лице“, вж. Циркулярно писмо на OMB № A-130, стр. 33 (определение на „информация за самоличността“).

⁽¹⁷⁶⁾ OMB Circular No. A-130, Managing Information as a Strategic Resource, Appendix II, Responsibilities for Managing Personally Identifiable Information, 81 Fed. Reg. 49,689 (Циркулярно писмо на OMB № A-130, Боравене с информация като стратегически ресурс, допълнение II, Отговорности при боравенето с информация за самоличността, 81 Fed. Reg. 49,689 (28 юли 2016 г.), стр. 17.

⁽¹⁷⁷⁾ Допълнение II, §5(a)—(h).

⁽¹⁷⁸⁾ 44 U.S.C. глава 36.

⁽¹⁷⁹⁾ 44 U.S.C. §§ 3544-3545.

⁽¹⁸⁰⁾ FAC, 44 U.S.C. § 3105.

⁽¹⁸¹⁾ 36 C.F.R. §§ 1228,150, и следв., 1228,228, и допълнение A.

⁽¹⁸²⁾ Вж. например Циркулярно писмо на OMB № A-130; NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations (Контрол на сигурността и неприкосновеността на личния живот за информационни системи и организации) (10 декември 2020 г.) и NIST Federal Information Processing Standards 200: Minimum Security Requirements for Federal Information and Information Systems (Федералните стандарти за обработване на информация на NIST 200: Минимални изисквания за сигурност на федералната информация и информационни системи).

Освен това всички федерални агенции (включително органите по наказателно правоприлагане) трябва, в съответствие с насоките на OMB, да поддържат и прилагат план за справяне с нарушения на сигурността на данните, включително когато става въпрос за реагиране при такива нарушения и оценка на рисковете от вреди ⁽¹⁸³⁾.

- (105) Що се отнася до съхраняването на данни, FRA ⁽¹⁸⁴⁾ изисква от федералните агенции на САЩ (включително органите по наказателно правоприлагане) да определят срокове за съхранение на своите записи (след което тези записи трябва да бъдат унищожени), които трябва да бъдат одобрени от Националната администрация на архивите и документите (National Archives and Record Administration) ⁽¹⁸⁵⁾. Продължителността на този период на съхранение се определя в зависимост от различни фактори, като например вида на разследването, това дали доказателствата все още са от значение за разследването и др. По отношение на ФБР в AGG-DOM се предвижда, че ФБР трябва да разполага с такъв план за съхранение на документи и да поддържа система, която може бързо да извлича информация относно състоянието и основанията на разследванията.
- (106) И накрая, Циркулярно писмо на OMB № A-130 също съдържа определени изисквания относно разпространяването на информация за самоличността. По принцип разпространението и разкриването на информация за самоличността трябва да бъде ограничено до тази, която е законно разрешена, релевантна и разумно считана за необходима за правилното изпълнение на функциите на агенцията ⁽¹⁸⁶⁾. Когато споделят информация за самоличността с други държавни органи федералните агенции на САЩ трябва да налагат, когато е уместно, условия (включително прилагането на конкретни мерки за сигурност и защита на личните данни), които уреждат обработването на информацията, чрез писмени споразумения (включително договори, споразумения за използване на данни, споразумения за обмен на информация и меморандуми за разбирателство) ⁽¹⁸⁷⁾. Що се отнася до основанията, на които информацията може да бъде разпространявана, в AGG-DOM и в Ръководството за национални оперативни дейности и разследвания на ФБР (FBI Domestic Investigations and Operations Guide (DIOG)) ⁽¹⁸⁸⁾ се предвижда например, че ФБР може да бъде подвластно на законово задължение да извършва това (например съгласно международно споразумение) или има право да разпространява информация при определени обстоятелства, например на други агенции на САЩ, ако разкриването е съвместимо с целта, за която е събрана информацията, и е свързано с техните отговорности; комисиите на Конгреса; до чуждестранни агенции, ако информацията е свързана с техните отговорности и разпространението е в съответствие с интересите на Съединените щати; ако разпространението е особено необходимо за защита на безопасността или сигурността на хората или имуществото, или за защита срещу или предотвратяване на престъпления или заплаха за националната сигурност и разкриването е съвместимо с целите, за които е събрана информацията ⁽¹⁸⁹⁾.

3.1.2 Надзор

- (107) Дейността на федералните агенции по наказателно правоприлагане подлежи на надзор от различни органи ⁽¹⁹⁰⁾. Както е обяснено в съображения 92—99, в повечето случаи това включва предварителен надзор от съдебната власт, която трябва да разреши индивидуални мерки за събиране, преди те да могат да бъдат използвани. Освен това други органи наблюдават различни етапи от дейността на органите по наказателно правоприлагане, включително събирането и обработването на лични данни. Заедно тези съдебни и несъдебни органи гарантират, че правоприлагащите органи са обект на независим надзор.

⁽¹⁸³⁾ Меморандум 17-12, Preparing for and Responding to a Breach of Personally Identifiable Information („Подготовка и реагиране при нарушаване на сигурността на информация за самоличността“), достъпен на адрес: https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf, и Циркулярно писмо на OMB № A-130. Например процедурите за отговор при нарушения на сигурността на данните на Министерството на правосъдието, вж. <https://www.justice.gov/file/4336/download>.

⁽¹⁸⁴⁾ FRA, 44 U.S.C. §§ 3101 и следв.

⁽¹⁸⁵⁾ Националната администрация на архивите и документите има правомощия да оценява практиките на агенциите за управление на записите и може да определя дали продължаването на съхранението на определени записи е оправдано (44 U.S.C., §§ 2904(c), 2906).

⁽¹⁸⁶⁾ Циркулярно писмо на OMB № A-130, раздел 5.f.1.(d)

⁽¹⁸⁷⁾ Циркулярно писмо на OMB № A-130, допълнение I, § 3(d).

⁽¹⁸⁸⁾ Вж. също Ръководство за национални оперативни дейности и разследвания на ФБР (FBI Domestic Investigations and Operations Guide (DIOG)), раздел 14.

⁽¹⁸⁹⁾ AGG-DOM, раздел VI, букви Б и В; Ръководство за национални оперативни дейности и разследвания на ФБР (DIOG), раздел 14.

⁽¹⁹⁰⁾ Посочените в настоящия раздел механизми се прилагат и по отношение на събирането и използването на данни от федералните органи за граждански и регулаторни цели. Федералните граждански и регулаторни агенции подлежат на проверка от съответните им главни инспектори и върху тях се упражнява надзор от страна на Конгреса, включително Правителствената одитна служба, Агенцията за одит и разследване на Конгреса. Освен ако агенцията има назначен служител по въпросите на неприкосновеността на личния живот и гражданските свободи — длъжност, която обикновено се среща в агенциите, като Министерството на правосъдието и Министерството на вътрешната сигурност (DHS) поради техните отговорности в областта на правоприлагането и националната сигурност — тези задължения попадат в обхвата на старши служителя на агенцията по въпросите на неприкосновеността на личния живот (SAOP). Всички федерални агенции са задължени по закон да определят SAOP, който носи отговорност за спазването от страна на агенцията на законите в областта на неприкосновеността на личния живот и наблюдава свързаните с това въпроси. Вж. например, OMB M-16-24, Role and Designation of Senior Agency Officials for Privacy (Роля и определяне на старши служители по въпросите на неприкосновеността на личния живот) (2016 г.).

- (108) На първо място, в рамките на различни отдели съществуват служители по въпросите на неприкосновеността на личния живот и гражданските свободи с правомощия в областта на наказателното правоприлагане ⁽¹⁹¹⁾. Въпреки че конкретните правомощия на тези служители може да се различават в известна степен в зависимост от законното основание за оправомощаването им, обикновено в тях се включва надзорът на процедурите с цел да се гарантира, че съответното министерство/агенция спазва по адекватен начин изискванията за неприкосновеност на личния живот и гражданските свободи и е въвело подходящи процедури за разглеждане на жалби от лица, които са счели, че неприкосновеността на личния им живот или гражданските им свободи са били нарушени. Ръководителите на всяко министерство или агенция трябва да гарантират, че служителите по въпросите на неприкосновеността на личния живот и гражданските свободи разполагат с материалите и ресурсите, необходими за изпълнение на мандата им, че им се предоставя достъп до всички материали и персонал, необходими за изпълнение на функциите им, и че са информирани за предложените промени в политиката и с тях се провеждат консултации ⁽¹⁹²⁾. Служителите по въпросите на неприкосновеността на личния живот и гражданските свободи периодично докладват пред Конгреса, включително за броя и характера на получените в министерството/агенцията жалби, и представят обобщение на разпорежданията по тези жалби, проведените проверки и разследвания и последиците от дейностите, извършени от служителя ⁽¹⁹³⁾.
- (109) На второ място, независим главен инспектор наблюдава дейността на Министерството на правосъдието, включително на ФБР ⁽¹⁹⁴⁾. Главните инспектори са независими по закон ⁽¹⁹⁵⁾ и отговарят за провеждането на независими разследвания, одити и инспекции на програмите и операциите на министерството. Те имат правомощия за достъп до всички записи, доклади, одити, прегледи, документи, писмени материали, препоръки или други съответни материали, ако е необходимо, чрез връчване на призовка, и могат да събират показания ⁽¹⁹⁶⁾. Докато главните инспектори могат да издават препоръки за корективни мерки с необвързващ характер, техните доклади, включително относно последващите действия (или липсата на такива) ⁽¹⁹⁷⁾, обикновено се оповестяват публично и се изпращат на Конгреса, който на тази основа може да упражни надзорните си функции (вж. съображение 111) ⁽¹⁹⁸⁾.

⁽¹⁹¹⁾ Вж. 42 U.S.C., § 2000ee-1. Това включва например Министерството на правосъдието, Министерството на вътрешната сигурност и ФБР. Освен това в Министерството на вътрешната сигурност (DHS) има главен служител по въпросите на неприкосновеността на личния живот, който отговаря за запазването и укрепването на защитата на личния живот и насърчването на прозрачността в рамките на министерството (6 U.S.C. 142, член 222) Всички системи, технологии, формуляри и програми на DHS, с които се събират лични данни или се оказва въздействие върху неприкосновеността на личния живот, подлежат на надзор от страна на главния служител по въпросите на неприкосновеността на личния живот, който има достъп до всички записи, доклади, одити, прегледи, документи, книжа, препоръки и други материали, с които разполага министерството, при необходимост и чрез връчване на призовка. Служителят по въпросите на неприкосновеността на личния живот трябва ежегодно да докладва пред Конгреса за дейностите на министерството, които засягат неприкосновеността на личния живот, включително жалбите за нарушения на неприкосновеността на личния живот.

⁽¹⁹²⁾ 42 U.S.C. § 2000ee-1(d).

⁽¹⁹³⁾ Вж. 42 U.S.C. §§ 2000ee-1 (f)(1)-(2). Например докладът на главния служител по въпросите на неприкосновеността на личния живот и гражданските свободи на Министерството на правосъдието и на Службата за неприкосновеността на личния живот и гражданските свободи, обхващащ периода октомври 2020 г. — март 2021 г., показва, че са извършени 389 прегледа на неприкосновеността на личния живот, включително на информационни системи и други програми (https://www.justice.gov/d9/pages/attachments/2021/05/10/2021-4-21opclsection803reportfy20sa1_final.pdf).

⁽¹⁹⁴⁾ По подобен начин със Закона за националната сигурност от 2002 г. беше създадена Служба главния генералния инспектор към Министерството на вътрешната сигурност.

⁽¹⁹⁵⁾ Главните инспектори са с постоянно назначение и могат да бъдат отстранени от длъжност само от президента, който трябва да информира Конгреса писмено относно причините за отстраняването.

⁽¹⁹⁶⁾ Вж. Закона за главния инспектор от 1978 г., § 6.

⁽¹⁹⁷⁾ Вж. в тази връзка например прегледа, изготвен от Службата на главния инспектор към Министерството на правосъдието, на направените от него препоръки и степента, в която те са изпълнени чрез последващи действия на отдела и агенцията, <https://oig.justice.gov/sites/default/files/reports/22-043.pdf>.

⁽¹⁹⁸⁾ Вж. Закона за главния инспектор от 1978 г., §§ 4(5), 5. Например Службата на главния инспектор към Министерството на правосъдието наскоро публикува своя шестмесечен доклад до Конгреса (1 октомври 2021 г. — 31 март 2022 г., <https://oig.justice.gov/node/23596>), в който се прави преглед на одитите, оценките, инспекциите, специалните прегледи и разследванията на програмите и операциите на Министерството на правосъдието. Тези дейности включваха разследване на бивш изпълнител във връзка с незаконно разкриване на електронно наблюдение (подслушване на физическо лице) в рамките на текущо разследване, което доведе до осъждането на изпълнителя. Службата на главния инспектор проведе и разследване на програмите и практиките за информационна сигурност на агенциите към Министерството на правосъдието, което включва проверка на ефективността на политиките, процедурите и практиките за информационна сигурност на представителна подгрупа от системи на агенциите.

- (110) На трето място, доколкото извършват дейности за борба с тероризма, отделите с правомощия в областта на наказателното право прилагане подлежат на надзор от страна на Надзорния съвет по въпросите на неприкосновеността на личния живот и гражданските свободи (PCLOB) — независима структура в рамките на изпълнителната власт, в чийто петчленен състав влизат членове, назначени от президента за определен шестгодишен мандат с одобрението на Сената ⁽¹⁹⁹⁾. Съгласно учредителния му устав на PCLOB са възложени отговорности в областта на политиките за борба с тероризма и тяхното прилагане с оглед на защитата на неприкосновеността на личния живот и гражданските свободи. При прегледа си той има право на достъп до всички съответни записи, доклади, одити, прегледи, документи, писмени материали и препоръки, включително до класифицирана информация, може да провежда изслушвания и да събира устни свидетелски показания ⁽²⁰⁰⁾. Той получава докладите на служителите по въпросите на гражданските свободи и неприкосновеността на личния живот от няколко федерални министерства/агенции ⁽²⁰¹⁾, може да издава препоръки към държавните и правоприлагащите органи и да докладва редовно пред комисии в Конгреса и пред президента ⁽²⁰²⁾. Докладите на PCLOB, включително тези до Конгреса, трябва да бъдат публично достъпни във възможно най-голяма степен ⁽²⁰³⁾.
- (111) И накрая, дейностите по прилагане на наказателното право са обект на надзор от страна на специални комисии в Конгреса на САЩ (правните комисии към Камарата на представителите и Сената). Правните комисии осъществяват редовен надзор по различни начини, по-специално чрез изслушвания, разследвания, прегледи и доклади ⁽²⁰⁴⁾.

3.1.3 Средства за правна защита

- (112) Както беше посочено, в повечето случаи органите по наказателно право прилагане трябва да получат предварително разрешение от съдебен орган, за да събират лични данни. Въпреки че това не се изисква за административните призовки, те са ограничени до специфични ситуации и ще подлежат на независим съдебен контрол, поне когато правителството иска мерки по принудително изпълнение по съдебен ред. По-специално получателите на административните призовки могат да ги оспорят в съда на основание тяхната неоснователност, т.е. че са прекомерни, репресивни или обременяващи ⁽²⁰⁵⁾.
- (113) Физическите лица могат преди всичко да подават искания или жалби до органите по наказателно право прилагане относно обработването на техните лични данни. Това включва възможността да се поиска достъп до личните данни и тяхното коригиране ⁽²⁰⁶⁾. Що се отнася до дейностите за борба с тероризма, физическите лица могат да подадат жалба и до служители по въпросите на неприкосновеността на личния живот и гражданските свободи (или други длъжностни лица по въпросите на неприкосновеността на личния живот) в рамките на правоприлагащите органи ⁽²⁰⁷⁾.
- (114) Освен това в законодателството на САЩ са предвидени редица възможности за правна защита на физическите лица срещу публичен орган или негово длъжностно лице, когато тези органи обработват лични данни ⁽²⁰⁸⁾. Тези възможности, които включват по-специално Закона за административното производство, Закона за свобода на информацията (FOIA) и Закона за неприкосновеността на електронните съобщения (Electronic Communications Privacy Act — ECPA), са достъпни за всички лица, независимо от тяхната националност, при спазване на всички приложими условия.

⁽¹⁹⁹⁾ Членовете на PCLOB трябва да бъдат избирани единствено въз основа на тяхната професионална квалификация, постижения, позиция в обществото, експертни познания в областта на гражданските свободи и неприкосновеността на личния живот и съответен експертен опит, без оглед на политическата им принадлежност. В никой от случаите не може да има повече от трима членове на PCLOB, които принадлежат към една и съща политическа партия. Лице, назначено в PCLOB, не може да бъде длъжностно лице на избираема длъжност, служител или наето лице във федералното правителство, освен в качеството си на член на PCLOB, докато работи в него. Вж. 42 U.S.C. § 2000ee (h).

⁽²⁰⁰⁾ 42 U.S.C. § 2000ee-1 (g).

⁽²⁰¹⁾ Вж. 42 U.S.C. § 2000ee-1 (f)(1)(A)(iii). Тук се включват най-малкото Министерството на правосъдието, Министерството на отбраната, Министерството на вътрешната сигурност, директорът на националното разузнаване, както и други министерства, агенции или структури на изпълнителната власт, определени от PCLOB като подходящи да бъдат обхванати от правомощията му.

⁽²⁰²⁾ 42 U.S.C. § 2000ee, (e).

⁽²⁰³⁾ 42 U.S.C. § 2000ee (f).

⁽²⁰⁴⁾ Например комисии организират тематични изслушвания (вж. например неотдавнашното изслушване на Комисията по правни въпроси на Камарата на представителите относно „цифровите мрежи“, <https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983>), както и редовни изслушвания за надзор, например на ФБР и Министерството на правосъдието, вж. <https://www.judiciary.senate.gov/meetings/08/04/2022/oversight-of-the-federal-bureau-of-investigation>; <https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4966> и <https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4899>.

⁽²⁰⁵⁾ Вж. приложение VI.

⁽²⁰⁶⁾ Циркулярно писмо на OMB № A-130, допълнение II, раздел 3, букви а) и е), в което от федералните агенции се изисква да осигурят подходящ достъп и коригиране при поискване от физически лица и да установят процедури за получаване и разглеждане на жалби и искания, свързани с неприкосновеността на личния живот.

⁽²⁰⁷⁾ Вж. 42 U.S.C. § 2000ee-1 по отношение например на Министерството на правосъдието и Министерството на вътрешната сигурност. Вж. също Меморандум на OMB M-16-24, *Role and Designation of Senior Agency Officials for Privacy* (Роля и определяне на старши служители по въпросите на неприкосновеността на личния живот).

⁽²⁰⁸⁾ Посочените в настоящия раздел механизми за правна защита се прилагат и по отношение на събирането и използването на данни от федералните органи за граждански и регулаторни цели.

(115) Като цяло съгласно разпоредбите за съдебния контрол на Закона за административното производство ⁽²⁰⁹⁾ „всяко лице, което е претърпяло правно нарушение поради действие на агенцията или е неблагоприятно засегнато или ошетен от действия на агенцията“, има право да поиска съдебен контрол ⁽²¹⁰⁾. Това включва възможността да се поиска от Съда да „обяви за незаконно и да отмени действие, констатации и заключения на агенцията, за които е установено, че представляват [...] произвол, каприз, злоупотреба с правото на преценка, или по друг начин не са в съответствие със закона“ ⁽²¹¹⁾.

(116) По-конкретно, в дял II на ЕCPA ⁽²¹²⁾ се предвижда система на законоустановените права на неприкосновеност на личния живот и по този начин се урежда достъпът за целите на правоприлагането до съдържанието на кабелни, устни или електронни съобщения, съхранявани от доставчици на услуги — трети страни ⁽²¹³⁾. Със закона достъпът до такива съобщения се обявява за незаконен (т.е. без разрешение от съда или допустим другоаче) и се дава възможност засегнатото физическо лице да предяви граждански иск във федерален съд в САЩ за действителни и наказателни щети, както и за компенсация или установително решение срещу държавен служител, който произволно е извършил такива незаконни действия, или срещу Съединените американски щати.

(117) Освен това няколко други закона дават на физическите лица право да завеждат дело срещу публичен орган или длъжностно лице в САЩ във връзка с обработването на личните им данни, като например Закона за телефонното подслушване (Wiretap Act) ⁽²¹⁴⁾, Закона за компютърните измами и злоупотреби (Computer Fraud and Abuse Act) ⁽²¹⁵⁾, Federal Torts Claim Act ⁽²¹⁶⁾, Закона за правото на неприкосновеност на личните финанси (Right to Financial Privacy Act) ⁽²¹⁷⁾ и Закона за оповестяване на информация за кредити (Fair Credit Reporting Act) ⁽²¹⁸⁾.

⁽²⁰⁹⁾ 5 U.S.C. § 702.

⁽²¹⁰⁾ Като цяло само „окончателно“ действие на агенцията, а не „предварително, процедурно или междинно“ действие на дадена агенция, подлежи на съдебен контрол. Вж. 5 U.S.C. § 704.

⁽²¹¹⁾ 5 U.S.C. § 706(2)(A).

⁽²¹²⁾ 18 U.S.C. §§ 2701-2712.

⁽²¹³⁾ Законът за неприкосновеността на електронните съобщения (ECPA) осигурява защита на съобщенията, държани от две определени категории доставчици на мрежови услуги, а именно доставчици на: i) електронни съобщителни услуги, като например телефонията или електронната поща; ii) отдалечени изчислителни услуги, като например услуги по компютърно съхранение или обработване.

⁽²¹⁴⁾ 18 U.S.C. §§ 2510 и следв. съгласно Закона за телефонното подслушване (18 U.S.C. § 2520), лице, чиито кабелни, устни или електронни съобщения се прихващат, разкриват или умишлено се използват, може да заведе гражданско дело за нарушение на Закона за телефонното подслушване, в това число при определени обстоятелства — срещу конкретен държавен служител или Съединените американски щати. Относно събирането на информация, която не се отнася за съдържание (например IP адрес, имейл адрес до/от), вж. също глава „Pen Registers and Trap and Trace Devices“ в дял 18 (18 U.S.C. §§ 3121-3127 и — за граждански искове, § 2707).

⁽²¹⁵⁾ 18 U.S.C. § 1030. Съгласно Закона за компютърните измами и злоупотреби (Computer Fraud and Abuse Act) дадено лице може да заведе иск срещу друго лице във връзка с преднамерен неразрешен достъп (или достъп, надхвърлящ разрешения) с цел получаване на информация от финансова институция, компютърна система на правителството на САЩ или друг конкретен компютър, включително при определени обстоятелства, срещу конкретен държавен служител.

⁽²¹⁶⁾ 28 U.S.C. §§ 2671 и следв. съгласно Закона за федералните претенции при непозволени действия (Federal Tort Claims Act) дадено лице може да заведе иск, при определени обстоятелства, срещу Съединените американски щати във връзка с „небрежност или неправомерно действие или бездействие на държавен служител, който е действал в рамките на служебните си задължения“.

⁽²¹⁷⁾ 12 U.S.C. §§ 3401 и следв. съгласно Закона за правото на неприкосновеност на личните финанси (Right to Financial Privacy Act) дадено лице може да заведе иск, при определени обстоятелства, срещу Съединените американски щати във връзка с получаването или разкриването на защитени финансови документи в нарушение на закона. Достъпът на държавата до защитени финансови документи като цяло е забранен, освен ако правителството не поиска това по силата на законна призовка или заповед за обиск или, при спазване на ограниченията, с официално писмено искане, а лицето, чиято информация се иска, бъде уведомено за подаденото искане.

⁽²¹⁸⁾ 15 U.S.C. §§ 1681-1681x. Съгласно Закона за оповестяване на информация за кредити (Fair Credit Reporting Act) дадено лице може да предяви иск срещу всяко лице, което не спазва изискванията (по-специално необходимостта от законно разрешение) по отношение на събирането, разпространението и използването на информация за кредитите на потребителите, или, при определени обстоятелства, срещу държавна агенция.

- (118) Също така, съгласно Закона за свобода на информацията (FOIA) ⁽²¹⁹⁾, 5 U.S.C. § 552, всяко лице има право да поиска достъп до документите на федерални агенции, включително когато те съдържат лични данни на лицето. След изчерпване на административните средства за защита, физическо лице може да се позове на такова право на достъп в съда, освен ако тези документи са защитени от публично оповестяване по силата на освобождаване или специално изключение във връзка с правоприлагането ⁽²²⁰⁾. В този случай съдът ще прецени дали е приложимо някакво изключение или съответния публичен орган се е позовал законно на него.

3.2. Достъп и използване от публични органи на САЩ за целите на националната сигурност

- (119) Законодателството на Съединените щати съдържа редица ограничения и гаранции по отношение на достъпа до лични данни и използването им за целите на националната сигурност и осигурява механизми за надзор и правна защита в тази област, които са в съответствие с изискванията, посочени в съображение 89 от настоящото решение. Условиата, при които може да се осъществява такъв достъп, и гаранциите, приложими за упражняването на тези правомощия, са подробно разгледани в следващите раздели.

3.2.1 Правни основания, ограничения и гаранции

3.2.1.1 Действаща правна уредба

- (120) Личните данни, предавани от Съюза на организациите, попадащи в обхвата на РЗЛД между ЕС и САЩ, могат да бъдат събирани от органите на САЩ за целите на националната сигурност въз основа на различни правни инструменти, при спазване на специфични условия и гаранции.
- (121) След като личните данни бъдат получени от организации, разположени в Съединените щати, разузнавателните агенции на САЩ могат да поискат достъп до такива данни за целите на националната сигурност само ако това е разрешено със закон, по-конкретно съгласно Закона за упражняване на надзор върху външното разузнаване (FISA) или законите разпоредби за писма във връзка с националната сигурност ⁽²²¹⁾. FISA съдържа няколко правни основания, които може да се използват за събиране (и последващо обработване) на лични данни на субекти на данни от Съюза, предавани съгласно РЗЛД в отношенията между ЕС и САЩ (член 105 от FISA ⁽²²²⁾, член 302 от FISA ⁽²²³⁾, член 402 от FISA ⁽²²⁴⁾, член 501 от FISA ⁽²²⁵⁾ и член 702 от FISA ⁽²²⁶⁾), както е описано по-подробно в съображения 142—152.

⁽²¹⁹⁾ 5 U.S.C. § 552.

⁽²²⁰⁾ Тези изключения обаче са формулирани. Например съгласно 5 U.S.C. § 552 (b)(7) правата по FOIA не се прилагат за „документи или информация, изготвени за целите на правоприлагането, но само доколкото съставянето на такива документи или информация А) може разумно да се очаква да възпрепятства процеса на правоприлагането, Б) би лишило лицето от правото на справедлив процес или безпристрастна присъда, В) може разумно да се очаква да представлява необосновано нарушение на неприкосновеността на личния живот, Г) може разумно да се очаква да разкрие самоличността на поверителен източник, в това число държавна, местна или чуждестранна агенция или орган или частна институция, които са предоставили информация на поверителна основа, и — за документ или информация, изготвени от орган по наказателно правоприлагане в хода на наказателно разследване, или от агенция, провеждаща законно наказателно разследване във връзка с националната сигурност — информация, предоставена от поверителен източник, Д) би разкрило техники и процедури за разследвания или наказателни преследвания за целите на правоприлагането или насоки за тях, ако може разумно да се очаква разкриването да предизвика риск от заобикаляне на закона, или Е) може разумно да се очаква да застраши живота или физическата безопасност на дадено физическо лице“. Също така „при искане, което предполага достъп по документи [чието съставяне може разумно да се очаква да възпрепятства процеса на правоприлагането] и А) разследването или производството предполага евентуално нарушение на наказателното право; и Б) има причина да се счита, че i) обектът на разследването или производството не е запознат с висиящото производство и ii) разкриването на наличието на документи може разумно да се очаква да възпрепятства процеса на правоприлагането, агенцията може да разглежда тези документи като документи, за които не се отнасят изискванията от настоящия раздел, само за толкова време, за колкото продължава съответното обстоятелство“ (5 U.S.C. § 552 (c)(1)).

⁽²²¹⁾ 12 U.S.C. § 3414; 15 U.S.C. §§ 1681u-1681v; и 18 U.S.C. § 2709. Вж. съображение 153.

⁽²²²⁾ 50 U.S.C. § 1804, който се отнася до традиционното индивидуализирано електронно наблюдение.

⁽²²³⁾ 50 U.S.C. § 1822, който се отнася до физическото претърсване за целите на външното разузнаване.

⁽²²⁴⁾ 50 U.S.C. § 1842 във връзка с § 1841(2) и раздел 3127 от дял 18, който се отнася до инсталирането на устройства за регистриране или проследяване.

⁽²²⁵⁾ 50 U.S.C. § 1861, който позволява на ФБР да подаде „молба за издаване на заповед, с която се разрешава на предоставящ общи превози превозвач, обект за обществено настаняване, физическо съоръжение за складиране или обект за отдаване на превозни средства под наем да предостави служебни документи, които притежава, за целите на разследване за събиране на външноразузнавателна информация или разследване, свързано с международен тероризъм“.

⁽²²⁶⁾ 50 U.S.C. Code § 1881a, който позволява на елементи от разузнавателната общност на САЩ да търсят достъп до информация, включително до съдържанието на интернет комуникации, от американски дружества, чрез целево събиране от определени лица, които не са граждани на САЩ и се намират извън Съединените щати, със задължителното съдействие на доставчици на електронни комуникации.

- (122) Разузнавателните агенции на САЩ също така имат възможност да събират лични данни извън Съединените щати, като това може да включва лични данни, пренасяни между Съюза и Съединените щати. Събирането на информация извън Съединените щати се основава на Изпълнителен декрет 12333 (ЕО 12333) ⁽²²⁷⁾, издаден от президента ⁽²²⁸⁾.
- (123) Събирането на радиоелектронни разузнавателни данни е формата на събиране на разузнавателни данни, която е от най-голямо значение за настоящата констатация относно адекватността, тъй като се отнася до събирането на електронни съобщения и данни от информационни системи. Такова събиране на данни може да се извършва от разузнавателните агенции на САЩ както на територията на САЩ (въз основа на FISA), така и по време на пренасянето на данни към САЩ (въз основа на Указ 12333).
- (124) На 7 октомври 2022 г. президентът на САЩ издаде Указ 14086 за засилване на защитните мерки за дейностите по радиоелектронно разузнаване на САЩ, с който се определят ограниченията и защитните мерки за всички дейности на САЩ в областта на радиоелектронното разузнаване. Този Указ заменя до голяма степен Изпълнителен указ на президента (Presidential Policy Directive) (PPD-28) ⁽²²⁹⁾, като засилва условията, ограниченията и защитните мерки, които се прилагат по отношение на всички дейности по радиоелектронно разузнаване (т.е. въз основа на FISA и Указ 12333), независимо от мястото, където се извършват ⁽²³⁰⁾, и създава нов механизъм за правна защита, чрез който тези защитни мерки могат да бъдат използвани и прилагани от физически лица ⁽²³¹⁾ (за повече подробности вж. съображения 176—194). По този начин с него в законодателството на САЩ се въвеждат резултатите от разговорите, проведени между ЕС и САЩ след отмяната от Съда на ЕС на решението на Комисията относно адекватното ниво на защита на Щита за защита на личните данни (вж. съображение 6). Поради това декретът е особено важен елемент от правната рамка, оценена в настоящото решение.
- (125) Въведените с Указ 14086 ограничения и гаранции допълват тези, предвидени в член 702 от FISA и Указ 12333. Посочените по-долу изисквания (в раздели 3.2.1.2 и 3.2.1.3) трябва да се прилагат от разузнавателните агенции, когато участва в дейности по радиоелектронно разузнаване съгласно член 702 от FISA и Указ 12333, например когато избират/идентифицират категории външноразузнавателна информация, която трябва да бъде придобита съгласно член 702 от FISA; събиране на външноразузнавателна или контраразузнавателна информация съгласно Указ 12333; и вземане на индивидуални решения за определяне на обект съгласно член 702 от FISA и Указ 12333.
- (126) Изискванията, определени в този изпълнителен декрет на президента, са задължителни за цялата разузнавателна общност. Те трябва да бъдат въведени с допълнителни политики и процедури на агенциите, с които те се транспонират в конкретни указания за всекидневната работа. В това отношение в Указ 14086 на разузнавателните агенции на САЩ се предоставя период от най-много една година за актуализиране на техните съществуващи политики и процедури (т.е. до 7 октомври 2023 г.), за да ги приведат в съответствие с изискванията на изпълнителния декрет. Такива актуализирани политики и процедури трябва да бъдат разработени в консултация с министъра на правосъдието, служителя по въпросите на гражданските свободи към Службата на директора на Националното разузнаване (CLPO към ODNI) и PCLOB — независим надзорен орган, упълномощен да извършва преглед на политиките на изпълнителната власт и тяхното прилагане с оглед защита на неприкосновеността на личния живот и гражданските свободи (вж. съображение 110 относно ролята и статута на PCLOB) — и да бъдат публично достъпни ⁽²³²⁾. Освен това, след като актуализираните политики и процедури бъдат въведени, PCLOB ще

⁽²²⁷⁾ Указ 12333: Разузнавателна дейност на Съединените щати, Федерален регистър, том 40, № 235 (8 декември 1981 г., изменен на 30 юли 2008 г.). Указ 12333 определя в по-общ смисъл целите, насоките, задълженията и отговорностите на разузнавателните усилия на САЩ (включително ролята на различни разузнавателни структури) и установява общите параметри за провеждането на разузнавателната дейност.

⁽²²⁸⁾ Според член II от Конституцията на САЩ отговорността за осигуряването на националната сигурност, включително в частност събирането на данни от външното разузнаване, попада в правомощията на президента в ролята му на главнокомандващ на въоръжените сили.

⁽²²⁹⁾ С Указ 14086 се отменя предишен президентски указ, Изпълнителен указ на президента 28, с изключение на раздел 3 от него и допълващото го приложение (в което е предвидено изискване разузнавателните агенции ежегодно да преразглеждат своите приоритети и изисквания в областта на радиоелектронното разузнаване, като вземат предвид ползите от дейностите по радиоелектронно разузнаване за националните интереси на САЩ, както и риска, който тези дейности представляват) и раздел 6 (който съдържа общи разпоредби), вж. меморандума за национална сигурност относно частичната отмяна на Изпълнителен указ на президента 28, достъпен на адрес <https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/national-security-memorandum-on-partial-revocation-of-presidential-policy-directive-28/>.

⁽²³⁰⁾ Вж. раздел 5, буква f) от Указ 14086, в който се обяснява, че изпълнителният декрет има същото приложно поле като Изпълнителен указ на президента 28, който, според бележка под линия 3 в него, се прилага за дейности по радиоелектронно разузнаване, извършвани с цел събиране на съобщения или информация за съобщения, с изключение на дейности по радиоелектронно разузнаване, предприети с цел изпитване или разработване на способности за радиоелектронно разузнаване.

⁽²³¹⁾ Вж. в тази връзка например раздел 5, буква h) от Указ 14086, в който се пояснява, че с мерките за защита в изпълнителния декрет се установява право и те могат да бъдат прилагани от физически лица чрез механизма за правна защита.

⁽²³²⁾ Вж. раздел 2(c)(iv)(C) от Указ 14086.

извършва преглед, за да гарантира, че те са в съответствие с изпълнителния декрет. В рамките на 180 дни от приключването на такъв преглед от страна на PCLOV всяка разузнавателна агенция трябва внимателно да обмисли и изпълни или по друг начин да се съобрази с всички препоръки на PCLOV. На 3 юли 2023 г. правителството на САЩ информира Европейската комисия, че тези политики и процедури са актуализирани ⁽²³³⁾.

3.2.1.2 Ограничения и гаранции по отношение на събирането на лични данни за целите на националната сигурност

- (127) С Указ 14086 се установяват редица всеобхватни изисквания, които се прилагат за всички дейности по радиоелектронно разузнаване (събиране, използване, разпространение и т.н. на лични данни).
- (128) На първо място, тези дейности трябва да се основават на закон или упълномощаване от президента и да се предприемат в съответствие със законодателството на САЩ, включително Конституцията ⁽²³⁴⁾.
- (129) На второ място, трябва да има подходящи мерки за защита, за да се гарантира, че неприкосновеността на личния живот и гражданските свободи са неразделна част от планирането на такива дейности ⁽²³⁵⁾.
- (130) По-специално, всяка дейност по радиоелектронно разузнаване може да се извършва само „след като въз основа на разумна оценка на всички съответни фактори се установи, че дейностите са необходими за постигане на обоснован приоритет по отношение на разузнаването“ (относно понятието „обоснован приоритет по отношение на разузнаването“ вж. съображение 135) ⁽²³⁶⁾.
- (131) Освен това такива дейности могат да се извършват само „в степен и по начин, които са пропорционални на обоснован приоритет по отношение на разузнаването, за който са били разрешени“ ⁽²³⁷⁾. С други думи, трябва да се постигне подходящ баланс „между важността на преследвания приоритет по отношение на разузнаването и въздействието върху неприкосновеността на личния живот и гражданските свободи на засегнатите лица, независимо от тяхната националност или местопребиваването им“ ⁽²³⁸⁾.
- (132) И накрая, за да се гарантира спазването на тези общи изисквания, които отразяват принципите на законност, необходимост и пропорционалност, дейностите по радиоелектронно разузнаване подлежат на надзор (вж. по-подробно раздел 3.2.2) ⁽²³⁹⁾.
- (133) Тези общи изисквания са допълнително обосновани по отношение на събирането на радиоелектронни разузнавателни данни чрез редица условия и ограничения, които гарантират, че намесата в правата на физическите лица е ограничена до това, което е необходимо и пропорционално за постигане на законна цел.
- (134) На първо място, с изпълнителния декрет основанията, на които могат да се събират данни като част от дейностите по радиоелектронно разузнаване, се ограничават по два начина. От една страна, в изпълнителния декрет се определят законните цели, които могат да бъдат преследвани чрез събирането на радиоелектронни разузнавателни данни, например разбиране или оценяване на възможностите, намеренията или дейностите на чуждестранни организации, включително международни терористични организации, които представляват настояща или потенциална заплаха за националната сигурност на Съединените щати; защита от чуждестранни военни способности и дейности; разбиране и оценяване на транснационалните заплахи, които оказват влияние върху глобалната сигурност, като изменението на климата и други екологични промени, рисковете за общественото здраве и хуманитарните заплахи ⁽²⁴⁰⁾. От друга

⁽²³³⁾ <https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguards-in-executive-order-14086>.

⁽²³⁴⁾ Член 2(a)(i) от Указ 14086.

⁽²³⁵⁾ Член 2(a)(ii) от Указ 14086.

⁽²³⁶⁾ Член 2(a)(ii)(A) от Указ 14086. Това не винаги означава, че радиоелектронното разузнаване е единственото средство за постигане на напредък по аспектите на даден обоснован приоритет по отношение на разузнаването. Например събирането на радиоелектронни разузнавателни данни може да се използва за осигуряване на алтернативни пътища за потвърждаване (например за потвърждаване на информация, получена от други разузнавателни източници) или за поддържане на надежден достъп до същата информация (раздел 2, буква c), подточка i), буква A) от Указ 14086).

⁽²³⁷⁾ Член 2(a)(ii)(B) от Указ 14086.

⁽²³⁸⁾ Член 2(a)(iii)(B) от Указ 14086.

⁽²³⁹⁾ Член 2(a)(iii) във връзка с раздел 2(d) от Указ 14086.

⁽²⁴⁰⁾ Член 2(b)(i) от Указ 14086. Поради ограничения списък с легитимни цели в Указа, който не включва възможни бъдещи заплахи, в Указа се предвижда възможност за актуализиране на списъка от президента, в случай че се появят нови изисквания за националната сигурност, като например нови заплахи за националната сигурност. Такива актуализации по принцип трябва да бъдат публикувани, освен ако президентът не прецени, че това би представлявало риск за националната сигурност на Съединените щати (раздел 2, буква b), подточка i), буква B от Указ 14086).

страна, в изпълнителния декрет се изброяват определени цели, които никога не трябва да се преследват чрез дейности по радиоелектронно разузнаване, например с цел потискане или затрудняване на критиката или несъгласието или свободното изразяване на идеи или политически мнения от отделни лица или пресата; поставяне в неблагоприятно положение на лица на основата на техния етнически или расов произход, пол, полова идентичност, сексуална ориентация или религия; или предоставяне на конкурентно предимство на американски дружества ⁽²⁴¹⁾.

- (135) Освен това легитимните цели, определени в Указ № 14086, не могат сами по себе си да бъдат използвани от разузнавателните агенции за обосноваване на събирането на радиоелектронни разузнавателни данни, а трябва да бъдат допълнително надлежно обосновани за оперативни цели с по-конкретни приоритети, за които може да се събират радиоелектронни разузнавателни данни. С други думи, действителното събиране може да се осъществи само за постигане на по-конкретен приоритет. Тези приоритети се определят чрез специален процес, целящ да гарантира спазването на приложимите правни изисквания, включително тези, свързани с неприкосновеността на личния живот и гражданските свободи. По-конкретно, приоритетите в областта на разузнаването се разработват първо от директора на Националното разузнаване (чрез т.нар. Рамка на националните разузнавателни приоритети) и се представят на президента за одобрение ⁽²⁴²⁾. Преди да предложи на президента приоритети в областта на разузнаването, директорът трябва, в съответствие с Указ 14086, да получи оценка от CLPO към ODNI за всеки приоритет относно това дали той 1) постига една или повече законни цели, изброени в Указа; 2) не е бил разработен с такава цел и не се очаква да доведе до събиране на радиоелектронни разузнавателни данни за забранена цел, посочена в Указа; и 3) е бил създадена след подходящо отчитане на неприкосновеността на личния живот и гражданските свободи на всички лица, независимо от тяхната националност или местоживеење ⁽²⁴³⁾. В случай че директорът не е съгласен с оценката на CLPO, двете становища трябва да бъдат представени на председателя ⁽²⁴⁴⁾.
- (136) Ето защо този процес гарантира, че съображенията, свързани с неприкосновеността на личния живот, се вземат предвид още на първоначалния етап, когато се разработват приоритетите на разузнаването.
- (137) На второ място, след като е установен приоритет по отношение на разузнаването, редица изисквания регулират решението дали и до каква степен може да се събират радиоелектронни разузнавателни данни за постигане на този приоритет. Тези изисквания въвеждат в действие всеобхватните стандарти за необходимост и пропорционалност, определени в раздел 2, буква а) от изпълнителния декрет.
- (138) По-специално, радиоелектронните разузнавателни данни могат да се събират само „след преценка, че въз основа на разумна оценка на всички съответни фактори събирането е необходимо за постигане на конкретен приоритет по отношение на разузнаването“ ⁽²⁴⁵⁾. При определянето на това дали конкретна дейност по събиране на радиоелектронни разузнавателни данни е необходима за постигане на обоснован приоритет по отношение на разузнаването, разузнавателните служби на САЩ трябва да вземат предвид наличието, осъществимостта и целесъобразността на други източници и методи с по-ниска степен на вмешателство, включително от дипломатически и обществени източници ⁽²⁴⁶⁾. Когато има такива алтернативни източници и методи с по-ниска степен на вмешателство, те трябва да се използват приоритетно ⁽²⁴⁷⁾.
- (139) Когато след прилагането на такива критерии събирането на радиоелектронни разузнавателни данни се счита за необходимо, то трябва да бъде „съобразено с конкретния случай, доколкото това е практически възможно“ и „да не оказва непропорционално въздействие върху неприкосновеността на личния живот и гражданските свободи“ ⁽²⁴⁸⁾. За да се гарантира, че неприкосновеността на личния живот и гражданските свободи не са непропорционално засегнати, т.е. за да се постигне подходящ баланс между нуждите на националната сигурност и защитата на неприкосновеността на личния живот и гражданските свободи, трябва надлежно да се вземат предвид всички съответни фактори, като например естеството на преследваната цел; степента на вмешателство на дейността по събиране, включително нейната продължителност; вероятният принос на събраните данни за постигане на преследваната цел; разумно предвидимите последици за лицата; и естеството и чувствителността на данните, които трябва да бъдат събрани ⁽²⁴⁹⁾.

⁽²⁴¹⁾ Член 2(b)(ii) от Указ 14086.

⁽²⁴²⁾ Член 102А от Закона за националната сигурност и раздел 2, буква б), подточка iii) от Указ 14086.

⁽²⁴³⁾ В изключителни случаи (по-специално, когато такъв процес не може да бъде осъществен поради необходимостта да се отговори на ново или променящо се изискване за разузнаване), такива приоритети могат да бъдат определени директно от президента или от ръководителя на елемент от разузнавателната общност, които по принцип трябва да прилагат същите критерии като тези, описани в раздел 2, буква б), подточка iii), буква А, подточки 1—3, вж. раздел 4, буква п) от Указ 14086.

⁽²⁴⁴⁾ Член 2(b)(iii)(C) от Указ 14086.

⁽²⁴⁵⁾ Член 2(b) и (c)(i)(A) от Указ 14086.

⁽²⁴⁶⁾ Член 2(c)(i)(A) от Указ 14086.

⁽²⁴⁷⁾ Член 2(c)(i)(A) от Указ 14086.

⁽²⁴⁸⁾ Член 2(c)(i)(B) от Указ 14086.

⁽²⁴⁹⁾ Член 2(c)(i)(B) от Указ 14086.

- (140) Що се отнася до вида на събирането на радиоелектронни разузнавателни данни, събирането на данни в Съединените щати, което е от най-голямо значение за настоящата констатация относно адекватното ниво на защита, тъй като се отнася до данни, които са били предадени на организации в САЩ, винаги трябва да бъде целево, както е обяснено по-подробно в съображения 142—153.
- (141) „Събирането на масиви от данни“ ⁽²⁵⁰⁾ може да се извършва само извън Съединените щати, въз основа на Указ ЕО 12333. И в този случай, съгласно Указ 14086, трябва да се отдава приоритет на целенасоченото събиране ⁽²⁵¹⁾. От друга страна, събирането на масиви от данни е разрешено само когато информацията, необходима за постигане на обоснован приоритет по отношение на разузнаването, не може да бъде получена по разумен начин чрез целенасочено събиране ⁽²⁵²⁾. Когато е необходимо да се извършва събиране на масиви от данни извън Съединените щати, се прилагат специфични гаранции съгласно Указ 14086 ⁽²⁵³⁾. На първо място, трябва да се прилагат методи и технически мерки, за да се ограничи събирането на данни само до това, което е необходимо за постигане на даден обоснован приоритет по отношение на разузнаването, като същевременно се сведе до минимум събирането на нерелевантна информация ⁽²⁵⁴⁾. На второ място, с изпълнителния декрет се ограничава използването на масово събирана информация (включително първичен анализ) до шест конкретни цели, включително защита срещу тероризъм, вземане на заложници и държане на лица в плен от или от името на чуждестранно правителство, организация или лице; защита срещу чуждестранен шпионаж, саботаж или убийство; защита от заплахи, произтичащи от разработването, притежаването или разпространението на оръжия за масово унищожение или свързани с тях технологии и заплахи и т.н. ⁽²⁵⁵⁾. И накрая, всеки първичен анализ на получени масиви от радиоелектронни разузнавателни данни може да се извършва само когато това е необходимо за постигане на обоснован приоритет по отношение на разузнаването, в изпълнение на тези шест цели и в съответствие с политики и процедури, които отчитат по подходящ начин въздействието на запитванията върху неприкосновеността на личния живот и гражданските свободи на всички лица, независимо от тяхната националност или местопребиваване им ⁽²⁵⁶⁾.
- (142) В допълнение към изискванията на Указ 14086, събирането на радиоелектронни разузнавателни данни, които са предадени на организация в Съединените щати, подлежи на специфични ограничения и гаранции, уредени в раздел 702 от FISA ⁽²⁵⁷⁾. С него се разрешава придобиването на външноразузнавателна информация чрез целево събиране от лица, които не са граждани на САЩ и са с местонахождение извън САЩ, при задължително съдействие от страна на доставчиците на електронни далекосъобщителни услуги в САЩ ⁽²⁵⁸⁾. За да могат да събират външноразузнавателна информация съгласно член 702 от FISA, министърът на правосъдието и директорът на националното разузнаване представят годишни удостоверения пред Съда по надзора върху външното разузнаване (FISC), в които се посочват

⁽²⁵⁰⁾ Т.е. събирането на големи количества радиоелектронни разузнавателни данни, които поради технически или оперативни съображения се придобиват без използването на разграничителни критерии (например без използването на специфични идентификатори или условия за подбор), вж. раздел 4, буква б) от Указ 14086. Съгласно Указ 14086 и както е обяснено допълнително в съображение 141, събирането на масиви от данни съгласно Указ 12333 се извършва само когато това е необходимо за постигане на конкретни утвърдени разузнавателни приоритети и подлежи на редица ограничения и предпазни мерки, които имат за цел да гарантират, че достъпът до данни не е безразборен. Следователно събирането на масиви от данни трябва да се противопостави на събирането на данни на обща и безразборна основа („масово наблюдение“) без ограничения и предпазни мерки.

⁽²⁵¹⁾ Раздел 2(c)(ii)(A) от ЕО 14086.

⁽²⁵²⁾ Раздел 2(c)(ii)(A) от ЕО 14086.

⁽²⁵³⁾ Специфичните правила за събиране на масиви от данни от Указ 14086 се прилагат и за целенасочена дейност по събиране на радиоелектронни разузнавателни данни, при която временно се използват данни, придобити без разграничителни критерии (например специфични условия за подбор или идентификатори), т.е. масиви от данни (което е възможно само извън територията на Съединените щати). Това не е така, когато такива данни се използват само за подпомагане на първоначалната техническа фаза на целенасочена дейност по събиране на радиоелектронни разузнавателни данни, запазват се само за кратък период от време, необходим за завършване на тази фаза, и се заличават веднага след това (член 2(c)(ii) (D) от Указ 14086). В този случай единствената цел на първоначалното събиране без разграничителни критерии е да се даде възможност за целенасоченото събиране на информация чрез прилагане на специфичен идентификатор или условие за подбор. При такъв сценарий в правителствените бази данни се въвеждат само данните, които отговарят на прилагането на определени разграничителни критерии, а останалите данни се унищожават. Поради това такова целенасочено събиране на информация продължава да се урежда от общите правила, които се прилагат за събирането на радиоелектронни разузнавателни данни, включително член 2(a) — (b) и член 2(c)(i) от Указ 14086.

⁽²⁵⁴⁾ Раздел 2(c)(ii)(A) от ЕО 14086.

⁽²⁵⁵⁾ Член 2(c)(ii)(B) от Указ 14086. В случай че се появят нови изисквания за национална сигурност, като например нови заплахи за националната сигурност, президентът може да актуализира този списък. Такива актуализации по принцип трябва да бъдат публично оповестени, освен ако президентът не пресени, че това само по себе си би представлявало риск за националната сигурност на Съединените щати (раздел 2, буква с), подточка ii), буква С) от Указ 14086). Що се отнася до търсенията за събиране на масиви от данни, вж. раздел 2, буква с), подточка iii), буква D) от Указ 14086.

⁽²⁵⁶⁾ Член 2, 2(a)(ii)(A) във връзка с раздел 2(c)(iii)(D) от Указ 14086. Вж. и приложение VII.

⁽²⁵⁷⁾ 50 U.S.C. § 1881.

⁽²⁵⁸⁾ 50 U.S.C. § 1881a (a). По-специално, както е отбелязано от PCLOB, наблюдението по раздел 702 „се състои изцяло от насочване към конкретни лица[, които не са граждани на САЩ], за които е направена индивидуална преценка“ (Надзорен съвет по въпросите на неприкосновеността на личния живот и гражданските свободи, Доклад за програмата за наблюдение, управлявана съгласно раздел 702 от Закона за упражняване на надзор върху външното разузнаване, 2 юли 2014 г., Доклад по раздел 702, стр. 111). Вж. също публикацията Изпълнение от страна на Агенцията за национална сигурност (АНС) на раздел 702 от FISA, 16 април 2014 г., на Службата за гражданските свободи и неприкосновеността на личния живот към АНС (NSA's Implementation of Foreign Intelligence Act Section 702). Понятието „доставчик на електронни съобщителни услуги“ е дефинирано в 50 U.S.C., § 1881 (a)(4).

категориите външно Разузнавателна информация, която трябва да бъде придобита⁽²⁵⁹⁾. Удостоверенията трябва да бъдат придружени от процедури за целево събиране, свеждане на данните до минимум и първичен анализ, които процедури също се одобряват от FISC и са правно обвързващи за разузнавателните агенции на САЩ.

- (143) FISC е независим съд⁽²⁶⁰⁾, създаден по силата на федерален закон, чиито решения могат да бъдат обжалвани пред Апелативния съд за наблюдение на чуждите разузнавателни служби (FISCR)⁽²⁶¹⁾ и в крайна сметка пред Върховния съд на Съединените щати⁽²⁶²⁾. FISC (и FISCR) се подпомага от постоянна работна група от петима адвокати и петима технически експерти с експертни знания и опит в областта на националната сигурност, както и в областта на гражданските свободи⁽²⁶³⁾. От тази група съдът определя едно лице, което изпълнява функциите на *amicus curiae* и съдейства за разглеждането на всички заявления за разпореждане или разглеждане, които според становището на съда представляват ново или съществено тълкуване на закон, освен ако съдът счита, че е уместно да не определя такова лице⁽²⁶⁴⁾. С това по-специално се гарантира, че съображенията за неприкосновеността на личния живот се отразяват по подходящ начин при преценката на съда. Също така съдът може да определи функциите на *amicus curiae* да изпълнява лице или организация, включително като предоставя техническа експертиза, когато бъде счетено за необходимо, или по предложение, да даде разрешение на дадено лице или организация да подаде подготвени от приятел на съда (*amicus curiae*) заключения⁽²⁶⁵⁾.
- (144) FISC прави преглед на сертифицираните и свързаните с тях процедури (по-специално процедурите за целево събиране и свеждане на данните до минимум) за съответствие с изискванията на FISA. Ако прецени, че изискванията не са изпълнени, той може изцяло или от части да откаже сертифицирането и да изиска изменение на процедурите⁽²⁶⁶⁾. В това отношение FISC многократно е потвърждавал, че прегледът на процедурите по член 702 за целево събиране и свеждане на данните до минимум не се ограничава само до писмените процедури, а включва и начина, по който те се прилагат от правителството⁽²⁶⁷⁾.
- (145) Индивидуалните решения за целево събиране се вземат от Агенцията за национална сигурност (АНС, разузнавателната агенция, отговорна за целевото събиране съгласно член 702 от FISA) в съответствие с одобрените от FISC процедури за целево събиране, които изискват АНС да прецени, въз основа на всички обстоятелства, дали целевото събиране на данни за конкретно лице има вероятност да доведе до придобиване на категория външно Разузнавателна информация, посочена при сертифицирането⁽²⁶⁸⁾. Тази преценка трябва да бъде конкретна и базирана на факти, да се основава на

⁽²⁵⁹⁾ 50 U.S.C. § 1881a (g).

⁽²⁶⁰⁾ В състава на Съда по надзора върху външното разузнаване влизат съдии, назначени от председателя на Върховния съд на САЩ измежду действащи окръжни съдии, които преди това са назначени от президента с утвърждението на Сената. Съдиите, които са с пожизнено назначение и могат да бъдат отстранявани от длъжност само с основателна причина, изпълняват задълженията си в Съда по надзора върху външното разузнаване с разпределен седемгодишен мандат. Съгласно Закона за упражняване на надзор върху външното разузнаване съдиите трябва да са подбрани от най-малко седем различни съдебни окръга на САЩ. Вж. 50 U.S.C. § 1803 (a). Работата на съдиите се подпомага от опитни помощник-съдии, които са назначен юридически персонал в съда и подготвят правни анализи по колективни искания. Вж. писмо от уважаемия Reggie B. Walton, председателстващ съдия, Съд на САЩ по надзора върху външното разузнаване, до уважаемия Patrick J. Leahy, председател на правната комисия на Сената (29 юли 2013 г.) (писмо Walton), стр. 2, налично на адрес <https://fas.org/irp/news/2013/07/fisc-leahy.pdf>.

⁽²⁶¹⁾ В състава на Апелативния съд за наблюдение на чуждите разузнавателни служби влизат съдии, назначени от главния съдия на САЩ и избрани измежду съдиите в окръжните и апелативните съдилища на САЩ, които изпълняват задълженията си с разпределен седемгодишен мандат. Вж. 50 U.S.C. § 1803(b).

⁽²⁶²⁾ Вж. 50 U.S.C. §§ 1803 (b), 1861 a (f), 1881 a (h), 1881 a (i)(4).

⁽²⁶³⁾ 50 U.S.C. § 1803 (i)(1),(3)(A).

⁽²⁶⁴⁾ 50 U.S.C. § 1803 (i)(2)(A).

⁽²⁶⁵⁾ 50 U.S.C. § 1803 (i)(2)(B).

⁽²⁶⁶⁾ Вж. например Становището на FISC от 18 октомври 2018 г., достъпно на адрес [athttps://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf](https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf), потвърдено от Апелативния съд за наблюдение на чуждите разузнавателни служби в Становището му от 12 юли 2019 г., достъпно на адрес [athttps://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf](https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf).

⁽²⁶⁷⁾ Вж. например FISC, Становище меморандум и разпореждане по член 35 (18 ноември 2020 г.) (разрешено за публично оповестяване на 26 април 2021 г.), (приложение D).

⁽²⁶⁸⁾ 50 U.S.C. § 1881a(a), Процедури, използвани от Агенцията за национална сигурност за целево събиране на данни за лица, които не са граждани на САЩ, за които има основание да се смята, че се намират извън Съединените щати, с цел получаване на външно разузнавателна информация съгласно член 702 от Закона за упражняване на надзор върху външното разузнаване от 1978 г., с измененията от март 2018 г. (Процедури на АНС по целево събиране), достъпни на адрес https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_NSA_Targeting_27Mar18.pdf, стр. 1—4, допълнително обяснени в доклада на PCLOB, стр. 41—42.

аналитична преценка, на специализираното обучение и експертния опит на анализатора, както и на естеството на външноразузнавателната информация, която трябва да бъде получена ⁽²⁶⁹⁾. Целевото събиране се извършва чрез използване на т.нар. критерии за подбор, които служат за идентифициране на конкретни технически средства за връзка, като например адрес на електронна поща или телефонен номер на целта, но не и ключови думи, нито имена на лицата, към които е насочено търсенето ⁽²⁷⁰⁾.

- (146) Анализаторите на АНС идентифицират лица, които не са граждани на САЩ и се намират извън територията на САЩ, и чието наблюдаване по преценка на анализаторите ще осигури съответните външноразузнавателни данни, посочени при сертифицирането ⁽²⁷¹⁾. Както е посочено в процедурите на АНС по целево събиране, АНС може да насочи наблюдението към даден обект на разследване само когато вече е научила нещо за него ⁽²⁷²⁾. Това може да произтича от информация от различни източници, например от агентурното разузнаване. Чрез тези други източници анализаторът трябва да научи и за конкретен критерий за подбор (т.е. профил в съобщително средство), използван от потенциалния обект на разследване. След като са идентифицирани тези отделни лица и определянето им като цели бъде одобрено чрез механизъм за подробно разглеждане в рамките на АНС ⁽²⁷³⁾, се възлага задача за определянето на критерии за подбор (т.е. тяхното разработване и прилагане), чрез които да се набележат съобщителните средства (например адреси на електронна поща), използвани от обектите на разследването ⁽²⁷⁴⁾.
- (147) АНС трябва да документира фактическите основания за избора на обекта на разследване ⁽²⁷⁵⁾ и на редовни интервали след първоначалното целево събиране да потвърждава, че стандартът за целево събиране продължава да се спазва ⁽²⁷⁶⁾. След като стандартът за целево събиране вече не е изпълнен, събирането трябва да бъде прекратено ⁽²⁷⁷⁾. Изборът на всеки обект на разследване от страна на АНС и записът на всяка регистрирана оценка и обосновка на целевото събиране се преглеждат за съответствие с процедурите по целево събиране на всеки два месеца от служители в службите за надзор на разузнаването в Министерството на правосъдието, които са задължени да докладват за всяко нарушение на FISC и на Конгреса ⁽²⁷⁸⁾. Писмената документация на АНС улеснява надзора на FISC върху това дали конкретни лица са правилно избрани за целево събиране на данни съгласно член 702 от FISA в съответствие с надзорните му правомощия, описани в съображения 173—174 ⁽²⁷⁹⁾. И накрая, директорът на националното разузнаване (DNI) е длъжен да докладва всяка година общия брой обекти на разследване по член 702 от FISA в публични годишни статистически доклади за прозрачност. Дружествата, които получават указания във връзка с член 702 от FISA, могат да публикуват обобщени данни (чрез доклади за прозрачност) за получените от тях искания ⁽²⁸⁰⁾.

⁽²⁶⁹⁾ Процедурите на АНС по целево събиране, стр. 4.

⁽²⁷⁰⁾ Вж. PCLOB, Доклад по член 702, стр. 32—33, 45 с допълнителни препратки. Вж. също Оценката за полугодieto на спазването на процедурите и насоките, издадени в съответствие с член 702 от Закона за упражняване на надзор върху външното разузнаване, представена от министъра на правосъдието и директора на националното разузнаване, отчетен период: 1 декември 2016 г. — 31 май 2017 г., стр. 41 (октомври 2018 г.), достъпна на адрес: https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf.

⁽²⁷¹⁾ PCLOB, Доклад по член 702, стр. 42—43.

⁽²⁷²⁾ Процедурите на АНС по целево събиране, стр. 2.

⁽²⁷³⁾ PCLOB, Доклад по член 702, стр. 46. Например АНС трябва да удостовери, че е налице връзка между целта и критерия за подбор, да документира външноразузнавателните данни, които се очаква да бъдат получени, данните трябва да бъдат разгледани и одобрени от двама старши анализатори на АНС и целият процес да бъде проследен с цел последващи прегледи за съответствие от страна на ODNI и Министерството на правосъдието. Вж. Изпълнение от страна на АНС на член 702 от FISA, публикация от 16 април 2014 г. на Службата за гражданските свободи и неприкосновеността на личния живот към АНС.

⁽²⁷⁴⁾ 50 U.S.C. § 1881a (h).

⁽²⁷⁵⁾ Процедурите на АНС по целево събиране, стр. 8. Вж. също PCLOB, Доклад по член 702, стр. 46. Непредставянето на писмена обосновка представлява нарушение, свързано със съответствието на документацията, за което трябва да се докладва пред FISC и пред Конгреса. Вж. Оценката за полугодieto на спазването на процедурите и насоките, издадени в съответствие с член 702 от Закона за упражняване на надзор върху външното разузнаване, представена от министъра на правосъдието и директора на националното разузнаване, отчетен период: 1 декември 2016 г. — 31 май 2017 г., стр. 41 (октомври 2018 г.), Доклад на Министерството на правосъдието/Националната разузнавателна служба (DOJ/ODNI) за съответствие с изискванията на FISC за периода декември 2016 г. — май 2017 г., стр. A-6, достъпен на адрес https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf.

⁽²⁷⁶⁾ Вж. U.S. Government Submission to Foreign Intelligence Surveillance Court, 2015 Summary of Notable Section 702 Requirements (Становище на правителството на САЩ до Съда по надзора върху външното разузнаване, обобщение от 2015 г. във връзка с изискванията по член 702), стр. 2—3 (15 юли 2015 г.) и информацията, предоставена в приложение VII.

⁽²⁷⁷⁾ Вж. U.S. Government Submission to Foreign Intelligence Surveillance Court, 2015 Summary of Notable Section 702 Requirements, стр. 2—3 (15 юли 2015 г.), в което се предвижда, че „[а]ко впоследствие правителството прецени, че не се очаква продължаването на използването на критерия за подбор на обект на разследването да доведе до получаване на външноразузнавателна информация, се изисква незабавно изключване на този критерий за подбор, а забавянето може да доведе до подлежащо на докладване нарушение на спазването на изискванията“. Вж. също информацията, предоставена в приложение VII.

⁽²⁷⁸⁾ PCLOB, Доклад по член 702, стр. 70—72; Правило 13(b) от Процедурния правилник на Съда за наблюдение на разузнавателните служби на Съединените щати, на разположение на адрес <https://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf>.

⁽²⁷⁹⁾ Вж. също Доклада на Министерството на правосъдието и Службата за национално разузнаване до FISC за периода декември 2016 г. — май 2017 г., стр. A-6.

⁽²⁸⁰⁾ 50 U.S.C. § 1874.

- (148) Що се отнася до другите правни основания за събиране на лични данни, предавани на организации в САЩ, се прилагат различни ограничения и мерки за защита. Като цяло събирането на масиви от данни е изрично забранено съгласно член 402 от FISA (електронни устройства за регистриране или проследяване) и чрез използването на писма във връзка с националната сигурност, като вместо това се изисква използването на специфични „условия за подбор“⁽²⁸¹⁾.
- (149) За провеждане на традиционно индивидуализирано електронно наблюдение (съгласно член 105 от FISA) разузнавателните служби трябва да подадат заявление до FISC с изложение на фактите и обстоятелствата, на които се позовават, за да обосноват убеждението, че е налице обосновано предположение, че обектът се използва или предстои да бъде използван от чужда сила или служител на чужда сила⁽²⁸²⁾. FISC ще направи преценка, наред с останалото, дали въз основа на посочените факти съществува обосновано предположение случаят наистина да е такъв⁽²⁸³⁾.
- (150) За да се извърши претърсване на помещения или имущество, което има за цел да доведе до проверка, изземване и т.н. на информация, материали или имущество (например компютърно устройство) въз основа на член 301 от FISA, се изисква заявление за издаване на разпореждане до Съда по надзора върху външното разузнаване (FISC)⁽²⁸⁴⁾. Такова заявление трябва, наред с другото, да показва, че има обосновано предположение, че обектът на претърсване е чужда сила или служител на чужда сила; че помещението или имуществото, което трябва да бъде претърсено, съдържа външноразузнавателна информация и че помещението, което трябва да бъде претърсено, е собственост, се използва или владее или се предава от или на (служител на) чужда сила⁽²⁸⁵⁾.
- (151) По подобен начин инсталирането на електронни устройства за регистриране или проследяване (съгласно член 402 от FISA) изисква да се подаде заявление за издаване на разпореждане до FISC (или до магистрат към окръжен съд на САЩ (U.S. Magistrate Judge) и да се използва специален критерий за подбор, т.е. понятие, което определя по специфичен начин дадено лице, сметка и др. и се използва за ограничаване в максимално възможната разумна степен на обхвата на исканата информация⁽²⁸⁶⁾. Този инструмент не се отнася за съдържанието на съобщенията, а по-скоро има за цел получаването на информация за клиента или абоната, който използва дадена услуга (например име, адрес, абонатен номер, продължителност/вид на получената услуга, източник/механизъм на плащане).
- (152) Член 501 от FISA⁽²⁸⁷⁾, който позволява събирането на търговска документация на предоставящ общи превози превозвач (т.е. всяко физическо или юридическо лице, което превозва хора или имущество по суша, релсов път, вода или въздух срещу заплащане), обект за обществено настаняване (например хотел, мотел или гостилница), обект за отдаване под наем на превозни средства или физическо съоръжение за складиране (т.е. обект, който предоставя пространство или услуги, свързани със складирането на стоки и материали)⁽²⁸⁸⁾, също изисква подаване на заявление до FISC или магистрат към окръжен съд. В заявлението трябва да се посочат търсените данни и конкретните и ясно изразени факти, които дават основание да се смята, че лицето, за което се отнасят данните, е чужда сила или служител на чужда сила⁽²⁸⁹⁾.
- (153) И накрая, писмата във връзка с националната сигурност са разрешени от различни закони и позволяват на разследващите органи да получават определена информация (невключваща съдържанието на съобщенията) от определени субекти (например финансови институции, агенции за оповестяване на информация за кредити, доставчици на електронни комуникации), съдържаща се в доклади за кредитите, финансови записи и електронни регистри на абонати и транзакции⁽²⁹⁰⁾. Законът относно писмата във връзка с националната сигурност, който разрешава достъп до електронни съобщения, може да се използва само от ФБР и изисква в заявленията да се използва термин, който конкретно идентифицира лице, организация, телефонен номер или сметка, и да се удостовери, че информацията е от значение само във връзка с разрешено разследване в сферата на националната сигурност за защита срещу международния тероризъм или секретни разузнавателни дейности⁽²⁹¹⁾. Получателите на писма във връзка с националната сигурност имат право да оспорят писмото в съда⁽²⁹²⁾.

⁽²⁸¹⁾ 50 U.S. Code § 1842(c)(3), а по отношение на писмата във връзка с националната сигурност — 12 U.S.C., § 3414(a)(2); 15 U.S.C. § 1681u; 15 U.S.C. § 1681v(a); и 18 U.S.C. § 2709(a).

⁽²⁸²⁾ Понятието „служител на чужда сила“ може да включва лица, които не са граждани на САЩ, които участват в международен тероризъм или международно разпространение на оръжия за масово унищожение (включително подготвителни действия) (50 U.S.C., § 1801 (b) (1)).

⁽²⁸³⁾ 50 U.S.C. § 1804. Вж. също § 1841(4) по отношение на избора на условия за подбор.

⁽²⁸⁴⁾ 50 U.S.C. § 1821(5).

⁽²⁸⁵⁾ 50 U.S.C. § 1823(a).

⁽²⁸⁶⁾ 50 U.S.C. § 1842 във връзка с § 1841(2) и раздел 3127 от дял 18.

⁽²⁸⁷⁾ 50 U.S.C. § 1862.

⁽²⁸⁸⁾ 50 U.S.C. §§ 1861-1862.

⁽²⁸⁹⁾ 50 U.S.C. § 1862(b).

⁽²⁹⁰⁾ 12 U.S.C. § 3414; 15 U.S.C. §§ 1681u-1681v; и 18 U.S.C. § 2709.

⁽²⁹¹⁾ 18 U.S.C. § 2709(b).

⁽²⁹²⁾ Например 18 U.S.C. § 2709(d).

3.2.1.3 По-нататъшно използване на събраната информация

- (154) Обработването на лични данни, събрани от разузнавателните агенции на САЩ чрез радиоелектронно разузнаване, подлежи на редица предпазни мерки.
- (155) На първо място, всяка разузнавателна агенция трябва да осигури подходяща сигурност на данните и да предотврати достъпа на неупълномощени лица до лични данни, събрани чрез радиоелектронно разузнаване. В това отношение различни инструменти, включително закони, насоки и стандарти, допълнително уточняват минималните изисквания за сигурност на информацията, които трябва да бъдат въведени (например многофакторно удостоверяване на автентичността, криптиране и др.) ⁽²⁹³⁾. Достъпът до събраните данни трябва да бъде ограничен до упълномощен, обучен персонал, който има нужда да знае информацията, за да изпълни задачата си ⁽²⁹⁴⁾. В по-общ план разузнавателните агенции трябва да осигурят подходящо обучение на служителите си, включително относно процедурите за докладване и разглеждане на нарушения на закона (включително Указ 14086) ⁽²⁹⁵⁾.
- (156) На второ място, разузнавателните агенции трябва да спазват стандартите на разузнавателната общност за точност и обективност, по-специално по отношение на осигуряването на качество и надеждност на данните, разглеждането на алтернативни източници на информация и обективността при извършването на анализите ⁽²⁹⁶⁾.
- (157) На трето място, що се отнася до съхраняването на данни, в Указ 14086 се пояснява, че личните данни на лица, които не са граждани на САЩ, подлежат на същите периоди на съхранение като тези, които се прилагат за данните на лица, граждани на САЩ ⁽²⁹⁷⁾. Разузнавателните агенции за задължени да определят конкретни срокове за съхранение и/или факторите, които трябва да се вземат предвид при определянето на продължителността на приложимите срокове за съхранение (например дали информацията представлява доказателства за извършено престъпление; дали информацията представлява външно разузнавателна информация; дали информацията е необходима за защита на безопасността на лица или организации, включително жертви или цели на международен тероризъм), които са определени в различни правни инструменти ⁽²⁹⁸⁾.
- (158) Четвърто, прилагат се специфични правила по отношение на разпространението на лични данни, събрани чрез радиоелектронно разузнаване. Като общо изискване личните данни за лица, които не са граждани на САЩ, могат да се разпространяват само ако включват същия вид информация, която може да се разпространява за лица, граждани на САЩ, например информация, необходима за защита на безопасността на дадено лице или организация (като цели, жертви или заложници на международни терористични организации) ⁽²⁹⁹⁾. Освен това личните данни не могат да се разпространяват единствено поради гражданството или държавата на пребиваване на дадено лице или с цел заобикаляне на изискванията на Указ 14086 ⁽³⁰⁰⁾. Разпространението на информация в рамките на правителството на САЩ може да се извършва само ако упълномощено и обучено лице има основателна увереност, че получателят има

⁽²⁹³⁾ Член 2(c)(iii)(B)(1) от Указ 14086. Вж. също дял VIII от Закона за националната сигурност (в който подробно са описани изискванията за достъп до класифицирана информация), Указ 12333, член 1.5 (изискваща от ръководителите на агенциите на разузнавателната общност да спазват насоките за обмен на информация и сигурност, неприкосновеността на личния живот и други законови изисквания), Указ 42 относно националната сигурност, „Национална политика за сигурност на телекомуникационните и информационните системи за национална сигурност“ (с който на Комитета по системите за национална сигурност се разпорежда да предоставя на изпълнителните департаменти и агенции насоки за системна сигурност на системите за национална сигурност) и Меморандум за националната сигурност 8, „Подобряване на киберсигурността на системите за национална сигурност, системите на Министерството на отбраната и разузнавателната общност“ (в който се установяват срокове и насоки за това как ще се прилагат изискванията за киберсигурност за системите за национална сигурност, включително многофакторно удостоверяване на автентичността, криптиране, облачни технологии и услуги за откриване на крайни точки).

⁽²⁹⁴⁾ Член 2(c)(iii)(B)(2) от Указ 14086. Освен това достъпът до лични данни, за които не е взето окончателно решение за запазване, може да бъде осъществен само с цел да се издаде или подкрепи такова решение или за да се осъществяват разрешени административни, тестови, развойни, охранителни или надзорни функции (член 2, буква с), подточка iii), буква В, точка 3 от Указ 14086).

⁽²⁹⁵⁾ Член 2(d)(ii) от Указ 14086.

⁽²⁹⁶⁾ Член 2(c)(iii)(C) от Указ 14086.

⁽²⁹⁷⁾ Член 2(c)(iii)(A)(2)(a)-(c) от Указ 14086. В по-общ план всяка агенция трябва да въведе политики и процедури, предназначени да сведат до минимум разпространението и съхранението на лични данни, събрани чрез радиоелектронно разузнаване (член 2, буква с), подточка iii), буква А от Указ 14086).

⁽²⁹⁸⁾ Вж. например член 309 от Закона за разрешаване на разузнавателни дейности за финансова 2015 година; процедури за свеждане на данните до минимум, приети от отделни разузнавателни служби съгласно член 702 от FISA и одобрени от FISC; процедури, одобрени от министъра на правосъдието и FRA (с които от федералните агенции на САЩ, включително агенциите за национална сигурност, се изисква да определят срокове за съхранение на своите записи, които трябва да бъдат одобрени от Националната администрация на архивите и документите (National Archives and Record Administration)).

⁽²⁹⁹⁾ Член 2(c)(iii)(A)(1)(a) и 5(d) Указ 14086, във връзка с член 2.3 от Указ 12333.

⁽³⁰⁰⁾ Член 2(c)(iii)(A)(1)(b) и (e) от Указ 14086.

нужда да знае информацията ⁽³⁰¹⁾ и ще я защити по подходящ начин ⁽³⁰²⁾. За да се определи дали личните данни могат да се разпространяват до получатели извън правителството на САЩ (включително чуждестранно правителство или международна организация), трябва да се вземат предвид целта на разпространението, естеството и обхватът на разпространяваните данни, както и потенциалът за вредно въздействие върху съответното(ите) лице(а) ⁽³⁰³⁾.

- (159) И накрая, включително с цел улесняване на надзора върху спазването на приложимите правни изисквания, както и с цел наличието на ефективните средства за правна защита, от всяка разузнавателна агенция се изисква съгласно Указ 14086 да води подходяща документация относно събирането на радиоелектронни разузнавателни данни. Изискванията за документиране обхващат елементи като фактическото основание за оценката, че конкретна дейност по събиране на информация е необходима за постигане на напредък по обоснован приоритет по отношение на разузнаването ⁽³⁰⁴⁾.
- (160) В допълнение към горепосочените гаранции, предвидени в Указ 14086, за използването на информация, събрана чрез радиоелектронно разузнаване, всички разузнавателни агенции на САЩ подлежат на по-обща изисквания относно ограничаването в рамките на целта, свеждането на данните до минимум, степента на точност, сигурността, запазването и разпространението, които следват по-специално от Циркулярно писмо на OMB № A-130, Закона за електронното правителство, Закона за федералните архиви (вж. съображения 101—106) и насоките от Комитета по системите за национална сигурност (CNSS) ⁽³⁰⁵⁾.

3.2.2 Надзор

- (161) Дейността на разузнавателните служби на САЩ подлежи на надзор от различни органи.
- (162) На първо място, Указ 14086 изисква всяка разузнавателна агенция да разполага с висши служители в областта на правото, надзора и съответствието, които да гарантират спазването на приложимото законодателство на САЩ ⁽³⁰⁶⁾. По-специално те трябва да извършват периодичен надзор над дейностите по радиоелектронно разузнаване и да гарантират, че всяко несъответствие се отстранява. Разузнавателните служби трябва да осигурят на тези служители достъп до цялата необходима информация, за да могат да изпълняват надзорните си функции, и не могат да предприемат никакви действия за възпрепятстване или неправомерно влияние върху надзорните им дейности ⁽³⁰⁷⁾. Освен това всеки съществен случай на несъответствие ⁽³⁰⁸⁾, установен от служител по надзора или друг служител, трябва незабавно да бъде докладван на ръководителя на разузнавателната агенция и на директора на националното разузнаване, който трябва да гарантира, че се предприемат всички необходими действия за отстраняване и предотвратяване на повторното възникване на съществения случай на несъответствие ⁽³⁰⁹⁾.
- (163) Тази надзорна функция се изпълнява от служители, на които е възложено да отговарят за спазването на изискванията, както и от служителите по въпросите на неприкосновеността на личния живот и гражданските свободи и от главни инспектори ⁽³¹⁰⁾.

⁽³⁰¹⁾ Вж. например в AGG-DOM се предвижда, че ФБР може да разпространява информация само, ако получателят има нужда да знае информацията, за да изпълни своята мисия или за защита на обществеността.

⁽³⁰²⁾ Член 2(с)(iii)(A)(1)(с) от Указ 14086. Разузнавателните агенции могат например да разпространяват информация при обстоятелства, свързани с наказателно разследване или свързани с престъпление, включително например чрез разпространяване на предупреждения за заплахи за убийство, тежка телесна повреда или отвлечение; разпространение на информация за киберзаплахи, инциденти или отговор на проникване; и уведомяване на жертви или предупреждаване на потенциални жертви на престъпление.

⁽³⁰³⁾ Член 2(с)(iii)(A)(1)(d) от Указ 14086.

⁽³⁰⁴⁾ Член 2(с)(iii)(E) от Указ 14086.

⁽³⁰⁵⁾ Вж. политика № 22 на CNSS, политика за управление на риска, свързан с киберсигурността, и указания 1253 на CNSS, в които се предоставят подробни насоки относно мерките за сигурност, които трябва да бъдат въведени за националните системи за сигурност.

⁽³⁰⁶⁾ Член 2(d)(i)(A)–(B) от Указ 14086.

⁽³⁰⁷⁾ Членове 2(d)(i)(B)—(C) от Указ 14086.

⁽³⁰⁸⁾ Т.е. системно или умишлено неспазване на приложимото законодателство на САЩ, което може да накърни репутацията или почтеността на елемент от разузнавателната общност или по друг начин да постави под съмнение коректността на дадена дейност на разузнавателната общност, включително с оглед на всяко значително въздействие върху интересите, свързани с неприкосновеността на личния живот и гражданските свободи на съответното лице или лица, вж. член 5, буква l) от Указ 14086.

⁽³⁰⁹⁾ Член 2(d)(iii) от Указ 14086.

⁽³¹⁰⁾ Раздел 2(d)(i)(B) от EO 14086.

- (164) Както при органите по наказателно правоприлагане, във всички разузнавателни агенции съществуват служители по въпросите на неприкосновеността на личния живот и гражданските свободи ⁽³¹¹⁾. Правомощията на тези служители обикновено включват надзора на процедурите с цел да се гарантира, че съответното министерство/агенция спазва по адекватен начин изискванията за неприкосновеност на личния живот и гражданските свободи и е въвело подходящи процедури за разглеждане на жалби от лица, които са счели, че неприкосновеността на личния им живот или гражданските им свободи са били нарушени (а в някои случаи, като например Службата на директора на Националното разузнаване (ODNI), могат да имат правомощия сами да провеждат разследвания по жалби ⁽³¹²⁾). Ръководителите на разузнавателните агенции трябва да гарантират, че служителите по въпросите на неприкосновеността на личния живот и гражданските свободи разполагат с необходимите ресурси, за да изпълняват мандата си, че им се предоставя достъп до всички материали и персонал, необходими за изпълнение на функциите им, и че са информирани за предложените промени в политиката и с тях се провеждат консултации ⁽³¹³⁾. Служителите по въпросите на гражданските свободи и неприкосновеността на личния живот периодично докладват пред Конгреса и Надзорния съвет по въпросите на неприкосновеността на личния живот и гражданските свободи, включително за броя и характера на получените в министерството/агенцията жалби, и предоставят обобщение на разпорежданията по тези жалби, проведените проверки и разследвания и последиците от дейностите, извършени от служителите ⁽³¹⁴⁾.
- (165) На второ място, всяка разузнавателна агенция има независим главен инспектор, в чиито отговорности се включва наред с останалото и упражняването на надзор върху дейностите по външно разузнаване. В рамките на ODNI това е Службата на главния инспектор по разузнавателните структури, която разполага с всеобхватна компетентност, обхващаща всички разузнавателни структури, и с правомощия да провежда разследвания въз основа на жалби или на информация относно обвинения в незаконни действия или злоупотреба с власт във връзка с програми и дейности на ODNI и/или на разузнавателните структури ⁽³¹⁵⁾. Както в случая с органите по наказателно правоприлагане (вж. съображение 109), тези главни инспектори са структури с независим статут ⁽³¹⁶⁾, които отговарят за провеждането на одити и разследвания във връзка с програмите и операциите, изпълнявани от съответната агенция за целите на националното разузнаване, включително по отношение на злоупотреби или закононарушения ⁽³¹⁷⁾. Те имат правомощия за достъп до всички записи, доклади, одити, прегледи, документи, писмени материали, препоръки или

⁽³¹¹⁾ Вж. 42 U.S.C., § 2000ee-1. Тук се включват например Държавният департамент, Министерството на правосъдието, Министерството на вътрешната сигурност, Министерството на отбраната, АНС, Централното разузнавателно управление (ЦРУ), ФБР и ODNI.

⁽³¹²⁾ Вж. член 3(c) от Указ 14086.

⁽³¹³⁾ 42 U.S.C. § 2000ee-1(d).

⁽³¹⁴⁾ Вж. 42 U.S.C. §§ 2000ee-1 (f)(1)-(2). Например докладът на Службата за граждански свободи, неприкосновеност на личния живот и прозрачност (Civil Liberties, Privacy and Transparency Office) към АНС за периода януари 2021 г. — юни 2021 г. показва, че тя е извършила 591 прегледа на въздействието върху гражданските свободи и неприкосновеността на личния живот в различни контексти, например по отношение на дейностите по събиране на данни, договореностите и решенията за обмен на информация, решенията за запазване на данни и др., като са взети предвид различни фактори, като например количеството и вида на информацията, свързана с дейността, участващите лица, целта и очакваното използване на данните, съществуващите предпазни мерки за намаляване на потенциалните рискове за неприкосновеност на личния живот и т.н. (https://media.defense.gov/2022/Apr/11/2002974486/-1/-1/1/REPORT%20_CLPT%20JANUARY%20-%20JUNE%202021%20_FINAL.PDF). По подобен начин докладите на Службата за неприкосновеност на личния живот и гражданските свободи (Office of Privacy and Civil Liberties — OPCL) към ЦРУ за периода януари — юни 2019 г. предоставят информация за надзорните дейности на службата, например преглед на спазването на насоките на министъра на правосъдието съгласно Указ 12333 по отношение на запазването и разпространението на информация, предоставените насоки относно прилагането на PPD 28 и изискванията за идентифициране и справяне с нарушенията на сигурността на данните, както и прегледи на използването и обработването на лични данни (<https://www.cia.gov/static/9d762fbef6669c7e6d7f17e227fad82c/2019-Q1-Q2-CIA-OPCL-Semi-Annual-Report.pdf>).

⁽³¹⁵⁾ Този главен инспектор се назначава от президента с утвърждаване от Сената и може да бъде отстранен от длъжност само от президента.

⁽³¹⁶⁾ Главните инспектори са с постоянно назначение и могат да бъдат отстранени от длъжност само от президента, който трябва да информира Конгреса писмено относно причините за отстраняването. Това не означава задължително, че те не получават никакви указания. В някои случаи ръководителят на министерството може да забрани на главния инспектор да инициира, извърши или завърши даден одит или разследване, когато счете това за необходимо за опазването на важни национални интереси (в областта на сигурността). Конгресът обаче трябва да е уведомен за упражняването на това правомощие и на тази основа може да потърси отговорност от съответния директор. Вж. например Закона за главния инспектор (Inspector General Act) от 1978 г., § 8 (на Министерството на отбраната); § 8E (на Министерството на правосъдието), § 8G (d)(2)(A),(B) (на АНС); 50. U.S.C. § 403q (b) (на ЦРУ); Закона за разрешаване на разузнавателни дейности за финансовата 2010 година (Intelligence Authorization Act For Fiscal Year 2010), Sec 405(f) (на структурите на разузнаването).

⁽³¹⁷⁾ Закон за главния инспектор от 1978 г. с измененията, публ. L. 117-108 от 8 април 2022 г. Например, както е обяснено в шестмесечните доклади до Конгреса, обхващащи периода 1 април 2021 г. — 31 март 2022 г., главният инспектор към АНС е извършил оценки на обработването на информация относно пенсите за лица, граждани на САЩ, събрана съгласно Указ 12333, на процеса за изчистване на данни от радиоелектронно разузнаване, на автоматизиран инструмент за целево събиране, използван от АНС, както и на спазването на правилата за документиране и първичен анализ по отношение на събирането на данни по член 702 от FISA, и е издал няколко препоръки в този контекст (вж. <https://oig.nsa.gov/Portals/71/Reports/SAR/NSA%20OIG%20SAR%20-%20APR%202021%20-%20SEP%202021%20-%20UNCLASSIFIED.pdf?ver=jbw2rCrJ00HJ9qDXGHqHLw%3d%3d×tamp=1657810395907>, стр. 5—8 и <https://oig.nsa.gov/Portals/71/Images/NSAOIGMAR2022.pdf?ver=jbw2rCrJ00HJ9qDXGHqHLw%3d%3d×tamp=1657810395907>, стр. 10—13). Вж. също неотдавнашните одити и разследвания, проведени от главния инспектор по разузнавателните структури относно информационната сигурност и неразрешеното разкриване на класифицирана информация, свързана с националната сигурност (https://www.dni.gov/files/ICIG/Documents/Publications/Semiannual%20Report/2021/ICIG_Semiannual_Report_April_2021_to_September_2021.pdf, стр. 8, 11 и https://www.dni.gov/files/ICIG/Documents/News/ICIGNews/2022/Oct21_SAR/Oct%202021-Mar%202022%20ICIG%20SAR_Unclass_FINAL.pdf, стр. 19—20).

други съответни материали, ако е необходимо, чрез връчване на призовка, и могат да събират показания ⁽³¹⁸⁾. Главните инспектори предават на ръководителите на агенциите случаи на предполагаеми криминални нарушения с цел започване на наказателно преследване и отправят препоръки за корективни мерки към ръководителите им ⁽³¹⁹⁾. Въпреки че препоръките им нямат задължителен характер, докладите им, включително относно последващите действия (или липсата на такива) ⁽³²⁰⁾, обикновено се оповестяват публично и се изпращат на Конгреса, който на тази основа може да упражнява собствената си надзорна функция (вж. съображение 168—169) ⁽³²¹⁾.

- (166) На трето място, Надзорният съвет по въпросите на разузнаването (Intelligence Oversight Board), създаден в рамките на Консултативния съвет по въпросите на разузнаването към президента (President's Intelligence Advisory Board), следи за спазването на Конституцията и всички приложими правила от страна на органите на САЩ, работещи в областта на разузнаването ⁽³²²⁾. Консултативният съвет по въпросите на разузнаването към президента е консултативен орган към административната канцелария на президента, който се състои от 16 членове, назначени от президента извън състава на правителството на САЩ. Надзорният съвет по въпросите на разузнаването се състои от максимум петима членове, определени от президента измежду членовете на Консултативния съвет по въпросите на разузнаването към президента. Съгласно Изпълнителен декрет 12333 ⁽³²³⁾ ръководителите на всички разузнавателни агенции са длъжни да докладват на Надзорния съвет по въпросите на разузнаването за всяка дейност за радиоелектронно разузнаване, за която има основание да се смята, че може да е незаконна или да противоречи на изпълнителен декрет или президентски указ. За да се гарантира, че Надзорният съвет по въпросите на разузнаването има достъп до информацията, необходима за изпълнение на функциите му, с Указ 13462 на директора на националното разузнаване и на ръководителите на разузнавателните агенции се разпорежда да предоставят всякаква информация и съдействие, които Надзорният съвет по въпросите на разузнаването определя като необходими за изпълнение на функциите си, доколкото това е позволено от закона ⁽³²⁴⁾. На свой ред Надзорният съвет по въпросите на разузнаването трябва да информира президента за дейности за разузнаване, за които смята, че може да са в нарушение на законите на САЩ (включително изпълнителни декрети) и по отношение на които министърът на правосъдието, директорът на националното разузнаване или ръководителят на дадена разузнавателна агенция не предприемат адекватни мерки ⁽³²⁵⁾. Освен това от Надзорния съвет по въпросите на разузнаването се изисква да информира министъра на правосъдието за евентуални нарушения на наказателното право.
- (167) На четвърто място, разузнавателните агенции подлежат на надзор от страна на PCLOB. Съгласно учредителния му устав на PCLOB са възложени отговорности в областта на политиките за борба с тероризма и тяхното прилагане с оглед на защитата на неприкосновеността на личния живот и гражданските свободи. При прегледа на действията на разузнавателните агенции той има право на достъп до всички съответни записи, доклади, одити, прегледи, документи, писмени материали и препоръки, включително до класифицирана информация, може да провежда изслушвания и да събира устни свидетелски показания ⁽³²⁶⁾. Той получава докладите на служителите по въпросите на гражданските свободи и неприкосновеността на личния живот от няколко федерални министерства/агенции ⁽³²⁷⁾, може да издава препоръки към държавни и разузнавателни агенции и докладва редовно пред комисиите в Конгреса и пред президента ⁽³²⁸⁾. Докладите на PCLOB, включително тези до Конгреса, трябва да бъдат публично достъпни във възможно най-голяма степен ⁽³²⁹⁾. PCLOB е публикувал няколко доклада относно надзора и последващите действия, включително анализ на програмите, изпълнявани въз основа на член 702 от FISA, и защитата на правото на неприкосновеност на личния живот в този контекст, прилагането на PPD 28 и на Изпълнителен декрет 12333 ⁽³³⁰⁾.

⁽³¹⁸⁾ Вж. Закона за главния инспектор от 1978 г., § 6.

⁽³¹⁹⁾ Вж. пак там §§ 4, 6—5.

⁽³²⁰⁾ Що се отнася до последващите действия, които се предприемат във връзка с докладите и препоръките на главните инспектори, вж. например отговора на доклад на главния инспектор към Министерството на правосъдието, в който се установява, че ФБР не е било достатъчно прозрачно по отношение на FISC в заявленията през периода 2014—2019 г., което доведе до реформи за подобряване на спазването, надзора и отчетността във ФБР (например директорът на ФБР разпореди повече от 40 корективни мерки, включително 12 специално за процедурите съгласно FISA, свързани с документирането, надзора, подтържането на досиета, обучението и одитите) (вж. <https://www.justice.gov/opa/pr/departments-justice-and-federal-bureau-investigation-announce-critical-reforms-enhance> и <https://oig.justice.gov/reports/2019/o20012.pdf>). Вж. например и одита от страна на главния инспектор към Министерството на правосъдието относно ролята и отговорностите на Службата на главния юрисконсулт към ФБР при надзора на спазването на приложимите закони, политики и процедури, свързани с дейностите на ФБР в областта на националната сигурност, както и допълнение 2, което включва писмо от ФБР, с което се приемат всички препоръки. В тази връзка в допълнение 3 е представен преглед на последващите действия и информация, които главният инспектор поиска от ФБР, за да може да закрие своите препоръки (<https://oig.justice.gov/sites/default/files/reports/22-116.pdf>).

⁽³²¹⁾ Вж. Закона за главния инспектор от 1978 г., §§ 4(5), 5.

⁽³²²⁾ Вж. Указ 13462.

⁽³²³⁾ Член 1.6(c) от Указ 12333.

⁽³²⁴⁾ Раздел 8(a) от ЕО 13462.

⁽³²⁵⁾ Член 6(b) от Указ 13462.

⁽³²⁶⁾ 42 U.S.C. § 2000ee-1(g).

⁽³²⁷⁾ Вж. 42 U.S.C. § 2000ee-1 (f)(1)(A)(iii). Тук се включват най-малкото Министерството на правосъдието, Министерството на отбраната, Министерството на вътрешната сигурност, директорът на националното разузнаване и Централното разузнавателно управление, както и други министерства, агенции или структури на изпълнителната власт, определени от PCLOB като подходящи да бъдат обхванати от правомощията му.

⁽³²⁸⁾ 42 U.S.C. § 2000ee (e).

⁽³²⁹⁾ 42 U.S.C. § 2000ee (f).

⁽³³⁰⁾ На разположение на адрес <https://www.pclob.gov/Oversight>.

PCLOV е натоварен и с изпълнението на конкретни надзорни функции по отношение на прилагането на Указ 14086, по-специално като проверява дали процедурите на агенциите са в съответствие с указа (вж. съображение 126) и оценява коректното функциониране на механизма за правна защита (вж. съображение 194).

- (168) На пето място, в допълнение към механизмите за надзор в рамките на изпълнителната власт, специални комисии в Конгреса на САЩ (Комисията по въпросите на разузнаването и Правната комисия към Камарата на представителите и Сената) са натоварени с отговорности по надзор на всички дейности на САЩ в областта на външното разузнаване. Членовете на тези комисии имат достъп до класифицирана информация, както и до разузнавателните методи и програми ⁽³³¹⁾. Комисиите упражняват надзорните си функции по различни начини, по-специално чрез изслушвания, разследвания, прегледи и доклади ⁽³³²⁾.
- (169) Комисиите на Конгреса получават редовни доклади относно разузнавателните дейности, включително от министъра на правосъдието, директора на националното разузнаване, разузнавателните агенции и други надзорни органи (например главни инспектори), вж. съображения 164—165. По конкретно, съгласно Закона за националната сигурност (National Security Act) „Президентът взема мерки комисии по въпросите на разузнаването в Конгреса да бъдат напълно и текущо информирани относно разузнавателните дейности на Съединените американски щати, включително за предвиждани значими разузнавателни дейности, както това се изисква съгласно настоящата подглава.“ ⁽³³³⁾. В допълнение „Президентът взема мерки на комисии по въпросите на разузнаването в Конгреса да бъде докладвано незабавно за всяка незаконна разузнавателна дейност, както и за всички корективни мерки, които са били взети или се планират във връзка с такава незаконна дейност.“ ⁽³³⁴⁾.
- (170) Освен това от конкретни закони произтичат допълнителни изисквания за докладване. Например във FISA се съдържа изискване към министъра на правосъдието да „информира в пълна степен“ комисията по въпросите на разузнаването и правната комисия към Камарата на представителите и Сената относно дейностите на правителството съгласно определени раздели от FISA ⁽³³⁵⁾. Също така в него се изисква правителството да предоставя на комисии на Конгреса копия от всички решения, заповеди или становища на FISC или FISCER, които включват „значими конструкции или тълкувания“ на разпоредбите на FISA. Във връзка с наблюдението съгласно член 702 от FISA парламентарният надзор се осъществява посредством изисквания по закон доклади до комисията по въпросите на разузнаването и правната комисия, както и чести брифинги и изслушвания. Към тях се включват шестмесечният доклад на министъра на правосъдието, в който се описва как е бил използван член 702 от FISA, с придружаващите го документи, включително докладите на Министерството на правосъдието и на ODNI за спазването на нормативната уредба, с описание на евентуални случаи на неспазване ⁽³³⁶⁾, както и отделна шестмесечна оценка от министъра на правосъдието и директора на Националното разузнаване, в която се описва спазването на процедурите за целево събиране и свеждане до минимум ⁽³³⁷⁾.

⁽³³¹⁾ 50 U.S.C. § 3091.

⁽³³²⁾ Например комисии организират тематични изслушвания (вж. например неотдавнашното изслушване на правната комисия към Камарата на представителите относно „цифровите мрежи“ (digital dragnets), <https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983>, и изслушването на комисията по въпросите на разузнаването към Камарата на представителите относно използването на изкуствен интелект от разузнавателната общност, <https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=114263>), редовни изслушвания с цел надзор, например на ФБР и отдела за национална сигурност към Министерството на правосъдието, вж. <https://www.judiciary.senate.gov/meetings/08/04/2022/oversight-of-the-federal-bureau-of-investigation>; <https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4966> и <https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4899>. Като пример за разследване вж. разследването на комисията по въпросите на разузнаването към Сената за намеса от страна на Русия в изборите в САЩ през 2016 г., вж. <https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures>. Що се отнася до докладването, вж. например прегледа на (надзорните) дейности на комисията в доклада до Сената на комисията по въпросите на разузнаването към Сената, обхващащ периода 4 януари 2019 г. — 3 януари 2021 г., <https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-covering-period-january-4>.

⁽³³³⁾ Вж. 50 U.S.C. § 3091(a)(1). В тази разпоредба се съдържат общите изисквания относно надзора, упражняван от Конгреса в областта на националната сигурност.

⁽³³⁴⁾ Вж. 50 U.S.C. § 3091(b).

⁽³³⁵⁾ Вж. 50 U.S.C. §§ 1808, 1846, 1862, 1871, 1881f.

⁽³³⁶⁾ Вж. 50 U.S.C. § 1881f.

⁽³³⁷⁾ Вж. 50 U.S.C. § 1881a(l)(1).

- (171) Освен това FISA съдържа изискване правителството на САЩ всяка година да оповестява пред Конгреса (и обществеността) наред с другото и броя на поисканите и получените разпореждания и указания съгласно FISA, както и изчисления за броя на лицата — граждани на САЩ, и лицата, които не са граждани на САЩ, които са били цел на наблюдение ⁽³³⁸⁾. Също така в закона се предвижда изискване за допълнително докладване пред обществеността относно броя на издадените писма във връзка с националната сигурност (ПНС), отново по отношение на лица — граждани на САЩ, и лица, които не са граждани на САЩ (като същевременно се предвижда получателите на разпореждания и сертифицирания съгласно FISA, както и на искания за ПНС, да публикуват доклади за прозрачност при определени условия) ⁽³³⁹⁾.
- (172) В по-общ план разузнавателната общност на САЩ полага различни усилия, за да осигури прозрачност на своите дейности по (външно) разузнаване. Например през 2015 г. ODNI прие Принципи за прозрачност на разузнаването и План за прилагане на прозрачността и разпреди на всяка разузнавателна агенция да назначи служител по прозрачността на разузнаването, който да насърчава прозрачността и да ръководи инициативи за прозрачност ⁽³⁴⁰⁾. Като част от тези усилия разузнавателната общност публикува и продължава да публикува разсекретени части от политиките, процедурите, докладите за надзор, докладите за дейностите по член 702 от FISA и по Изпълнителен декрет 12333, решенията на FISC и други материали, включително на специална уебстраница „IC on the Record“, управлявана от ODNI ⁽³⁴¹⁾.
- (173) И накрая, събирането на лични данни съгласно член 702 от FISA подлежи, в допълнение към надзора от страна на надзорните органи, посочени в съображения 162—168, на надзор от страна на FISC ⁽³⁴²⁾. Съгласно правило 13 от Процедурния правилник на FISC служителите по съответствието в разузнавателните агенции на САЩ са длъжни да докладват за всички нарушения на процедурите за целево събиране, свеждане до минимум и първичен анализ по член 702 от FISA на Министерството на правосъдието и на ODNI, които от своя страна ги докладват на FISC. Освен това Министерството на правосъдието и Службата на директора на Националното разузнаване (ODNI) представят на FISC шестмесечни съвместни доклади за оценка на надзора, в които се посочват тенденциите при спазването на изискванията по отношение на целевото събиране; предоставят се статистически данни; описват се категориите инциденти, свързани със съответствието; описват се подробно причините, поради които са възникнали определени инциденти, свързани със спазването на целевото събиране, и се очертават мерките, които разузнавателните агенции са предприели, за да избегнат повтарянето им ⁽³⁴³⁾.
- (174) Когато е необходимо (например при установяване на нарушения на процедурите за определяне на обектите на разследване), FISC може да нареди на съответната разузнавателна агенция да предприеме правни действия за защита ⁽³⁴⁴⁾. Тези въпросни правни средства за защита варират от индивидуални до структурни мерки, например от прекратяване на събирането на данни и заличаването на незаконно получените данни до промяна на практиките за събиране на данни, включително по отношение на предоставянето на насоки и обучението на персонала ⁽³⁴⁵⁾. Освен

⁽³³⁸⁾ 50 U.S.C. § 1873(b). В допълнение към това, съгласно член 402 „директорът на Националното разузнаване, в консултация с министъра на правосъдието, извършва преглед за разсекретяване на всяко решение, разпореждане или становище на Съда по надзора върху външното разузнаване или на Апелативния съд за наблюдение на чуждите разузнавателни служби (както това е предвидено в член 601, буква е), в което се съдържат значими конструкции или тълкувания на някоя законова разпоредба, включително нови или значими конструкции или тълкувания на понятието „конкретен критерий за подбор“, и съгласно този преглед обявява публично, доколкото това е практически възможно, всяко такова решение, разпореждане или становище“.

⁽³³⁹⁾ 50 U.S.C. §§ 1873(b)(7) и 1874.

⁽³⁴⁰⁾ <https://www.dni.gov/index.php/ic-legal-reference-book/the-principles-of-intelligence-transparency-for-the-ic>.

⁽³⁴¹⁾ Вж. „IC on the Record“, на разположение на адрес <https://icontherecord.tumblr.com/>.

⁽³⁴²⁾ В миналото FISC е направил заключението, че „съдът е наясно, че изпълнителните агенции, както и ODNI и Отделът за национална сигурност на Министерството на правосъдието отделили значителни ресурси за своите отговорности по спазването и надзора във връзка с член 702. Като общо правило случаите на несъответствие се установяват незабавно и се предприемат подходящи коригиращи действия, които включват изчистване на информацията, която е била неправомерно получена или по друг начин подлежи на изискванията за унищожаване съгласно приложимите процедури“. FISA Court, Memorandum Opinion and Order (Становище меморандум и разпореждане) [заглавието е редактирано] (2014 г.), достъпно на адрес <https://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf>.

⁽³⁴³⁾ Вж. например DOJ/ODNI FISA 702 Compliance Report to FISC for June 2018 - Nov. 2018 (Доклад на Министерството на правосъдието и Националната служба за охрана за съответствие с FISA 702 за периода юни 2018 г. — ноември 2018 г.), 21—65.

⁽³⁴⁴⁾ 50 U.S.C. § 1803(h). Вж. също PCLOB, Доклад по член 702, стр. 76. Вж. в допълнение Становище меморандум и разпореждане на FISC от 3 октомври 2011 г. като пример за заповед за отстраняване на недостатъци, в която на правителството е наредено да отстрани установените недостатъци в срок от 30 дни. На разположение на адрес <https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and-Order-20140716.pdf>. Вж. писмото на Walton, член 4, стр. 10—11. Вж. също така Становището на FISC от 18 октомври 2018 г., достъпно на адрес https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf, потвърдено от Апелативния съд за наблюдение на чуждите разузнавателни служби в Становището му от 12 юли 2019 г., достъпно на адрес https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opinion_12Jul19.pdf, в което FISC, наред с другото, нарежда на правителството да спазва определени изисквания за уведомяване, документиране и докладване пред FISC.

⁽³⁴⁵⁾ Вж. например FISC, Становище меморандум и разпореждане по член 76 (6 декември 2019 г.) (разрешено за публично публикуване на 4 септември 2020 г.), в което FISC нареди на правителството да представи писмен доклад до 28 февруари 2020 г. относно стъпките, които правителството предприема, за да подобри процесите за идентифициране и премахване на доклади, получени въз основа на информацията по FISA 702, които са били оттеглени поради съображения за съответствие, както и по други въпроси. Вж. и приложение VII.

това по време на годишния преглед на сертифициранятия по член 702 FISC разглежда случаите на несъответствие, за да определи дали представените удостоверения отговарят на изискванията на FISA. По подобен начин, ако FISC установи, че сертифициранятия от страна на правителството не са били задоволителни, включително поради конкретни случаи на неспазване, той може да издаде така наречената „заповед за отстраняване на недостатъци“, изискваща от правителството да отстрани нарушението в срок от 30 дни или да прекрати или да не започва да прилага сертифициране по член 702. И накрая, FISC оценява тенденциите, които наблюдава по отношение на проблемите със спазването на изискванията, и може да поиска промени в процедурите или допълнителен надзор и докладване, за да се справи с тези тенденции ⁽³⁴⁶⁾.

3.2.3 Средства за правна защита

- (175) Както е обяснено по-подробно в настоящия раздел, редица способности в Съединените щати предоставят на субектите на данни от Съюза възможността да предявяват иск пред независим и безпристрастен съд с обвързващи правомощия. Взети заедно те дават възможност на физическите лица да имат достъп до своите лични данни, да поискат проверка на законосъобразността на правителствения достъп до техните данни и, ако бъде установено нарушение, да поискат отстраняване на това нарушение, включително чрез коригиране или заличаване на техните лични данни.
- (176) На първо място, в съответствие с Указ 14086 е създаден специален механизъм за правна защита, допълнен от Наредбата на МП за създаване на Апелативен съд в областта на защитата на личните данни, който да разглежда и решава жалби на физически лица относно дейностите на САЩ по радиоелектронно разузнаване. Всяко физическо лице в ЕС има право да подаде жалба в рамките на механизма за правна защита във връзка с предполагаемо нарушение на законодателството на САЩ, уреждащо дейностите по радиоелектронно разузнаване (например Указ 14086, член 702 от FISA, Указ 12333), което засяга неблагоприятно интересите му в областта на неприкосновеността на личния живот и гражданските свободи ⁽³⁴⁷⁾. Този механизъм за правна защита е достъпен за физически лица от държави или регионални организации за икономическа интеграция, които са били посочени от министъра на правосъдието на САЩ като „квалифицирани държави“ ⁽³⁴⁸⁾. На 30 юни 2023 г. Европейският съюз и трите държави от Европейската асоциация за свободна търговия, които съставляват Европейското икономическо пространство, бяха посочени от министъра на правосъдието на САЩ като „квалифицирани държави“ съгласно член 3(f) от Указ 14086 ⁽³⁴⁹⁾. Това посочване не засяга член 4, параграф 2 от Договора за Европейския съюз.
- (177) Субектът на данни в Съюза, желаещ да внесе такава жалба, трябва да внесе жалбата до надзорен орган в държава — членка на ЕС, компетентен за надзора на обработването на лични данни от страна на публични органи (ОЗД) ⁽³⁵⁰⁾. Това осигурява лесен достъп до механизма за правна защита, като позволява на лицата да се обръщат към орган, който е „близо до дома им“ и с който могат да общуват на собствения си език. След като съответствието с изискванията за подаване на жалба, посочени с въображение 178, е проверено, компетентният ОЗД, посредством секретариата на Европейския комитет по защита на данните, ще насочи жалбата към механизма за правна защита.
- (178) Подаването на жалба до механизма за правна защита подлежи на ниски изисквания за допустимост, тъй като не е необходимо лицата да доказват, че техните данни действително са били обект на дейности за радиоелектронно разузнаване от страна на САЩ ⁽³⁵¹⁾. В същото време, за да се осигури отправна точка за извършване на преглед чрез механизма за правна защита, трябва да се предостави определена основна информация, например относно личните данни, за които има разумно основание да се смята, че са били предадени на САЩ, и средствата, чрез които се смята, че са били предадени; идентификация на държавните органи на САЩ, за които се смята, че са замесени в предполагаемото нарушение (ако са известни); основанията, на което се твърди, че е извършено нарушение на правото на САЩ (въпреки че и тук това не изисква да се докаже, че действително са били събирани лични данни от разузнавателните служби на САЩ); и естеството на исканото обезщетение.

⁽³⁴⁶⁾ Вж. приложение VII.

⁽³⁴⁷⁾ Вж. член 4, буква к), подточка iv) от Указ 14086, който предвижда, че жалба чрез механизма за правна защита трябва да бъде подадена от жалбоподател, действащ в лично качество (т.е. не като представител на правителство, неправителствена или междуправителствена организация). Понятието „неблагоприятно засегнат“ не изисква жалбоподателят да отговаря на определен праг, за да има достъп до механизма за правна защита (вж. в тази връзка съображение 178). По-скоро с него се разяснява, че на CLPO и Апелативния съд в областта на защитата на личните данни (DPRC) към ODNI се предоставя правомощието да коригират нарушенията на законодателството на САЩ, уреждащо дейностите по радиоелектронно разузнаване, които засягат неблагоприятно интересите на жалбоподателя в областта на неприкосновеността на личния живот и гражданските свободи. Обратно, нарушенията на изискванията съгласно приложимото законодателство на САЩ, които не са предназначени да защитават лица (напр. бюджетни изисквания), биха попадали извън компетентността на CLPO и DPRC към ODNI.

⁽³⁴⁸⁾ Член 3(f) от Указ 14086.

⁽³⁴⁹⁾ <https://www.justice.gov/opcl/executive-order-14086>.

⁽³⁵⁰⁾ Раздел 4(d)(v) от EO 14086.

⁽³⁵¹⁾ Вж. член 4(k)(i)—(iv) от Указ 14086.

- (179) Първоначалното разследване на жалби, подадени до този механизъм за правна защита, се извършва от CLPO към ODNİ, чиято съществуваща законова роля и правомощия бяха разширени, за да обхванат тези конкретните действия, предприети съгласно Указ 14086 ⁽³⁵²⁾. В рамките на разузнавателната общност CLPO отговаря, *inter alia*, за гарантирането на това защитата на гражданските свободи и на неприкосновеността на личния живот да бъде включена по подходящ начин в политиките и процедурите на ODNİ и разузнавателните агенции; за надзора на спазването от страна на ODNİ на приложимите изисквания във връзка с гражданските свободи и неприкосновеността на личния живот; и за извършването на оценки на въздействието върху неприкосновеността на личния живот ⁽³⁵³⁾. CLPO към ODNİ може да бъде уволнен от директора на националното разузнаване само по причина, т.е. в случай на неправомерно поведение, злоупотреба, нарушаване на сигурността, пренебрегване на задълженията или неспособност ⁽³⁵⁴⁾.
- (180) При извършването на прегледа CLPO към ODNİ има достъп до информацията, необходима за неговата оценка, и може да разчита на задължително съдействие от страна на служителите по въпросите на неприкосновеността на личния живот и гражданските свободи в различните разузнавателни агенции ⁽³⁵⁵⁾. На разузнавателните агенции е забранено да възпрепятстват или да оказват неправомерно влияние върху прегледите на CLPO към ODNİ. В това число влиза и директорът на националното разузнаване, който не трябва да се намесва в прегледа ⁽³⁵⁶⁾. При разглеждането на жалба CLPO към ODNİ трябва „да прилага закона безпристрастно“, като взема предвид както интересите на националната сигурност, свързани с дейностите по радиоелектронно разузнаване, така и мерките за защита на неприкосновеността на личния живот ⁽³⁵⁷⁾.
- (181) В рамките на прегледа CLPO към ODNİ определя дали е извършено нарушение на приложимото право на САЩ и, ако това е така, взема решение за подходящи коригиращи мерки ⁽³⁵⁸⁾. Последното се отнася до мерки, с които напълно се отстранява установеното нарушение, като прекратяване на незаконното придобиване на данни, заличаване на незаконно събрани данни, заличаване на резултатите от неподходящо проведени търсения за иначе законно събрани данни, ограничаване на достъпа до законно събрани данни до подходящо обучен персонал или изтегляне на разузнавателни доклади, съдържащи данни, придобити без законно разрешение или които са били незаконно разпространени ⁽³⁵⁹⁾. Решенията на CLPO към ODNİ по индивидуални жалби (включително за отстраняване на нередности) са задължителни за съответните разузнавателни агенции ⁽³⁶⁰⁾.
- (182) CLPO към ODNİ трябва да съхранява документацията от прегледа и да изготви решение, съдържащо класифицирана информация, в което да обясни основанието за фактическите си констатации, решението по отношение на това дали е извършено попадане в приложното поле нарушение и определянето на подходящата корективна мярка ⁽³⁶¹⁾. Ако при прегледа на CLPO към ODNİ се разкрие нарушение на някое от правомощията, подлежащи на надзор от страна на FISC, CLPO трябва също така да предостави съдържащ класифицирана информация доклад на заместник-министъра на правосъдието по въпросите на националната сигурност, който от своя страна е длъжен да докладва за несъответствието на FISC, който може да предприеме по-нататъшни действия по правоприлагане (в съответствие с процедурата, описана в съображения 173—174) ⁽³⁶²⁾.
- (183) След приключване на прегледа CLPO към ODNİ информира жалбоподателя чрез националния орган, че „при прегледа или не са установени никакви попадащи в приложното поле нарушения, или CLPO към ODNİ е издал решение, налагащо подходящи корективни мерки“ ⁽³⁶³⁾. Това позволява да се защити поверителността на дейностите, извършвани с цел защита на националната сигурност, като същевременно на лицата се предоставя решение, потвърждаващо, че жалбата им е била надлежно разследвана и разглеждана. Освен това, това решение може да бъде оспорено от лицето. За тази цел то ще бъде информирано за възможността да обжалва пред DPCR за преразглеждане на решенията на CLPO (вж. съображение 184 и следващите) и че в случай на сезиране на съда ще бъде избран специален адвокат, който да защитава интересите на жалбоподателя ⁽³⁶⁴⁾.

⁽³⁵²⁾ Член 3(c)(iv) от Указ 14086. Вж. също Закона за националната сигурност от 1947 г., 50 U.S.C. § 403-3d, член 103D относно ролята на CLPO в рамките на ODNİ.

⁽³⁵³⁾ 50 U.S.C. § 3029 (b).

⁽³⁵⁴⁾ Член 3(c)(iv) от Указ 14086.

⁽³⁵⁵⁾ Член 3(c)(iii) от Указ 14086.

⁽³⁵⁶⁾ Член 3(c)(iv) от Указ 14086.

⁽³⁵⁷⁾ Член 3(c)(i)(B)(i) и (iii) от Указ 14086.

⁽³⁵⁸⁾ Член 3(c)(i) от Указ 14086.

⁽³⁵⁹⁾ Раздел 4(a) от ЕО 14086.

⁽³⁶⁰⁾ Член 3(c)(d) от Указ 14086.

⁽³⁶¹⁾ Член 3(c)(i)(F)—(G) от Указ 14086.

⁽³⁶²⁾ Вж. също член 3(c)(i)(D) от Указ 14086.

⁽³⁶³⁾ Член 3(c)(i)(E)(1) от Указ 14086.

⁽³⁶⁴⁾ Членове 3(c)(i)(E)(2)—(3) от Указ 14086.

- (184) Всеки жалбоподател, както и всяка структура на разузнавателната общност, може да поиска преразглеждане на решението на CLPO към ODNI пред Апелативния съд в областта на защитата на личните данни (DPRC). Такива молби за преразглеждане трябва да бъдат подадени в срок от 60 дни след получаване на уведомлението от CLPO към ODNI, че преразглеждането е приключило, и да включват всякаква информация, която лицето желае да предостави на DPRC (например доводи по правни въпроси или прилагането на правото към фактите по делото) ⁽³⁶⁵⁾. Субектите на данни от Съюза могат отново да подадат заявлението си до компетентния ОЗД (вж. съображение 177).
- (185) DPRC е независим трибунал, създаден от министъра на правосъдието въз основа на Изпълнителен декрет 14086 ⁽³⁶⁶⁾. Той се състои от най-малко шестима съдии, които се назначават от министъра на правосъдието след консултации с PCLOB, министъра на търговията и директора на националното разузнаване за срок от четири години с възможност за подновяване на мандата ⁽³⁶⁷⁾. Назначаването на съдиите от министъра на правосъдието се основава на критериите, използвани от изпълнителната власт при оценката на кандидатите за федералната съдебна власт, като се отдава значение на всеки предишен правораздавателен опит ⁽³⁶⁸⁾. Освен това съдиите трябва да са практикуващи юристи (т.е. активни членове на адвокатската колегия с добра репутация и надлежно лицензирани да практикуват право) и да имат подходящ опит в областта на правото на неприкосновеност на личния живот и националната сигурност. Министърът на правосъдието трябва да се стреми да гарантира, че поне половината от съдиите във всеки един момент имат предишен правораздавателен опит, а всички съдии трябва да притежават разрешение за достъп до класифицирана информация, свързана с националната сигурност ⁽³⁶⁹⁾.
- (186) За членове на DPRC могат да бъдат назначавани само лица, които отговарят на изискванията, посочени в съображение 185, и които не са служители на изпълнителната власт към момента на назначаването им или през предходните две години. Също така по време на мандата си в DPRC съдиите не могат да имат никакви официални задължения или да заемат официална длъжност в правителството на САЩ (освен като съдии в DPRC) ⁽³⁷⁰⁾.
- (187) Независимостта на процеса на произнасяне се постига чрез редица гаранции. По-специално, на изпълнителната власт (министъра на правосъдието и разузнавателните служби) е забранено да се намесва или да оказва неправомерно влияние върху прегледа, извършван от DPRC ⁽³⁷¹⁾. Самият DPRC е длъжен да се произнася безпристрастно по делата ⁽³⁷²⁾ и да работи съгласно собствения си процедурен правилник (приет с мнозинство). Освен това съдиите от DPRC могат да бъдат уволнени само от министъра на правосъдието и само по определена причина (т.е. неправомерно поведение, злоупотреба, нарушаване на сигурността, пренебрегване на служебните задължения или неспособност), след като надлежно се вземат предвид стандартите, приложими за федералните съдии, установени в Правилата за поведение на съдиите и производства за установяване на неправомерност ⁽³⁷³⁾.
-
- ⁽³⁶⁵⁾ Членове 201.6(a)–(б) от Наредбата на МП.
- ⁽³⁶⁶⁾ Член 3(d)(i) и Наредбата на МП. Върховният съд на Съединените щати е признал възможността министърът на правосъдието да създава независими органи с правомощия за вземане на решения, включително да се произнася по отделни дела, вж. по-специално *United States ex rel. Accardi/Shughnessy*, 347 U.S. 260 (1954 г.) и *United States/Nixon*, 418 U.S. 683, 695 (1974 г.). Спазването на различните изисквания на Указ 14086, например критериите и процедурата за назначаване и уволняване на съдии от DPRC, е предмет по-специално на надзора на главния инспектор на Министерството на правосъдието (вж. също съображение 109 относно законовите правомощия на главните инспектори).
- ⁽³⁶⁷⁾ Член 3(d)(i)(A) от Указ 14086 и член 201.3(a) от Наредбата на МП.
- ⁽³⁶⁸⁾ Член 201.3(b) от Наредбата на МП.
- ⁽³⁶⁹⁾ Раздел 3(d)(i)(B) от Указ 14086.
- ⁽³⁷⁰⁾ Член 3(d)(i)(A) от Указ 14086 и член 201.3(a) и (с) от Наредбата на МП. Лицата, назначени за членове на DPRC, могат да участват в извънсъдебни дейности, включително стопански дейности, финансови дейности, дейности за набиране на средства с нестопанска цел, фидуциарни дейности и правоприлагане, когато посочените дейности не възпрепятстват безпристрастното изпълнение на техните задължения или ефективността или независимостта на DPRC (вж. член 201.7(c) от Наредбата на МП).
- ⁽³⁷¹⁾ Член 3(d)(iii)–(iv) от Указ 14086 и член 201.7(d) от Наредбата на МП.
- ⁽³⁷²⁾ Член 3(d)(i)(D) от Указ 14086 и член 201.9 от Наредбата на МП.
- ⁽³⁷³⁾ Член 3(d)(iv) от Указ 14086 и член 201.7(d) от Наредбата на МП. Вж. също *Витар/Съединени американски щати*, 252 U.S., 512, 515 (1920 г.), в което се потвърждава дългогодишният принцип в законодателството на САЩ, че правомощието за отстраняване е свързано с правомощието за назначаване (както е припомнено от Службата на правния съветник към Министерството на правосъдието в Конституционното разделение на властите между президента и Конгреса, 20 Op. O.L.C. 124, 166 (1996 г.)).

- (188) Заявленията до DPRC се разглеждат от състави от трима съдии, включително председателстващ съдия, които трябва да действат в съответствие с Кодекса за поведение на съдиите на САЩ ⁽³⁷⁴⁾. Всеки съдебен състав се подпомага от специален адвокат ⁽³⁷⁵⁾, който има достъп до цялата информация, свързана със случая, включително класифицирана информация ⁽³⁷⁶⁾. Ролята на специалния адвокат е да гарантира, че интересите на жалбоподателя са представени и че съставът на DPRC е добре информиран за всички правни и фактически въпроси от значение ⁽³⁷⁷⁾. За да предостави допълнителна информация за позицията си по молба за преразглеждане, подадена до DPRC от физическо лице, специалният адвокат може да потърси информация от жалбоподателя чрез писмени въпроси ⁽³⁷⁸⁾.
- (189) DPRC разглежда решенията, взети от CLPO към ODNi (както по отношение на това дали е извършено нарушение на приложимото право на САЩ, така и по отношение на подходящите корективни мерки), като се основава най-малко на протокола от разследването на CLPO към ODNi, както и на всякаква информация и документи, предоставени от жалбоподателя, специалния адвокат или разузнавателна агенция ⁽³⁷⁹⁾. Съставът на DPRC има достъп до цялата информация, необходима за извършване на прегледа, която може да получи чрез CLPO към ODNi (съставът може например да поиска от CLPO да допълни записите с допълнителна информация или факти, ако това е необходимо за извършване на прегледа) ⁽³⁸⁰⁾.
- (190) В заключение на прегледа DPRC може 1) да реши, че няма доказателства, които да сочат, че са извършени дейности по радиоелектронно разузнаване, включващи лични данни на жалбоподателя, 2) да реши, че решенията на CLPO към ODNi са правилни от правна гледна точка и са подкрепени със съществени доказателства, или, 3) ако DPRC не е съгласен с решенията на CLPO към ODNi (за това дали е извършено нарушение на приложимото право на САЩ или за подходящите корективни мерки), да издаде свои собствени решения ⁽³⁸¹⁾.

⁽³⁷⁴⁾ Член 3(d)(i)(B) от Указ 14086 и член 201.7(a)-(c) от Наредбата на МП. Службата за неприкосновеността на личния живот и гражданските свободи (Office of Privacy and Civil Liberties (OPCL) към Министерството на правосъдието, която отговаря за предоставянето на административна подкрепа на DPRC и специалните адвокати (вж. член 201.5 от Наредбата на МП), избира тричленен състав на ротационен принцип, като се стреми да гарантира, че във всеки състав има поне един съдия с предишен правораздавателен опит (ако никой от съдиите в състава няма такъв опит, председателят ще бъде съдията, избран първи от OPCL).

⁽³⁷⁵⁾ Член 201.4 от Наредбата на МП. Най-малко двама специални адвокати се назначават от министъра на правосъдието след консултация с министъра на търговията, директора на националното разузнаване и PCLOV за срок от два мандата, който може да бъде подновен. Специалните адвокати трябва да имат подходящ експертен опит в областта на правото на неприкосновеност на личния живот и националната сигурност, да са опитни адвокати, активни членове на адвокатската колегия с добра репутация и надлежно лицензирани да практикуват право. Освен това към момента на първоначалното им назначаване те не трябва да са били служители на изпълнителната власт през предходните две години. За всяко разглеждане на молба председателстващият съдия избира специален адвокат, който да подпомага състава, вж. член 201.8(a) от Наредбата на МП.

⁽³⁷⁶⁾ Член 201.8(b) и 201.11 от Наредбата на МП.

⁽³⁷⁷⁾ Член 3(d)(i)(C) от Указ 14086 и член 201.8(e) от Наредбата на МП. Специалният адвокат не действа като представител на жалбоподателя и не е във взаимоотношения между адвокат и клиент с него.

⁽³⁷⁸⁾ Вж. член 201.8(d)(e) от Наредбата на МП. Такива въпроси първо се разглеждат от OPCL, след консултация със съответната структура на разузнавателната общност, с цел да се идентифицира и изключи всякаква класифицирана, привилегирована или защитена информация, преди да бъдат изпратени на жалбоподателя. Допълнителната информация, получена от специалния адвокат в отговор на тези въпроси, се включва в становищата на специалния адвокат до DPRC.

⁽³⁷⁹⁾ Член 3(d)(i)(D) от Указ 14086.

⁽³⁸⁰⁾ Член 3(d)(iii) от Указ 14086 и член 201.9(b) от Наредбата на МП.

⁽³⁸¹⁾ Член 3(d)(i)(E) от Указ 14086 и член 201.9(c)—(e) от Наредбата на МП. Съгласно определението на „корективни мерки“ в член 4(a) от Указ 14086, когато взема решение за корективна мярка с цел противодействие на дадено нарушение DPRC трябва да вземе предвид „начините, по които обикновено се противодейства на установения вид нарушение“, т.е. DPRC ще разгледа, наред с други фактори, по какъв начин подобни проблеми със съответствието са коригирани в миналото, за да се гарантира, че средството за защита е ефективно и подходящо.

- (191) Във всички случаи DPRC приема писмено решение с мнозинство. В случай че при прегледа се установи нарушение на приложимите правила, в решението се посочват всички подходящи корективни мерки, които включват заличаване на незаконно събрани данни, заличаване на резултатите от неподходящо проведени търсения, ограничаване на достъпа до законно събрани данни до подходящо обучен персонал или изтегляне на разузнавателни доклади, съдържащи данни, придобити без законно разрешение или които са били незаконно разпространени ⁽³⁸²⁾. Решението на DPRC е задължително и окончателно по отношение на жалбата, с която е сезиран трибуналет ⁽³⁸³⁾. Освен това, ако при прегледа се установи нарушение на някое от правомощията, подлежащи на надзор от страна на FISC, DPRC трябва също така да предостави съдържащ класифицирана информация доклад на заместник-министъра на правосъдието по въпросите на националната сигурност, който от своя страна е длъжен да докладва за несъответствието на FISC, който може да предприеме по-нататъшни действия по правоприлагане (в съответствие с процедурата, описана в съображения 173—174) ⁽³⁸⁴⁾.
- (192) Всяко решение на състава на DPRC се предава на CLPO към ODNI ⁽³⁸⁵⁾. В случаите, в които прегледът на DPRC е въз основа на молба от жалбоподателя, жалбоподателят се уведомява чрез националния орган, че DPRC е приключил прегледа си и че „при прегледа или не са установени никакви попадащи в приложното поле нарушения, или DPRC е издал решение, налагащо подходящи корективни мерки“ ⁽³⁸⁶⁾. Службата за неприкосновеността на личния живот и гражданските свободи към Министерството на правосъдието поддържа регистър на цялата информация, разглеждана от DPRC, и на всички издадени решения, които се предоставя за справка като база данни с необвързващи прецеденти на бъдещи състави на DPRC ⁽³⁸⁷⁾.
- (193) От Министерството на търговията се изисква също така да поддържа регистър на всички жалбоподатели, които са подали жалба ⁽³⁸⁸⁾. За да се повиши равнището на прозрачност, поне веднъж на всеки пет години Министерството на търговията трябва да се свързва със съответните разузнавателни служби, за да провери дали информацията, отнасяща се до прегледа, извършен от DPRC, е била разсекретена ⁽³⁸⁹⁾. Ако случаят е такъв, физическото лице ще бъде уведомено, че такава информация може да бъде налична съгласно приложимото право (т.е. че то може да поиска достъп до нея съгласно Закона за свобода на информацията, вж. съображение 199).
- (194) И накрая, правилното функциониране на този механизъм за правна защита ще подлежи на редовна и независима оценка. По-конкретно, съгласно Указ 14086 функционирането на механизма за правна защита подлежи на ежегоден преглед от PCLOB — независим орган (вж. съображение 110) ⁽³⁹⁰⁾. Като част от този преглед PCLOB ще оценява, наред с другото, дали CLPO и DPRC към ODNI са обработвали жалбите своевременно; дали са получавали пълен достъп до необходимата информация; дали съществени предпазни мерки съгласно Указ 14086 са били надлежно вземани предвид в процеса на преглед; и дали разузнавателната общност се е съобразила изцяло с констатациите, направени от CLPO и DPRC към ODNI. PCLOB ще изготвя доклад за резултатите от прегледа до президента, министъра на правосъдието, директора на националното разузнаване, ръководителите на разузнавателните агенции, CLPO към ODNI и комисиите по разузнаване на Конгреса, който ще бъде публикуван и в неклассифициран вариант — и на свой ред ще бъде използван при периодичния преглед на функционирането на настоящото решение, който ще се извършва от Комисията. Министърът на правосъдието, директорът на националното разузнаване, CLPO към ODNI и ръководителите на разузнавателните агенции са длъжни да изпълняват или да се съобразяват по друг начин с всички препоръки, включени в тези доклади. Освен това PCLOB ежегодно ще извършва публично сертифициране на механизма за правна защита по отношение на това дали жалбите се разглеждат в съответствие с изискванията на Указ 14086.

⁽³⁸²⁾ Раздел 4(a) от EO 14086.

⁽³⁸³⁾ Член 3(d)(ii) от Указ 14086 и член 201.9(g) от Наредбата на МП. Предвид факта, че решението на DPRC е окончателно и задължително, то не може да бъде отменено от друга/друг изпълнителна/ен или административна/ен институция/орган (включително президента на Съединени щати). Това се потвърждава и от съдебната практика на Върховния съд, в която се разяснява, че чрез делегирането на министъра на правосъдието на единствено по рода си правомощие в рамките на изпълнителната власт да издава задължителни решения на независим орган, министърът на правосъдието лишава себе си от възможността да диктува решението на този орган по какъвто и да е начин (вж. *United States ex rel. Accardi/Shughnessy*, 347 U.S. 260 (1954 г.)).

⁽³⁸⁴⁾ Член 3(d)(i)(F) от Указ 14086 и член 201.9(i) от Наредбата на МП.

⁽³⁸⁵⁾ Член 201.9(з) от Наредбата на МП.

⁽³⁸⁶⁾ Член 3(d)(i)(H) от Указ 14086 и член 201.9(h) от Наредбата на МП. По отношение на естеството на уведомлението вж. член 201.9 (h) (3) от Наредбата на МП.

⁽³⁸⁷⁾ Член 201.9(j) от Наредбата на МП.

⁽³⁸⁸⁾ Член 3(d)(v)(A) от Указ 14086.

⁽³⁸⁹⁾ Раздел 3(d)(v) от EO 14086.

⁽³⁹⁰⁾ Член 3(e) от Указ 14086. Вж. също [https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20\(FINAL\).pdf](https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL).pdf).

- (195) В допълнение към специалния механизъм за правна защита, установен с Указ 14086, за всички лица (независимо от тяхната националност или местопребиваването им) съществуват и възможности за обжалване пред обикновените съдилища в САЩ ⁽³⁹¹⁾.
- (196) По-конкретно FISA и свързаната правна уредба предвижда възможността физическите лица да предявят срещу Съединените американски щати граждански иск за обезщетяване на финансови вреди, когато информацията за тях е била неправомерно и умишлено използвана или разкрита ⁽³⁹²⁾; да заведат дело срещу длъжностни лица от правителството на САЩ в лично качество за финансови вреди ⁽³⁹³⁾; и да оспорват законността на наблюдението (и да искат заличаване на събраната информация), в случай че правителството на САЩ възнамерява да използва или разкрива информация, получена или производна от електронно наблюдение срещу лицето, в съдебни или административни производства в САЩ ⁽³⁹⁴⁾. В по-общ план, ако правителството възнамерява да използва информация, получена по време на разузнавателни операции, срещу заподозрян по наказателно дело, конституционните и законовите изисквания ⁽³⁹⁵⁾ налагат задължения за разкриване на определена информация, така че обвиняемият да може да оспори законността на събирането и използването на доказателствата от страна на правителството.
- (197) Нещо повече, има няколко специфични възможности за търсене на правна защита срещу длъжностни лица при неправомерен достъп или използване на лични данни от страна на правителството, включително за възнамеряваните цели на националната сигурност (т.е. Законът за компютърните измами и злоупотреби (Computer Fraud Abuse Act) ⁽³⁹⁶⁾; Законът за неприкосновеност на електронните съобщения (Electronic Communications Privacy Act) ⁽³⁹⁷⁾; и Законът за правото на неприкосновеност на личните финанси (Right to Financial Privacy Act) ⁽³⁹⁸⁾). Всички тези основания за подаване на иск се отнасят за конкретни данни, цели и/или видове достъп (например достъп от разстояние до един компютър чрез интернет) и могат да се ползват при определени условия (например преднамерено/умишлено поведение, поведение, излизащо извън служебните задължения, наличие на претърпени вреди).
- (198) В Закона за административното производство (APA) ⁽³⁹⁹⁾ се дава възможност за по-обща правна защита — „всяко лице, което е претърпяло правно нарушение поради действие на агенцията или е неблагоприятно засегнато или ошетеното от действия на агенцията“, има право да поиска съдебен контрол ⁽⁴⁰⁰⁾. Това включва възможността да се поиска от Съда да „обяви за незаконно и да отмени действие, констатации и заключения на агенцията, за които е установено, че представляват [...] произвол, каприз, злоупотреба с правото на преценка, или по друг начин не са в съответствие със закона“ ⁽⁴⁰¹⁾. Например през 2015 г. федерален апелативен съд се произнесе по иск по APA, според който събирането на масиви от метаданни за телефонни разговори от страна на правителството на САЩ не е разрешено от член 501 от FISA ⁽⁴⁰²⁾.
-
- ⁽³⁹¹⁾ Достъпът до тези способности е обвързан с доказването на „основания за завеждане на дело“. Този стандарт, който се прилага за всяко лице, независимо от неговото гражданство, произтича от изискването за „case of controversy“ („дело или противоречие“) съгласно член III от Конституцията на САЩ. Според Върховния съд това изисква 1) лицето да е претърпяло „фактическа вреда“ (т.е. вреда на законово защитен интерес, която е конкретна и специфична и действителна или непосредствена), 2) да е налице причинно-следствена връзка между вредата и оспорваното пред съда поведение и 3) да е вероятно, а не съмнително, че благоприятно решение на съда ще отстрани вредата (вж. решението *Lujan/Defenders of Wildlife*, U.S. 555 (1992)).
- ⁽³⁹²⁾ 18 U.S.C. § 2712.
- ⁽³⁹³⁾ 50 U.S.C. § 1810.
- ⁽³⁹⁴⁾ 50 U.S.C. § 1806.
- ⁽³⁹⁵⁾ Вж. съответно *Brady/Maryland*, 373 U.S. 83 (1963) и Закона *Jencks*, 18 U.S.C. § 3500.
- ⁽³⁹⁶⁾ 18 U.S.C. § 1030.
- ⁽³⁹⁷⁾ 18 U.S.C. §§ 2701-2712.
- ⁽³⁹⁸⁾ 12 U.S.C. § 3417.
- ⁽³⁹⁹⁾ 5 U.S.C. § 702.
- ⁽⁴⁰⁰⁾ Като цяло само „окончателно“ действие на агенцията, а не „предварително, процедурно или междинно“ действие на дадена агенция, подлежи на съдебен контрол. Вж. 5 U.S.C. § 704.
- ⁽⁴⁰¹⁾ 5 U.S.C. § 706(2)(A).
- ⁽⁴⁰²⁾ *ACLU/Clapper*, 785 F.3d 787 (2d Cir. 2015 г.), оспорваната по тези дела програма за събиране на масиви от данни за телефонни разговори беше прекратена със Закона за свободата в САЩ (USA FREEDOM Act) през 2015 г.

- (199) И накрая, в допълнение към начините за правна защита, посочени в съображения 176—198, всяко лице има право да иска достъп до съществуващи документи на федералните агенции по силата на Закона за свобода на информацията, включително когато те съдържат лични данни на лицето ⁽⁴⁰³⁾. Получаването на такъв достъп може също така да улесни завеждането на дела пред обикновените съдилища, включително в подкрепа на доказването на основания за завеждане на дело. Агенциите може да отказват информация, която попада в обхвата на някои изброени изключения, включително достъп до класифицирана информация във връзка с националната сигурност и информация относно разследвания на правоприлагащите органи ⁽⁴⁰⁴⁾, но жалбоподателите, които не са доволни от отговора, имат възможност да го оспорят, като поискат административен и впоследствие съдебен контрол (пред федералните съдилища) ⁽⁴⁰⁵⁾.
- (200) От гореизложеното следва, че когато правоприлагащите органи и органите за национална сигурност на САЩ имат достъп до лични данни, попадащи в обхвата на настоящото решение, този достъп се урежда от правна уредба, в която са определени условията, при които може да се съществува достъпът, и се гарантира, че достъпът до данните и по-нататъшното им използване са ограничени до това, което е необходимо и пропорционално за преследваната цел, свързана с обществен интерес. На тези гаранции могат да се позовават лица, които се ползват с ефективни права на правна защита.

4. ЗАКЛЮЧЕНИЕ

- (201) Комисията счита, че Съединените щати — чрез принципите, издадени от Министерството на търговията на САЩ, осигурява за личните данни, предавани от Европейския съюз на сертифицирани организации в САЩ по РЗЛД в отношенията между ЕС и САЩ ниво на защита, което по същество е равностойно на нивото, гарантирано от Регламент (ЕС) 2016/679.
- (202) Комисията счита освен това, че ефективното прилагане на принципите е гарантирано от задълженията за прозрачност и от управлението на РЗЛД от страна на Министерството на търговията. В допълнение, като цяло механизмите за упражняване на надзор и възможностите за правна защита, предвидени от правото на САЩ, позволяват нарушенията на правилата за защита на личните данни да бъдат установени и реално наказани и предоставят на субекта на данните правни средства за защита за получаване на достъп до отнасящите се за него лични данни и в крайна сметка за коригиране или заличаване на такива данни.
- (203) Накрая, въз основа на наличната информация за правния ред на САЩ, в това число информацията, посочена в приложения VI и VII, Комисията смята, че всяка намеса за цели от обществен интерес, по-специално за целите на прилагането на наказателно право и националната сигурност, от страна на публичните органи на САЩ в основните права на физическите лица, чиито лични данни се предават от Съюза на Съединените американски щати по силата на РЗЛД в отношенията между ЕС и САЩ, ще бъде ограничено до строго необходимото за постигане на въпросната законосъобразна цел, както и че съществува реална правна защита срещу такава намеса. Поради това, с оглед на горните констатации, следва да се вземе решение, че Съединените щати осигуряват адекватно ниво на защита по смисъла на член 45 от Регламент (ЕС) 2016/679, тълкуван в светлината на Хартата на основните права на Европейския съюз, за личните данни, предавани от Европейския съюз на организации, сертифицирани съгласно РЗЛД в отношенията между ЕС и САЩ.
- (204) Като се има предвид, че ограниченията, предпазните мерки и механизмът за правна защита, установени с Указ 14086, са съществени елементи от правната уредба на САЩ, на която се основава оценката на Комисията, приемането на настоящото решение се основава главно на приемането на актуализирани политики и процедури за прилагане на Указ 14086 от всички разузнавателни агенции на САЩ и от определянето на Съюза като квалифицирана организация за целите на механизма за правна защита, които се състояха съответно на 3 юли 2023 г. (вж. съображение 126) и 30 юни 2023 г. (вж. съображение 176).

⁽⁴⁰³⁾ 5 U.S.C. § 552. Подобни закони съществуват и в отделните щати.

⁽⁴⁰⁴⁾ Ако случаят е такъв, лицето обикновено получава само стандартен отговор, с който агенцията отказва да потвърди или да отрече наличието на някакви записи. Вж. *ACLU v CIA*, 710 F.3d 422 (D.C. Cir. 2014 г.). Критериите и продължителността на класифицирането са определени в Указ 13526, в който, като общо правило се предвижда, че трябва да се установят конкретна дата или събитие за разсекретяване, което се основава на продължителността на чувствителността на информацията за националната сигурност, като в този момент информацията трябва да бъде автоматично разсекретена (вж. член 1.5 от Указ 13526).

⁽⁴⁰⁵⁾ Съдът се произнася отново с решение дали регистрите правомерно не са били предоставени и може да задължи правителството да предостави достъп до регистрите (5 U.S.C. § 552(a)(4)(B)).

5. ПОСЛЕДИЦИ ОТ НАСТОЯЩОТО РЕШЕНИЕ И ДЕЙСТВИЯ НА ОРГАНИТЕ ЗА ЗАЩИТА НА ДАННИТЕ

- (205) Държавите членки и техните органи са задължени да предприемат необходимите мерки за спазване на актовете на институциите на Съюза, тъй като тези актове по презумпция са законосъобразни и съответно произвеждат правно действие, докато не бъдат оттеглени, отменени вследствие на жалба за отмяна или обявени за невалидни вследствие на производство по постановяване на преюдициално запитване или възражение за незаконосъобразност.
- (206) Следователно решение на Комисията относно адекватното ниво на защита, прието съгласно член 45, параграф 3 от Регламент (ЕС) 2016/679, е обвързващо за всички органи на държавите членки, адресати на решението, включително за независимите им надзорни органи. По-специално предаването на данни от администратор или обработващ лични данни в Съюза на сертифицирани организации в Съединените щати може да се извършва, без да е необходимо да се получава допълнително разрешение.
- (207) Следва да се припомни, че съгласно член 58, параграф 5 от Регламент (ЕС) 2016/679 и както е обяснено от Съда на ЕС в решението по делото *Schrems* ⁽⁴⁰⁶⁾, когато национален орган за защита на данните поставя под въпрос, включително въз основа на получена жалба, съгласуваността на дадено решение на Комисията относно адекватното ниво на защита с основните права на неприкосновеност на личния живот и на защита на данните на физическото лице, националното законодателство трябва да предвижда правни средства, позволяващи на съответния орган да представи възраженията си пред национална юрисдикция, която може да бъде длъжна да отправи преюдициално запитване до Съда на ЕС ⁽⁴⁰⁷⁾.

6. МОНИТОРИНГ И ПРЕРАЗГЛЕЖДАНЕ НА НАСТОЯЩОТО РЕШЕНИЕ

- (208) Според практиката на Съда на ЕС ⁽⁴⁰⁸⁾ и както е предвидено в член 45, параграф 4 от Регламент (ЕС) 2016/679, след като приеме решение относно адекватното ниво на защита, Комисията следва непрекъснато да наблюдава релевантните промени в третата държава, за да прецени дали третата държава продължава да гарантира ниво на защита, което по същество е равностойно на нивото в Европейския съюз. Такава проверка е наложителна във всички случаи, когато Комисията получи информация, която поражда основателни съмнения в това отношение.
- (209) Поради това Комисията следва непрекъснато да наблюдава положението в Съединените щати по отношение на правната уредба и действителните практики за обработване на лични данни, както са оценени в настоящото решение. За да се улесни този процес, органите на САЩ следва своевременно да информират Комисията за всяка материалноправна промяна в правния ред на САЩ, която оказва въздействие върху правната уредба, която е предмет на настоящото решение, както и за всяко развитие на практиките, свързани с обработването на личните данни, оценени в настоящото решение, както по отношение на обработването на лични данни от сертифицирани организации в Съединените американски щати, така и по отношение на ограниченията и гаранциите, приложими относно достъпа на публичните органи до лични данни.
- (210) На следващо място, за да се даде възможност на Комисията да изпълнява ефективно функцията си по извършване на наблюдение, държавите членки следва да я информират за всички релевантни действия, предприети от националните органи по защита на данните, по-специално във връзка със запитвания или жалби на субекти на данни от Съюза във връзка с предаване на лични данни от Съюза към сертифицирани организации в Съединените американски щати. Комисията следва да бъде информирана и за всякакви признаци, че действията на публичните органи на САЩ, отговарящи за предотвратяването, разследването, разкриването или наказателното преследване на престъпления или за националната сигурност, включително надзорните органи, не гарантират изискваното ниво на защита.

⁽⁴⁰⁶⁾ Решение по делото *Schrems*, т. 65.

⁽⁴⁰⁷⁾ Решение по делото *Schrems*, т. 65: „В това отношение националният законодател трябва да предвиди правни средства, позволяващи на съответния национален надзорен орган да изложи твърденията за нарушения, които смята за основателни, пред националните юрисдикции, така че ако последните споделят съмненията на органа относно валидността на решението на Комисията, да отправят преюдициално запитване с цел проверка на валидността на решението.“

⁽⁴⁰⁸⁾ Решение по делото *Schrems*, т. 76.

- (211) В изпълнение на член 45, параграф 3 от Регламент (ЕС) 2016/679 ⁽⁴⁰⁹⁾, след приемането на настоящото решение Комисията следва периодично да преразглежда дали констатациите, свързани с адекватността на нивото на защита, осигурено от Съединените американски щати по силата на РЗЛД в отношенията между ЕС и САЩ, остават фактически и правно обосновани. Тъй като по-специално Указ 14086 и Наредбата на МП изискват създаването на нови механизми и прилагането на нови предпазни мерки, настоящото решение следва да бъде подложено на първи преглед в рамките на една година след влизането му в сила, за да се провери дали всички съответни елементи са напълно приложени и функционират ефективно на практика. След този първи преглед и в зависимост от резултата от него Комисията ще реши, в тесни консултации с комитета, създаден съгласно член 93, параграф 1 от Регламент (ЕС) 2016/679 и Европейски комитет по защита на данните, каква да бъде периодичността на следващите прегледи ⁽⁴¹⁰⁾.
- (212) За да извърши прегледите, Комисията следва да се срещне с представители на Министерството на търговията, Федералната търговска комисия и Министерството на транспорта, придружени при необходимост от представители на други министерства и агенции, участващи в прилагането на РЗЛД в отношенията между ЕС и САЩ, както и, по въпроси, свързани с правителствения достъп до данни, с представители на Министерството на правосъдието, Службата на директора на Националното разузнаване (включително със служителя по въпросите на гражданските свободи), други структури от разузнавателната общност, DPRC, както и специалните адвокати. В тази среща следва да могат да участват представители на членовете на Европейския комитет по защита на данните.
- (213) Прегледът следва да обхваща всички аспекти от функционирането на настоящото решение по отношение на обработването на лични данни в Съединените щати, и по-специално прилагането и привеждането в действие на принципите, като се обръща специално внимание на защитата в случай на последващо предаване; развития в съответната съдебна практика; на ефективността на упражняването на индивидуалните права; на наблюдението и прилагането на спазването на принципите; както и на ограниченията и гаранциите по отношение на достъпа на правителството, и особено на изпълнението и прилагането на въведените с Указ 14086 гаранции, включително чрез политики и процедури, разработени от разузнавателни агенции; взаимодействието между Указ 14086 и член 702 от FISA и Указ 12333; и ефективността на механизмите за надзор и средствата за правна защита (включително функционирането на новия механизъм за правна защита, установен с Указ 14086). В контекста на тези прегледи ще се обърне внимание и на сътрудничеството между органите за защита на данните и компетентните органи на Съединените щати, включително разработването на насоки и други инструменти за тълкуване на прилагането на принципите, както и на други аспекти на функционирането на рамката.
- (214) Въз основа на съвместния преглед Комисията следва да изготви публичен доклад, който се представя на Европейския парламент и на Съвета.

7. СПИРАНЕ НА ДЕЙСТВИЕТО, ОТМЯНА ИЛИ ИЗМЕНЕНИЕ НА НАСТОЯЩОТО РЕШЕНИЕ

- (215) Когато наличната информация, по-специално информацията, получена в резултат на наблюдението на настоящото решение или предоставена от органите на САЩ или от органите на държавите членки, показва, че нивото на защита, предоставено за данните, предавани съгласно настоящото решение, може вече да не е адекватно, Комисията следва да информира своевременно компетентните органи на САЩ за това и да поиска предприемането на подходящи мерки в определен разумен срок.
- (216) Ако при изтичането на посочения срок компетентните органи на САЩ не предприемат тези мерки или не докажат по друг задоволителен начин, че настоящото решение продължава да се основава на адекватно ниво на защита, Комисията ще започне процедурата, посочена в член 93, параграф 2 от Регламент (ЕС) 2016/679, с оглед частично или пълно спиране или отмяна на настоящото решение.
- (217) Като алтернативна възможност Комисията ще започне тази процедура с оглед изменение на решението, по-специално като обвърже предаването на данни с допълнителни условия или като ограничи обхвата на констатацията за адекватност само до предаването на данни, за което продължава да се осигурява адекватно ниво на защита.

⁽⁴⁰⁹⁾ Съгласно член 45, параграф 3 от Регламент (ЕС) 2016/679 „в акта за изпълнение се предвижда механизъм за периодичен преглед най-малко веднъж на четири години, при който се отчитат всички имащи отношение промени в третата държава или международната организация“.

⁽⁴¹⁰⁾ В член 45, параграф 3 от Регламент (ЕС) 2016/679 се предвижда, че периодичният преглед трябва да се извършва „най-малко веднъж на четири години“. Вж. също Референтния документ на Европейския комитет по защита на данните за адекватното ниво на защита, WP 254 rev. 01.

- (218) По-специално Комисията следва да инициира процедурата за суспендиране или отмяна в случай на:
- а) признаци, че организациите, които са получили лични данни от Съюза по силата на настоящото решение, не спазват принципите и че това неспазване не се разглежда ефективно от компетентните органи по надзор и правоприлагане;
 - б) признаци, че органите на САЩ не спазват приложимите условия и ограничения за достъп на публичните органи на САЩ за целите на правоприлагането и националната сигурност до лични данни, предавани съгласно РЗЛД в отношенията между ЕС и САЩ; или на
 - в) невъзможност за ефективно разглеждане на жалби от субекти на данни от Съюза, включително от CLPO към ODNI и/или DPRC.
- (219) Комисията следва също така да обмисли възможността за започване на процедура за изменение, спиране на действието или отмяна на настоящото решение, ако компетентните органи на САЩ не предоставят информацията или разясненията, необходими за оценката на нивото на защита, предоставено на личните данни, предавани от Съюза на Съединените щати, или по отношение на спазването на настоящото решение. Във връзка с това Комисията следва да взема предвид степента, в която съответната информация може да бъде набавена от други източници.
- (220) При надлежно обосновани наложителни причини за спешност, например ако Указ 14086 или Наредбата на МП бъдат изменени по начин, който подкопава нивото на защита, описано в настоящото решение, или ако определянето на Съюза от министъра на правосъдието като квалифицирана организация за целите на механизма за правна защита е оттеглено, Комисията ще използва възможността да приеме, в съответствие с процедурата, посочена в член 93, параграф 3 от Регламент (ЕС) 2016/679, актове за изпълнение с незабавно приложение за спиране на прилагането, отмяна или изменение на настоящото решение.

8. ЗАКЛЮЧИТЕЛНИ СЪОБРАЖЕНИЯ

- (221) Европейският комитет по защита на данните публикува становището си ⁽⁴¹¹⁾, като то бе взето предвид при изготвянето на настоящото решение.
- (222) Европейският парламент прие резолюция относно адекватността на защитата, осигурявана от Рамката за защита на личните данни в отношенията между ЕС и САЩ ⁽⁴¹²⁾.
- (223) Мерките, предвидени в настоящото решение, са в съответствие със становището на комитета, създаден по силата на член 93, параграф 1 от Регламент (ЕС) 2016/679,

ПРИЕ НАСТОЯЩОТО РЕШЕНИЕ:

Член 1

За целите на член 45 от Регламент (ЕС) 2016/679 Съединените щати осигуряват адекватно ниво на защита на личните данни, предавани от Съюза на организации в Съединените щати, които са включени в „Списъка към Рамката за защита на личните данни“, който е публично достъпен и се поддържа от Министерството на търговията на САЩ, в съответствие с раздел I.3 от приложение I.

Член 2

Когато компетентните органи в държавите членки упражнят, с цел защита на физическите лица във връзка с обработването на техни лични данни, правомощията си по член 58 от Регламент (ЕС) 2016/679 по отношение на предаването на данни, посочено в член 1 от настоящото решение, съответната държава членка уведомява Комисията незабавно.

⁽⁴¹¹⁾ Становище 5/2023 относно проекта на Решение за изпълнение на Европейската комисия относно адекватното ниво на защита на личните данни съгласно Рамката за личните данни в отношенията между ЕС и САЩ от 28 февруари 2023 г.

⁽⁴¹²⁾ Резолюции на Европейския парламент от 11 май 2023 г. относно адекватността на защитата, осигурявана от Рамката за защита на личните данни в отношенията между ЕС и САЩ (2023/2501(RSP)).

Член 3

1. Комисията наблюдава непрекъснато прилагането на правната рамка, която е предмет на настоящото решение, включително условията, при които се извършват последващите предавания, условията, при които се упражняват индивидуалните права и при които публичните органи на САЩ имат достъп до данните, предадени въз основа на настоящото решение, с цел да прецени дали Съединените американски щати продължават да осигуряват адекватно ниво на защита по смисъла на член 1.
2. Държавите членки и Комисията взаимно се уведомяват за случаите, когато изглежда, че органите в Съединените американски щати, които имат законоустановени правомощия да привеждат в изпълнение спазването на принципите, установени в приложение I, не осигуряват ефективни механизми за откриване и надзор, които да позволяват идентифицирането на нарушения на принципите, изложени в приложение I, и наказването им на практика.
3. Държавите членки и Комисията взаимно се уведомяват за евентуални признаци, че намесата от страна на публичните органи на САЩ, които отговарят за обезпечаването на националната сигурност, правоприлагането или други обществени интереси, в правото на физическите лица на защита на личните им данни надхвърля необходимото и пропорционалното, и/или че няма ефективна правна защита срещу подобна намеса.
4. В срок от една година от датата на нотифицирането на настоящото решение до държавите членки, а след това с периодичност, за която ще бъде взето решение при тесни консултации с комитета, създаден съгласно член 93, параграф 1 от Регламент (ЕС) 2016/679, и Европейския комитет по защита на данните, Комисията ще извършва оценка на констатацията, съдържаща се в член 1, параграф 1, въз основа на цялата налична информация, включително получената като част от съвместния преглед, извършен заедно с компетентните органи на Съединените американски щати.
5. Ако Комисията открие признаци, че вече не се осигурява адекватно ниво на защита, тя информира компетентните органи на Съединените американски щати. Ако е необходимо, тя ще реши да спре прилагането, да измени или да отмени настоящото решение, или да ограничи приложното му поле в съответствие с член 45, параграф 5 от Регламент (ЕС) 2016/679. Комисията може да приеме такова решение и когато липсата на съдействие от страна на правителството на САЩ не позволява на Комисията да определи дали Съединените американски щати продължават да осигуряват адекватно ниво на защита.

Член 4

Адресати на настоящото решение са държавите членки.

Съставено в Брюксел на 10 юли 2023 година.

За Комисията
Didier REYNDERS
Член на Комисията

ПРИЛОЖЕНИЕ I

ПРИНЦИПИ НА РАМКата ЗА ЛИЧНИТЕ ДАННИ В ОТНОШЕНИЯТА МЕЖДУ ЕС И САЩ,
ИЗДАДЕНИ ОТ МИНИСТЕРСТВОТО НА ТЪРГОВИЯТА НА САЩ

I. ОБЩ ПРЕГЛЕД

1. Въпреки че Съединените щати и Европейският съюз („ЕС“) споделят ангажимент за повишаване на защитата на неприкосновеността на личния живот, върховенството на закона и признаването на значението на трансатлантическите потоци от данни за нашите граждани, икономики и общества, Съединените щати прилагат различен подход към защитата на неприкосновеността на личния живот от този на ЕС. Съединените щати прилагат секторен подход, който се основава на законови и подзаконови разпоредби, както и кодекси за саморегулиране. Министерството на търговията на САЩ (наричано по-нататък „министерството“) издава Принципиите на Рамката за личните данни в отношенията между ЕС и САЩ, включително Допълнителните принципи (наричани общо „Принципите“) и приложение I към Принципиите („приложение I“), в рамките на своите законоустановени правомощия за насърчаване, поощряване и развитие на международната търговия (15 U.S.C. § 1512). Принципиите бяха разработени в консултации с Европейската комисия („Комисията“), представители на промишлеността и други заинтересовани страни с цел насърчаване на търговията между Съединените щати и ЕС. Принципиите, които са ключов елемент от Рамката за защита на личните данни в отношенията между ЕС и САЩ („РЗЛД в отношенията между ЕС и САЩ“), предоставят на организациите в Съединените щати надежден механизъм за предаване на лични данни към САЩ от ЕС, като същевременно се гарантира, че субектите на данни от ЕС ще продължават да се ползват с ефективни гаранции и защита, както това се изисква съгласно европейското законодателство по отношение на обработването на личните им данни, когато те се предават на държави извън ЕС. Принципиите са предназначени единствено за отговарящите на изискванията организации в Съединените щати, които получават лични данни от ЕС, с цел тези организации да изгълнят условията съгласно РЗЛД в отношенията между ЕС и САЩ и по този начин да се ползват от решението на Комисията относно адекватното ниво на защита ⁽¹⁾. Принципиите не засягат прилагането на Регламент (ЕС) 2016/679 („Общия регламент относно защитата на данните“ или „ОРЗД“) ⁽²⁾, който се прилага за обработването на лични данни в държавите — членки на ЕС. По същия начин Принципиите не ограничават задълженията по отношение на неприкосновеността на личния живот, които по принцип се прилагат съгласно правото на САЩ.
2. За да се основава на РЗЛД в отношенията между ЕС и САЩ при извършването на предавания на лични данни с произход от ЕС, дадена организация трябва да се самосертифицира пред министерството (или определен от него орган), че ще спазва Принципиите. Независимо, че решенията на организациите да се присъединят по този начин към РЗЛД в отношенията между ЕС и САЩ са напълно доброволни, ефективното спазване е задължително: организациите, които са се самосертифицирали пред министерството и са обявили публично своя ангажимент да спазват Принципиите, трябва да ги спазват в пълна степен. За да се присъедини към РЗЛД в отношенията между ЕС и САЩ, дадена организация трябва: а) да бъде обект на правомощията за разследване и правоприлагане на Федералната търговска комисия („ФТК“), Министерството на транспорта (МТ) на САЩ или друг законоустановен орган, който гарантира за ефективното спазване на Принципиите (в бъдеще могат да бъдат добавени в приложение и други законоустановени органи на САЩ, признати от ЕС); б) да обяви публично ангажимента си да спазва Принципиите; в) да предостави за публичен достъп политиките си в областта на неприкосновеността на личния живот в съответствие с тези Принципи; и г) да ги прилага в пълна степен ⁽³⁾. Организация, която не спазва Принципиите, подлежи на действия по правоприлагане от страна на ФТК съгласно член 5 от Закона за Федералната търговска комисия (ФТК), с който се забраняват нелоялните или измамните практики в търговията или засягащи търговията (15 U.S.C. § 45); от страна на МТ съгласно 49 U.S.C. § 41712, с който се забранява на превозвач или билетна агенция всяка нелоялна или измамна практика при въздушните транспортни услуги или при продажбата на въздушни транспортни услуги; или съгласно друг закон или подзаконен акт, с който се забраняват тези практики.

⁽¹⁾ Предвид това, че Решението на Комисията относно адекватността на защитата, осигурена от РЛД в отношенията между ЕС и САЩ, се прилага в Исландия, Лихтенщайн и Норвегия, РЛД в отношенията между ЕС и САЩ ще обхване както ЕС, така и тези три държави. Следователно упоменаванията на ЕС и неговите държави членки ще се тълкуват като включващи Исландия, Лихтенщайн и Норвегия.

⁽²⁾ РЕГЛАМЕНТ (ЕС) 2016/679 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните).

⁽³⁾ Рамковите принципи на Щита за личните данни в отношенията между ЕС и САЩ са изменени като „Принципи на Рамката за личните данни в отношенията между ЕС и САЩ“. (Вж. допълнителния принцип за самосертифицирането).

3. Министерството ще поддържа и предоставя за публичен достъп официален списък на организациите в САЩ, които са се самосертифицирали пред министерството и са обявили ангажимента си да спазват Принципите („Списък към Рамката за личните данни“). Организацията се ползва с предимствата на РЗЛД в отношенията между ЕС и САЩ, считано от датата, на която министерството я включи в Списъка към Рамката за личните данни. Министерството ще извади от Списъка към Рамката за личните данни онези организации, които доброволно се оттеглят от РЗЛД в отношенията между ЕС и САЩ или не изпълняват изискването за ежегодно повторно сертифициране в министерството; тези организации трябва да продължат да прилагат Принципите по отношение на личната информация, която получават съгласно РЗЛД в отношенията между ЕС и САЩ, и ежегодно да потвърждават пред министерството ангажимента си за това (*т.е.* докато съхраняват такава информация), да осигуряват „адекватна“ защита на информацията чрез други разрешени средства (например, като използват договор, в който изцяло са включени изискванията по съответните одобрени от Комисията стандартни договорни клаузи) или да върнат или заличат информацията. Също така министерството ще извади от Списъка към Рамката за личните данни организациите, които трайно не спазват Принципите; тези организации трябва да върнат или заличат личната информация, която са получили съгласно РЗЛД в отношенията между ЕС и САЩ. Изваждането на дадена организация от Списъка към Рамката за личните данни означава, че тя вече няма право да се възползва от предимствата на решението на Комисията относно адекватното ниво на защита при получаването на лична информация от ЕС.
4. Също така министерството ще поддържа и предоставя за публичен достъп официален регистър на организациите в САЩ, които по-рано са били самосертифицирани в министерството, но са извадени от Списъка към Рамката за личните данни. Министерството ще отправя ясно предупреждение, че тези организации не участват в РЗЛД в отношенията между ЕС и САЩ; че изваждането от Списъка към Рамката за личните данни означава, че тези организации не могат да твърдят, че спазват изискванията съгласно РЗЛД в отношенията между ЕС и САЩ, и трябва да избягват да правят всякакви изявления или подвеждащи действия, които водят до заключението, че участват в РЗЛД в отношенията между ЕС и САЩ; и че тези организации вече нямат право да се възползват от предимствата на решението относно адекватното ниво на защита на Комисията при получаването на лична информация от ЕС. Спрямо организация, която продължава да твърди, че участва в РЗЛД в отношенията между ЕС и САЩ, или по друг начин прави погрешно представяне на информация във връзка с РЗЛД в отношенията между ЕС и САЩ, след като е била извадена от Списъка към Рамката за личните данни, може да бъдат предприети действия по правоприлагане от страна на ФТК, МТ или други правоприлагащи органи.
5. Придържането към тези Принципи може да бъде ограничено: а) до необходимата степен за изпълнение на съдебно разпореждане или за удовлетворяване на обществен интерес или изискванията, свързани с правоприлагането или националната сигурност, включително, когато закон или правителствена наредба поражда противоречия си задължения; б) със закон, съдебно разпореждане или правителствена наредба, с която се предвиждат изрични разрешителни, при положение че дадена организация, която е поискала подобно разрешително, може да докаже, че неспазването на Принципите е ограничено до необходимата степен за гарантиране на първостепенните законни интереси, за които е поискано разрешителното; или в) ако действието на ОРЗД предвижда изключения или дерогации при определените в него условия, при условие че тези изключения или дерогации се прилагат в съпоставими контексти. В този контекст гаранциите в правото на САЩ за защита на неприкосновеността на личния живот и гражданските свободи включват гаранциите, които се изискват съгласно Указ 14086 ^(*) при определените в него условия (включително изискванията за необходимост и пропорционалност). Съгласно целта за по-голяма защита на неприкосновеността на личния живот организациите следва да се стремят да прилагат тези Принципи изцяло и прозрачно, включително, като се стремят да посочат в своите политики за защита на неприкосновеността на личния живот в кои области ще се прилагат изключенията по отношение на Принципите, предвидени в буква б) по-горе. По същата причина, когато Принципите и/или законодателството на САЩ позволяват на организациите да направят избор, от тях се изисква да изберат, когато е възможно, по-високата степен на защита.
6. Организациите са задължени да прилагат Принципите за всички лични данни, предавани съгласно РЗЛД в отношенията между ЕС и САЩ, след като се присъединят към РЗЛД в отношенията между ЕС и САЩ. Организация, която е избрала да се ползва от предимствата на РЗЛД в отношенията между ЕС и САЩ за лична информация за човешки ресурси, която се предава от ЕС, за да бъде използвана в контекста на трудови правоотношения, трябва да посочи това, когато се самосертифицира пред министерството, и трябва да спазва изискванията, определени в допълнителния принцип за самосертифицирането.

^(*) Указ от 7 октомври 2022 г., „Enhancing Safeguards for United States Signals Intelligence Activities“ [„Засилване на гаранциите за дейностите на САЩ за радиоелектронно разузнаване“].

7. За въпроси, свързани с тълкуването и спазването на Принципите и на съответните политики в областта на неприкосновеността на личния живот от страна на организациите, участващи в РЗЛД в отношенията между ЕС и САЩ, се прилага правото на САЩ, с изключение на случаите, когато тези организации са поели ангажимент да си сътрудничат с органите за защита на данните („ОЗД“) на ЕС. Освен ако е посочено друго, всички разпоредби на Принципите се прилагат, когато са уместни.
8. Определения:
- a. „Лични данни“ и „лична информация“ означават данни относно идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано, които са в обхвата на ОРЗД, предадени са от ЕС на организация в Съединените щати и са записани под каквато и да е форма.
 - б. „Обработване“ на лични данни означава всяка операция или съвкупност от операции, извършвана с лични данни чрез автоматични или други средства, като събиране, записване, организиране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване или разпространяване и изтриване или унищожаване.
 - в. „Администратор“ означава физическо лице или организация, която сама или съвместно с други определя целите и средствата за обработването на лични данни.
9. Датата, от която Принципите и приложение I към Принципите ще се прилагат ефективно, е датата на влизане в сила на решението относно адекватното ниво на защита на Европейската комисия.

II. ПРИНЦИПИ

1. УВЕДОМЯВАНЕ

- a. Всяка организация трябва да уведомява физическите лица за:
 - i. участието си в РЗЛД в отношенията между ЕС и САЩ и да предоставя електронна връзка към Списъка към Рамката за личните данни или адреса на уебстраницата,
 - ii. видовете лични данни, които се събират, и правните субекти или дъщерните дружества на организацията в САЩ, които също се придържат към Принципите, когато това е приложимо,
 - iii. ангажимента си да прилага Принципите за всички лични данни, които получава от ЕС съгласно РЗЛД в отношенията между ЕС и САЩ,
 - iv. целите, с които събира и използва лична информация за тях,
 - v. как да се свържат с организацията, ако имат запитвания или оплаквания, включително съответни организации в ЕС, които могат да отговорят на тези запитвания или оплаквания,
 - vi. видовете или самоличността на трети страни, на които личната информация ще бъде разкрита, и целите, с които се извършва това,
 - vii. правото на физическите лица на достъп до личните им данни,
 - viii. възможностите за избор и средствата, които предлага организацията на физическите лица с оглед ограничаване на използването и разкриването на личните им данни,
 - ix. определения независим орган за решаване на спорове, към който да се адресират жалби и който следва да предоставя подходящи средства за защита безплатно за физическото лице, и дали това е: 1) панелът, създаден от ОЗД, 2) организация за алтернативно решаване на спорове, установена в ЕС, или 3) организация за алтернативно решаване на спорове, установена в Съединените щати,
 - x. това, че за нея се прилагат правомощията за разследване и правоприлагане на ФТК, МТ или друг оправомощен законоустановен орган на САЩ,
 - xi. възможността при определени условия физическото лице да използва правнообвързващ арбитраж ⁽³⁾,
 - xii. изискването да бъде разкривана лична информация в отговор на законни искания на публични органи, включително за удовлетворяване на изискванията, свързани с националната сигурност или правоприлагането, и
 - xiii. отговорността на организацията в случаите на последващи предавания към трети страни.

⁽³⁾ Вж. например буква в) от принципа за защита, прилагане и отговорност за причинени вреди.

- б. Уведомяването трябва да бъде направено на ясен и разбираем език, когато физическите лица бъдат поканени за пръв път да предоставят личната информация на организацията или веднага след като стане възможно, но във всеки случай, преди тази информация да бъде използвана от организацията за цел, различна от тази, за която е била първоначално събрана или обработена от организацията, която извършва предаването, или да бъде разкрита за пръв път на трета страна.

2. ИЗБОР

- а. Всяка организация трябва да предлага на физическите лица възможността да изберат (*т.е.* клауза за неучастие) дали личната информация за тях: може да бъде разкрита на трета страна или ii) може да бъде използвана за несъвместими по същество цели с предназначението или предназначенията, за които е била първоначално събрана или за които по-късно е дадено разрешение от физическите лица. Физическите лица трябва да разполагат с ясни, разбираеми и леснодостъпни механизми, за да направят своя избор.
- б. Чрез дерогация от предходната буква не е необходимо да се предоставя избор, когато разкриването се извършва пред трета страна, която изпълнява функциите на представител за изпълнение на задача(и) от името на организацията и под нейните указания. Организацията обаче винаги сключва договор с представителя.
- в. Що се отнася до чувствителна информация (*т.е.* лична информация, свързана с медицинското или здравословното състояние, с расов или етнически произход, политически възгледи, вероизповедание или философски убеждения, членство в синдикат или сексуални предпочитания), организацията трябва да получи от лицата утвърждаващо изрично съгласие (*т.е.* opt in), при условие че информацията трябва да бъде: разкрита на трета страна или ii) използвана с цел, различна от тази, за която е била първоначално събрана или за която по-късно е дадено разрешение от физическите лица посредством упражняването на правото им на изрично съгласие. Освен това организацията следва да третира всяка лична информация, получена от трета страна, като чувствителна информация, ако последната определя и третира тази информация като такава.

3. ОТЧЕТНОСТ ЗА ПОСЛЕДВАЩОТО ПРЕДАВАНЕ

- а. За да предават лична информация на трета страна, която изпълнява функциите на администратор, организацията трябва да спазват принципите на уведомяването и на избора. Организацията трябва също така да сключат договор с третата страна администратор, в който да бъде предвидено, че тези данни могат да бъдат обработвани само с ограничена и конкретна цел в съответствие с даденото съгласие от физическото лице, както и че получателят ще осигури същата степен на защита, която се осигурява от Принципите, и ще уведоми организацията, ако констатира, че вече не е в състояние да изпълнява това задължение. В договора се предвижда, че когато тази констатация е направена, третата страна администратор прекратява обработването или предприема други обосновани и съответни мерки за отстраняване на последиците.
- б. За да предават лични данни на трета страна, която изпълнява функциите на представител, организацията трябва: i) да предават тези данни само с ограничена и конкретна цел; ii) да определят, че представителят е задължен да осигури най-малко същата степен на защита на неприкосновеността на личния живот, която се изисква съгласно Принципите; iii) да предприемат обосновани и съответни мерки, за да гарантират, че представителят ефективно обработва предадената лична информация по начин, който съответства на задълженията на организацията съгласно Принципите; iv) да изискват от представителя да уведоми организацията, ако констатира, че вече не е в състояние да изпълнява своето задължение да осигурява същата степен на защита на неприкосновеността на личния живот, която се изисква съгласно Принципите; v) при уведомяване, включително съгласно подточка iv), да предприемат обосновани и съответни мерки да преустановят и отстранят последиците от неразрешено обработване; и vi) при поискване да предоставят на министерството обобщение или представително копие на съответните разпоредби във връзка с неприкосновеността на личния живот от договора с представителя.

4. СИГУРНОСТ

- а. Организацията, които създават, поддържат, използват или разпространяват лична информация, трябва да вземат обосновани и подходящи мерки, за да предотвратят загубата, злоупотребата, непозволения достъп, разкриването, изменението и унищожаването на тази информация, като надлежно вземат под внимание рисковете, свързани с обработването, и характера на личните данни.

5. ЦЯЛОСТ НА ДАННИТЕ И ОГРАНИЧАВАНЕ В РАМКИТЕ НА ЦЕЛТА

- a. Съгласно Принципите личната информация трябва да бъде ограничена до необходимата за целите на обработването ⁽⁶⁾. Никоя организация не може да обработва лична информация по начин, несъвместим с целите, за които тя е била събрана или за които по-късно е дадено разрешение от физическото лице. Доколкото е необходимо за тези цели, всяка организация трябва да вземе обосновани мерки, за да гарантира надеждността на личните данни по отношение на предвиденото им използване, както и тяхната точност, пълнота и актуалност. Организацията трябва да се придържа към Принципите през цялото време, докато съхранява тази информация.
- б. Информация може да бъде съхранявана във форма, която идентифицира ⁽⁷⁾ или позволява да се идентифицира физическото лице, само докато служи за целта на обработването по смисъла на точка 5, буква а). Това задължение не възпира организациите да обработват лична информация за по-дълги периоди, т.е. докогато и дотолкова, доколкото това обработване е от определена полза за целите на архивирането в интерес на обществото, журналистиката, литературата и изкуството, научни или исторически изследвания и статистически анализ. В тези случаи обработването е подчинено на другите принципи и разпоредби на РЗЛД в отношенията между ЕС и САЩ. Организациите следва да предприемат обосновани и подходящи мерки за спазване на тази разпоредба.

6. ДОСТЪП

- a. Физическите лица трябва да имат достъп до личната информация за тях, с която разполага дадена организация, и да имат възможността да я коригират, променят или заличават, когато е неточна или се обработва в нарушение на Принципите, освен когато затрудненията или разходите по предоставяне на достъп биха били несъразмерни спрямо рисковете за неприкосновеността на личния живот на физическото лице във въпросния случай или когато биха били нарушени правата на лица, различни от заинтересованото.

7. ПРАВНА ЗАЩИТА, ПРИЛАГАНЕ И ОТГОВОРНОСТ ЗА ПРИЧИНЕНИ ВРЕДИ

- a. Ефективната защита на неприкосновеността на личния живот трябва да включва сигурни механизми, които да гарантират спазването на Принципите, право на защита за физическите лица, засегнати от неспазването на Принципите, както и санкциониране на организациите, когато не спазват Принципите. Тези механизми трябва да включват най-малко:
 - i. леснодостъпни независими механизми за защита, които да позволят да се разгледат и експедитивно да се решат жалбите или споровете на всяко физическо лице — безплатно за лицето и при позоваване на Принципите, както и предоставяне на обезщетения, когато приложимото законодателство или инициативите в частния сектор предвиждат това;
 - ii. процедури на предприемане на последващи действия, за да се провери дали уверенията и твърденията, предоставени от организациите за техните практики в областта на неприкосновеността на личния живот, са верни и дали тези практики се прилагат действително, както се твърди, и по-специално по отношение на случаите на неспазване на Принципите; както и
 - iii. задължения за решаване на проблемите, произтичащи от неспазването на Принципите от страна на организациите, които обявяват, че се придържат към тях, и последствия за тези организации. Санкциите трябва да са достатъчно строги, за да гарантират спазването на Принципите от организациите.
- б. Организациите и избраните от тях независими механизми за защита отговарят в кратки срокове на запитвания и искания за информация от страна на министерството във връзка с РЗЛД в отношенията между ЕС и САЩ. Всички организации трябва да отговарят експедитивно на жалби във връзка със спазването на Принципите, насочени към тях от органи на държавите — членки на ЕС, чрез министерството. Организациите, които са избрали да си сътрудничат с ОЗД, включително обработващите данни за човешки ресурси, трябва да отговарят директно на тези органи във връзка с разследването и разрешаването на жалби.

⁽⁶⁾ В зависимост от обстоятелствата примерите за съвместими цели на обработването може да включват тези, които са от определена полза по отношение на връзките с клиенти, съображения относно спазването и правни съображения, одит, сигурност и предотвратяване на измами, опазване или защита на законните права на организацията или други цели, съответстващи на разумни очаквания в контекста на събирането на данни.

⁽⁷⁾ В този контекст, ако предвид средствата за идентифициране, които е доста вероятно да бъдат използвани (като се имат предвид наред с останалото разходите и количеството време, необходими за идентифицирането, както и наличните технологии към момента на обработването), и формата, в която данните се съхраняват, физическо лице може да бъде идентифицирано от организацията или от трета страна, при условие че има достъп до данните, тогава лицето е „лице, което може да бъде идентифицирано“.

- в. Организацията са задължени да участват в арбитраж по отношение на жалбите и да спазват условията, посочени в приложение I, при условие че дадено физическо лице е отнесло въпроса за решаване чрез правнообвързващ арбитраж, като е уведомило въпросната организация и е спазило процедурите и условията, посочени в приложение I.
- г. В контекста на последващо предаване всяка участваща организация носи отговорност за обработването на личната информация, която получава съгласно РЗЛД в отношенията между ЕС и САЩ и впоследствие предава на трета страна, която изпълнява функциите на представител от нейно име. Участващата организация продължава да носи отговорност съгласно Принципите, ако нейният представител обработва тази лична информация по начин, който не съответства на Принципите, освен ако организацията докаже, че не носи отговорност за събитието, породило вредата.
- д. Когато по отношение на организация е издадено съдебно разпореждане във връзка с неспазване или заповед във връзка с неспазване от законоустановен орган на САЩ (например ФТК или МТ), включен в Принципите или в бъдещо приложение към Принципите, организацията обявява публично всички съответно свързани с РЗЛД Части от евентуален доклад за спазването или за оценка, свързани с РЗЛД в отношенията между ЕС и САЩ е, представен на съда или на законоустановения орган на САЩ, доколкото позволяват изискванията за поверителност. Министерството създаде специализирано звено за контакт с ОЗД относно проблеми на спазването от страна на участващи организации. ФТК и МТ ще разглеждат приоритетно случаите на неспазване на Принципите, за които са сезирани от министерството и органите на държавите — членки на ЕС, и ще обменят своевременно информация относно случаи, за които са сезирани, с органите на съответната държава при условията на съществуващите ограничения за поверителност.

III. ДОПЪЛНИТЕЛНИ ПРИНЦИПИ

1. Чувствителни данни

- а. От организациите не се изисква да получат утвърждаващо изрично съгласие (т.е. клауза за участие) по отношение на чувствителни данни, когато обработването:
 - i. е от жизненоважен интерес за субекта на данните или за друго лице;
 - ii. е необходимо, за да се установи право на иск или право на защита;
 - iii. е необходимо, за да се оказат медицински грижи или да се определи диагноза;
 - iv. се извършва в хода на законни дейности от фондация, асоциация или друга организация с нестопанска цел и с политическа, философска, религиозна или профсъюзна цел, както и при условие че обработването се отнася единствено до членовете на организацията или до лицата, които поддържат с нея редовни контакти във връзка с предназначението ѝ, и че тези данни не се разкриват на трета страна без съгласието на субектите на данните;
 - v. е необходимо, за да се гарантира спазването на задълженията на организацията по отношение на трудовото право; или
 - vi. е свързано с данни, които ясно са били оповестени публично от физическото лице.

2. Изключения за журналистически цели

- а. С оглед на предвидените съгласно Конституцията на САЩ защиты за свободата на печата, когато правата на свободен печат, заложили в Първата поправка на Конституцията на САЩ, се пресичат с интересите за защита на неприкосновеността на личния живот, Първата поправка трябва да се прилага така, че да балансира тези интереси по отношение на дейностите на лица или организации в САЩ.
- б. Личната информация, събрана с цел публикуване, излъчване или други форми на обществена комуникация във вид на журналистически материали, независимо дали ще се използва или не, както и информацията, съдържаща се в публикувани преди това материали, разпространявани от медийни архиви, не е предмет на изискванията съгласно Принципите.

3. Вторична отговорност

- а. Доставчиците на интернет услуги („ДИУ“), телекомуникационните оператори и други организации не носят отговорност съгласно Принципите, когато само предават, маршрутизират, комутират или кешират информация от името на друга организация. РЗЛД в отношенията между ЕС и САЩ не поражда вторична отговорност. Не може да се търси отговорност на дадена организация, когато тя осъществява обикновен пренос на данни, предавани от трети страни, и не определя нито целите, нито средствата за обработване на тези лични данни.

4. Извършване на комплексни проверки и провеждане на одити

- a. В дейностите на одиторите и на инвестиционните банкери може да се наложи обработване на лични данни без съгласието или без знанието на заинтересованото лице. Това се допуска съгласно принципите на уведомяването, на избора и на достъпа при описаните по-нататък обстоятелства.
- б. Публичните акционерни дружества и дружествата с малък брой акционери, включително участващите организации, подлежат на редовно одитиране. Ако информацията за такива одити бъде разкрита преждевременно, това може да застраши целта им особено когато се отнася до потенциални нарушения. По същия начин участваща организация, която се включва в потенциално сливане или поглъщане, е необходимо да проведе комплексна проверка или да бъде подложена на такава. Това често налага събиране и обработване на лични данни, като например информация за служители на висши ръководни постове и друг ключов персонал. Ако информацията бъде разкрита преждевременно, това може да попречи на сделката или дори да бъде в нарушение на приложимата правна уредба за ценните книжа. Инвестиционните банкери и адвокатите, работещи по комплексната проверка, или одиторите, провеждащи одита, може да обработват информация без знанието на физическото лице само в необходимите рамки и период от време за целите на спазването на законовите изисквания или изискванията от публичен интерес, както и при други обстоятелства, при които прилагането на тези Принципи би засегнало законните интереси на организацията. Сред тези законни интереси са контролът на спазването от страна на организациите на техните правни задължения и законни счетоводни дейности, както и необходимостта от поверителност, свързана с евентуални придобивания, сливания, съвместни предприятия или други сделки със сходен характер, извършвани от инвестиционните банкери или одиторите.

5. Ролята на органите за защита на данните

- a. Организациите ще изпълняват ангажимента си да си сътрудничат с ОЗД, както е описано по-нататък. Съгласно РЗЛД в отношенията между ЕС и САЩ организациите в САЩ, които получават лични данни от ЕС, трябва да поемат ангажимента да използват ефективни механизми, за да гарантират спазването на Принципите. По-специално, както е определено в принципа за защита, прилагане и отговорност за причинени вреди, участващите организации трябва да осигурят: а) i) средства за защита за физическите лица, за които се отнасят данните; а) ii) процедури на предприемане на последващи действия, за да се провери дали уверенията и твърденията, предоставени от организациите за техните практики в областта на неприкосновеността на личния живот, са верни; и а) iii) задължения за решаване на проблемите, произтичащи от неспазването на Принципите, и последствията за тези организации. Организация може да изпълни условията по буква а), подточки i) и iii) от принципа за правна защита, прилагане и отговорност за причинени вреди, ако спазва изложените тук изисквания за сътрудничество с ОЗД.
- б. Всяка организация може да поеме ангажимент да си сътрудничи с ОЗД, като декларира при самосертифицирането си съгласно РЗЛД в отношенията между ЕС и САЩ пред министерството (вж. допълнителния принцип за самосертифицирането), че:
 - i. избира да спазва изискванията по буква а), подточки i) и iii) от принципа за защита, прилагане и отговорност за причинени вреди, като поема ангажимента да си сътрудничи с ОЗД;
 - ii. ще си сътрудничи с ОЗД във връзка с разследването и разрешаването на подадените жалби съгласно Принципите; както и
 - iii. ще се съобрази с всяка препоръка, дадена от ОЗД, според която организацията трябва да вземе конкретни мерки, за да спазва Принципите, включително мерки, свързани със средства за правна защита или обезщетение в полза на физически лица, които са засегнати от неспазването на Принципите, и ще уведоми писмено ОЗД за взетите мерки по този повод.
- в. Функциониране на панелите на ОЗД
 - i. Сътрудничеството на ОЗД ще се изразява в предоставяне на информация и препоръки, както следва:
 1. Препоръките на ОЗД ще бъдат предоставяни чрез неформален панел на ОЗД, създаден на равнището на ЕС, който ще помогне наред с другото за осигуряването на хармонизиран и съгласуван подход.
 2. Панелът ще дава препоръки на съответните организации в САЩ по повод на жалби от физически лица, по които няма приети решения и които се отнасят до третирането на лична информация, която е била предадена от ЕС съгласно РЗЛД в отношенията между ЕС и САЩ. Препоръките ще предвиждат гарантирането на правилното прилагане на Принципите и ще включват средствата за правна защита за съответното(ите) физическо(и) лице(а), които ОЗД считат за подходящи.

3. Панелът ще дава тези препоръки в отговор на случаи, за които е сезиран от заинтересованите организации, и/или на жалби, получени директно от физически лица срещу организации, които са поели ангажимент да си сътрудничат с ОЗД с оглед спазването на РЗЛД в отношенията между ЕС и САЩ, като същевременно ще насърчава и при необходимост ще подпомага тези физически лица да използват първо вътрешните механизми за разглеждане на жалбите, с които организацията разполага.
 4. Препоръките ще се дават едва след като двете страни по спора са имали възможността да представят своите коментари и евентуално своите доказателства. Панелът ще се стреми да предостави препоръките си в най-кратки срокове, като спазва изискването за законосъобразната процедура. По принцип панелът ще се произнася най-късно в срок от 60 дни, считано от получаването на жалбата или сезирането, а когато е възможно, и по-бързо.
 5. Ако сметне за необходимо, панелът ще направи публично достояние резултатите от разглеждането на жалбите, по които е бил сезиран.
 6. Препоръките, предоставени от панела, не поражда отговорност нито за панела, нито за ОЗД, които го съставляват.
- ii. Както беше отбелязано по-горе, организациите, които избера този начин за решаване на споровете, трябва да поемат задължението да спазват препоръките, дадени от ОЗД. Ако някоя организация не изпълни препоръките в срок от 25 дни от получаването им, без да посочи убедително обяснение за закъснението, панелът ще оповести намерението си да отнесе въпроса до ФТК, МТ или друг федерален или държавен орган на САЩ, който има законови правомощия да предприема действия по правоприлагане в случаи на измама или погрешно представяне, или да заключи, че е допуснато сериозно нарушение по отношение на споразумението за сътрудничество, което в такъв случай ще се счита за недействително. В последния случай панелът ще информира министерството, за да може Списъкът към Рамката за личните данни да бъде надлежно изменен. Всяко неспазване на задължението за сътрудничество с ОЗД, както и всяко неспазване на Принципите подлежи на санкциониране като измамна практика съгласно член 5 от Закона за ФТК (15 U.S.C. § 45), 49 U.S.C. § 41712 или друг сравним закон.
- г. Всяка организация, която желае да се ползва с предимствата на РЗЛД в отношенията между ЕС и САЩ за данните за човешки ресурси, предавани от ЕС в контекста на трудовите правоотношения, трябва да поеме ангажимента да си сътрудничи с ОЗД по отношение на тези данни (вж. допълнителния принцип за данни за човешки ресурси).
- д. Организациите, които са избрали този вариант, ще трябва да плащат годишна такса, предназначена за покриване на оперативните разходи на панела. Може допълнително да бъде поискано да поемат евентуално налагащи се разходи за превод, произтичащи от разглеждането от страна на панела на случаите на сезиране или жалбите срещу тях. Размерът на таксата се определя от министерството след консултация с Комисията. Събирането на таксата може да се извършва от трета страна, избрана от министерството да изпълнява функциите на попечител на събраните за тази цел средства. Министерството ще си сътрудничи тясно с Комисията и ОЗД за установяването на подходящи процедури за разпределяне на средствата, събрани чрез таксата, както и за други процедурни и административни аспекти на панела. Министерството и Комисията може да се споразумеят да променят честотата на събиране на таксата.

6. Самосертифициране

- а. Организацията се ползва с предимствата на РЗЛД в отношенията между ЕС и САЩ, считано от датата, на която министерството я включи в Списъка към Рамката за личните данни. Министерството ще включи дадена организация в Списъка към Рамката за личните данни само след като установи, че информацията в заявлението за първоначално самосертифициране на организацията е пълна, и ще извади организацията от този списък, ако тя доброволно се оттегли, не изпълни изискването за ежегодно повторно сертифициране или ако трайно не спазва Принципите (вж. допълнителния принцип за решаване на спорове и прилагане).
- б. За първоначално самосертифициране или последващо повторно сертифициране за участие в РЗЛД в отношенията между ЕС и САЩ дадена организация трябва при всеки отделен случай да подава в министерството заявление от корпоративен служител от името на организацията, която се самосертифицира или сертифицира повторно (според случая) във връзка с придържането ѝ към Принципите (*), което съдържа най-малко следната информация:

(*) Подаването на заявлението трябва да бъде направено чрез уебсайта на Рамката за личните данни на министерството от физическо лице в рамките на организацията, което е упълномощено да прави изявления от нейно име и от името на който и да е от субектите, които тя обхваща, относно придържането към Принципите.

- i. наименованието на организацията в САЩ, която се самосертифицира или сертифицира повторно, както и наименованието(ята) на всеки от нейните субекти или дъщерни дружества в САЩ, които също се придържат към Принципите и които организацията желае да обхване;
 - ii. описание на дейностите на организацията по отношение на личната информация, която ще се получава от ЕС съгласно РЗЛД в отношенията между ЕС и САЩ;
 - iii. описание на съответната(ите) политика(и) на организацията в областта на неприкосновеността на личния живот по отношение на тази лична информация, включително:
 - 1. ако организацията има публичен уебсайт, тя трябва да предостави съответния URL адрес, на който е предоставила на разположение политиката си в областта на неприкосновеността на личния живот, а ако организацията няма публичен уебсайт, тя трябва да посочи къде е предоставила на разположение за публичен достъп политиката си в областта на неприкосновеността на личния живот; както и
 - 2. датата, от която тази политика се прилага ефективно;
 - iv. служба за контакт в рамките на организацията, която разглежда жалби, искания за достъп и други въпроси, произтичащи съгласно Принципите ⁽⁹⁾, включително:
 - 1. името(ната), длъжността(ите) (според случая), електронния(ите) адрес(и) и телефонния(ите) номер(а) на съответното(ите) лице(а) или съответната(ите) служба(и) за контакт в рамките на организацията; както и
 - 2. съответния пощенски адрес на организацията в САЩ;
 - v. конкретния законоустановен орган, който е компетентен да разглежда жалби срещу организацията във връзка с евентуални неприятели или измамни практики и нарушения на законите или разпоредбите, уреждащи неприкосновеността на личния живот (и който е посочен в Принципите или в бъдещо приложение към Принципите);
 - vi. наименованието на всяка програма относно неприкосновеността на личния живот, в която членува организацията;
 - vii. метода на проверка (т.е. самооценка; или външни прегледи на спазването, включително третата страна, която извършва тези прегледи) ⁽¹⁰⁾; както и
 - viii. съответния(те) независим(и) механизъм(и) за защита, който(които) е(са) на разположение за разследване на жалби, свързани с Принципите, по които няма приети решения ⁽¹¹⁾.
- v. Когато организацията желае да се ползва с предимствата на РЗЛД в отношенията между ЕС и САЩ по отношение на информацията за човешки ресурси, която се предава от ЕС, за да бъде използвана в контекста на трудовите правоотношения, тя може да направи това, когато съществува законоустановен орган, посочен в Принципите или в бъдещо приложение към Принципите, който е компетентен да разглежда жалби срещу организацията, произтичащи от обработването на информация за човешки ресурси. Освен това организацията трябва да посочи това в своето заявление за първоначално самосертифициране, както и във всички заявления за повторно сертифициране и да обяви ангажимента си да си сътрудничи със съответния орган или органи на ЕС съгласно допълнителните принципи за данни за човешки ресурси и за ролята на органите за защита на данните (според случая), както и че ще се съобразява с препоръките, давани от тези органи. Също така организацията трябва да предостави на министерството копие от политиката си в областта на неприкосновеността на личния живот за човешките ресурси и да посочи къде е предоставила на разположение на засегнатите служители тази политика, за да могат да я разгледат.

⁽⁹⁾ Не е възможно външни за организацията лица да изпълняват функциите на основно „лице за контакт с организацията“ и „корпоративен служител на организацията“ (например външен съветник или външен консултант).

⁽¹⁰⁾ Вж. допълнителния принцип за проверката.

⁽¹¹⁾ Вж. допълнителния принцип за решаване на спорове и прилагане.

- г. Министерството ще поддържа и предоставя за публичен достъп Списъка към Рамката за личните данни с организациите, които са подали попълнени заявления за първоначално самосертифициране, и ще актуализира този списък въз основа на попълнените заявления за ежегодно повторно сертифициране, както и уведомленията, получени съгласно допълнителния принцип за решаване на спорове и прилагане. Тези заявления за повторно сертифициране трябва да се подават ежегодно; в противен случай организацията ще бъде извадена от Списъка към Рамката за личните данни и няма да продължи да се ползва с предимствата, които РЗЛД в отношенията между ЕС и САЩ осигурява. Всички организации, които министерството е включило в Списъка към Рамката за личните данни, трябва да имат съответни политики в областта на неприкосновеността на личния живот, които са в съответствие с принципа на уведомяването, и да упоменават в тези политики, че се придържат към Принципите ⁽¹²⁾. Ако политиката на дадена организация в областта на неприкосновеността на личния живот е на разположение онлайн, в нея трябва да се предостави хипервръзка към уебсайта на Рамката за личните данни на министерството, както и хипервръзка към уебсайта или към формуляра за подаване на жалба на независимия механизъм за защита, който е на разположение за разглеждане на жалби, свързани с Принципите, по които няма приети решения, безплатно за физическото лице.
- д. Принципите се прилагат незабавно след самосертифицирането. Участващите организации, които преди това са самосертифицирали придържането си към Рамковите принципи на Щита за личните данни в отношенията между ЕС и САЩ ще трябва да актуализират своите политики в областта на неприкосновеността на личния живот и вместо това да упоменат „Принципите на Рамката за личните данни в отношенията между ЕС и САЩ“. Тези организации включват това упоменаване във възможно най-кратък срок и във всеки случай не по-късно от три месеца от датата, от която Принципите на Рамката за личните данни в отношенията между ЕС и САЩ се прилагат ефективно.
- е. Всяка организация трябва да прилага Принципите за всички лични данни, които получава от ЕС съгласно РЗЛД в отношенията между ЕС и САЩ. Задължението за спазване на Принципите не е ограничено във времето по отношение на личните данни, получени през периода, когато организацията се ползва от предимствата на РЗЛД в отношенията между ЕС и САЩ; това задължение означава, че тя ще продължи да прилага Принципите за тези данни, докато ги съхранява, използва или разкрива, дори ако по някаква причина впоследствие напусне РЗЛД в отношенията между ЕС и САЩ. Организация, която желае да се оттегли от РЗЛД в отношенията между ЕС и САЩ, трябва предварително да уведоми министерството за това. В уведомлението трябва също така да се посочи какво ще направи организацията с личните данни, които е получила съгласно РЗЛД в отношенията между ЕС и САЩ (т.е. дали ще запази, върне или заличи данните, както и ако запази данните, какви ще са разрешените средства, чрез които ще ги защити). Организация, която се оттегли от РЗЛД в отношенията между ЕС и САЩ, но желае да запази тези данни, трябва ежегодно да потвърждава пред министерството ангажмента си, че ще продължи да прилага Принципите по отношение на данните, или да осигури „адекватна“ защита на данните чрез други разрешени средства (например, като използва договор, в който изцяло са включени изискванията по съответните приети от Комисията стандартни договорни клаузи); в противен случай организацията трябва да върне или заличи информацията ⁽¹³⁾. Организация, която се оттегли от РЗЛД в отношенията между ЕС и САЩ, трябва да премахне от съответната си политиката в областта на неприкосновеността на личния живот всички упоменавания на РЗЛД в отношенията между ЕС и САЩ, които могат да водят до заключението, че организацията продължава да участва и се ползва от предимствата от участието си в РЗЛД в отношенията между ЕС и САЩ.

⁽¹²⁾ Организация, която се самосертифицира за пръв път, не може да посочи, че участва в РЛД в отношенията между ЕС и САЩ, в окончателната си политика в областта на неприкосновеността на личния живот, докато министерството не уведоми организацията, че може да го направи. Когато подава заявлението за първоначалното си самосертифициране, организацията трябва да предостави на министерството проект на политика в областта на неприкосновеността на личния живот, която е в съответствие с Принципите. След като министерството определи, че информацията в заявлението за първоначално самосертифициране на организацията е пълна, то ще я уведоми, че следва да финализира (например публикува, когато е приложимо) своята политика в областта на неприкосновеността на личния живот, съответстваща на РЛД в отношенията между ЕС и САЩ. Организацията трябва незабавно да уведоми министерството веднага щом бъде финализирана съответната политика в областта на неприкосновеността на личния живот, след което министерството ще включи организацията в Списъка към Рамката за личните данни.

⁽¹³⁾ Ако към момента на оттеглянето си дадена организация избере да запази личните данни, които е получила съгласно РЛД в отношенията между ЕС и САЩ, и да потвърждава ежегодно пред министерството, че продължава да прилага Принципите по отношение на тези данни, организацията трябва да удостоверява пред министерството веднъж годишно след оттеглянето си (т.е. освен ако и докато организацията не осигури „адекватна“ защита на тези данни с други разрешени средства или не върне или заличи всички тези данни и не уведоми министерството за това действие) какво е направила с тези лични данни, какво ще прави с всички тези лични данни, които продължава да съхранява, и кой ще изпълнява функциите на постоянно лице за контакт по въпроси, свързани с Принципите.

- ж. Организация, която престане да съществува като самостоятелно юридическо лице поради промяна в корпоративния статут, като например в резултат на сливане, поглъщане, несъстоятелност или прекратяване, трябва предварително да уведоми за това министерството. В уведомлението следва също така да се посочи дали образуването, произтичащо от промяната в корпоративния статут, i) ще продължи да участва в РЗЛД в отношенията между ЕС и САЩ чрез съществуващо самосертифициране; ii) ще се самосертифицира като нов участник в РЗЛД в отношенията между ЕС и САЩ (например, когато новото образуване или образуването, останало след трансформацията, все още няма съществуващо самосертифициране, чрез което може да участва в РЗЛД в отношенията между ЕС и САЩ); или iii) ще въведе други гаранции, като например писмено споразумение, които ще гарантират, че Принципите ще продължат да се прилагат по отношение на всички лични данни, които организацията е получила съгласно РЗЛД в отношенията между ЕС и САЩ и които ще бъдат запазени. Когато не се прилага нито i), ii) или iii), всички лични данни, получени съгласно РЗЛД в отношенията между ЕС и САЩ, трябва незабавно да бъдат върнати или заличени.
- з. Когато по някаква причина организация напусне РЗЛД в отношенията между ЕС и САЩ, тя трябва да премахне всички твърдения, които могат да водят до заключението, че продължава да участва или да се ползва от предимствата от участието си в РЗЛД в отношенията между ЕС и САЩ. Също така трябва да премахне и сертификационния знак на РЗЛД в отношенията между ЕС и САЩ, ако го използва. Всяко погрешно представяне пред обществеността относно придържането на дадена организация към Принципите може да подлежи на санкциониране от ФТК, МТ или друг съответен държавен орган. Погрешно представяне пред министерството може да бъде санкционирано по силата на Закона за неверните твърдения (18 U.S.C. § 1001).

7. Проверка

- а. Организацията трябва да предвидят процедури на предприемане на последващи действия, за да се провери дали уверенията и твърденията им относно техните практики в областта на неприкосновеността на личния живот съгласно РЗЛД в отношенията между ЕС и САЩ са верни и дали тези практики се прилагат, както са представени, и съгласно Принципите.
- б. За да се изпълнят изискванията за проверка съгласно принципа за защита, прилагане и отговорност за причинени вреди, организацията трябва да удостовери верността на тези уверения и твърдения чрез самооценка или външни прегледи на спазването.
- в. Когато организацията е избрала самооценка, при проверката трябва да се установи, че нейната политика в областта на неприкосновеността на личния живот по отношение на личната информация, получена от ЕС, е точна, изчерпателна, леснодостъпна, съответства на Принципите и се прилага изцяло (*т.е.* се спазва). Също така тя трябва да покаже, че физическите лица са информирани за съществуването на вътрешни процедури за разглеждане на жалби и независим(и) механизъм(и) за защита, до който(които) те може да отнесат жалбите си; че има процедури за подготовка на служителите за прилагането на тази политика и за дисциплинарна отговорност при неспазване; и че има вътрешни процедури за периодично провеждане на обективен преглед на спазването на горното. Поне веднъж годишно корпоративен служител или друг упълномощен представител на организацията трябва да подписва декларация, удостоверяваща, че самооценката е изпълнена, като тя трябва да бъде предоставяна на физическите лица при поискване или в рамките на разследване или жалба за неспазване.
- г. Когато организацията е избрала външен преглед на спазването, при проверката трябва да се установи, че нейната политика в областта на неприкосновеността на личния живот по отношение на личната информация, получена от ЕС, е точна, изчерпателна, леснодостъпна, съответства на Принципите и се прилага изцяло (*т.е.* се спазва). Трябва също така да се демонстрира, че физическите лица са информирани за механизма(ите), до който(които) може да отнесат жалбите си. Методите за преглед може да включват без ограничение одит, случайни проверки, използване на „сържжения с лъжлива цел“ или на технологични инструменти според случая. Поне веднъж годишно проверяващият, корпоративният служител или друг упълномощен представител на организацията трябва да подписва декларация, удостоверяваща, че успешно е извършен външен преглед на изпълнението, като тя трябва да бъде предоставяна на физическите лица при поискване или в рамките на разследване или жалба за неспазване.
- д. Организацията трябва да съхраняват документацията си за прилагането на своите практики в областта на неприкосновеността на личния живот съгласно РЗЛД в отношенията между ЕС и САЩ и да представят тази документация — при поискване в рамките на разследване или жалба за неспазване — на независимия орган за решаване на спорове, отговорен за разглеждане на жалбите, или на институцията, която е компетентна в областта на нелоялните и измамните практики. Организацията трябва също така да предоставят своевременно отговори на запитвания и други искания за информация на министерството във връзка със спазването от тяхна страна на Принципите.

8. Достъп

а. Принципът на достъпа на практика

- i. Съгласно Принципите правото на достъп е основен елемент от защитата на неприкосновеността на личния живот. По-конкретно то позволява на физическите лица да проверяват точността на наличната информация относно тях. Принципът на достъпа означава, че физическите лица имат право:
 1. да получат от дадена организация потвърждение дали тя обработва лични данни, свързани с тях, или не ⁽¹⁴⁾;
 2. да им бъдат съобщени тези данни, за да могат да проверят дали са точни и дали обработването се извършва законосъобразно; както и
 3. да поискат да бъдат коригирани, изменени или заличени данните, когато са неточни или се обработват в нарушение на Принципите.
- ii. От физическите лица не се изисква да обосновават исканията си за достъп до личните си данни. Когато отговорят на искания за достъп от страна на физическите лица, организациите следва да се ръководят преди всичко от мотивите на лицата. Например, ако искането за достъп е неясно или много общо по съдържание, организацията може да обсъди това с физическото лице, за да разбере по-точно мотивите му във връзка с искането и да потърси подходящата информация. Организацията може да поиска да разбере с коя(и) нейна(и) структура(и) физическото лице е имало контакти или какво е естеството или употребата на информацията, която е предмет на искането за достъп.
- iii. Като се има предвид, че правото на достъп представлява основно право, организациите следва винаги да полагат добросъвестни усилия, за да предоставят достъп. Например, ако трябва да се защити някаква информация и тя може лесно да бъде отделена от останалата лична информация, която е предмет на искане за достъп, организацията следва да отдели защитената информация и да предостави останалата. Ако организацията реши да ограничи достъпа в конкретен случай, тя следва да предостави на физическото лице, което иска достъп, обяснение за това свое решение и да посочи лице за контакт за допълнителни запитвания.

б. Затруднения или разходи по предоставянето на достъп

- i. Правото на достъп до лични данни може да бъде ограничавано при извънредни обстоятелства, когато биха били нарушени законните права на лица, различни от заинтересованото, или когато тежестта или разходите по предоставяне на достъп биха били несъразмерни спрямо рисковете за неприкосновеността на личния живот на физическото лице във въпросния случай. Разходите и тежестта са важни фактори и следва да бъдат взети предвид, но те не са решаващи при определяне на основателността на предоставянето на достъп.
- ii. Така например, ако личната информация се използва, за да се вземат решения, които ще имат сериозни последици за физическото лице (например отказ или предоставяне на важни предимства, като застраховка, ипотека или работа), организацията е длъжна съобразно останалите разпоредби на Допълнителните принципи да разкрие тази информация, дори ако това се окаже относително трудно или скъпо. Ако исканата лична информация не е с чувствителен характер и не се използва, за да се вземат решения, които ще имат сериозни последици за физическото лице, но е леснодостъпна и разходите за предоставянето ѝ не са високи, организацията трябва да осигури достъп до нея.

в. Поверителна търговска информация

- i. Поверителната търговска информация е информация, която организацията полага усилия да предпази от разкриване, в случай че нейното разкриване ще помогне на конкурент на пазара. Организациите може да откажат или да ограничат достъпа, доколкото предоставянето на пълен достъп ще разкрие тяхна собствена поверителна търговска информация, като например маркетингови концепции или класификации, изготвени от самата организация, или поверителна търговска информация, принадлежаща на други организации, която е предмет на договорни задължения за поверителност.

⁽¹⁴⁾ Организацията следва да отговаря на искания на физическите лица относно целите на обработването, категориите лични данни, за които се отнася, и получателите или категориите получатели, на които се разкриват личните данни.

- ii. Ако поверителната търговска информация може лесно да се отдели от останалата лична информация, която е предмет на искане за достъп, организацията следва да отдели поверителната търговска информация и да предостави неповерителната информация.

г. Организиране на бази данни

- i. Достъпът може да се предостави като разкриване на съответната лична информация от организацията на физическото лице, без да се налага достъп от страна на физическото лице до базата данни на организацията.
- ii. Достъпът се осигурява дотолкова, доколкото организацията съхранява личната информация. Принципът на достъпа сам по себе си не поражда никакво задължение за запазване, поддържане, реорганизиране или реструктуриране на файловете с лична информация.

д. Кога може да бъде ограничаван достъпът

- i. Тъй като организациите трябва винаги да полагат добросъвестни усилия, за да предоставят достъп на физическите лица до техните лични данни, обстоятелствата, при които те може да ограничават този достъп, са ограничени и всички мотиви за това трябва да бъдат конкретни. Както е установено в ОРЗД, организацията може да ограничава достъпа до информация, доколкото нейното разкриване има вероятност да засегне опазването на важни обществени интереси като националната сигурност, отбраната или обществената сигурност, отбраната общественения ред и сигурност. Достъпът може също така да бъде отказан, когато личната информация се обработва единствено за целите на научни изследвания или за статистически цели. Други мотиви за отказ или ограничаване на достъпа са:
 - 1. накърняване на изпълнението или прилагането на законодателството или на частноправен иск, включително предотвратяването, разследването или разкриването на престъпления или упражняването на правото на справедлив съдебен процес;
 - 2. разкриване, което ще наруши законните права или важни интереси на други лица;
 - 3. нарушаване на правна или друга професионална привилегия или задължение;
 - 4. нарушаване на разследванията на служителите по отношение на сигурността или на процедурите за подаване на оплаквания или във връзка с планиране на нови назначения и реорганизации на дружествата; или
 - 5. нарушаване на поверителността, необходима при извършване на мониторинг, инспекции или изпълнение на регулаторни функции във връзка с доброто управление или при бъдещи или текущи преговори, в които организацията участва.
- ii. Задължение на организацията е, когато се позовава на изключение, да докаже неговата наложителност, както и да представи на физическите лица мотивите си за ограничаване на достъпа и да посочи лице за контакт за допълнителни запитвания.

е. Право на получаване на потвърждение и определяне на такса за покриване на разходите по предоставяне на достъп

- i. Всяко физическо лице има право да получи потвърждение дали дадена организация разполага с лични данни, свързани с него. Също така всяко физическо лице има право да му бъдат съобщени личните данни, свързани с него. Организацията може да определи такса, която не е прекалено висока.
- ii. Определянето на такса може да е основателно, когато например исканията за достъп са явно прекомерни, и по-специално поради техния повтарящ се характер.
- iii. Достъпът не може да бъде отказан по финансови причини, ако физическото лице предложи да поеме разходите.

ж. Искания за достъп с повтарящ се или злонамерен характер

- i. Всяка организация може да определи допустимо ограничение на броя на исканията за достъп, подавани от конкретно физическо лице за определен период. Когато определя тези ограничения, организацията следва да отчита фактори като честотата на актуализиране на информацията, целта, с която се използват данните, и естеството на информацията.

з. Искания за достъп с измамен характер

- i. Организацията не е длъжна да предоставя достъп, ако не получи необходимата информация за потвърждаване на самоличността на лицето, отправило искането.

и. Срок за отговор

- i. Организацията следва да отговарят на искания за достъп в рамките на разумни срокове, по разумен начин и във форма, която е лесно разбираема за физическото лице. Организация, която предоставя информация на субектите на данни през редовни интервали от време, може да изпълни искане за достъп от физическо лице с редовното предоставяне на информация, ако това няма да доведе до прекомерно забавяне.

9. **Данни за човешки ресурси**

а. Попадане в обхвата на РЗЛД в отношенията между ЕС и САЩ

- i. Когато лична информация относно наети лица (бивши или настоящи), събирана в рамките на трудовите правоотношения, се предава от организация в ЕС на участващо в РЗЛД в отношенията между ЕС и САЩ предприятие майка, свързано предприятие или доставчик на услуги, който не е свързано предприятие, в Съединените щати, това предаване се ползва от предимствата на РЗЛД в отношенията между ЕС и САЩ. В този случай събирането на информацията, както и обработването ѝ преди предаването ще се уреждат от националното законодателство на държавата — членка на ЕС, където е било извършено събирането, и ще трябва да се спазват всички условия или ограничения по предаването ѝ в съответствие с това законодателство.
- ii. Принципите са приложими само в случай на предаване или на достъп до информация, с която се идентифицират или могат да се идентифицират отделни лица. Статистическата информация, която се основава на обобщени данни за заетостта и не съдържа лични данни, или използването на анонимизирани данни не поражда опасения за неприкосновеността на личния живот.

б. Прилагане на принципите на уведомяването и на избора

- i. Организация в САЩ, която е получила от ЕС информация за наети лица съгласно РЗЛД в отношенията между ЕС и САЩ, може да я разкрива на трети страни или да я използва за други цели само ако са спазени принципите на уведомяването и на избора. Например, ако организация в САЩ възнамерява да използва личната информация, събрана в рамките на трудови правоотношения, за цели, които не са свързани с трудовите правоотношения, като например маркетингови съобщения, тя трябва преди това да даде възможност за избор на засегнатите физически лица, освен ако последните не са дали вече своето разрешение информацията да бъде използвана за тази цел. Това използване не трябва да бъде несъвместимо с целите, за които личната информация е била събрана или впоследствие е дадено разрешение от физическото лице. Освен това такъв избор не трябва да бъде използван, за да бъдат ограничавани възможностите, произтичащи от трудовите правоотношения, или за предприемане на наказателни действия срещу тези наети лица.
- ii. Следва да се отбележи, че някои общоприложими условия за предаването на данни от страна на някои държави — членки на ЕС, може да изключват други употреби на такава информация дори след предаването ѝ извън територията на ЕС, като такива условия трябва да бъдат спазвани.
- iii. В допълнение към това работодателите следва да се стремят да вземат предвид предпочитанията на наетите лица в областта на неприкосновеността на личния живот. Това може да включва например ограничаване на достъпа до личните данни, анонимизиране на някои данни или кодиране или псевдонимизиране, когато за целите на управлението не се изисква използване на истинските имена.
- iv. В рамките на необходимото и за срока, необходим, за да се избегне накърняването на законните права на организацията да извършва повишаване в длъжност, назначения или вземане на други подобни решения в областта на заетостта, не е необходимо организацията да спазва принципите на уведомяването и на избора.

в. Прилагане на принципа на достъпа

- i. В допълнителния принцип на достъпа се предоставят насоки относно причините, на които може да се основава отказът или ограничаването на поискан достъп в контекста на човешките ресурси. В ЕС, разбира се, работодателите трябва да спазват правните разпоредби, приложими в тяхната държава, и да гарантират, че наетите лица в ЕС имат достъп до информацията съгласно законодателствата на техните държави независимо от мястото, където се извършва обработването и съхраняването на данните. В контекста на РЗЛД в отношенията между ЕС и САЩ организация, която обработва такива данни в Съединените щати, ще трябва да сътрудничи при предоставяне на такъв достъп или пряко, или чрез работодателя от ЕС.

г. Правоприлагане

- i. Доколкото личната информация се използва само в рамките на трудовите правоотношения, основната отговорност за данните по отношение на наетото лице носи организацията в ЕС. От това следва, че ако европейски наети лица възразят срещу нарушаване на правата им за защита на данните и не са удовлетворени от резултатите от вътрешните процедури за преглед, разглеждане на жалбите и обжалване (или от всяка друга процедура за подаване на оплаквания, приложима по силата на сключен договор с профсъюз), те следва да бъдат насочвани към щатския или националния орган по защита на данните или към орган, занимаващ се с трудовоправните отношения, в чийто район на компетентност работят наетите лица. Тук се включват и случаите, когато за предполагаемото нарушение на правата при третирането на личната информация е отговорна организацията в САЩ, която е получила информацията от работодателя, и следователно е налице предполагаемо нарушение на Принципите. Това ще бъде най-ефективният начин за решаване на проблемите, които се проявяват често между припокриващите се права и задължения, определени от националните законодателства в областта на трудовото право и от трудовите договори, както и от законодателството в областта на защитата на данните.
- ii. Организация в САЩ, участваща в РЗЛД в отношенията между ЕС и САЩ, която използва данни от ЕС относно човешки ресурси, предадени от Съюза в рамките на трудовите правоотношения, и която желае това предаване да бъде обхванато от РЗЛД в отношенията между ЕС и САЩ, трябва за тази цел да поеме ангажимента да сътрудничи при разследвания от страна на компетентните органи на ЕС и да спазва препоръките им.

д. Прилагане на принципа на отчетност за последващото предаване

- i. За свързани с трудовоправните отношения оперативни нужди със случаен характер на участващата организация, които касаят лични данни, предавани съгласно РЗЛД в отношенията между ЕС и САЩ, като например резервация на полет, стая в хотел или застраховка, предаванията на лични данни на малко на брой наети лица към администратори могат да се извършват, без да се прилага принципът на достъпа или да се сключва договор с третата страна администратор, както иначе се изисква по силата на принципа на отчетност за последващото предаване, при условие че участващата организация е спазвала принципите на уведомяването и на избора.

10. **Задължителни договори за последващите предавания**

а. Договори за обработване на данни

- i. Когато предаването на лични данни от ЕС към Съединените щати се извършва само за целите на обработването, се изисква договор независимо дали обработващият лични данни е организация, която участва в РЗЛД в отношенията между ЕС и САЩ.
- ii. От администраторите на лични данни в ЕС се изисква винаги да подписват договор, когато се извършва предаване за целите само на обработване на данните независимо дали това обработване се извършва в ЕС или извън него и дали обработващият лични данни е организация, която участва в РЗЛД в отношенията между ЕС и САЩ. Предназначението на договора е да се гарантира, че обработващият лични данни:
1. действа единствено по указания на администратора;
 2. осигурява подходящи технически и организационни мерки за защита на личните данни от случайно или неправомерно унищожаване или случайна загуба, промяна, неразрешено разкриване или достъп и е наясно дали е разрешено последващото предаване; както и
 3. като взема предвид естеството на обработването, подпомага администратора да отговори на искания на физически лица за упражняване на предвидените в Принципите права.

- iii. Като се има предвид, че участващите организации осигуряват адекватна защита, договорите само за целите на обработването, сключени с такива организации, не изискват предварително разрешение.

6. Предавания в рамките на група дружества или група субекти под общ контрол

- i. Когато личната информация се предава между два администратора в рамките на група дружества или група субекти под общ контрол, невината се изисква договор в съответствие с принципа на отчетност за последващото предаване. Администраторите на лични данни в рамките на група дружества или група субекти под общ контрол може да се основават при тези предавания на данни на други инструменти, като например задължителните фирмени правила на ЕС или други вътрешногрупови инструменти (например програми за спазване и контрол), които гарантират непрекъснатост на защитата на личната информация съгласно Принципите. В случаи на такива предавания участващата организация остава отговорна за спазването на Принципите.

в. Предавания на данни между администратори

- i. При предавания на данни между администратори не е необходимо получателят да бъде участваща организация или да разполага с независим механизъм за защита. Участващата организация трябва да сключи договор с получателя от трета страна, изпълняващ функциите на администратор, в който да се предвижда същата степен на защита, която осигурява РЗЛД в отношенията между ЕС и САЩ, без да се включва изискването към администратора от трета страна да е участваща организация или да разполага с независим механизъм за защита, при условие че той осигурява еквивалентен механизъм.

11. **Решаване на спорове и прилагане**

- а. В принципа за защита, прилагане и отговорност за причинени вреди се определят изискванията за прилагане съгласно РЗЛД в отношенията между ЕС и САЩ. В допълнителния принцип за проверката е определен начинът да се удовлетворят изискванията, формулирани в буква а), подточка ii) от принципа. В посочения допълнителен принцип се определят решения съгласно формулираните условия в буква а), подточки i) и iii), в които се поставя изискване за независими механизми за защита. Тези механизми може да имат различна форма, но трябва да отговарят на изискванията на принципа за защита, прилагане и отговорност за причинени вреди. Организациите удовлетворяват изискванията чрез следното: i) като се съобразяват с разработени от частния сектор програми за неприкосновеността на личния живот, в чиито правила са залегнали Принципите и в които са предвидени ефективни механизми за прилагане от същото естество като описаните в принципа на защита, прилагане и отговорност за причинени вреди; ii) като се съобразяват с указанията на законоустановените или регулаторните органи за надзор, които осигуряват разглеждането на жалби на физическите лица и решаването на споровете; или iii) като се ангажират да си сътрудничат с ОЗД в рамките на ЕС или с техните упълномощени представители.
- б. Настоящият списък е примерен и не е ограничаващ. Частният сектор може да предвиди други механизми за прилагане, при условие че отговарят на изискванията на принципа за защита, прилагане и отговорност за причинени вреди и на Допълнителните принципи. Имайте предвид, че изискванията съгласно принципа за защита, прилагане и отговорност за причинени вреди допълват изискването, че мерките за саморегулиране трябва да подлежат на принудително изпълнение съгласно член 5 от Закона за ФТК (15 U.S.C. § 45), с който се забраняват нелоялните или измамните практики, 49 U.S.C. § 41712, с който се забранява на превозвач или билетна агенция всяка нелоялна или измамна практика при въздушните транспортни услуги или при продажбата на въздушни транспортни услуги, или съгласно друг закон или подзаконен акт, с който се забраняват тези практики.
- в. С цел да спомогнат за гарантиране на спазването на ангажиментите си съгласно РЗЛД в отношенията между ЕС и САЩ и да подпомогнат управлението на програмата организациите и техните независими механизми за защита трябва да предоставят информация във връзка с РЗЛД в отношенията между ЕС и САЩ при поискване от министерството. Освен това организациите трябва да отговарят експедитивно на жалби във връзка със спазването от тяхна страна на Принципите, насочени към тях от ОЗД чрез министерството. В отговора следва да се дава преценка по същество на жалбата и информация как организацията ще реши проблема, ако случаят е такъв. Министерството ще осигури защита на поверителността на информацията, която получава, в съответствие с изискванията на законодателството на САЩ.

г. Механизми за защита

- i. Физическите лица следва да бъдат насърчавани да подават жалбите, които евентуално може да повдигнат, до съответната организация, преди да се обърнат към независими механизми за защита. Организациите трябва да отговорят на физическото лице в срок от 45 дни, считано от получаването на жалбата. Независимостта на механизма за защита се преценява на фактическа основа, като се доказва чрез критерии като безпристрастност, прозрачност по отношение на неговия състав и на неговото финансиране и доказан професионален опит. Както се предвижда съгласно принципа за защита, прилагане и отговорност за причинени вреди, подаването на жалби, което е право на физическите лица, трябва да е лесноосъществимо и безплатно за тях. Независимите органи за решаване на спорове следва да разглеждат всички получени жалби от физическите лица освен в случаите, когато са неоснователни или явно необосновани. Това условие не възпрепятства установяването от страна на независимия орган за решаване на спорове, който разглежда жалбите в рамките на механизма за защита, на критерии за допустимост, но те следва да бъдат прозрачни и обосновани (например да се изключват жалби, които не са в обхвата на програмата или които са от компетентността на други инстанции) и не следва да засягат ангажмента да се разглеждат законосъобразните жалби. Освен това механизмите за защита следва да дават на физическите лица пълна и леснодостъпна информация за функционирането на процедурата по решаване на спорове, когато подават жалба. Тази информация следва да включва уведомяване относно практиките на механизма в областта на неприкосновеността на личния живот съгласно Принципите. Също така механизмите следва да си сътрудничат за разработването на инструменти за улесняване на процеса по решаване на споровете, като например стандартни формуляри за подаване на жалби.
- ii. Независимите механизми за защита трябва да включват в своите публични уебсайтове информация относно Принципите и услугите, които предоставят съгласно РЗЛД в отношенията между ЕС и САЩ. Тази информация трябва да включва: 1) информация или електронна връзка към изискванията относно независимите механизми за защита съгласно Принципите; 2) електронна връзка към уебсайта на Рамката за личните данни на министерството; 3) пояснение, че техните услуги по решаване на споровете съгласно РЗЛД в отношенията между ЕС и САЩ са безплатни за физическите лица; 4) описание на това как може да бъде подадена жалба във връзка с Принципите; 5) сроковете, в които се разглеждат жалбите във връзка с Принципите; и 6) описание на набора от възможни средства за правна защита.
- iii. Независимите механизми за защита трябва да публикуват годишен доклад с обобщена статистическа информация относно своите услуги по решаване на спорове. В годишния доклад трябва да бъдат включени: 1) общият брой на получените през отчетната година жалби във връзка с Принципите; 2) видът на получените жалби; 3) качествени показатели за решаването на спора например времето за обработването на жалбите; и 4) резултатите от получените жалби, а именно броят и видовете средства за правна защита или санкции, които са били наложени.
- iv. Както е разгледано в приложение I, на разположение на физическото лице е възможност за арбитраж за нерешените жалби, чрез който може да се определи дали участваща организация е нарушила задълженията си съгласно Принципите по отношение на това физическо лице и дали това нарушение е останало изцяло или частично неотстранено. Тази възможност е предвидена само за тези цели. Такава възможност не се предвижда например по отношение на изключенията от Принципите⁽¹⁵⁾ или на твърдения относно адекватността на РЗЛД в отношенията между ЕС и САЩ. Съгласно тази процедура за арбитраж „панелът по Рамката за личните данни в отношенията между ЕС и САЩ“ (в чийто състав влизат един или трима арбитри според договореното между страните) има правомощието да налага специфични за конкретното физическо лице непарични безпристрастни мерки (например предоставяне на достъп, коригиране, заличаване или връщане на въпросните данни на физическото лице), необходими като корективно действие срещу нарушаването на Принципите единствено по отношение на физическото лице. Физическите лица и участващите организации могат да отнасят арбитражните решения за съдебен контрол и принудително изпълнение по силата на законодателството на САЩ съгласно Федералния арбитражен закон.

д. Средства за правна защита и санкции

- i. Средствата за правна защита, предоставени от независимия орган за решаване на споровете, следва да доведат — в рамките на възможното — до анулиране или коригиране от страна на организацията на последиците от неспазването на Принципите и до спазване на Принципите при по-нататъшното обработване на личните данни от същата организация или според случая до преустановяване на обработването на личните данни на физическото лице, подало жалбата. Санкциите трябва да са достатъчно строги, за да гарантират спазването на Принципите от страна на организацията. Набор от санкции с различна степен на строгост ще позволи на органите за решаване на спорове да предприемат подходящи ответни мерки спрямо различните степени на неспазване. Санкциите следва да включват даване на

⁽¹⁵⁾ Принципите, „Общ преглед“, т. 5.

публичност в случаите на установяване на неспазване и изискване да се заличат данните при определени обстоятелства ⁽¹⁶⁾. Други санкции могат да включват спиране и отнемане на разрешителното, обезщетение за физическите лица за загубите, претърпени в резултат на неспазването, и разпореждания за прекратяване. Органите за решаване на спорове и саморегулиращите се органи от частния сектор трябва да уведомят държавния орган със съответна юрисдикция или съдилищата според случая, както и министерството относно участващите организации, които не спазват техните решения.

е. Действия на ФТК

- i. ФТК се ангажира да разглежда с предимство случаи на неспазване на Принципите, за които е била сезирана от: i) саморегулиращи се органи в областта на неприкосновеността на личния живот и други независими органи за решаване на спорове; ii) държавите — членки на ЕС; и iii) министерството, за да определи дали е нарушен член 5 от Закона за ФТК, с който се забраняват нелоялните или измамните действия или практики в търговията. Ако ФТК заключи, че има основание да счете, че член 5 е бил нарушен, тя може да реши въпроса, като изиска административна заповед за преустановяване и прекратяване, забраняваща оспорваните практики, или като внесе жалба пред федерален окръжен съд, който, ако признае жалбата, може да се произнесе с разпореждане със същото действие. Тук се включват неверни твърдения за спазване на Принципите или за участие в РЗЛД в отношенията между ЕС и САЩ от страна на организации, които вече не са в Списъка към Рамката за личните данни или никога не са се самосертифицирали пред министерството. ФТК може да поиска граждански санкции при неизпълнение на административна заповед за преустановяване и прекратяване и да преследва нарушителя за незачитане на съда — по реда на гражданското или наказателното право — ако не изпълни разпореждане на федерален съд. ФТК уведомява министерството за всички подобни действия, които предприема. Министерството насърчава другите държавни органи да го уведомяват за изхода на всички подобни случаи на сезиране или други решения, определящи спазването на Принципите.

ж. Трайно неспазване

- i. Ако дадена организация трайно не спазва Принципите, тя повече няма право да се ползва от предимствата на РЗЛД в отношенията между ЕС и САЩ. Организации, които трайно не спазват Принципите, се заличават от Списъка към Рамката за личните данни от министерството и трябва да върнат или заличат личната информация, която са получили съгласно РЗЛД в отношенията между ЕС и САЩ.
- ii. Трайно неспазване е налице, когато организация, която се е самосертифицирала пред министерството, отказва да изпълнява окончателното решение на саморегулиращ се орган в областта на неприкосновеността на личния живот, на независим орган за решаване на спорове или на държавен орган или когато даден орган, включително министерството, констатира, че организация често нарушава Принципите до толкова, че нейното твърдение за спазване вече не е достоверно. В случаите, когато такова решение е взето от орган, различен от министерството, организацията трябва незабавно да уведоми за това министерството. В противен случай тя може да бъде санкционирана по силата на Закона за неверните твърдения (18 U.S.C. § 1001). Оттеглянето на дадена организация от програма на частния сектор за саморегулиране в областта на неприкосновеността на личния живот или от независим механизъм за решаване на спорове не я освобождава от задължението да спазва Принципите и ще се счита за трайно неспазване.
- iii. Министерството ще извади организация от Списъка към Рамката за личните данни поради трайно неспазване, включително в отговор на постъпило уведомление за такова неспазване от самата организация, от саморегулиращ се орган в областта на неприкосновеността на личния живот, от друг независим орган за решаване на спорове или от държавен орган, но едва след като е изпратило на организацията тридесетдневно предизвестие и е дало възможност за отговор ⁽¹⁷⁾. В Списъка към Рамката за личните данни, поддържан от министерството, съответно ще се посочва кои организации се ползват от предимствата на РЗЛД в отношенията между ЕС и САЩ и кои вече не могат да се ползват от тях.
- iv. Всяка организация, която заяви, че иска да участва в саморегулиращ се орган, за да може отново да изпълни изискванията съгласно РЗЛД в отношенията между ЕС и САЩ, трябва да предостави на този орган пълна информация относно предишното си участие в РЗЛД в отношенията между ЕС и САЩ.

⁽¹⁶⁾ Независимите органи за решаване на спорове решават по свое усмотрение относно обстоятелствата, при които да прилагат тези санкции. Един от факторите, които трябва да се отчитат, когато се взема решение дали ще се наложи данните да бъдат заличени, е дали това са чувствителни данни, както и дали организацията е събрала, използвала или разкрила информацията при явно неспазване на Принципите.

⁽¹⁷⁾ Министерството ще посочи в предизвестията срока, в който организацията трябва да предостави своя отговор, като той задължително ще бъде по-кратък от 30 дни.

12. Избор — момент на прилагане на клаузата за неучастие

- a. Като цяло принципът на избора има за цел да гарантира, че личната информация се използва и разкрива съгласно очакванията и избора на физическото лице. Следователно, когато лична информация се използва в рамките на директния маркетинг, всяко физическо лице следва да има възможност да упражни правото си на неучастие във всеки един момент и в определени допустими граници, установени от организацията, като например в срок, в който да може организацията да направи неучастието ефективно. Организацията може също така да изиска достатъчно информация, за да потвърди самоличността на физическото лице, което иска упражняването на правото на неучастие. В Съединените щати това право може да се упражнява от физическите лица чрез централна програма за неучастие. Във всеки случай за упражняването на тази възможност физическото лице следва да разполага с леснодостъпен механизъм на приемлива цена.
- б. По същия начин организацията може да използва информацията за някои цели на директния маркетинг, когато условията не позволяват да се осигури възможност на физическото лице за неучастие преди използването на данните, при условие че след това в кратки срокове (и във всеки един момент при поискване) организацията осигури такава възможност на лицето да откаже (без разходи за него) да получава други съобщения за директен маркетинг и уважи желанието на физическото лице.

13. Информация, свързана с пътуване

- a. Данни за резервации на пътниците във въздушния транспорт и друга информация, свързана с пътуване, като информация за редовни клиенти или за резервации за хотели, както и за специфични нужди, като например предпочитания за храната в зависимост от изискванията на религията или необходимостта от физическа помощ при пътуването, може да се предават на организации извън ЕС при няколко различни обстоятелства. Съгласно ОРЗД при липса на решение относно адекватното ниво на защита личните данни може да бъдат предадени на трета държава, ако са предвидени подходящи гаранции за защита на данните съгласно член 46 от ОРЗД или — в конкретни ситуации — ако е изпълнено едно от условията по член 49 от ОРЗД (например, когато субектът на данните изрично е дал съгласието си за предаването на данни). Организацията в САЩ, присъединили се към РЗЛД в отношенията между ЕС и САЩ, осигуряват адекватна защита на личните данни и следователно може да получават данни от ЕС въз основа на член 45 от ОРЗД, без да е необходимо да въвеждат инструмент за предаване на данни съгласно член 46 от ОРЗД или да изпълняват условията, посочени в член 49 от ОРЗД. Тъй като в РЗЛД в отношенията между ЕС и САЩ се съдържат специфични правила относно чувствителната информация, такава информация (която може да е необходимо да бъде събирана например във връзка с нуждата на клиенти от физическа помощ) може да бъде включена в предаванията на данни на участващите организации. Във всички случаи обаче организацията, която предава информацията, трябва да спазва законодателството на държавата — членка на ЕС, в която осъществява дейността си, като в това законодателство може наред с останалото да са определени и специални условия за обработването на чувствителни данни.

14. Фармацевтични и медицински продукти

- a. Прилагане на законодателството на ЕС/държавите членки или на Принципите
 - i. Законодателството на ЕС/държавите членки се прилага за събирането на личните данни и за всяко обработване, което се извършва преди предаването в Съединените щати. Принципите се прилагат за данните, след като те са били предадени в Съединените щати. За да бъдат използвани за фармацевтични научни изследвания и други цели, данните следва да бъдат анонимизирани, когато това е уместно.
- б. Бъдещи научни изследвания
 - i. Личните данни, събрани по време на специфични медицински или фармацевтични научни изследвания, често играят важна роля в бъдещите научни изследвания. Когато личните данни, събрани за едно научно изследване, се предават на организация в САЩ, участваща в РЗЛД в отношенията между ЕС и САЩ, тази организация може да ги използва за нови научни изследвания, ако преди това съответно е уведомила за това и е предоставила възможност за избор. С това уведомяване следва да се предостави информация за всяка бъдеща специфична употреба на данните, като например за периодичен последващ контрол, свързани проучвания или търговски цели.

- ii. Разбираемо е, че не могат да бъдат уточнени всички видове бъдеща употреба на данните, тъй като ново приложение за целите на научните изследвания може да е налице и когато се прави нов анализ на първоначалните данни, нови медицински открития и разработки, както и при развитието в областта на общественото здраве и нормативната уредба. Следователно уведомяването следва да включва по целесъобразност и пояснение, че личните данни може да бъдат използвани в бъдещи медицински и фармацевтични научни изследвания, които не е възможно да бъдат предвидени. Ако тази употреба не е съвместима с общите научноизследователски цели, за които личните данни са били събрани първоначално или за които физическото лице е дало съгласието си впоследствие, трябва да бъде получено ново съгласие.
- в. Оттегляне от клинично изпитване
 - i. Участниците в клинично изпитване могат във всеки един момент да решат да се оттеглят от него или да бъдат помолени за това. Всички лични данни, събрани преди оттеглянето, може да бъдат обработвани заедно с другите данни, събрани в рамките на клиничното изпитване, но при условие че това е било ясно посочено на участника при уведомяването в момента, когато той е дал съгласието си за участие.
- г. Предавания на данни за регулаторни и надзорни цели
 - i. На дружествата за фармацевтични и медицински изделия се позволява да предоставят личните данни, извлечени от клинични изпитвания, осъществени в ЕС, на органи в Съединените щати за регулаторни и надзорни цели. По същия начин се позволява предаване на данни на други страни освен регулаторните органи, като например обекти на дружеството на друго място или други изследователи, съгласно принципите на уведомяването и на избора.
- д. „Заслепени“ проучвания
 - i. За да се гарантира обективността, при много клинични изпитвания достъпът до информацията, отнасяща се до лечението, проведено на всеки от участниците, е забранен за самите тях, а често пъти и за изследователите. Противното би поставило под въпрос валидността на проучването и на резултатите. За участниците в такива клинични изпитвания (наричани „заслепени“ проучвания) не е необходимо да се осигурява достъп до данните, отнасящи се до лечението им по време на изпитването, ако това ограничение е било обяснено, когато е започнало изпитването, и ако разкриването на тази информация би навредило на надеждността на изследователската работа.
 - ii. Съгласието да се участва в изпитването при тези условия предполага и отказ от правото на достъп. След приключването на изпитването и анализа на резултатите участниците следва да получат достъп до своите данни, ако поискат това. Те следва да се обърнат първо към лекаря или другите доставчици на здравно обслужване, които са провеждали лечението им по време на клиничното изпитване, или на второ място — към организацията възложител.
- е. Контрол на безопасността и ефикасността на продуктите
 - i. Не е необходимо дружествата за фармацевтични или медицински изделия да прилагат Принципите за своите дейности по контрол на безопасността и ефикасността на продуктите, що се отнася до принципите на уведомяването, на избора, на отчетността за последващото предаване и на достъпа, включително за докладите за нежелани събития и за проследяването на пациенти/субекти, използващи определени лекарствени продукти или медицински изделия, доколкото придържането към Принципите е в противоречие със спазването на нормативните изисквания. Това се отнася както за докладите, изготвяни например от доставчиците на здравно обслужване за дружествата за фармацевтични и медицински изделия, така и за докладите на дружествата за фармацевтични и медицински изделия, изготвяни за държавни институции, като например Администрацията по храните и лекарствата на САЩ.
- ж. Данни, кодирани с ключ
 - i. Научноизследователските данни обикновено са кодирани с уникален ключ още в мястото им на произход от главния изследовател, за да не бъде разкрита самоличността на отделните субекти на данните. Фармацевтичните дружества, които възлагат подобни научни изследвания, не получават ключа на кода. Единствено изследователят съхранява уникалния ключ на кода, за да може да идентифицира субекта на изследването при извънредни обстоятелства (например, ако се налага последваща медицинска помощ). Предаването от ЕС към Съединените щати на данни, кодирани по този начин, които представляват лични данни съгласно правото на ЕС, ще попадне в обхвата на Принципите.

15. Публични регистри и информация, достъпна за широката общественост

- a. Всяка организация трябва да прилага принципите за сигурността, за целостта на данните и ограничаването в рамките на целта, както и за защитата, прилагането и отговорността за причинени вреди спрямо личните данни от източници с публичен достъп. Тези Принципи се прилагат и за всички лични данни, събрани от публични регистри (т.е. от регистрите, водени от държавните институции или организации на всяко равнище, които са на разположение на широката общественост за справки).
- б. Не е необходимо принципите на уведомяването, на избора или на отчетността за последващото предаване да се прилагат за информацията в публичните регистри, стига тя да не е съчетана с информация от непублични регистри и да са спазени всички условия за ползването ѝ за справки, установени от компетентните органи. Също така обикновено не е необходимо да се прилагат принципите на уведомяването, на избора или на отчетността за последващото предаване за информацията, предоставена за публичен достъп, освен когато европейската предаваща организация е указала, че тази информация подлежи на ограничения, които налагат организацията получател да прилага тези принципи при използването ѝ за целите, за които възнамерява. Организацията не носи отговорност за това как се използва тази информация от лица, които са я придобили от публикувани материали.
- в. Ако се окаже, че дадена организация умишлено е публикувала лична информация в нарушение на принципите по такъв начин, че тя или други лица да могат да се ползват от тези изключения, тогава тя ще бъде изключена от участие в РЗЛД в отношенията между ЕС и САЩ.
- г. Не е необходимо принципът на достъпа да се прилага за информация в публичните регистри, стига тя да не е съчетана с друга лична информация (освен малко количество данни, използвани за индексирание или организиране на информацията в публичните регистри); трябва обаче да се спазят всички условия за ползването ѝ за справки, установени от компетентните органи. За разлика от това, когато информацията в публичните регистри е съчетана с друга информация от непублични регистри (с изключение на случая, изрично посочен по-горе), организацията е длъжна да предостави достъп до цялата такава информация, при положение че за нея не се прилагат други разрешени изключения.
- д. Както при информацията в публичните регистри, не е необходимо да се предоставя достъп до информация, която вече е предоставена на разположение на широката общественост, стига тази информация да не е съчетана с такава, която не е за публичен достъп. Организацията, които участват в дейности по продажба на достъпна за обществеността информация, може да удовлетворяват исканията за достъп срещу заплащане на обичайната такса, която са определили за това. По избор физическите лица може да поискат достъп до информацията, която ги засяга, като се обърнат към организацията, която първоначално е събрала данните.

16. Искания за достъп от публични органи

- a. За да се осигури прозрачност във връзка със законни искания на публични органи за достъп до лична информация, участващите организации може при желание да издават периодични доклади за прозрачност с броя на исканията за лична информация, които са получили от публични органи за целите на правоприлагането или националната сигурност, доколкото това разкриване е разрешено съгласно приложимото право.
- б. Предоставената информация в тези доклади от участващите организации наред с публикуваната информация от разузнавателните структури и друга информация може да се използва за целите на периодичния съвместен преглед на функционирането на РЗЛД в отношенията между ЕС и САЩ, както това е предвидено в Принципите.
- в. Ако не е направено уведомяване съгласно изискванията на буква а), подточка хii) от принципа на уведомяването, това не възпрепятства и не ограничава възможността на организацията да отговаря на всички законни искания.

ПРИЛОЖЕНИЕ I: АРБИТРАЖЕН МОДЕЛ

В настоящото приложение I се определят условията, при които организациите, участващи в РЗЛД в отношенията между ЕС и САЩ, са задължени да решават жалбите чрез арбитраж съгласно принципа за защита, прилагане и отговорност за причинени вреди. Възможността за правнообвързващ арбитраж, описана по-долу, се прилага за някои нерешени жалби относно данни, предавани съгласно РЗЛД в отношенията между ЕС и САЩ. С тази възможност се цели да се предостави бърз, независим и справедлив механизъм, който по избор на физическите лица може да бъде прилаган за решаване на жалби за нарушаване на Принципите, по които няма определено решение чрез някой от другите механизми съгласно РЗЛД в отношенията между ЕС и САЩ.

A. Обхват

Тази възможност за арбитраж е на разположение на физическото лице за нерешените жалби, за да може да се определи дали участваща организация е нарушила задълженията си съгласно Принципите по отношение на това физическо лице и дали това нарушение е останало изцяло и частично неотстранено. Тази възможност е предвидена само за тези цели. Такава възможност не се предвижда например по отношение на изключенията от Принципите ⁽¹⁾ или на твърдения относно адекватността на РЗЛД в отношенията между ЕС и САЩ.

Б. Налични средства за правна защита

Съгласно тази процедура за арбитраж „панелът по Рамката за личните данни в отношенията между ЕС и САЩ“ (панелът по арбитража, в чийто състав влизат един или трима арбитри според договореното между страните) има правомощието да налага специфични за конкретното физическо лице непарични безпристрастни мерки (например предоставяне на достъп, коригиране, заличаване или връщане на въпросните данни на физическото лице), необходими като корективно действие срещу нарушаването на Принципите единствено по отношение на физическото лице. Панелът по Рамката за личните данни в отношенията между ЕС и САЩ разполага единствено с тези правомощия във връзка със средствата за правна защита. Когато определя корективните действия, от панела по Рамката за личните данни в отношенията между ЕС и САЩ се изисква да взема предвид и другите средства за правна защита, които са били определени преди това от други механизми съгласно РЗЛД в отношенията между ЕС и САЩ. Не се предоставя правна защита по отношение на претърпени вреди, направени разходи, заплатени такси и други. Всяка страна по спора сама поема разходите по хонорарите на адвокати.

В. Изисквания преди арбитраж

Когато дадено физическо лице реши да използва тази възможност за арбитраж, то трябва да предприеме следните стъпки, преди да инициира арбитражно производство: 1) да подаде жалбата срещу нарушението направо пред организацията и да предостави възможност на тази организация да намери решение на проблема в рамките на срока, определен в буква г), подточка i) от допълнителния принцип за решаване на спорове и прилагане; 2) да използва безплатно независимия механизъм за защита съгласно Принципите; и 3) да отнесе проблема до министерството чрез съответния ОЗД и да предостави възможност на министерството да положи максимални усилия да реши проблема в рамките на срока, определен в писмото на Администрацията по международна търговия към министерството, безплатно за физическото лице.

Тази възможност за арбитраж не може да се използва, ако по жалба на физическото лице срещу същото нарушение на Принципите: 1) вече е прилаган правнообвързващ арбитраж; 2) е определено окончателно решение след съдебен процес, по който физическото лице е било страна; или 3) вече е постигнато споразумение между страните. Освен това тази възможност за арбитраж не може да се използва, ако ОЗД: 1) е компетентен съгласно допълнителния принцип за ролята на органите за защита на данните или допълнителния принцип за данни за човешки ресурси; или 2) е компетентен да определи решение по жалбата срещу нарушение директно с организацията. Компетентността на ОЗД да определи решение по същата жалба срещу администратор на лични данни от ЕС сама по себе си не изключва възможността да бъде използвана тази възможност за арбитраж срещу друго юридическо лице, спрямо което този ОЗД няма правомощия.

Г. Задължителна сила на решенията

Решението на дадено физическо лице да използва тази възможност за правнообвързващ арбитраж е напълно доброволно. Арбитражните решения ще бъдат задължителни за всички страни по арбитражното производство. Инициирането на арбитраж означава, че физическото лице се отказва от възможността да търси решение по жалбата срещу същото нарушение пред друга инстанция, с изключение на това, че ако определените непарични безпристрастни мерки не коригират напълно извършеното нарушение, инициирането на арбитраж не изключва възможността за физическото лице да поиска обезщетение за вреди в обикновените съдилища.

⁽¹⁾ Принципите, „Общ преглед“, т. 5.

Д. Контрол и принудително изпълнение

Физическите лица и участващите организации могат да отнасят арбитражните решения за съдебен контрол и принудително изпълнение по силата на законодателството на САЩ съгласно Федералния арбитражен закон ⁽²⁾. В тези случаи отнасянето става във федералния окръжен съд, в чиято териториална компетентност се намира основното място на стопанска дейност на участващата организация.

Тази възможност за арбитраж е предназначена за решаване на индивидуални спорове и арбитражните решения нямат действието на убедителен или обвързващ прецедент по въпроси, в които участват други страни, включително за бъдещи арбитражни производства или за съдилищата в ЕС или в САЩ, както и за производства на ФТК.

Е. Специална група по арбитража

Страните ще избират арбитри, които да влязат в състава на панела по Рамката за личните данни в отношенията между ЕС и САЩ, от списъка, разгледан по-нататък.

В съответствие с приложимото законодателство министерството и Комисията ще съставят списък с най-малко 10 арбитри, подбрани въз основа на тяхната независимост, почтеност и опит. Във връзка с този процес се прилага следното:

Арбитрите:

- 1) ще остават включени в списъка за срок от 3 години освен при извънредни обстоятелства или основателни причини за отстраняване, като този срок може да бъде удължен за нови 3 години от министерството, след като първо уведоми Комисията;
- 2) не действат под указания на която и да е от страните, на участваща организация, на правителствена институция, публичен орган или правоприлагащ орган на САЩ, ЕС, държава — членка на ЕС, или друг такъв орган, както и не са обвързани с такива; както и
- 3) трябва да имат разрешение да практикуват юридическа професия в Съединените щати, да бъдат специалисти в законодателството на САЩ в областта на неприкосновеността на личния живот и да имат експертен опит и познания относно законодателството на ЕС в областта на защитата на данните.

⁽²⁾ Съгласно глава 2 от Федералния арбитражен закон (Federal Arbitration Act) („ФАЗ“) „арбитражно споразумение или арбитражно решение, произтичащо от правни взаимоотношения, включително договорни, които могат да бъдат считани за търговски по характер, включително сделка, договор или споразумение от вида на описаните [в раздел 2 от ФАЗ], се включва в обхвата на Конвенцията [относно признаването и изпълнението на чуждестранни арбитражни решения от 10 юни 1958 г., 21 U.S.T. 2519, T.I.A.S. № 6997 („Конвенцията от Ню Йорк“)].“ 9 U.S.C. 2519, T.I.A.S. № 6997 („Конвенцията от Ню Йорк“)]. 9 U.S.C. § 202; Освен това във ФАЗ е предвидено, че „споразумение или решение, произтичащо от такива взаимоотношения, в които участват само граждани на Съединените щати, не се включва в обхвата на Конвенцията [от Ню Йорк] освен когато в тези взаимоотношения участва недвижимо имущество с местонахождение в чужбина, когато се предвижда изпълнение на дейност или прилагане в чужбина или по друг начин е налице някаква основателна връзка с една или повече чужди държави.“ Пак там. Съгласно глава 2 „всяка от страните по арбитражното дело може да се отнесе до съд с юрисдикция съгласно разпоредбите в настоящата глава, за да поиска разпореждане в потвърждение на арбитражното решение, постановено срещу някоя от другите страни по арбитражното дело. Съдът потвърждава решението освен когато констатира, че е налице едно от основанията за отказ или отсрочване на признаването или изпълнението на решението, както това е определено в посочената Конвенция [от Ню Йорк].“ Пак там § 207. По-нататък в глава 2 е предвидено, че „окръжните съдилища в Съединените щати . . . са компетентни в . . . първоначалното производство [съгласно Конвенцията от Ню Йорк], независимо от размерите на спора.“ Пак там § 203.

Също така в глава 2 е предвидено, че „Разпоредбите съгласно глава 1 се прилагат за иски и производства, инициирани съгласно разпоредбите в настоящата глава, доколкото разпоредбите в глава 1 не влизат в противоречие с тези в настоящата глава или в Конвенцията [от Ню Йорк], както е ратифицирана от Съединените щати.“ Пак там § 208. От друга страна в глава 1 е предвидено, че „писмени разпоредби в . . . договор за търговска сделка, отнасящи се до решаване чрез арбитраж на спорове, произтичащи от такъв договор или сделка или от отказ да бъде изпълнен договорът изцяло или частично, както и писмено споразумение да бъде иницирано арбитражно дело по съществуващ спор, възникнал въз основа на такъв договор, сделка или отказ, се считат за валидни, неотменими и подлежащи на принудително изпълнение освен когато са налице съществуващи по закон основания или справедливи основания за отмяна на договора.“ Пак там § 2. По-нататък в глава 1 е предвидено, че „всяка страна по арбитражния спор може да изиска от посочения съд разпореждане за потвърждаване на решението, след което съдът е задължен да издаде такова разпореждане, освен когато решението е било отменено, изменено или поправено, както това е предвидено в членове 10 и 11 [от ФАЗ].“ Пак там § 9.

Ж. Арбитражни процедури

Съобразно приложимото законодателство министерството и Комисията се договориха относно приемането на правила за арбитраж, които да уреждат производствата пред панела по Рамката за личните данни в отношенията между ЕС и САЩ ⁽³⁾. В случай че правилата, уреждащи производствата, трябва да бъдат променени, министерството и Комисията ще се договорят относно изменението на тези правила или приемането на различен набор от действащи и утвърдени арбитражни процедури в САЩ според случая при спазване на всяко от следните съображения:

1. Всяко физическо лице може да инициира правнообвързващ арбитраж при спазване на изискванията преди арбитраж, разгледани по-горе, като изпрати „Уведомление“ на организацията. В уведомлението се съдържа обобщение на стъпките, предприети съгласно точка В за намиране на решение по жалбата, описание на предполагаемото нарушение и по избор на физическото лице евентуални придружаващи документи и материали и/или правно изложение във връзка с твърдението за нарушение.
2. Процедурите трябва да бъдат изпълнени така, че да се гарантира, че няма да има дублиране на средствата или процедурите за правна защита по жалбата на физическото лице срещу същото нарушение.
3. Действията на ФТК може да се предприемат успоредно с арбитражното производство.
4. В тези арбитражни производства не може да участва представител на правителствена институция, публичен орган или правоприлагащ орган на САЩ, ЕС, държава — членка на ЕС, или друг такъв орган, като по искане на физическото лице от ЕС ОЗД може да оказват съдействие само за изготвянето на уведомлението, но те не може да имат достъп до разкрития или каквито и да е други материали във връзка с арбитражните производства.
5. Мястото на провеждане на арбитража ще е в Съединените щати, а физическото лице може да избере да участва чрез видео- или телефонна връзка, която се осигурява безплатно за него. Не е наложително да участва лично.
6. Езикът, на който ще се води арбитражното дело, ще бъде английски освен когато страните са се споразумели за друго. При мотивирано искане и като се взема предвид дали физическото лице се представлява от адвокат, ще се осигурява безплатно устен превод по време на изслушването и писмен превод на материалите по арбитражното дело освен когато по преценка на панела по Рамката за личните данни в отношенията между ЕС и САЩ при конкретните обстоятелства по арбитража това би довело до необосновани или непропорционални разходи.
7. Предоставените на арбитражите материали ще се третираят като поверителна информация и ще бъдат използвани само във връзка с арбитражното дело.
8. Ако е необходимо, може да се допусне да бъдат представени специални разкрития на физическото лице, които ще бъдат третирани от страните като поверителна информация и ще бъдат използвани само във връзка с арбитражното дело.
9. Арбитражните дела следва да приключат в срок до 90 дни, считано от изпращането на уведомлението до въпросната организация, освен когато страните са се договорили за друго.

⁽³⁾ Международният център за решаване на спорове (ICDR) — международното подразделение на Американската арбитражна асоциация (AAA) (наричани заедно ICDR-AAA), беше избран от министерството да администрира арбитражните производства съгласно приложение I към Принципите и да управлява арбитражния фонд, посочен в споменатото приложение. На 15 септември 2017 г. министерството и Комисията се договориха относно приемането на набор от правила за арбитраж, които да уреждат правнообвързващите арбитражни производства, посочени в приложение I към Принципите, както и на кодекс за поведение на арбитражите, който е в съответствие с общоприетите етични стандарти за арбитражите по търговски спорове и с приложение I към Принципите. Министерството и Комисията се договориха относно адаптирането на правилата за арбитраж и кодекса за поведение така, че да отразят актуализациите съгласно РПД в отношенията между ЕС и САЩ, като министерството ще работи с ICDR-AAA за извършването на тези актуализации.

3. Разходи

Арбитрите следва да предприемат подходящи мерки за свеждане до минимум на разходите или таксите по арбитражните дела.

В съответствие с приложимото законодателство министерството ще съдейства за поддържането на фонд, в който участващите организации ще трябва да правят вноски, зависещи отчасти от размера на организацията, и който ще покрива разходите за арбитраж, включително хонорарите на арбитрите, като ще има „таван“ на покриваните суми. Фондът ще се управлява от трета страна, която редовно ще докладва на министерството за работата му. Министерството заедно с третата страна периодично ще извършват преглед на работата на фонда, включително необходимостта от промяна на размера на вноските или на тавана на разходите за арбитраж, като наред с останалото ще вземат предвид броя на арбитражните дела и разходите и времетраенето им, като идеята е да не се създава прекомерна финансова тежест за участващите организации. Министерството ще уведомява Комисията за резултата от съвместните прегледи с третата страна и ще предоставя на Комисията предварително уведомление за всякакви корекции на размера на вноските. Таксите за хонорари на адвокати няма да се поемат съобразно настоящата разпоредба, нито от фонда, създаден, както това е предвидено в нея.

ПРИЛОЖЕНИЕ II



МИНИСТЕРСТВО НА ТЪРГОВИЯТА НА САЩ

Търговски секретар

Washington, D.C. 20230

6 юли 2023 г.

До уважаемия Дидие Рейндерс
Комисар по въпросите на правосъдието
European Commission
Rue de la Loi/Westraat 200
1049 Brussels
Белгия

Уважаеми комисар Рейндерс,

От името на Съединените щати имам удоволствието да Ви изпратя пакет от материали към Рамката за личните данни в отношенията между ЕС и САЩ, който в съчетание с Указ 14086 Enhancing Safeguards for United States Signals Intelligence Activities [Засилване на гаранциите за дейностите на САЩ за радиоелектронно разузнаване] и 28 CFR, част 201 за изменение на разпоредбите на Министерството на правосъдието с цел създаване на „съд, извършващ съдебен контрол на защитата на данните“ отразява важни и подробни преговори за укрепване на защитата на неприкосновеността на личния живот и гражданските свободи. Тези преговори доведоха до предоставянето на нови гаранции, с които да се подсигурира, че дейностите на САЩ за радиоелектронно разузнаване са необходими и пропорционални за постигането на определените цели в областта на националната сигурност, както и до създаването на нов механизъм, чрез който физическите лица от Европейския съюз („ЕС“) да търсят правна защита, ако считат, че по незаконен начин са станали обект на дейности за радиоелектронно разузнаване, като заедно те ще гарантират неприкосновеността на личните данни от ЕС. Рамката за личните данни в отношенията между ЕС и САЩ ще бъде в основата на приобщаваща и конкурентоспособна цифрова икономика. И двамата трябва да се гордеем с подобренията, включени в тази Рамка, които ще повишат защитата на неприкосновеността на личния живот в целия свят. Наред с указа, подзаконовите актове и другите материали, които са на разположение от публични източници, този пакет осигурява много солидна основа за нови констатации на Европейската комисия относно адекватното ниво на защита ⁽¹⁾.

Приложени са следните материали:

- Принципите на Рамката за личните данни в отношенията между ЕС и САЩ, включително Допълнителните принципи (наричани общо „Принципите“) и приложение I към Принципите (*т.е.* приложение, в което се посочват условията, при които организациите, участващи в Рамката за личните данни, са задължени да решават чрез арбитраж някои нерешени жалби, отнасящи се до личните данни, обхванати от Принципите);
- Писмо от Администрацията по международна търговия към министерството, която управлява програмата за Рамката за личните данни, в което се разглеждат ангажиментите, които нашето министерство е поело, за да гарантира ефективното функциониране на Рамката за личните данни в отношенията между ЕС и САЩ;
- Писмо от Федералната търговска комисия, в което се разглеждат действията от нейна страна по прилагането на Принципите;
- Писмо от Министерството на транспорта, в което се разглеждат действията от негова страна по прилагането на Принципите;
- Писмо, изготвено от Службата на директора на Националното разузнаване, относно гаранциите и ограниченията, които се прилагат за органите на националната сигурност на САЩ; както и
- Писмо, изготвено от Министерството на правосъдието, относно гаранциите и ограниченията по отношение на достъпа от страна на правителството на САЩ за целите на правоприлагането и за цели от обществен интерес.

⁽¹⁾ Предвид това, че Решението на Комисията относно адекватността на защитата, осигурена от Рамката за личните данни в отношенията между ЕС и САЩ, се прилага в Исландия, Лихтенщайн и Норвегия, пакетът към Рамката за личните данни в отношенията между ЕС и САЩ ще обхване както Европейския съюз, така и тези три държави.

Пълният пакет към Рамката за личните данни в отношенията между ЕС и САЩ ще бъде публикуван в уебсайта на Рамката за личните данни на министерството, а Принципите и приложение I към Принципите ще започнат да се прилагат ефективно от датата на влизане в сила на решението на Европейската комисия относно адекватното ниво на защита.

Можете да бъдете сигурен, че Съединените щати гледат сериозно на тези ангажменти. Очакваме с нетърпение да работим с Вас по отношение на прилагането на Рамката за личните данни в отношенията между ЕС и САЩ и да започнем заедно следващия етап от този процес.

С уважение,



Gina M. Raimondo

ПРИЛОЖЕНИЕ III



UNITED STATES DEPARTMENT OF COMMERCE
International Trade Administration
Washington, D C 20230

12 декември 2022 г.

До уважаемия Дидие Рейндерс
Комисар по въпросите на правосъдието
European Commission
Rue de la Loi/Westraat 200
1049 Brussels
Белгия

Уважаеми комисар Рейндерс,

От името на Администрацията по международна търговия (ИТА) имам удоволствието да представя ангажиментите, които Министерството на търговията („министерството“) е поело, за да гарантира защитата на личните данни чрез управлението и надзора на програмата за Рамката за личните данни. Финализирането на Рамката за личните данни в отношенията между ЕС и САЩ („РЗЛД в отношенията между ЕС и САЩ“) е голямо постижение за защитата на неприкосновеността на личния живот и за предприятията от двете страни на Атлантическия океан, тъй като ще даде увереност на физическите лица от ЕС, че техните данни ще бъдат защитени и че те ще разполагат със средства за правна защита, чрез които да се справят с опасенията, свързани с техните данни, и ще предостави възможност на хиляди предприятия да продължат да инвестират и по друг начин да участват в търговията от двете страни на Атлантическия океан в полза на нашите икономики и граждани. РЗЛД в отношенията между ЕС и САЩ е свидетелство за дългогодишната усилена работа и сътрудничество с Вас и Вашите колеги от Европейската комисия („Комисията“). Очакваме с нетърпение да продължим да работим с Комисията, за да гарантираме ефективното функциониране на тези съвместни усилия.

РЗЛД в отношенията между ЕС и САЩ ще донесе съществени ползи както за физическите лица, така и за предприятията. На първо място, тя осигурява важен набор от защити за неприкосновеността на личния живот по отношение на данните на физическите лица от ЕС, предавани в Съединените щати. Тя изисква от участващите организации в САЩ да разработят съответна политика в областта на неприкосновеността на личния живот; да се ангажират публично да спазват „Принципите на Рамката за личните данни в отношенията между ЕС и САЩ“, включително Допълнителните принципи (наричани общо „Принципите“) и приложение I към Принципите (т.е. приложение, в което се посочват условията, при които организациите, участващи в РЗЛД в отношенията между ЕС и САЩ, са задължени да решават чрез арбитраж някои нерешени жалби, отнасящи се до личните данни, обхванати от Принципите), така че ангажиментите им да подлежат на прилагане съгласно законодателството на САЩ⁽¹⁾; ежегодно да сертифицират повторно спазването пред министерството; да осигурят възможност за физическите лица от ЕС за безплатно, независимо решаване на спорове; и по отношение на тях законоустановен орган на САЩ, включен в Принципите (например Федералната търговска комисия („ФТК“) и Министерството на транспорта („МТ“)) или в бъдещо приложение към Принципите, да упражнява правомощията си за разследване и правоприлагане. Въпреки че решението на една организация да се самосертифицира е доброволно, след като тя се ангажира публично с РЗЛД в отношенията между ЕС и САЩ, нейният ангажимент подлежи на прилагане съгласно законодателството на САЩ от ФТК, МТ или друг законоустановен орган на САЩ в зависимост от това кой орган е

⁽¹⁾ Организациите, които са се самосертифицирали във връзка с ангажимента си да спазват Рамковите принципи на Щита за личните данни в отношенията между ЕС и САЩ и желат да се ползват от предимствата на участието си в РЗЛД в отношенията между ЕС и САЩ, трябва да спазват „Принципите на Рамката за личните данни в отношенията между ЕС и САЩ“. Ангажиментът за спазване на „Принципите на Рамката за личните данни в отношенията между ЕС и САЩ“ се посочва в политиките в областта на неприкосновеността на личния живот на тези организации във възможно най-кратък срок и във всеки случай не по-късно от три месеца от датата, от която „Принципите на Рамката за личните данни в отношенията между ЕС и САЩ“ се прилагат ефективно. (Вж. буква д) от допълнителния принцип за самосертифицирането).

компетентен по отношение на участващата организация. На второ място, РЗЛД в отношенията между ЕС и САЩ ще даде възможност на дружествата в Съединените щати, включително дъщерни предприятия на европейски дружества, намиращи се в Съединените щати, да получават лични данни от Европейския съюз в улеснение на потоците от данни, които са в основата на трансатлантическата търговия. Потоците от данни между Съединените щати и Европейския съюз са най-мощните в света и са в основата на икономическите отношения между САЩ и ЕС на стойност 7,1 трилиона долара, които осигуряват милиони работни места от двете страни на Атлантическия океан. Предприятията, които разчитат на трансатлантически потоци от данни, са представители на всички промишлени сектори и включват както големи дружества — сред първите 500 според класацията на Fortune, така и много малки и средни предприятия. Трансатлантическите потоци от данни позволяват на организации в САЩ да обработват данни, необходими за предлагането на стоки, услуги и възможности за трудова заетост на лица от Европа.

Министерството се ангажира да работи в тясно и продуктивно сътрудничество с нашите партньори от ЕС за ефективно управление и надзор на програмата за Рамката за личните данни. Този ангажимент се потвърждава от разработването и непрекъснатото усъвършенстване от страна на министерството на различни ресурси за подпомагане на организациите в процеса на самосертифициране, създаването на уебсайт за предоставяне на целенасочена информация на заинтересованите страни, сътрудничеството с Комисията и европейските органи за защита на данните (ОЗД) за разработване на насоки, които изясняват важни елементи на РЗЛД в отношенията между ЕС и САЩ, информационните дейности за подобряване на разбирането на задълженията на организациите за защита на данните и надзора и мониторинга на спазването от страна на организациите на изискванията на програмата.

Продължавашото ни сътрудничество с уважаваните партньори от ЕС ще даде възможност на министерството да гарантира ефективното функциониране на РЗЛД в отношенията между ЕС и САЩ. Правителството на Съединените щати отдавна работи с Комисията за насърчаване на общи принципи за защита на данните, като по този начин се преодоляват различията в съответните ни правни подходи и същевременно се подпомагат търговията и икономическият растеж в Европейския съюз и в Съединените щати. Считаме, че РЗЛД в отношенията между ЕС и САЩ, която е пример за това сътрудничество, ще даде възможност на Комисията да издаде ново решение относно адекватното ниво на защита, което ще позволи на организациите да използват РЗЛД в отношенията между ЕС и САЩ за предаване на лични данни от Европейския съюз към Съединените щати в съответствие с правото на ЕС.

Управление и надзор на програмата за Рамката за личните данни от Министерство на търговията

Министерството е твърдо ангажирано с ефективното управление и надзор на програмата за Рамката за личните данни и ще положи необходимите усилия и ще отдели съответните ресурси, за да гарантира постигането на този резултат. Министерството ще поддържа и предоставя за публичен достъп официален списък на организациите в САЩ, които са се самосертифицирали пред министерството и са обявили ангажимента си да спазват Принципите („Списък към Рамката за личните данни“), който ще актуализира въз основа на заявленията за ежегодно повторно сертифициране, подадени от участващите организации, и като изважда организации, когато те доброволно се оттеглят, не изпълнят изискването за ежегодно повторно сертифициране в съответствие с процедурите на министерството или се установи, че трайно не спазват Принципите. Също така министерството ще поддържа и предоставя за публичен достъп официален регистър на организациите в САЩ, които са извадени от Списъка към Рамката за личните данни, и ще посочва причината, поради която всяка организация е била извадена. Горепосоченият официален списък и регистър остават на разположение за публичен достъп в уебсайта на Рамката за личните данни на министерството. В уебсайта на Рамката за личните данни на видно място ще има обяснение, в което се посочва, че всяка организация, извадена от Списъка към Рамката за личните данни, трябва да престане да твърди, че участва или спазва РЗЛД в отношенията между ЕС и САЩ и че може да получава лична информация съгласно РЗЛД в отношенията между ЕС и САЩ. Въпреки това такава организация трябва да продължи да прилага Принципите по отношение на личната информация, която е получила по време на участието си в РЗЛД в отношенията между ЕС и САЩ, докато продължава да съхранява тази информация. В изпълнение на своя всеобхватен и постоянен ангажимент за ефективно управление и надзор на програмата за Рамката за личните данни министерството се ангажира по-специално да направи следното:

Проверява изискванията за самосертифициране

- Преди финализирането на първоначалното самосертифициране или ежегодното повторно сертифициране на дадена организация (наричани общо „самосертифициране“) и включването или запазването на организация в Списъка към Рамката за личните данни министерството проверява дали организацията е изпълнила най-малко съответните изисквания, посочени в допълнителния принцип за самосертифицирането, относно информацията, която дадена организация трябва да предостави в своето заявление за самосертифициране до министерството, и дали е предоставила в подходящ момент съответна политика в областта на неприкосновеността на личния живот, която осведомява физическите лица за всичките 13 изброени елемента, посочени в принципа на уведомяването. Министерството ще провери дали организацията:

- е определила организацията, която подава заявление за самосертифициране, както и всички субекти или дъщерни дружества в САЩ на самосертифициращата се организация, които също се придържат към Принципите и които организацията желае да попаднат в обхвата на самосертифицирането;
- е предоставила необходимата информация за връзка с нея (например информация за връзка с конкретно(и) лице (а) и/или служба(и) в рамките на самосертифициращата се организация, отговаряща(и) за разглеждането на жалби, искания за достъп и всякакви други въпроси, възникващи във връзка с РЗЛД в отношенията между ЕС и САЩ);
- е посочила целта(ите), за която(които) ще събира и използва лична информация, получена от Европейския съюз;
- е посочила каква лична информация ще бъде получавана от Европейския съюз въз основа на РЗЛД в отношенията между ЕС и САЩ и следователно ще попада в обхвата на самосертифицирането ѝ;
- ако организацията има публичен уебсайт, е предоставила URL адреса, на който съответната политика в областта на неприкосновеността на личния живот е леснодостъпна в този уебсайт, или ако организацията няма публичен уебсайт, е предоставила на министерството копие от съответната политика в областта на неприкосновеността на личния живот и местоположението, където тази политика е достъпна за преглед от засегнатите физически лица (*т. е.* засегнатите служители, ако съответната политика в областта на неприкосновеността на личния живот е политика за защита на данни за човешки ресурси, или обществеността, ако съответната политика в областта на неприкосновеността на личния живот не е политика за защита на данни за човешки ресурси);
- е включила в съответната си политика в областта на неприкосновеността на личния живот в подходящия момент (*т. е.* първоначално само в проект на политика в областта на неприкосновеността на личния живот, предоставен заедно със заявлението, ако то е за първоначално самосертифициране; в противен случай в окончателна и — според случая — публикувана политика в областта на неприкосновеността на личния живот) декларация, че тя се придържа към Принципите, и хипервръзка към уебсайта на Рамката за личните данни на министерството или URL адреса на този уебсайт (например началната страница или уебстраницата на Списъка към Рамката за личните данни);
- е включила в съответната си политика в областта на неприкосновеността на личния живот в подходящия момент останалите 12 изброени елемента, посочени в принципа на уведомяването (например възможността при определени условия засегнатото физическо лице от ЕС да използва правнообвързващ арбитраж; изискването да бъде разкривана лична информация в отговор на законни искания на публични органи, включително за удовлетворяване на изискванията, свързани с националната сигурност или правоприлагането, и както и отговорността на организацията в случаите на последващи предавания към трети страни);
- конкретния законоустановен орган, който е компетентен да разглежда жалби срещу организацията във връзка с евентуални нелоялни или измамни практики и нарушения на законите или разпоредбите, уреждащи неприкосновеността на личния живот (и който е посочен в Принципите или в бъдещо приложение към Принципите);
- е определила програма за неприкосновеността на личния живот, на която организацията е член;
- е определила дали съответният метод (*т. е.* процедури на предприемане на последващи действия, които тя трябва да предвиди) за проверка на спазването на Принципите от нейна страна е „самооценка“ (*т. е.* вътрешна проверка) или „външен преглед на спазването“ (*т. е.* проверка от трета страна) и ако е определила съответния метод като външен преглед на спазването, дали също така е посочила третата страна, която е извършила този преглед;
- е определила подходящия независим механизъм за защита, който е на разположение за разглеждане на жалби, подадени съгласно Принципите, и за осигуряване на подходящо безплатно средство за защита на засегнатото физическо лице.
- Ако организацията е избрала независим механизъм за защита, който се осигурява от орган за алтернативно решаване на спорове от частния сектор, дали тя е включила в съответната си политика в областта на неприкосновеността на личния живот хипервръзка или URL адреса на съответния уебсайт или формуляр за подаване на жалби на механизма, който е на разположение за разследване на нерешени жалби, подадени съгласно Принципите.
- Ако от организацията се изисква (*т. е.* по отношение на данни за човешки ресурси, предавани от Европейския съюз в контекста на трудовите правоотношения) или е избрала да си сътрудничи със съответните ОЗД при разследването и решаването на жалби, подадени съгласно Принципите, дали тя е декларирала ангажимента си за такова сътрудничество с ОЗД и за изпълняване на съответните им препоръки да предприеме конкретни действия за спазване на Принципите.

- Министерството също така ще провери дали заявлението за самосертифициране на организацията е в съответствие с нейната(ите) политика(и) в областта на неприкосновеността на личния живот. Когато самосертифицираща се организация желае да обхване някой от нейните субекти или дъщерни дружества в САЩ, които имат отделни политики в областта на неприкосновеността на личния живот, министерството ще прегледа и съответните политики в областта на неприкосновеността на личния живот на тези обхванати субекти или дъщерни дружества, за да гарантира, че те включват всички изисквани елементи, посочени в принципа на уведомяването.
- Министерството ще работи със законоустановените органи (*например* ФТК и МТ), за да провери дали организациите попадат в рамките на компетентността на съответния законоустановен орган, посочен в техните заявления за самосертифициране, в случаите, когато министерството има основания да се съмнява, че те попадат в рамките на компетентността на този орган.
- Министерството ще работи с органите за алтернативно решаване на спорове от частния сектор, за да провери дали организациите действително са регистрирани към независимия механизъм за защита, посочен в техните заявления за самосертифициране; и ще работи също така с тези органи, за да провери дали организациите действително са регистрирани за външния преглед на спазването, посочен в техните заявления за самосертифициране, когато тези органи предлагат и двата вида услуги.
- Министерството ще работи с третата страна, избрана от него да изпълнява функциите на попечител на средствата, събрани от таксата за панела на ОЗД (*т.е.* годишната такса, предназначена за покриване на оперативните разходи на панела на ОЗД), за да провери дали организациите са платили тази такса за съответната година, когато са определили ОЗД като съответния независим механизъм за защита.
- Министерството ще работи с третата страна, избрана от него да администрира арбитражните производства съгласно приложение I към Принципите и да управлява арбитражния фонд, посочен в споменатото приложение, за да провери дали организациите са направили необходимите вноски в този арбитражен фонд.
- Когато министерството установи някакви проблеми по време на прегледа на заявленията за самосертифициране на организациите, то ги информира, че трябва да отстранят всички тези проблеми в рамките на съответния срок, определен от него ⁽²⁾. Министерството ще ги информира също така, че липсата на отговор в сроковете, определени от него, или неуспешното извършване на самосертифицирането в съответствие с процедурите на министерството ще доведе до това тези заявления за самосертифициране да се считат за отказани и че всяко погрешно представяне на информация относно участието на дадена организация в РЗЛД в отношенията между ЕС и САЩ или спазването на изискванията, предвидени в нея, може да стане причина за предприемане на действия по правоприлагане от страна на ФТК, МТ или друг съответен държавен орган. Министерството ще информира организациите чрез средствата за връзка, които те са му предоставили.

Улеснява сътрудничеството с органите за алтернативно решаване на спорове, които предоставят услуги, свързани с Принципите

- Министерството ще работи с органите за алтернативно решаване на спорове от частния сектор, предоставящи независими механизми за защита, които са на разположение за разследване на нерешени жалби, подадени съгласно Принципите, за да провери дали те отговарят най-малко на изискванията, определени в допълнителния принцип за решаване на спорове и прилагане. Министерството ще провери дали те:
 - включват в своите публични уебсайтове информация относно Принципите и услугите, които предоставят съгласно РЗЛД в отношенията между ЕС и САЩ, която трябва да е съставена от: 1) информация или хипервръзка към изискванията относно независимите механизми за защита съгласно Принципите; 2) хипервръзка към уебсайта на Рамката за личните данни на министерството; 3) пояснение, че техните услуги по решаване на споровете съгласно РЗЛД в отношенията между ЕС и САЩ са безплатни за физическите лица; 4) описание на това как може да бъде подадена жалба във връзка с Принципите; 5) сроковете, в които се разглеждат жалбите във връзка с Принципите; и 6) описание на набора от възможни средства за правна защита. Министерството ще уведомява своевременно органите за извършване от негова страна на съществени промени в надзора и управлението на програмата за Рамката за личните данни, когато такива промени предстоят или вече са направени и са от значение за ролята, която изпълняват органите съгласно РЗЛД в отношенията между ЕС и САЩ;

⁽²⁾ *Например*, що се отнася до повторното сертифициране, очаква се организациите да отстранят всички проблеми в срок от 45 дни, освен ако министерството не определи друг подходящ срок.

- публикуват годишен доклад с обобщена статистическа информация относно своите услуги по решаване на спорове, който трябва да включва: 1) общият брой на получените през отчетната година жалби във връзка с Принципите; 2) видът на получените жалби; 3) качествени показатели за решаването на спора например времето за обработването на жалбите; и 4) резултатите от получените жалби, а именно броят и видовете средства за правна защита или санкции, които са били наложени. Министерството ще даде на органите конкретни допълнителни насоки относно информацията, която те следва да предоставят в годишните доклади, като там ще се разгледат тези изисквания (например посочване на конкретните критерии, на които трябва да отговаря дадена жалба, за да се счита, че е свързана с Принципите за целите на годишния доклад) и ще се определят други видове информация, която те следва да представят (*например*, ако органът предоставя и услуги за проверка във връзка с Принципите, следва да се опише начинът, по който органът избягва всякакъв действителен или потенциален конфликт на интереси в ситуации, в които предоставя на дадена организация както услуги за проверка, така и услуги по решаване на спорове). В допълнителните насоки, предоставени от министерството, ще бъде посочена и датата, до която органите следва да публикуват своите годишни доклади за съответния период на докладване.

Предприема последващи действия по отношение на организациите, които желаят да бъдат извадени от Списъка към Рамката за личните данни или вече са извадени от него

- Ако дадена организация желае да се оттегли от РЗЛД в отношенията между ЕС и САЩ, министерството ще изиска от организацията да премахне от съответната си политика в областта на неприкосновеността на личния живот всички упоменавания на РЗЛД в отношенията между ЕС и САЩ, които могат да водят до заключението, че тя продължава да участва в РЗЛД в отношенията между ЕС и САЩ и че може да получава лични данни съгласно РЗЛД в отношенията между ЕС и САЩ (*вж.* описанието на ангажимента на министерството да търси неверни твърдения за участие). Министерството също така ще изиска от организацията да попълни и да му представи съответен въпросник, за да потвърди:
 - желанието си да се оттегли;
 - кое от следните действия ще предприеме по отношение на личните данни, които е получила съгласно РЗЛД в отношенията между ЕС и САЩ, докато е участвала в РЗЛД в отношенията между ЕС и САЩ: а) ще запази тези данни, ще продължи да прилага Принципите по отношение на тези данни и ще потвърждава ежегодно пред министерството ангажимента си да прилага Принципите по отношение на тези данни; б) ще запази тези данни и ще осигури „адекватна“ защита за тях чрез други разрешени средства; или в) ще върне или ще заличи всички тези данни до определена дата; както и
 - кой в рамките на организацията ще изпълнява функциите на постоянно лице за контакт по въпроси, свързани с Принципите.
- Ако дадена организация избере буква а), както е описано непосредствено по-горе, министерството ще изисква от нея също така да попълва и да му представя всяка година след оттеглянето си (*т.е.* до първата годишнина от оттеглянето си, както и до всяка следваща годишнина, освен ако и докато организацията не осигури „адекватна“ защита на тези данни чрез други разрешени средства или не върне или изтрие всички тези данни и не уведоми министерството за това действие) съответен въпросник, за да удостоверява какво е направила с тези лични данни, какво ще прави с всички лични данни, които продължава да съхранява, и кой в организацията ще изпълнява функциите на постоянно лице за контакт по въпроси, свързани с Принципите.
- Ако дадена организация е допуснала нейното самосертифициране да стане невалидно (*т.е.* нито е изпълнила ежегодното повторно сертифициране за придържане към Принципите, нито е била извадена от Списъка към Рамката за личните данни по друга причина, като например оттегляне), министерството ще ѝ възложи да попълни и да му представи съответен въпросник, за да потвърди дали желае да се оттегли или да се сертифицира повторно:
 - ако желае да се оттегли, трябва допълнително да удостовери какво ще направи с личните данни, които е получила съгласно РЗЛД в отношенията между ЕС и САЩ, докато е участвала в РЗЛД в отношенията между ЕС и САЩ (*вж.* описанието по-горе на това какво трябва да удостовери дадена организация, ако желае да се оттегли);
 - ако възнамерява да се сертифицира повторно, трябва допълнително да удостовери, че докато сертифицирането ѝ е било невалидно, е прилагала Принципите спрямо личните данни, получени съгласно РЗЛД в отношенията между ЕС и САЩ, и да изясни какви стъпки ще предприеме, за да се справи с неотстранените проблеми, които са забавили повторното сертифициране.

- Ако дадена организация бъде извадена от Списъка към Рамката за личните данни поради някоя от следните причини: а) оттегляне от РЗЛД в отношенията между ЕС и САЩ, б) незавършване на ежегодното повторно сертифициране за придържане към Принципите (*т.е.* или е започнала, но не е завършила своевременно процеса на ежегодно повторно сертифициране, или дори не го е започнала) или в) „трайно неспазване“, министерството ще изпрати уведомление до контакта(ите), определен(и) в заявлението за самосертифициране на организацията, в което ще бъде посочена причината за изваждането от Списъка и ще бъде обяснено на организацията, че трябва да престане да твърди — изрично или косвено — че участва или спазва РЗЛД в отношенията между ЕС и САЩ и че може да получава лични данни съгласно РЗЛД в отношенията между ЕС и САЩ. В уведомлението, което може да включва и друго съдържание, съобразено с причината за изваждането, ще се посочва, че спрямо организациите, които представят невярна информация за своето участие или спазване на РЗЛД в отношенията между ЕС и САЩ, включително, когато посочват, че участват в РЗЛД в отношенията между ЕС и САЩ, след като са били извадени от Списъка към Рамката за личните данни, може да бъдат предприети действия по правоприлагане от страна на ФТК, МТ или друг съответен държавен орган.

Търси неверни твърдения за участие и намира решения

- Текущо, когато една организация: а) се оттегли от участие в РЗЛД в отношенията между ЕС и САЩ, б) не успее да завърши ежегодното повторно сертифициране за придържане към Принципите (*т.е.* или е започнала, но не е завършила своевременно процеса на ежегодно повторно сертифициране, или дори не го е започнала), в) бъде отстранена от участие в РЗЛД в отношенията между ЕС и САЩ, по-специално поради „трайно неспазване“, или г) не успее да завърши първоначалното самосертифициране за придържане към Принципите (*т.е.* започнала е, но не е завършила своевременно процеса на първоначално самосертифициране), министерството ще предприеме по служебен път проверка, за да удостовери, че в съответната публикувана политика на организацията в областта на неприкосновеността на личния живот не се съдържат упоменавания на РЗЛД в отношенията между ЕС и САЩ, които могат да водят до заключението, че организацията участва в РЗЛД в отношенията между ЕС и САЩ и че може да получава лични данни съгласно РЗЛД в отношенията между ЕС и САЩ. Когато министерството констатира такива упоменавания, то ще информира организацията, че ще отнесе въпроса според случая до съответната инстанция за евентуално предприемане на действия по правоприлагане, ако организацията продължава да представя невярна информация за своето участие в РЗЛД в отношенията между ЕС и САЩ. Министерството ще информира организацията чрез средствата за връзка, които тя му е предоставила, или когато е необходимо, чрез други подходящи средства. Ако организацията нито премахва упоменаванията, нито самосертифицира своето съответствие по отношение на РЗЛД в отношенията между ЕС и САЩ съгласно процедурите на министерството, то ще отнесе въпроса по служебен път до ФТК, МТ или друг съответен правоприлагащ орган или ще предприеме други подходящи действия, за да гарантира правилното използване на сертификационния знак на РЗЛД в отношенията между ЕС и САЩ;
- Министерството ще положи други усилия да установи неверни твърдения за участие и неправилно използване на сертификационния знак на РЗЛД в отношенията между ЕС и САЩ, включително от организации, които за разлика от организациите, разглеждани по-горе, дори не са започнали процеса на самосертифициране (например провеждане на подходящо търсене в интернет за откриване на упоменавания на РЗЛД в отношенията между ЕС и САЩ в политиките на организациите в областта на неприкосновеността на личния живот). Когато чрез тези усилия министерството установи неверни твърдения за участие и неправилно използване на сертификационния знак на РЗЛД в отношенията между ЕС и САЩ, то ще информира организацията, че ще отнесе въпроса според случая до съответната инстанция за евентуално предприемане на действия по правоприлагане, ако организацията продължава да представя невярна информация за своето участие в РЗЛД в отношенията между ЕС и САЩ. Министерството ще информира организацията чрез средствата за връзка, ако има такива, които тя му е предоставила, или когато е необходимо, чрез други подходящи средства. Ако организацията нито премахва упоменаванията, нито самосертифицира своето съответствие по отношение на РЗЛД в отношенията между ЕС и САЩ съгласно процедурите на министерството, то ще отнесе въпроса по служебен път до ФТК, МТ или друг съответен правоприлагащ орган или ще предприеме други подходящи действия, за да гарантира правилното използване на сертификационния знак на РЗЛД в отношенията между ЕС и САЩ;
- Министерството своевременно ще разглежда и намира решения на конкретни обосновани жалби относно неверни твърдения за участие в РЗЛД в отношенията между ЕС и САЩ, които то получава (*например* жалби, получени от ОЗД, независими механизми за защита, предоставяни от органи за алтернативно решаване на спорове от частния сектор, субекти на данни, предприятия в ЕС и САЩ и други видове трети страни); както и
- Министерството може да предприеме други подходящи коригиращи действия. Погрешно представяне пред министерството може да бъде санкционирано по силата на Закона за неверните твърдения (18 U.S.C. § 1001).

Извършва периодични служебни прегледи и оценки на спазването на програмата за Рамката за личните данни

- Министерството ще полага постоянни усилия да следи ефективното спазване от страна на организациите на РЗЛД в отношенията между ЕС и САЩ, за да открива проблеми, които може да налагат последващи действия. По-специално министерството ще извършва по служебен път рутинни внезапни проверки на произволно избрани организации, участващи в РЗЛД в отношенията между ЕС и САЩ, както и *ad hoc* внезапни проверки на конкретни организации, участващи в РЗЛД в отношенията между ЕС и САЩ, когато бъдат установени потенциални пропуски в спазването (например потенциални пропуски в спазването, за които министерството е било уведомено от трети страни), за да провери: а) дали е(са) налично(и) звено(а) за контакт, отговарящо(и) за разглеждането на жалби, искания за достъп и други въпроси, възникващи съгласно РЗЛД в отношенията между ЕС и САЩ; б) когато е приложимо, дали публичната политика на организацията в областта на неприкосновеността на личния живот е леснодостъпна за преглед от обществеността както в публичния уебсайт на организацията, така и чрез хипервръзка в Списъка към Рамката за личните данни; в) дали политиката на организацията в областта на неприкосновеността на личния живот продължава да отговаря на изискванията за самосертифициране, описани в Принципите; и г) дали независимият механизъм за защита, определен от организацията, е на разположение за разглеждане на жалби, подадени съгласно РЗЛД в отношенията между ЕС и САЩ. Министерството също така ще следи активно новините за информация, която предоставя достоверни доказателства за неспазване от страна на организациите на РЗЛД в отношенията между ЕС и САЩ;
- Като част от прегледа на спазването министерството ще изиска от дадена организация, участваща в РЗЛД в отношенията между ЕС и САЩ, да попълни и да му представи подробен въпросник, когато: а) министерството е получило конкретни обосновани жалби по отношение на спазването на Принципите от страна на организацията, б) организацията не отговаря задоволително на запитвания от страна на министерството за информация, свързана с РЗЛД в отношенията между ЕС и САЩ, или в) има достоверни доказателства, че организацията не спазва ангажиментите си съгласно РЗЛД в отношенията между ЕС и САЩ. Когато министерството изпрати такъв подробен въпросник на дадена организация и тя не отговори задоволително на въпросника, то я информира, че ще отнесе въпроса според случая до съответната инстанция за евентуално предприемане на действия по правоприлагане, ако не получи навременен и задоволителен отговор от организацията. Министерството ще информира организацията чрез средствата за връзка, които тя му е предоставила, или когато е необходимо, чрез други подходящи средства. Ако организацията не предостави навременен и задоволителен отговор, министерството ще отнесе въпроса по служебен път до ФТК, МТ или друг съответен правоприлагащ орган или ще предприеме други подходящи действия за гарантиране на спазването. Когато е уместно, министерството се консултира с компетентните органи за защита на данните относно тези прегледи на спазването; както и
- Министерството ще извършва периодична оценка на управлението и надзора на програмата за Рамката за личните данни, за да гарантира, че неговите усилия за наблюдение, включително всички подобни усилия, положени при използването на инструменти за търсене (например за проверка на неработещи хипервръзки към политиките в областта на неприкосновеността на личния живот на организациите, участващи в РЗЛД в отношенията между ЕС и САЩ), са подходящи за решаване на съществуващите проблеми и на всички нови проблеми, когато възникнат.

Адаптира уебсайта на Рамката за личните данни според целевите групи

Министерството ще адаптира уебсайта на Рамката за личните данни с насоченост върху следните целеви групи: физически лица от ЕС, предприятия от ЕС, предприятия от САЩ и ОЗД. Включването на материал, насочен пряко към физическите лица от ЕС и предприятията от ЕС, ще съдейства за прозрачността по няколко начина. По отношение на физическите лица от ЕС в уебсайта ще бъдат ясно пояснени: 1) правата, които РЗЛД в отношенията между ЕС и САЩ дава на физическите лица от ЕС; 2) механизмите за защита, с които разполагат физическите лица от ЕС, когато считат, че дадена организация нарушава ангажиментите си да спазва Принципите; и 3) как да намерят информация, отнасяща се до самосертифицирането на дадена организация съгласно РЗЛД в отношенията между ЕС и САЩ. По отношение на предприятията от ЕС ще се улесни проверката: 1) дали дадена организация участва в РЗЛД в отношенията между ЕС и САЩ; 2) за вида на информацията, която е включена в самосертифицирането на дадена организация съгласно РЗЛД в отношенията между ЕС и САЩ; 3) за политиката в областта на неприкосновеността на личния живот, която се прилага за включената информация; и 4) за метода, който организацията използва за удостоверяване на спазването на Принципите. По отношение на предприятията от САЩ ще бъдат ясно пояснени: 1) ползите от участието в РЗЛД в отношенията между ЕС и САЩ; 2) начинът, по който да се присъединят към РЗЛД в отношенията между ЕС и САЩ, както и начинът, по който да се сертифицират повторно и да се оттеглят от РЗЛД в отношенията между ЕС и САЩ; и 3) начинът, по който Съединените щати управляват и прилагат РЗЛД в отношенията между ЕС и САЩ. Включването на материал, насочен пряко към ОЗД (например информация за специалното звено на министерството за контакт с ОЗД и хипервръзка към съдържанието, свързано с принципите, в уебсайта на ФТК), ще съдейства както за сътрудничеството, така и за прозрачността. Министерството също така ще работи на *ad hoc* принцип с Комисията и Европейския комитет по защита на данните („ЕКЗД“) за разработване на допълнителни актуални материали (например отговори на често задавани въпроси), които да се използват в уебсайта на Рамката за личните данни, когато такава информация би улеснила ефикасното управление и надзор на програмата за Рамката за личните данни.

Улеснява сътрудничеството с ОЗД

За увеличаване на възможностите за сътрудничество с ОЗД в министерството ще бъде осигурено конкретно лице за контакт, което да изпълнява функциите на връзка с ОЗД. В случаите, когато даден ОЗД счита, че организация, участваща в РЗЛД в отношенията между ЕС и САЩ, не спазва Принципите, включително след подадена жалба от физическо лице от ЕС, ОЗД ще може да се свърже с конкретното лице за контакт в министерството, за да посочи организацията за допълнителен преглед. Министерството ще полага всички възможни усилия да съдейства за решаването на жалбата съвместно с организацията, участваща в РЗЛД в отношенията между ЕС и САЩ. В срок до 90 дни от получаването на жалбата министерството ще информира ОЗД за актуалното състояние. Конкретното лице за контакт ще получава също така сезирания за организации, които неправомерно твърдят, че участват в РЗЛД в отношенията между ЕС и САЩ. Това лице за контакт ще проследява всички сезирания на министерството от ОЗД относно жалби, а министерството ще предоставя доклад с обобщен анализ на жалбите, които са получени през годината, в разгледания по-долу съвместен преглед. Лицето за контакт ще съдейства на ОЗД, търсещи информация, свързана със самосертифицирането на конкретна организация или предишно участие в РЗЛД в отношенията между ЕС и САЩ, и ще отговаря на запитвания от ОЗД във връзка с изпълнението на конкретни изисквания съгласно РЗЛД в отношенията между ЕС и САЩ. Министерството ще си сътрудничи също така с Комисията и ЕКЗД относно процедурните и административните аспекти на панела на ОЗД, включително за установяването на подходящи процедури за разпределяне на средствата, събрани чрез таксата за панела на ОЗД. Наясно сме, че Комисията ще работи с министерството, за да съдейства за решаването на всякакви проблеми, които може да възникнат във връзка с тези процедури. Освен това министерството ще предостави на ОЗД материали във връзка с РЗЛД в отношенията между ЕС и САЩ, които те да включат в уебсайтовете си за повишаване на прозрачността за физическите лица от ЕС и предприятията от ЕС. Повишаването на информираността относно РЗЛД в отношенията между ЕС и САЩ и правата и отговорностите, които произтичат от нея, следва да улесни установяването на проблемите при тяхното възникване, за да могат да бъдат решавани по подходящ начин.

Изпълнява ангажиментите си съгласно приложение I към Принципите

Министерството ще изпълнява ангажиментите си съгласно приложение I към Принципите, включително ще поддържа списък с арбитри, избрани в сътрудничество с Комисията въз основа на тяхната независимост, почтеност и експертен опит, както и ще подпомага, когато е уместно, третата страна, избрана от него да администрира арбитражните производства съгласно приложение I към Принципите и да управлява арбитражния фонд, посочен в споменатото приложение ⁽³⁾. Министерството ще работи с третата страна, за да провери наред с другото дали третата страна поддържа уебсайт с насоки относно арбитражния процес, включително: 1) начина за иницииране на арбитражно производство и за подаване на документи; 2) списъка с арбитрите, поддържан от министерството, и начина за избиране на арбитри от този списък; 3) уреждащите арбитражни процедури и кодекса за поведение на арбитрите, приети от министерството и Комисията ⁽⁴⁾; и 4) събирането и плащането на хонорари на арбитрите. Освен това министерството заедно с третата страна периодично ще извършват преглед на работата на арбитражния фонд, включително необходимостта от промяна на размера на вноските или на тавана (*т.е.* максималната сума) на разходите за арбитраж, като наред с останалото ще вземат предвид броя на арбитражните дела и разходите и времетраенето им, като идеята е да не се създава прекомерна финансова тежест за организациите, участващи в РЗЛД в отношенията между ЕС и САЩ. Министерството ще уведомява Комисията за резултата от съвместните прегледи с третата страна и ще предоставя на Комисията предварително уведомление за всякакви корекции на размера на вноските.

Провежда съвместни прегледи на функционирането на РЗЛД в отношенията между ЕС и САЩ

Министерството и други агенции според случая ще провеждат периодични срещи с Комисията, заинтересовани ОЗД и съответни представители на ЕКЗД, на които министерството ще предоставя актуална информация относно РЗЛД в отношенията между ЕС и САЩ. На срещите ще се провеждат дискусии по текущи въпроси, свързани с функционирането, изпълнението, надзора и прилагането на програмата за Рамката за личните данни. На срещите може според случая да се обсъждат свързани теми, като например други механизми за предаване на данни, които се ползват от гаранциите съгласно РЗЛД в отношенията между ЕС и САЩ.

⁽³⁾ Международният център за решаване на спорове (ICDR) — международното подразделение на Американската арбитражна асоциация (AAA) (наричани заедно ICDR-AAA), беше избран от министерството да администрира арбитражните производства съгласно приложение I към Принципите и да управлява арбитражния фонд, посочен в споменатото приложение.

⁽⁴⁾ На 15 септември 2017 г. министерството и Комисията се договориха относно приемането на набор от правила за арбитраж, които да уреждат правнообвързващите арбитражни производства, посочени в приложение I към Принципите, както и на кодекс за поведение на арбитрите, който е в съответствие с общоприетите етични стандарти за арбитрите по търговски спорове и с приложение I към Принципите. Министерството и Комисията се договориха относно адаптирането на правилата за арбитраж и кодекса за поведение така, че да отразят актуализациите съгласно РЗЛД в отношенията между ЕС и САЩ, като министерството ще работи с ICDR-AAA за извършването на тези актуализации.

Актуализиране на законодателството

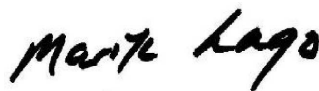
Министерството ще положи усилия в рамките на разумното, за да информира Комисията за съществени промени в законодателството на САЩ, доколкото те са от значение за РЗЛД в отношенията между ЕС и САЩ в областта на защитата на личните данни и за ограниченията и гаранциите, приложими към достъпа до лични данни от страна на органите на САЩ и последващото им използване.

Достъп на правителството на САЩ до лични данни

В Съединените щати бяха издадени Указ 14086 Enhancing Safeguards for United States Signals Intelligence Activities [Засилване на гаранциите за дейностите на САЩ за радиоелектронно разузнаване] и 28 CFR, част 201 за изменение на разпоредбите на Министерството на правосъдието с цел създаване на съд, извършващ съдебен контрол на защитата на данните (DPRC), които осигуряват силна защита на личните данни, що се отнася до достъпа на правителството до данни за целите на националната сигурност. Предоставената защита включва: укрепване на гаранциите за неприкосновеност на личния живот и граждански свободи, с които да се подсигурава, че дейностите на САЩ за радиоелектронно разузнаване са необходими и пропорционални за постигането на определените цели в областта на националната сигурност; създаване на нов механизъм за правна защита с независими и обвързващи правомощия; и засилване на съществуващия строг и многостепенен надзор на дейностите на САЩ за радиоелектронно разузнаване. Чрез тези средства физическите лица от ЕС може да потърсят правна защита от нов многостепенен механизъм за правна защита, който включва независим DPRC, съставен от лица извън правителството на САЩ, които ще имат пълни правомощия да се произнасят по жалби и да определят корективни мерки при необходимост. Министерството ще поддържа регистър на физическите лица от ЕС, които са подали отговаряща на условията жалба в съответствие с Указ 14086 и 28 CFR, част 201. Пет години след датата на настоящото писмо и на всеки пет години след това министерството ще се свързва със съответните агенции относно това дали информацията, отнасяща се до разглеждането на отговарящи на условията жалби или до разглеждането на заявления за преразглеждане, подадени до DPRC, е била разсекретена. Ако такава информация е била разсекретена, министерството ще работи със съответния ОЗД, за да информира физическото лице от ЕС. С тези подобрения се потвърждава, че личните данни от ЕС, предавани на Съединените щати, ще бъдат обработвани по начин, съответстващ на правните изисквания на ЕС по отношение на достъпа на правителството до данни.

Въз основа на Принципите, Указ 14086, 28 CFR, част 201 и придружаващите писма и материали, включително ангажиментите на министерството по отношение на управлението и надзора на програмата за Рамката за личните данни, очакваме Комисията да определи, че РЗЛД в отношенията между ЕС и САЩ осигурява адекватна защита за целите на правото на ЕС и че ще продължат да се предават данни от Европейския съюз към организациите, които участват в РЗЛД в отношенията между ЕС и САЩ. Очакваме също така, че прехвърлянията на данни към организации от САЩ, извършвани въз основа на стандартните договорни клаузи на ЕС или задължителните фирмени правила на ЕС, ще бъдат допълнително улеснени от условията на тези договорености.

С уважение,



Marisa Lago

ПРИЛОЖЕНИЕ IV



СЪЕДИНЕНИ АМЕРИКАНСКИ ЩАТИ
Федерална търговска комисия
WASHINGTON, D.C. 20580

Бюро на председателя

9 юни 2023 г.

Дидие Рейндерс
Комисар по въпросите на правосъдието
European Commission
Rue de la Loi/Wetstraat 200
1049 Brussels
Белгия

Уважаеми комисар Рейндерс,

Федералната търговска комисия („ФТК“) на Съединените щати оценява възможността да представи своите действия по прилагане на Принципите на Рамката за личните данни в отношенията между ЕС и САЩ („РЗЛД в отношенията между ЕС и САЩ“). ФТК отдавна се е ангажира с трансграничната защита на потребителите и неприкосновеността на личния живот, като поемаме ангажимент също да прилагаме свързаните с търговския сектор аспекти на тази Рамка. ФТК изпълнява тази роля от 2000 г. насам във връзка с Рамката за сфера на неприкосновеност на личния живот, а от 2016 г. насам — във връзка с Рамката на Щита за личните данни в отношенията между ЕС и САЩ ⁽¹⁾. На 16 юли 2020 г. Съдът на Европейския съюз обяви за невалидно решението на Европейската комисия относно адекватното ниво на защита, стоящо в основата на Рамката на Щита за личните данни в отношенията между ЕС и САЩ, въз основа на проблеми, различни от търговските принципи, които ФТК прилага. Оттогава САЩ и Европейската комисия водят преговори във връзка с Рамката за личните данни в отношенията между ЕС и САЩ в отговор на това решение на Съда на Европейския съюз.

Пиша Ви, за да потвърдя ангажимента на ФТК за стриктно прилагане на Принципите на РЗЛД в отношенията между ЕС и САЩ. По-специално потвърждаваме своя ангажимент в три основни направления: 1) отдаване на приоритет на сезирания и разследване; 2) изискване на заповеди и контрол по тях; и 3) сътрудничество в областта на правоприлагането с органите за защита на данните („ОЗД“) от ЕС.

I. Въведение

а. Работа на ФТК за изпълнение на изискванията за неприкосновеност на личния живот и съответната политика

ФТК разполага с широки правомощия за правоприлагане с гражданскоправни средства за повишаване на защитата на потребителите и насърчаване на конкуренцията в сферата на търговията. Като част от правомощията ѝ в областта на защитата на потребителите ФТК осигурява прилагането на широка гама от закони за защита на неприкосновеността на

⁽¹⁾ Писмо от председателя Edith Ramirez до Вера Йоурова, комисар по въпросите на правосъдието, потребителите и равнопоставеността между половете от Европейската комисия, в което се разглеждат действията от страна на Федералната търговска комисия по прилагането на новата Рамка на Щита за личните данни в отношенията между ЕС и САЩ (29 февруари 2016 г.), достъпно на адрес <https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/letter-chairwoman-edith-ramirez-vera-jourova-commissioner-justice-consumers-gender-equality-european>. Преди това ФТК се ангажира също да прилага програмата за сфера на неприкосновеност на личния живот. Писмо от Robert Pitofsky, председател на ФТК, до John Mogg, директор на ГД „Вътрешен пазар“, Европейска комисия (14 юли 2000 г.), достъпно на адрес <https://www.federalregister.gov/documents/2000/07/24/00-18489/issuance-of-safe-harbor-principles-and-transmission-to-european-commission> Настоящото писмо заменя тези предишни ангажименти.

личния живот и сигурността на потребителите и на техните данни. Основният закон, който ФТК прилага — Законът за ФТК — забранява „нелоялни“ или „измамни“ действия или практики в търговията или засягащи търговията ⁽²⁾. Също така ФТК прилага специални закони за защита на информацията относно здравословното състояние, заеми и други финансови въпроси, както и онлайн информация за деца и е издала разпоредби за прилагането на всеки един от тези закони ⁽³⁾.

ФТК също така наскоро предприе редица инициативи за укрепване на своята дейност в областта на неприкосновеността на личния живот. През август 2022 г. ФТК обяви, че обмисля въвеждането на правила за ограничаване на вредното събиране на данни за лица с търговска цел и слабата сигурност на данните ⁽⁴⁾. С проекта се цели да се създаде солиден публичен регистър, който да даде информация дали ФТК следва да издаде правила за справяне с практиките за събиране на данни за лица с търговска цел и за преодоляване на проблемите със сигурността на данните и как евентуално да изглеждат тези правила. Приветстваме коментарите на заинтересованите страни от ЕС относно тази и други инициативи.

Нашите конференции PrivacyCon продължават да събират водещи изследователи, за да обсъждат най-новите изследвания и тенденции, свързани с неприкосновеността на личния живот на потребителите и сигурността на техните данни. Също така повишихме способността на институцията да бъде в крак с развитието на технологиите, които са в центъра на нашата дейност в областта на неприкосновеността на личния живот, като създадохме нарастващ екип от технологи и интердисциплинарни изследователи. Както знаете, стартирахме също така съвместен диалог с Вас и Вашите колеги от Европейската комисия, който включва разглеждане на теми, свързани с неприкосновеността на личния живот, като тъмни модели и модели на стопанска дейност, характеризирани с повсеместно събиране на данни ⁽⁵⁾. Неотдавна публикувахме и доклад до Конгреса, в който предупреждаваме за вредите, свързани с използването на изкуствен интелект („ИИ“) за справяне с онлайн проблемите, установени от Конгреса. В този доклад се изразяват опасения във връзка с неточността, предубежденията, дискриминацията и събирането на данни, които впоследствие се използват за цели, различни от първоначалните ⁽⁶⁾.

Б. Правни инструменти за защита в САЩ, от които могат да се ползват потребителите от ЕС

РЗПД в отношенията между ЕС и САЩ функционира в общия контекст на инструменти в САЩ в областта на неприкосновеността на личния живот, които осигуряват и защита за потребителите от ЕС по редица начини. Забраната за нелоялни или измамни действия или практики в Закона за ФТК не се ограничава до защитата на потребителите в САЩ срещу дружества от САЩ, тъй като се отнася за практики, които 1) нанасят или са в състояние да нанесат разумно предвидими вреди в Съединените щати или 2) се отнасят за действия по същество, извършвани в Съединените щати. Освен това, когато защитава чуждестранни потребители ФТК може да използва всички средства за правна защита, с които разполага за защита на националните потребители ⁽⁷⁾.

ФТК прилага и други специални закони, в които защитата обхваща и потребители извън САЩ, като например Закона за защита на неприкосновеността на личния живот на децата онлайн (COPPA). Наред с останалото в този закон се поставя изискване към операторите на уебсайтове и онлайн услуги, предназначени за деца, или общодостъпни сайтове, които съзнателно събират лична информация от деца на възраст под 13 години, да уведомяват за това родителите и да изискват родителско съгласие, което може да се провери. Уебсайтовете и услугите, базирани в САЩ, за които се прилага COPPA и които събират лична информация от деца извън САЩ, са задължени да спазват този закон. Чуждестранните уебсайтове и онлайн услуги също са задължени да спазват COPPA, ако дейностите им са насочени към деца в Съединените щати или

⁽²⁾ 15 U.S.C. § 45(a). ФТК не е компетентна по отношение на прилагането на наказателното право или по въпроси на националната сигурност и няма правомощия по повечето от останалите действия на правителството. Освен това има изключения от компетентността на ФТК за търговските дейности, включително по отношение на банките, въздушните превозвачи, застрахователната дейност и дейностите на доставчиците на далекосъобщителни услуги в качеството им на общи преносители. Също така ФТК не е компетентна по отношение на повечето нестопански организации, но е компетентна по отношение на фиктивните благотворителни организации или други нестопански организации, които реално работят за печалба. Компетентността на ФТК обхваща и нестопански организации, които работят за печалба в полза на свои стопански членове, включително, като им осигуряват значителни икономически ползи. В някои случаи компетентността на ФТК съпада с тази на други правоприменяващи агенции. Изградили сме стабилни работни взаимоотношения с федералните и щатските органи и работим в тясно взаимодействие с тях за координиране на разследванията или за сезиране, когато е необходимо.

⁽³⁾ Вж. Privacy and Security [Неприкосновеност на личния живот и сигурност], <https://www.ftc.gov/business-guidance/privacy-security>.

⁽⁴⁾ Вж. Съобщение за пресата, ФТК, FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices [ФТК обмисля правила за ограничаване на практиките за събиране на данни за лица с търговска цел и за преодоляване на проблемите със слабата сигурност на данните] (11 август 2022 г.), <https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices>.

⁽⁵⁾ Вж. Joint press statement by Didier Reynders, Commissioner for Justice of the European Commission and Lina Khan, Chair of the United States Federal Trade Commission [Съвместно изявление за медиите на Дидие Рейндерс, комисар по въпросите на правосъдието от Европейската комисия, и Lina Khan, председател на Федералната търговска комисия на Съединените щати] (30 март 2022 г.), достъпно на адрес https://www.ftc.gov/system/files/ftc_gov/pdf/joint%20FTC-EC%20Statement%20informal%20dialogue%20consumer%20protection%20issues.pdf.

⁽⁶⁾ Вж. Съобщение за пресата, ФТК, FTC Report Warns About Using Artificial Intelligence to Combat Online Problems [Доклад на ФТК предупреждава за използването на изкуствен интелект за борба с онлайн проблемите] (16 юни 2022 г.), достъпен на адрес <https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-report-warns-about-using-artificial-intelligence-combat-online-problems>.

⁽⁷⁾ 15 U.S.C. § 45(a)(4)(B). Освен това към „нелоялни или измамни действия или практики“ спадат такива действия или практики за международна търговия, които i) нанасят или са в състояние да нанесат разумно предвидими вреди в Съединените щати; или ii) се отнасят за действия по същество, извършвани в Съединените щати. 15 U.S.C. § 45(a)(4)(A).

съзнателно събират лична информация от деца в Съединените щати. Освен федералните закони, които прилага ФТК, допълнителни ползи за потребителите от ЕС може да предоставят и други федерални и щатски закони в областта на защитата на потребителите, нарушенията на сигурността на данните и неприкосновеността на личния живот.

в. Дейност по правоприлагане на ФТК

ФТК заведе дела съгласно Рамката за сфера на неприкосновеност на личния живот и Рамката на Щита за личните данни в отношенията между ЕС и САЩ и продължи да прилага Щита за личните данни в отношенията между ЕС и САЩ дори след като Съдът на Европейския съюз обяви за невалидно решението относно адекватното ниво на защита, стоящо в основата на Рамката на Щита за личните данни в отношенията между ЕС и САЩ⁽⁸⁾. В няколко от неотдавнашните жалби на ФТК се съдържат твърдения, че дружества са нарушили разпоредбите на Щита за личните данни в отношенията между ЕС и САЩ, включително в производствата срещу Twitter⁽⁹⁾, CafePress⁽¹⁰⁾ и Flo⁽¹¹⁾. В рамките на действията по правоприлагане на ФТК срещу Twitter на платформата се наложи да плати 150 милиона долара за нарушаване на предишна заповед на ФТК с практики, засягащи над 140 милиона потребители, включително нарушаване на Принцип 5 от Щита за личните данни в отношенията между ЕС и САЩ (Цялост на данните и ограничаване в рамките на целта). Освен това в заповедта на институцията се изисква Twitter да даде възможност на потребителите да използват сигурни методи за многофакторно удостоверяване, които не изискват от тях да предоставят телефонните си номера.

В жалбата срещу CafePress ФТК твърди, че дружеството не е успяло да защити чувствителната информация на потребителите, прикрило е голямо нарушение на сигурността на данните и е нарушило Принципи 2 (Избор), 4 (Сигурност) и 6 (Достъп) на Щита за личните данни в отношенията между ЕС и САЩ. Със заповедта на ФТК от дружеството се изисква да замени неподходящите мерки за удостоверяване с многофакторно удостоверяване, да ограничи значително обема на данните, които събира и съхранява, да шифрова социалноосигурителните номера, както и да възложи на трета страна да оцени програмите му за информационна сигурност и да предостави на ФТК копие, което може да бъде публикувано.

В жалбата срещу Flo ФТК твърди, че приложението за проследяване на фертилността е разкрило здравна информация за потребителите на доставчици на услуги за анализ на данни от трети страни, след като е поет ангажимент тази информация да остане поверителна. В жалбата на ФТК изрично се посочва взаимодействието на дружеството с потребители от ЕС и че Flo е нарушило Принципи 1 (Уведомяване), 2 (Избор), 3 (Отчетност за последващото предаване) и 5 (Цялост на данните и ограничаване в рамките на целта) на Щита за личните данни в отношенията между ЕС и САЩ. Наред с другото заповедта на институцията задължава Flo да уведоми засегнатите потребители за разкриването на личната им информация и да инструктира всяка трета страна, получила здравна информация за потребителите, да я унищожи. Важно е да се отбележи, че заповедите на ФТК осигуряват защита за всички потребители от целия свят, които имат взаимоотношения с предприятия от САЩ, а не само за тези, които са подали жалби.

Много от предишните случаи на правоприлагане, свързани със сферата на неприкосновеност на личния живот и Щита за личните данни в отношенията между ЕС и САЩ, се отнасяха за организации, които са изпълнили първоначалното самосертифициране пред Министерството на търговията, но не са извършвали годишното си самосертифициране, въпреки че са продължили да твърдят, че са настоящи участници. Други случаи са свързани с неверни твърдения за участие на организации, които никога не са извършвали първоначално самосертифициране пред Министерството на търговията. В бъдеще очакваме усилията ни за проактивно правоприлагане да се съсредоточат още повече върху видовете съществени нарушения на Принципиите на РЗЛД в отношенията между ЕС и САЩ, за които се твърди, че са извършени в случаи като Twitter, CafePress и Flo. Междувременно Министерството на търговията ще управлява и контролира процеса на самосертифициране, ще поддържа официалния списък на участниците в РЗЛД в отношенията между ЕС и САЩ и ще разглежда други проблеми, свързани с твърденията за участие в програмата⁽¹²⁾. Важно е да се отбележи, че по отношение на организациите, които твърдят, че участват в РЗЛД в отношенията между ЕС и САЩ, може да бъдат предприети действия по прилагане по същество на Принципиите на РЗЛД в отношенията между ЕС и САЩ, дори да не извършат или да не повтарят самосертифицирането си пред Министерството на търговията.

⁽⁸⁾ Вж. допълнение А за списък с делата, заведени от ФТК във връзка със сферата на неприкосновеност на личния живот и Щита за личните данни.

⁽⁹⁾ Вж. Съобщение за пресата, ФТК, FTC Charges Twitter with Deceptively Using Account Security Data to Sell Targeted Ads [ФТК обвинява Twitter в измамно използване на данни за сигурността на акаунтите за продажба на целенасочени реклами] (25 май 2022 г.), достъпно на адрес <https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using-account-security-data-sell-targeted-ads>.

⁽¹⁰⁾ Вж. Съобщение за пресата, ФТК, FTC Takes Action Against CafePress for Data Breach Cover Up [ФТК предприема действия срещу CafePress за прикриване на нарушение на сигурността на данните] (15 март 2022 г.), достъпно на адрес <https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-cafepress-data-breach-cover>.

⁽¹¹⁾ Вж. Съобщение за пресата, ФТК, FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others [ФТК финализира заповедта за Flo Health — приложение за проследяване на фертилността, което е споделяло чувствителни здравни данни с Facebook, Google и други] (22 юни 2021 г.), достъпно на адрес <https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google>.

⁽¹²⁾ Писмо от Marisa Lago, заместник-министър на търговията, отговарящ за международната търговия, до уважаемия Дидие Рейндерс, комисар по въпросите на правосъдието, Европейска комисия (12 декември 2022 г.).

II. Отдаване на приоритет на сезирания и разследване

Както и по Рамката за сфера на неприкосновеност на личния живот и Рамката на Щита за личните данни в отношенията между ЕС и САЩ, ФТК се ангажира да разглежда с предимство случаите, по които е сезирана от Министерството на търговията и държавите — членки на ЕС, съгласно Принципите на РЗЛД в отношенията между ЕС и САЩ. Ще разглеждаме приоритетно също така случаите на неспазване на Принципите на РЗЛД в отношенията между ЕС и САЩ, за които сме сезирани от саморегулиращи се организации за защита на неприкосновеността на личния живот и други независими органи за решаване на спорове.

За улесняване на сезиранията съгласно РЗЛД в отношенията между ЕС и САЩ от държавите — членки на ЕС, ФТК създаде стандартизиран процес за сезиране и даде насоки на тези държави относно вида на информацията, която би подпомогнала най-много ФТК при събирането на доказателства по случая. Като част от тези усилия ФТК определи лице за връзка с институцията относно сезирания от държавите — членки на ЕС. Особено полезно е, когато сезиращият орган е събрал доказателства по твърдението за нарушение и може да сътрудничи на ФТК при разследването.

След като бъде сезирана от Министерството на търговията, държава — членка на ЕС, саморегулираща се организация или други независими органи за решаване на спорове, ФТК може да предприеме редица действия за решаване на посочените проблеми. Например можем да направим преглед на политиките на организацията в областта на неприкосновеността на личния живот, да получим допълнителна информация директно от организацията или от трети страни, да осъществим последващ контрол съвместно със сезиращия субект, да направим оценка дали има модел на извършване на нарушенията или са засегнати значителен брой потребители, да определим дали сезирането засяга въпроси, които са от компетентността на Министерството на търговията, да направим преценка дали допълнителните усилия за уведомяване на участниците на пазара ще са от полза, и ако е необходимо, да инициираме производство по принудително изпълнение.

В допълнение към отдаването на приоритет на случаите, свързани с Принципите на РЗЛД в отношенията между ЕС и САЩ, за които ФТК е сезирана от Министерството на търговията, държавите — членки на ЕС, саморегулиращи се организации за защита на неприкосновеността на личния живот или други независими органи за решаване на спорове ⁽¹³⁾, тя ще продължи да разследва значителни нарушения на Принципите на РЗЛД в отношенията между ЕС и САЩ по собствена инициатива, когато е целесъобразно, като използва набор от инструменти. Като част от програмата на ФТК за разследване на проблеми, свързани с неприкосновеността на личния живот и сигурността, в които имат участие търговски организации, институцията редовно проверява дали въпросният субект представя информация за участие в Щита за личните данни в отношенията между ЕС и САЩ. Ако субектът е представил такава информация и при разследването се разкрият явни нарушения на Принципите на Щита за личните данни в отношенията между ЕС и САЩ, ФТК включва твърденията за нарушения на Щита за личните данни в отношенията между ЕС и САЩ в своите действия по правоприлагане. Ще продължим да прилагаме този проактивен подход сега и по отношение на Принципите на РЗЛД в отношенията между ЕС и САЩ.

III. Изискване на заповеди и контрол по тях

ФТК потвърждава също ангажимента си да изисква заповеди за принудително изпълнение и да упражнява контрол по тях, за да гарантира спазването на Принципите на РЗЛД в отношенията между ЕС и САЩ. Ние ще изискваме Принципите на РЗЛД в отношенията между ЕС и САЩ да бъдат спазвани посредством различни подходящи разпоредби за прекратяване, предвидени в бъдещите заповеди на ФТК съгласно Принципите на РЗЛД в отношенията между ЕС и САЩ. Неизпълнението на административна заповед на ФТК може да води до налагане на гражданскоправни санкции в размер до 50 120 USD за всяко нарушение или 50 120 USD на ден за продължаващо нарушаване ⁽¹⁴⁾, като санкцията може да достигне милиони долари при практики, засягащи голям брой потребители. Всяка заповед за съгласие съдържа също разпоредби за докладване и спазване. Субектите, по отношение на които е издадена заповед, трябва да пазят документацията, доказваща изпълнението, за срок от определен брой години. Заповедите трябва също така да бъдат сведени до знанието на служителите, които отговарят за гарантиране на изпълнението им.

ФТК провежда системен контрол на изпълнението на съществуващите заповеди съгласно Принципите на Щита за личните данни в отношенията между ЕС и САЩ, както прави с всички свои заповеди, и предприема действия за принудителното им изпълнение, когато е необходимо ⁽¹⁵⁾. Важно е да се отбележи, че заповедите на ФТК ще продължат да осигуряват защита за всички потребители от целия свят, които имат взаимоотношения с предприятия, а не само за тези, които са подали жалби. И накрая, ФТК ще поддържа онлайн списък на дружествата, по отношение на които са издадени заповеди във връзка с прилагането на Принципите на РЗЛД в отношенията между ЕС и САЩ ⁽¹⁶⁾.

⁽¹³⁾ Въпреки че ФТК не издава решения и не е медиатор по индивидуални жалби на потребители, тя потвърждава ангажимента си да разглежда с предимство случаите, за които е сезирана от ОЗД на ЕС съгласно Принципите на РЛД в отношенията между ЕС и САЩ. Освен това ФТК използва жалбите, въведени в нейната база данни за потребители (до която имат достъп много други правоприлагащи агенции), за да определя тенденциите, приоритетите при прилагането и потенциалните обекти за разследване. Физическите лица от ЕС могат да използват същата система, с която разполагат потребителите в САЩ, за да подават жалби до ФТК, достъпна на адрес: <https://reportfraud.ftc.gov/>. За предпочитане е обаче физическите лица от ЕС да подават индивидуалните си жалби по Принципите на РЛД в отношенията между ЕС и САЩ до ОЗД в своята държава членка или до независим орган за решаване на спорове.

⁽¹⁴⁾ 15 U.S.C. § 45(m); 16 C.F.R. § 1.98. Тази сума се коригира периодично спрямо инфлацията.

⁽¹⁵⁾ Миналата година ФТК гласува за оптимизиране на процеса на разследване на системните нарушители. Вж. Съобщение за пресата, ФТК, FTC Authorizes Investigations into Key Enforcement Priorities [ФТК разрешава разследвания по ключови приоритети на прилагането] (1 юли 2021 г.), достъпна на адрес <https://www.ftc.gov/news-events/news/press-releases/2021/07/ftc-authorizes-investigations-key-enforcement-priorities>.

⁽¹⁶⁾ Сравни ФТК, Щит за личните данни, <https://www.ftc.gov/business-guidance/privacy-security/privacy-shield>.

IV. Сътрудничество при правоприлагането с ОЗД от ЕС

ФТК признава важната роля на ОЗД от ЕС за спазването на Принципите на РЗЛД в отношенията между ЕС и САЩ и насърчава засилването на консултациите и сътрудничеството при правоприлагането. Действително координираният подход спрямо предизвикателствата, породени от настоящото развитие на цифровия пазар и от моделите на стопанска дейност, при които се използват големи обеми от данни, придобива все по-голямо значение. ФТК ще обменя информация по случаите, за които е била сезирана, със сезиращите правоприлагащи органи, включително относно етапа на разглеждане на случаите, при спазване на законите и ограниченията относно поверителността. Доколкото е възможно предвид броя и вида на случаите на сезиране, предоставената информация ще включва оценка на въпросите, повдигнати в сезирането, включително описание на значимите проблеми, които са повдигнати, и на евентуално предприетите действия за отстраняване на нарушенията на законите в рамките на компетентността на ФТК. Освен това ФТК ще предоставя информация на сезиращия орган относно вида на получените сезирания, за да бъде повишена ефективността на усилията за справяне с неправомерните действия. Ако сезиращ правоприлагащ орган търси информация относно етапа на разглеждане на конкретен случай на сезиране за целите на собственото си производство по принудително изпълнение, ФТК ще предоставя отговор, като взема предвид броя на сезиранията, които са в процес на разглеждане, както и изискванията за поверителност и други законови условия.

ФТК ще работи в тясно взаимодействие и с ОЗД от ЕС, за да предоставя съдействие при правоприлагането. В случаите, когато е уместно, това може да се изразява във взаимен обмен на информация и съдействие при разследвания в съответствие със Закона за безопасен интернет на САЩ, с който се разрешава на ФТК да оказва съдействие на чужди правоприлагащи институции, когато предприемат действия по прилагането на закони, забраняващи практики, които по същество са еднакви с тези, които се забраняват със законите, които ФТК прилага⁽¹⁷⁾. Като част от това съдействие ФТК може да споделя информация, получена във връзка с разследване на ФТК, да инициира задължителен процес от името на ОЗД от ЕС, провеждащ собствено разследване, и да взема устни показания от свидетели или ответници във връзка с производството по принудително изпълнение на ОЗД, ако това съответства на изискванията на Закона за безопасен интернет на САЩ. ФТК редовно използва правомощията си да съдейства на други органи по света по случаи в областта на неприкосновеността на личния живот и защитата на потребителите.

Освен с евентуалните консултации със сезиращите ОЗД от ЕС по специфични за всеки случай въпроси ФТК ще участва в периодични срещи с определени представители на Европейския комитет по защита на данните („ЕКЗД“) за обсъждане на възможности за подобряване на сътрудничеството при правоприлагането. ФТК също така ще участва заедно с Министерството на търговията, Европейската комисия и представители на ЕКЗД в периодичния преглед на РЗЛД за обсъждане на нейното прилагане. ФТК насърчава също така и разработването на инструменти, чрез които да се подобри сътрудничеството при правоприлагането с ОЗД от ЕС, както и с други правоприлагащи органи в областта на неприкосновеността на личния живот от целия свят. ФТК с удоволствие потвърждава ангажимента си за прилагането на свързаните с търговския сектор аспекти на РЗЛД в отношенията между ЕС и САЩ. Ние възприемаме партньорството си с колегите от ЕС като важна част от осигуряването на защита на неприкосновеността на личния живот както за нашите, така и за Вашите граждани.

С уважение,



Lina M. Khan

Председател, Федерална търговска комисия

⁽¹⁷⁾ Когато определя дали да упражни правомощията си по силата на Закона за безопасен интернет на САЩ, ФТК взема предвид наред с останалото и следното: „А) дали отправилата искането институция се е съгласила да предостави или ще предостави реципрочно съдействие на комисията; Б) дали удовлетворяването на искането би засегнало обществен интерес на Съединените щати; В) дали разследването или производството по принудително изпълнение на отправилата искането институция засяга действия или практики, които нанасят или са в състояние да нанесат вреда на значителен брой лица.“ 15 U.S.C. § 46(j)(3). Тези правомощия не важат за прилагането на законите в областта на конкуренцията.

Допълнение А

Правоприлагане във връзка с Щита за личните данни и сферата на неприкосновеност на личния живот

	Преписка/досие на ФТК №	Дело	Връзка
1	Досие на ФТК № 2023062 Дело № 3:22-cv-03070 (Окръжен съд, Северен окръг на Калифорния)	САЩ срещу Twitter, Inc.	Twitter
2	Досие на ФТК № 192 3209	Относно Residual Pumpkin Entity, LLC, предишно търговско наименование CafePress , и PlanetArt, LLC, търговско наименование CafePress	CafePress
3	Досие на ФТК № 192 3133 Преписка № C-4747	Относно Flo Health, Inc.	Flo Health
4	Досие на ФТК № 192 3050 Преписка № C-4723	Относно Ortho-Clinical Diagnostics, Inc.	Ortho-Clinical
5	Досие на ФТК № 192 3092 Преписка № C-4709	Относно T&M Protection, LLC	T&M Protection
6	Досие на ФТК № 192 3084 Преписка № C-4704	Относно TDARX, Inc.	TDARX
7	Досие на ФТК № 192 3093 Преписка № C-4706	Относно Global Data Vault, LLC	Global Data
8	Досие на ФТК № 192 3078 Преписка № C-4703	Относно Incentive Services, Inc.	Incentive Services
9	Досие на ФТК № 192 3090 Преписка № C-4705	Относно Click Labs, Inc.	Click Labs
10	Досие на ФТК № 182 3192 Преписка № C-4697	Относно Medable, Inc.	Medable
11	Досие на ФТК № 182 3189 Преписка № 9386	Относно NTT Global Data Centers Americas, Inc. в качеството му на правопреемник на RagingWire Data Centers, Inc.	RagingWire
12	Досие на ФТК № 182 3196 Преписка № C-4702	Относно Thru, Inc.	Thru
13	Досие на ФТК № 182 3188 Преписка № C-4698	Относно DCR Workforce, Inc.	DCR Workforce
14	Досие на ФТК № 182 3194 Преписка № C-4700	Относно LotaData, Inc.	LotaData
15	Досие на ФТК № 182 3195 Преписка № C-4701	Относно EmpiriStat, Inc.	EmpiriStat

16	Досие на ФТК № 182 3193 Преписка № С-4699	Относно 214 Technologies, Inc., също така с търговско наименование Trueface.ai	Trueface.ai
17	Досие на ФТК № 182 3107 Преписка № 9383	Относно Cambridge Analytica, LLC	Cambridge Analytica
18	Досие на ФТК № 182 3152 Преписка № С-4685	Относно SecureTest, Inc.	SecurTest
19	Досие на ФТК № 182 3144 Преписка № С-4664	Относно VenPath, Inc.	VenPath
20	Досие на ФТК № 182 3154 Преписка № С-4666	Относно SmartStart Employment Screening, Inc.	SmartStart
21	Досие на ФТК № 182 3143 Преписка № С-4663	Относно mResource LLC , търговско наименование Loop Works LLC	mResource
22	Досие на ФТК № 182 3150 Преписка № С-4665	Относно IDmission LLC	IDmission
23	Досие на ФТК № 182 3100 Преписка № С-4659	Относно ReadyTech Corporation	ReadyTech
24	Досие на ФТК № 172 3173 Преписка № С-4630	Относно Decusoft, LLC	Decusoft
25	Досие на ФТК № 172 3171 Преписка № С-4628	Относно Tru Communication, Inc.	Tru
26	Досие на ФТК № 172 3172 Преписка № С-4629	Относно Md7, LLC	Md7
30	Досие на ФТК № 152 3198 Преписка № С-4543	Относно Jhayrmaine Daniels (търговско наименование California Skate-Line)	Jhayrmaine Daniels
31	Досие на ФТК № 152 3190 Преписка № С-4545	Относно Dale Jarrett Racing Adventure, Inc.	Dale Jarrett
32	Досие на ФТК № 152 3141 Преписка № С-4540	Относно Golf Connect, LLC	Golf Connect
33	Досие на ФТК № 152 3202 Преписка № С-4546	Относно Inbox Group, LLC	Inbox Group
34	Досие № 152 3187 Преписка № С-4542	Относно IOActive, Inc.	IOActive
35	Досие на ФТК № 152 3140 Преписка № С-4549	Относно Jubilant Clinsys, Inc.	Jubilant
36	Досие на ФТК № 152 3199 Преписка № С-4547	Относно Just Bagels Manufacturing, Inc.	Just Bagels

37	Досие на ФТК № 152 3138 Преписка № C-4548	Относно NAICS Association, LLC	NAICS
38	Досие на ФТК № 152 3201 Преписка № C-4544	Относно One Industries Corp.	One Industries
39	Досие на ФТК № 152 3137 Преписка № C-4550	Относно Pinger, Inc.	Pinger
40	Досие на ФТК № 152 3193 Преписка № C-4552	Относно SteriMed Medical Waste Solutions	SteriMed
41	Досие на ФТК № 152 3184 Преписка № C-4541	Относно Contract Logix, LLC	Contract Logix
42	Досие на ФТК № 152 3185 Преписка № C-4551	Относно Forensics Consulting Solutions, LLC	Forensics Consulting
43	Досие на ФТК № 152 3051 Преписка № C-4526	Относно American Int'l Mailing, Inc.	AIM
44	Досие на ФТК № 152 3015 Преписка № C-4525	Относно TES Franchising, LLC	TES
45	Досие на ФТК № 142 3036 Преписка № C-4459	Относно American Apparel, Inc.	American Apparel
46	Досие на ФТК № 142 3026 Преписка № C-4469	Относно Fantage.com, Inc.	Fantage
47	Досие на ФТК № 142 3017 Преписка № C-4461	Относно Apperian, Inc.	Apperian
48	Досие на ФТК № 142 3018 Преписка № C-4462	Относно Atlanta Falcons Football Club, LLC	Atlanta Falcons
49	Досие на ФТК № 142 3019 Преписка № C-4463	Относно Baker Tilly Virchow Krause, LLP	Baker Tilly
50	Досие на ФТК № 142 3020 Преписка № C-4464	Относно BitTorrent, Inc.	BitTorrent
51	Досие на ФТК № 142 3022 Преписка № C-4465	Относно Charles River Laboratories, Int'l	Charles River
52	Досие на ФТК № 142 3023 Преписка № C-4466	Относно DataMotion, Inc.	DataMotion
53	Досие на ФТК № 142 3024 Преписка № C-4467	Относно DDC Laboratories, Inc. , търговско наименование DNA Diagnostics Center	DDC
54	Досие на ФТК № 142 3028 Преписка № C-4470	Относно Level 3 Communications, LLC	Level 3

55	Досие на ФТК № 142 3025 Преписка № C-4468	Относно PDB Sports, Ltd. , търговско наименование Denver Broncos Football Club, LLP	Broncos
56	Досие на ФТК № 142 3030 Преписка № C-4471	Относно Reynolds Consumer Products, Inc.	Reynolds
57	Досие на ФТК № 142 3031 Преписка № C-4472	Относно Receivable Management Services Corporation	Receivable Mgmt
58	Досие на ФТК № 142 3032 Преписка № C-4473	Относно Tennessee Football, Inc.	Tennessee Football
59	Досие на ФТК № 102 3058 Преписка № C-4369	Относно Myspace LLC	Myspace
60	Досие на ФТК № 092 3184 Преписка № C-4365	Относно Facebook, Inc.	Facebook
61	Досие на ФТК № 092 3081 Граждански иск № 09-CV-5276 (Окръжен съд, Централен окръг на Калифорния)	FTC срещу Javian Karnani и Balls of Kryptonite, LLC , търговско наименование Bite Size Deals, LLC, и Best Priced Brands, LLC	Balls of Kryptonite
62	Досие на ФТК № 102 3136 Преписка № C-4336	Относно Google, Inc.	Google
63	Досие на ФТК № 092 3137 Преписка № C-4282	Относно World Innovators, Inc.	World Innovators
64	Досие на ФТК № 092 3141 Преписка № C-4271	Относно Progressive Gaitways LLC	Progressive Gaitways
65	Досие на ФТК № 092 3139 Преписка № C-4270	Относно Onyx Graphics, Inc.	Onyx Graphics
66	Досие на ФТК № 092 3138 Преписка № C-4269	Относно ExpatEdge Partners, LLC	ExpatEdge
67	Досие на ФТК № 092 3140 Преписка № C-4281	Относно Directors Desk LLC	Directors Desk
68	Досие на ФТК № 092 3142 Преписка № C-4272	Относно Collectify LLC	Collectify

ПРИЛОЖЕНИЕ V

THE SECRETARY OF TRANSPORTATION
WASHINGTON, DC 20590

6 юли 2023 г.

Комисар Дидие Рейндерс
European Commission
Rue de la Loi/Wetstraat 200
1049 Brussels
Белгия

Уважаеми комисар Рейндерс,

Министерството на транспорта на Съединените щати („министерството“ или „МТ“) благодари за възможността да опише своята роля при прилагането на Принципите на Рамката за личните данни в отношенията между ЕС и САЩ („РЗЛД в отношенията между ЕС и САЩ“). РЗЛД в отношенията между ЕС и САЩ ще има решаваща роля за защитата на личните данни, които се предоставят при извършването на търговски сделки в един все по-взаимосвързан свят. Тя ще позволи на предприятията да осъществяват важни операции в глобалната икономика, като същевременно ще гарантира, че потребителите от ЕС ще продължат да се ползват от съществена защита на неприкосновеността на личния живот.

Преди повече от 22 години МТ за пръв път пое публично ангажимент да прилага Рамката за сфера на неприкосновеност на личния живот в писмо, изпратено до Европейската комисия — ангажименти, които бяха потвърдени отново и разширени в писмо от 2016 г. относно Рамката на Щита за личните данни в отношенията между ЕС и САЩ. В тези писма МТ се ангажира да прилага активно принципите на сферата на неприкосновеност на личния живот, а след това и Принципите на Щита за личните данни в отношенията между ЕС и САЩ. Ангажиментът на МТ обхваща и Принципите на РЗЛД в отношенията между ЕС и САЩ, а настоящото писмо означава този ангажимент.

По-специално МТ потвърждава ангажимента си да работи в следните основни области: 1) приоритетно разследване на предполагаеми нарушения на Принципите на РЗЛД в отношенията между ЕС и САЩ; 2) подходящи действия по принудително изпълнение срещу субекти, които правят неверни или измамни твърдения за участие в РЗЛД в отношенията между ЕС и САЩ; и 3) контрол по изпълнението и публично оповестяване на заповеди по принудително изпълнение във връзка с нарушения на Принципите на РЗЛД в отношенията между ЕС и САЩ. Предоставяме информацията относно всеки от тези ангажименти и в необходимия контекст — съответния минал опит във връзка с ролята на МТ за защита на неприкосновеността на личния живот на потребителите и прилагането на Принципите на РЗЛД в отношенията между ЕС и САЩ.

1. Контекст

A. Правомощия на МТ в областта на неприкосновеността на личния живот

Министерството е силно ангажирано с гарантирането на неприкосновеността на личния живот при предоставянето на информация от потребителите на въздушните превозвачи и билетните агенции.

МТ е упълномощено да предприема действия в тази област по силата на 49 U.S.C. 41712, с който се забранява на превозвач или билетна агенция всяка „нелоялна или измамна практика“ при въздушните транспортни услуги или при продажбата на въздушни транспортни услуги. Раздел 41712 е изработен по модела на раздел 5 от Закона за Федералната търговска комисия (ФТК) (15 U.S.C. 45).

Неотдавна МТ издаде наредби за определяне на нелоялните и измамните практики в съответствие с прецедентите на МТ и на ФТК (14 CFR § 399.79). По-конкретно под „нелоялна“ практика се разбира практика, която нанася или има вероятност да нанесе сериозни вреди, които при нормални обстоятелства не могат да бъдат избегнати и които не са компенсирани с предимства за потребителите или конкуренцията.

Под „измамна“ практика за потребителите се разбира практика, която има вероятност да заблуди потребител, който действа по разумен начин в дадените обстоятелства, по отношение на съществен въпрос. Даден въпрос е съществен, ако е вероятно да е повлиял на поведението или решението на потребителя по отношение на продукт или услуга. Освен тези общи принципи по-специално според тълкуването на МТ на член 41712 се забранява на превозвачите и билетните агенции: 1) да нарушават условията на своите политики в областта на неприкосновеността на личния живот; 2) да нарушават някой от изпълнителните актове, издадени от министерството, с който конкретни практики в областта на неприкосновеността на личния живот се определят като нелоялни или измамни; 3) да нарушават Закона за защита на неприкосновеността на личния живот на децата онлайн (СОРРА) или актовете на ФТК за изпълнение на СОРРА; или 4) в качеството им на участници в РЗЛД в отношенията между ЕС и САЩ да не спазват Принципите на РЗЛД в отношенията между ЕС и САЩ ⁽¹⁾.

Както бе посочено по-горе, съгласно федералното законодателство МТ има изключителни правомощия да регулира практиките на въздушните превозвачи в областта на неприкосновеността на личния живот и споделени правомощия с ФТК във връзка с практиките на билетните агенции в областта на неприкосновеността на личния живот при продажбата на въздушни транспортни услуги.

В тази си функция министерството може да използва законоустановените правомощия съгласно член 41712, за да гарантира спазването на Принципите на РЗЛД в отношенията между ЕС и САЩ, когато превозвач или продавач на въздушни транспортни услуги публично се е ангажирал да спазва тези Принципи. Следователно, когато даден пътник предостави информация на превозвач или билетна агенция, която е поела задължението да спазва Принципите на РЗЛД в отношенията между ЕС и САЩ, всяко едно нарушаване на това задължение от страна на превозвача или билетната агенция ще бъде нарушение на член 41712.

Б. Практики по принудително изпълнение

Службата за защита на потребителите в областта на авиацията (ОАСР) ⁽²⁾ към министерството разглежда делата и придвижва производствата в случаи по силата на 49 U.S.C. 41712. Тя предприема принудително изпълнение по законовата забрана съгласно член 41712 срещу нелоялни и измамни практики предимно чрез преговори и изготвяне на заповеди за преустановяване и прекратяване и за оценка на размера на гражданскоправни санкции. Службата получава информация за предполагаеми нарушения главно от жалби, подадени от физически лица, туристически агенции, въздушни превозвачи и правителствени органи на САЩ и други държави. Потребителите може да използват уебсайта на МТ да подават жалби във връзка с неприкосновеността на личния живот срещу въздушни превозвачи и билетни агенции ⁽³⁾.

Ако по дадено дело не бъде постигнато разумно и подходящо решение, ОАСР има правомощия да започне производство по принудително изпълнение с изслушване за събиране на доказателства пред съдия по административно право на министерството. Този съдия има правомощия да издава заповеди за преустановяване и прекратяване и за налагане на гражданскоправни санкции. Неспазването на разпоредбите на член 41712 може да доведе до издаването на заповеди за преустановяване и прекратяване и налагането на гражданскоправни санкции в размер до 37 377 USD за всяко нарушаване на разпоредбите на член 41712.

Министерството не е компетентно да отпуска обезщетения или парични компенсации на физическите лица жалбоподатели. То обаче има правомощието да одобрява споразумения, постигнати в резултат на разследвания, проведени от ОАСР, които предвиждат предоставянето директно на обезщетения на потребителите (например средства в брой, ваучери) като компенсация на паричните санкции, които иначе са дължими на правителството на САЩ. Има примери на такова уреждане в миналото, като то може да се използва и в контекста на Принципите на РЗЛД в отношенията между ЕС и САЩ, когато обстоятелствата го налагат. Повтарянето на нарушенията по член 41712 от страна на въздушен превозвач поставя под съмнение добрата воля на този превозвач по отношение на спазването на поетото задължение. В крайни случаи може да се реши, че той повече не отговаря на условията да извършва дейност и следователно да загуби лиценза си за упражняване на икономическа дейност.

Към днешна дата МТ е получило сравнително малко на брой жалби по обвинения за нарушаване от страна на билетни агенции или въздушни превозвачи на принципите на неприкосновеност на личния живот. Когато се получат такива, те се разглеждат съгласно изложените по-горе принципи.

В. Правни инструменти за защита, осигурявани от МТ, от които могат да се възползват потребителите от ЕС

Забраната срещу нелоялни или измамни практики при предоставянето или продажбата на въздушни транспортни услуги, предвидена съгласно член 41712, се прилага за въздушни превозвачи и билетни агенции от САЩ и от други държави. МТ често предприема действия срещу въздушни превозвачи от САЩ и от други държави за практики, които засягат едновременно чуждестранни и американски потребители, на основание на това, че практиките на този превозвач са се осъществили в процеса на предоставянето на въздушни транспортни услуги до или от Съединените щати. МТ прилага и ще продължи да прилага всички средства за правна защита, с които разполага, за да защитава едновременно чуждестранни и американски потребители от нелоялни или измамни практики във въздушните транспортни услуги от страна на субектите, които подлежат на регулиране.

⁽¹⁾ <https://www.transportation.gov/individuals/aviation-consumer-protection/privacy>.

⁽²⁾ Известна преди като Службата по принудително изпълнение и производства в областта на авиацията.

⁽³⁾ <http://www.transportation.gov/airconsumer/privacy-complaints>.

МТ прилага по отношение на въздушните превозвачи и други закони, които предвиждат защита за потребители извън САЩ, като например Закона за защита на неприкосновеността на личния живот на децата онлайн (COPPA). Наред с останалото в COPPA се поставя изискване към операторите на уебсайтове и онлайн услуги, предназначени за деца, или общодостъпни сайтове, които съзнателно събират лична информация от деца на възраст под 13 години, да уведомяват за това родителите и да изискват родителско съгласие, което може да се провери. Уебсайтовете и услугите, базирани в САЩ, за които се прилага COPPA и които събират лична информация от деца извън САЩ, са задължени да спазват този закон. Чуждестранните уебсайтове и онлайн услуги също са задължени да спазват COPPA, ако дейностите им са насочени към деца в Съединените щати или съзнателно събират лична информация от деца в Съединените щати. МТ е компетентно да предприема действия по принудително изпълнение за нарушаване на COPPA от страна на американски и чуждестранни въздушни превозвачи, доколкото те осъществяват дейността си в Съединените щати.

II. Принудително изпълнение във връзка с Принципите на РЗЛД в отношенията между ЕС и САЩ

Ако даден въздушен превозвач или билетна агенция избере да участва в РЗЛД в отношенията между ЕС и САЩ и в министерството бъде получена жалба срещу такъв субект по обвинение за нарушаване на Принципите на РЗЛД в отношенията между ЕС и САЩ, министерството ще предприеме следните действия за стриктното прилагане на Принципите на РЗЛД в отношенията между ЕС и САЩ.

A. Отдаване на приоритет на разследвания на обвинения за нарушаване

ОАСР към министерството ще разглежда всяка жалба по обвинение за нарушаване на

Принципите на РЗЛД в отношенията между ЕС и САЩ, включително жалби, получени от органите за защита на данните („ОЗД“) от ЕС, и ще предприема действия по принудително изпълнение, когато са налице доказателства за нарушение. Освен това ОАСР ще си сътрудничи с ФТК и с Министерството на търговията и ще отдава приоритет на обвинения срещу подлежащите на регулиране субекти в неспазване на ангажиментите за защита на неприкосновеността на личния живот, които те са поели като част от РЗЛД в отношенията между ЕС и САЩ.

Когато получи твърдения за нарушаване на Принципите на РЗЛД в отношенията между ЕС и САЩ, ОАСР може да предприеме редица действия като част от своето разследване. Например тя може да направи преглед на политиките в областта на неприкосновеността на личния живот на билетната агенция или въздушния превозвач, да получи допълнителна информация от тях или от трети страни, да осъществи последващ контрол съвместно със сезиращия субект и да направи оценка дали има модел на извършване на нарушенията или са засегнати значителен брой потребители. Освен това службата може да определи дали случаят засяга въпроси, които са от компетентността на Министерството на търговията или ФТК, да направи преценка дали ще е от полза да се проведе обучение на потребителите и на предприятията и ако е необходимо, да инициира производство по принудително изпълнение.

Ако министерството получи информация за евентуални нарушения на Принципите на РЗЛД в отношенията между ЕС и САЩ от страна на билетни агенции, то ще работи по случая в координация с ФТК. Също така ще информира ФТК и Министерството на търговията за резултатите от действията по принудително изпълнение съгласно Принципите на РЗЛД в отношенията между ЕС и САЩ.

B. Предприемане на действия по неверни или измамни твърдения за участие

Министерството остава ангажирано да провежда разследвания за нарушения на Принципите на РЗЛД в отношенията между ЕС и САЩ, включително за неверни или измамни твърдения за участие в РЗЛД в отношенията между ЕС и САЩ. Ние ще разглеждаме с предимство случаите, по които сме сезирани от Министерството на търговията във връзка с организации, за които е определено, че погрешно твърдят, че участват в РЗЛД в отношенията между ЕС и САЩ, или използват сертификационния знак на РЗЛД в отношенията между ЕС и САЩ без разрешение.

Освен това трябва да отбележим, че ако в политиката в областта на неприкосновеността на личния живот на една организация се твърди, че тя спазва Принципите на РЗЛД в отношенията между ЕС и САЩ, и тя не се самосертифицира или не повтаря самосертифицирането си в Министерството на търговията, това само по себе си вероятно няма да е причина МТ да не предприеме действия по принудително изпълнение на тези ангажименти по отношение на тази организация.

B. Контрол по изпълнението и публично оповестяване на заповеди по принудително изпълнение във връзка с нарушения на РЗЛД

ОАСР към министерството ще продължава да спазва също и ангажимента за контрол по заповедите за принудително изпълнение според необходимостта, за да гарантира спазването на Принципите на РЗЛД в отношенията между ЕС и САЩ. По-специално, когато службата издаде заповед, с която указва на въздушен превозвач или билетна агенция да преустанови и прекрати бъдещи нарушения на Принципите на РЗЛД в отношенията между ЕС и САЩ и на член 41712, тя ще упражнява контрол върху спазването от страна на субекта на разпоредбата за преустановяване и прекратяване на нарушения, включена в заповедта. Освен това службата ще следи за публикуването в своя уебсайт на заповедите, издадени по дела във връзка с Принципите на РЗЛД в отношенията между ЕС и САЩ.

Очакваме с нетърпение да продължим да работим съвместно с нашите федерални партньори и заинтересованите страни от ЕС по въпроси във връзка с РЗЛД в отношенията между ЕС и САЩ.

Надявам се тази информация да е полезна. Ако имате въпроси или се нуждаете от допълнителна информация, не се колебайте да се свържете с мен.

С уважение,



Pete Buttigieg

ПРИЛОЖЕНИЕ VI



Министерство на правосъдието на САЩ

Наказателен отдел

Кабинет на помощник главния прокурор

Washington, D.C. 20530

23 юни 2023 г.

Г-жа Ана Гайего Торес
Генерален директор на ГД „Правосъдие и потребители“
European Commission
Rue Montoyer/Montoyerstraat 59
1049 Brussels
Белгия

Уважаема г-жо генерален директор Гайего Торес,

В настоящото писмо е направен кратък преглед на основните средства за разследване, използвани за получаването на търговска информация и други справочни данни от дружествата в Съединените щати за целите на правоприлагането в наказателната сфера или в сферата на обществените интереси (гражданскоправната и регулаторната сфера), включително ограниченията за достъпа, определени в тези законови разпоредби ⁽¹⁾. Всички процеси на призоваване, разгледани в настоящото писмо, са недискриминационни, тъй като се прилагат за получаване на информация от дружествата в Съединените щати, включително такива, които ще се самосертифицират съгласно Рамката за личните данни в отношенията между ЕС и САЩ, независимо от гражданството или местопребиваването на субекта на данните. Освен това дружествата, които са призовани по този начин в Съединените щати, може да обжалват това в съда, както ще бъде разгледано по-нататък ⁽²⁾.

От специално значение за изземването на информация от страна на публичните органи е четвъртата поправка в Конституцията на Съединените щати, в която се предвижда, че „правото на хората на лична сигурност, сигурност на дома, документите и действията им, срещу извършване на неоснователни обиски и изземвания, не трябва да бъде нарушавано и не трябва да бъдат издавани заповеди за такива действия, освен когато е налице правдоподобна причина и издаването става под клетва или с официална декларация, с точно описание на мястото на обиска и лицата или вещите, които подлежат на изземване“, Конституция на САЩ, IVта поправка. IV. Както постанови Върховният съд на Съединените щати по делото *Berger* с/у щата Ню Йорк, „основната цел на тази поправка, както това се признава в множество решения на този съд, е да бъдат защитени неприкосновеността на личния живот и сигурността на физическите лица срещу произволни посегателства на длъжностни лица на правителството“. 388 U.S. 41, 53 (1967) (цитирано в *Самага* с/у Районен съд на Сан Франциско, 387 U.S. 523, 528 (1967 г.)) За националните наказателни разследвания в Четвъртата поправка се поставя общо изискване към длъжностните лица в правоприлагането да получат заповед по съдебно разпореждане, преди да извършат обиск. Вж. *Katz* срещу Съединените щати, 389 U.S. 347, 357 (1967 г.). За заповедите за физическо претърсване и изземване, както

⁽¹⁾ В този преглед не се разглеждат инструментите за разследвания в националната сигурност, които се използват при правоприлагането в областта на тероризма и други разследвания в националната сигурност, включително писмата във връзка с националната сигурност за някои видове справочна информация в справки за кредити, финансова информация и електронни регистри за абонати и трансакции, вж. 12 U.S.C. § 3414; 15 U.S.C. § 1681u; 15 U.S.C. § 1681v; 18 U.S.C. § 2709, 50 U.S.C. § 3162, и за електронно наблюдение, заповеди за обиск, търговски регистри и друг вид събиране на информация съгласно Закона за упражняване на надзор върху външното разузнаване, вж. 50 U.S.C. § 1801 и следв.

⁽²⁾ Настоящото писмо се отнася за федералното правоприлагане и федералните регулаторни режими. Нарушения на щатското право се разследват от щатските правоприлагащи органи и делата по тях се водят в щатските съдилища. Щатските правоприлагащи органи използват заповеди и призовки, издадени съгласно щатското право, което по същество се извършва по същия ред, както това е разгледано в настоящия документ, но е възможно за процеса на призоваване в щатите да се прилагат защити, предвидени в щатските конституции, които са с по-висока степен от предвидените в Конституцията на САЩ. Защитите съгласно щатското право трябва да са най-малкото равни по степен на предвидените в Конституцията на САЩ, включително, но не само в Четвъртата поправка.

и за заповедите за съхраняване съдържание на електронни съобщения, издадени по реда на Закона за съхраняването на съобщения, както е разгледано по-долу, се прилагат стандартите за издаване на заповед, като например изискванията за обосновано предположение и за конкретност. Когато изискването за заповед не се прилага, действията на правителството все пак подлежат на проверка за „основателност“ съгласно Четвъртата поправка. Следователно в самата Конституция е гарантирано, че правителството на САЩ няма неограничени или произволни права да изземва поверителна информация ⁽³⁾.

Правомощия в наказателното правоприлагане:

Федералните прокурори, които са служители на Министерството на правосъдието (МП), и федералните следователи, включително във Федералното бюро за разследвания (ФБР), което е правоприлагаща служба в рамките на МП, могат да задължат дружества в Съединените щати да им предоставят документи и друга регистрирана информация за целите на наказателни разследвания чрез няколко вида процеси за задължително призоваване, включително призовки на „голямото жури“, административни разпореждания и заповеди за обиск, и могат да придобиват друг вид съобщителна информация съгласно правомощията си за подслушване и използване на устройства за регистриране за целите на федерални наказателни разследвания.

Призовки на „голямото жури“ или по конкретен съдебен процес: Призовките в наказателното правосъдие се използват за оказване на съдействие по конкретни разследвания в правоприлагането. Призовката на „голямото жури“ е официално искане, издадено от „голямото жури“ (обикновено по искане на федерален прокурор) за съдействие по разследване на „голямото жури“ по конкретно предполагаемо нарушение на наказателното право. „Голямото жури“ е разследващо поделение на съда, което се свиква от съдия или магистрат. С призовката може да се изиска от дадено лице да даде свидетелски показания по съдебен процес или да извлече или предостави на разположение търговска информация, данни, съхранени по електронен път, или други материали. Информацията трябва да е от значение за целите на разследването и призовката не може да е неоснователна поради прекалено широко формулиране или понеже е с репресивен или обременяващ характер. Получателят може да подаде предложение за оспорване в съда на призовка на тези основания. Вж. Федерален регистър наказ. дела 17. В ограничени случаи могат да бъдат издавани призовки за документи по конкретен процес, след като „голямото жури“ повдигне обвинение по делото.

Правомощия за административни разпореждания: Правомощията за издаване на административни разпореждания могат да бъдат упражнявани в наказателноправни или гражданскоправни разследвания. В контекста на наказателното правоприлагане няколко федерални закона дават правомощия за използването на административни разпореждания за извличане или предоставяне на разположение на търговска информация, данни, съхранени по електронен път, или други материали от значение за разследвания за измами в здравеопазването, малтретиране на деца, защита на тайните служби, по дела за контролирани вещества и в разследвания на главни инспектори, в които са въвлечени правителствени институции. Ако правителството предприеме принудително изпълнение в съда на административно разпореждане, получателят на това разпореждане, подобно на получателя на призовка на „голямото жури“, може да оспори неговата основателност поради прекалено широко формулиране или репресивен или обременяващ характер.

Съдебни разпореждания за устройства за регистриране и проследяване: Съгласно разпоредбите за устройствата за регистриране и проследяване в наказателни разследвания правоприлагащите органи могат да получат съдебно разпореждане за придобиване в реално време на информация, която не се отнася за съдържание, във връзка с набиране, направление, адресиране и радиоелектронна информация относно даден телефонен номер или електронна поща, след като удостоверят, че предоставената информация е от значение за провеждащо се наказателно разследване. Вж. 18 U.S.C. §§ 3121—3127. Неправомерното използване или монтиране на такива устройства е престъпление по федералните закони.

Закон за неприкосновеност на електронните съобщения (ЕСРА): Достъпът на правителството до информация за абонати, данни за трафика и съхранено съдържание на разговори и съобщения, с които разполагат доставчиците на интернет услуги, телефонните дружества и други доставчици на услуги от трети страни, се урежда от допълнителни правила съгласно дял II от ЕСРА, който се нарича също Закон за съхраняването на съобщения (SCA), 18 U.S.C. §§ 2701—2712. С този закон се определя система от законоустановени права на неприкосновеност на личния живот, с които се ограничава достъпът за целите на правоприлагането до данни за клиенти и абонати на доставчици на интернет услуги, който надхвърля изискванията съгласно конституционното право. С SCA се предвижда повишаване на нивото на защита на неприкосновеността на личния живот в зависимост от степента на намеса при събирането на информацията. За целите на наказателното правоприлагане органите са задължени да получат разпореждане, за да се добиет с информация за регистрация на абонати,

⁽³⁾ Що се отнася до принципите на Четвъртата поправка относно защитата на неприкосновеността на личния живот и сигурността, които са разгледани по-горе, съдилищата в САЩ редовно прилагат тези принципи спрямо новите видове инструменти за разследвания при правоприлагането, които са достъпни благодарение на развитието на технологиите. Например през 2018 г. Върховният съд постанови, че придобиването от страна на правителството на историческа информация за местоположението на мобилен телефон чрез комуникацията му с базова станция от дружество за предоставяне на услуги за мобилни телефони за продължителен период от време в рамките на разследване при правоприлагането представлява „обиск“, който подлежи на изискването за заповед съгласно Четвъртата поправка. *Carpen ter* срещу Съединените щати, 138 S. Ct. 2206 (2018).

адреси на интернет протокола (IP) и съответните удостоверения за време, както и информация за заплащането. За повечето други видове съхранена информация, която не се отнася за съдържание, като например заглавен ред на електронни съобщения без реда „Относно“, правораздавателните органи задължително трябва да представят пред съдия конкретни факти в доказателство, че исканата информация е от значение и се отнася по същество за провеждащо се наказателно разследване. За да се съобщи със съхраненото съдържание на електронни съобщения, обикновено органите в наказателното право прилагане трябва да получат разпореждане от съдия на основание обосновано предположение, поради което се счита, че въпросният профил съдържа доказателства за извършено престъпление. В SCA се предвиждат също така гражданскоправни и наказателни санкции ⁽⁴⁾.

Съдебни разпореждания за наблюдение съгласно Федералния закон за подслушванията: В допълнение правоприлагащите органи могат да подслушват в реално време кабелни, устни или електронни съобщения за целите на наказателни разследвания съгласно Федералния закон за подслушванията. Вж. 18 U.S.C. §§ 2510—2523. Това правомощие се дава само със съдебно разпореждане, в което наред с останалото се съдържат констатации на съдия, че е налице обосновано предположение да се счита, че подслушването или прихващането по електронен път ще даде доказателства за престъпление срещу федералните закони или информация за местонахождението на лице, укриващо се с цел избягване на наказателно преследване. Законът предвижда гражданскоправни и наказателни санкции за нарушения на разпоредбите за подслушване.

Заповед за обиск — правило 41 от Федералния наказателнопроцесуален кодекс: Правоприлагащите органи могат да извършват физическо претърсване на помещения в Съединените щати, когато им е дадено разрешение за това от съдия. Те трябва да докажат пред съдията въз основа на явно обосновано предположение, че е било извършено или предстои да бъде извършено престъпление и че има вероятност на мястото, посочено в заповедта, да бъдат намерени вещи, свързани с престъплението. Това правомощие често се използва, когато е необходимо да се извърши физическо претърсване на помещения от полицията, поради опасност от унищожаване на доказателствата, ако на дружеството бъде връчена призовка или друго процесуално разпореждане. Физическо лице, което е обект на претърсване или чието имущество е обект на претърсване, може да предприеме действия за спиране разглеждането на доказателства, получени чрез неправомерен обиск, ако тези доказателства са представени срещу това физическо лице по време на наказателно производство. Вж. *Марп срещу Охайо*, 367 U.S. 643 (1961 г.). Когато от притежател на данни се изисква да разкрие данни съгласно заповед, задължената страна може да оспори изискването за разкриване като неоправдано обременително. Вж. *In re Application of United States*, 610 F.2d 1148, 1157 (3d Cir. 1979) (в което се постановява, че „надлежното провеждане на съдебния процес изисква изслушване по въпроса за тежестта, преди да се принуди телефонното дружество да предостави“ съдействие за издаване на заповед за обиск); *In re Application of United States*, 616 F.2d 1122 (9th Cir. 1980) (в което се стига до същото заключение въз основа на надзорните правомощия на съда).

Насоки и политики на МП: В допълнение към тези основани на Конституцията, законите и правилата ограничения за достъпа от страна на правителството до данни главният прокурор издаде насоки, с които се определят допълнителни ограничения за достъпа до данни за целите на правоприлагането и в които се съдържат също и защити за неприкосновеността на личния живот и гражданските свободи. Например в насоките на главния прокурор за национални оперативни дейности на ФБР от септември 2008 г. (наричани по-нататък „насоки за ФБР от ГП“), които са достъпни на адрес: <http://www.justice.gov/archive/opa/docs/guidelines.pdf>, се определят ограничения за използването на разузнавателни средства за набиране на информация във връзка с разследвания по престъпления срещу федералните закони. В тези насоки се поставя изискване към ФБР да използва методи на разследване, които са с най-ниската практически възможна степен на вмешателство, отчитайки последиците за неприкосновеността на личния живот и гражданските свободи и евентуалното уронване на доброто име. Освен това в тях се отбелязва, че „е задължително ФБР да провежда разследванията и другите си дейности по законосъобразен и разумен начин при уважаване на свободата и неприкосновеността на личния живот и избягване на ненужно вмешателство в живота на лица, които спазват законите“. Насоки за ФБР от ГП на стр. 5. ФБР е привело в изпълнение тези насоки чрез Ръководство за национални оперативни дейности и разследвания (DIOG) на ФБР, което е достъпно на адрес: <https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29> и представлява изчерпателен наръчник, в който са включени подробно разгледани ограничения за използването на средства за разследване и насоки за гарантиране на защитата на гражданските свободи и неприкосновеността на личния живот във всяко разследване. Допълнителни правила и политики, с които се предвиждат ограничения за разследващите дейности на федералните прокурори, са определени в Наръчника по правораздаване, който е достъпен онлайн на адрес: <https://www.justice.gov/jm/justice-manual>.

Гражданскоправни и регулаторни правомощия (обществен интерес):

⁽⁴⁾ Освен това съгласно член 2705(b) от SCA се дава разрешение правителството да получи съдебно разпореждане въз основа на доказана необходимост от защита от разкриване, с което се забранява на доставчик на комуникационни услуги доброволно да уведомява своите потребители за призоваването по SCA. През октомври 2017 г. заместник-главният прокурор Rod Rosenstein издаде меморандум до прокурорите и представителите на МП, в който се дават насоки, за да се гарантира, че молбите за такива обезпечителни заповеди са съобразени с конкретните факти и опасения, свързани с дадено разследване, и се установява общ едногодишен таван на срока, за който може да се иска отлагане на уведомяването в молбата. През май 2022 г. заместник-главният прокурор Lisa Monago издаде допълнителни насоки по темата, в които, наред с други въпроси се установяват вътрешни изисквания за одобрение на МП за молби за удължаване на срока на обезпечителната заповед след първоначалния едногодишен срок и се изисква прекратяване на обезпечителните заповеди след приключване на разследването.

Съществуват и значителни ограничения за достъпа до данни, с които разполагат дружествата в Съединените щати, за целите на гражданскоправното и регулаторното правоприлагане (т.е. правоприлагане в „обществен интерес“). Институциите, които имат гражданскоправни и регулаторни отговорности, могат да издават разпореждания за дружествата във връзка с търговска информация, данни, съхранени по електронен път, или други материали. Тези институции са ограничени при упражняването на правомощията си за издаване на административни или гражданскоправни разпореждания не само съгласно законите, с които се урежда статутът им, но и чрез независимия съдебен контрол на разпорежданията преди евентуалното принудително изпълнение по съдебен ред. Вж. напр. Федерален регистър гражд. дела 45. Институциите могат да искат достъп само до данни, които са от значение за въпросите в обхвата на техните регулаторни правомощия. Освен това получател на административно разпореждане може да оспори изпълнението му в съда, като представи доказателства, че институцията не е действала съобразно с основните изисквания за основателност, както това беше разгледано по-горе.

Съществуват и други правни основания за оспорване от страна на дружествата на искания за информация от административни институции според конкретния отрасъл и вида на данните, с които разполагат. Например финансовите институции могат да оспорят административни разпореждания, с които се изисква конкретен вид информация в нарушение на Закона за банковата тайна и подзаконовите разпоредби за прилагането му. 31 U.S.C. § 5318; 31 C.F.R. глава X. Други предприятия могат да се основат на Закона за оповестяване на информация за кредити, 15 U.S.C. § 1681b, или множество други закони, специфични за конкретния сектор. Злоупотребата с правото за издаване на разпореждане от страна на дадена институция може да доведе до подвеждане под отговорност на институцията или на нейни служители за причинени вреди. Вж. например Закона за правото на неприкосновеност на личните финанси, 12 U.S.C. §§ 3401—3423. По този начин съдилищата в Съединените щати са в ролята на защитник срещу неправомерни регулаторни искания и осигуряват независим надзор на действията на федералните институции.

И накрая, всяко законоустановено правомощие на административните органи да извършват физическо изземване на информация от дружество в Съединените щати по силата на административно разпореждане за обиск трябва да е съобразено с изискванията въз основа на Четвъртата поправка. Вж. *See* срещу град Сиатъл, 387 U.S. 541 (1967 г.).

Заклучение:

Всички правоприлагащи и регулаторни дейности в Съединените щати трябва да са съобразени с приложимото законодателство, включително с Конституцията на САЩ, законите, правилата и подзаконовите разпоредби. Тези дейности трябва да са съобразени също и с приложимите политики, включително с насоките на главния прокурор, от които се ръководят дейностите във федералното правоприлагане. Разгледаната по-горе правна уредба ограничава възможността за правоприлагащите и регулаторните органи на САЩ да получават информация от дружества в Съединените щати независимо дали тя се отнася за граждани на САЩ или на други държави и в допълнение към това позволява да се осъществява съдебен контрол на всяко искане за данни от страна на правителството съгласно тези правомощия.



Bruce C. Swartz
Deputy Assistant Attorney General and
Counselor for International Affairs

ПРИЛОЖЕНИЕ VII

СЛУЖБА НА ДИРЕКТОРА НА НАЦИОНАЛНОТО РАЗУЗНАВАНЕ СЛУЖБА НА ГЛАВНИЯ
ЮРИСКОНСУЛТ

WASHINGTON, DC 20511

9 декември 2022 г.

Leslie B. Kiernan
Главен юрисконсулт
U.S. Department of
Commerce 1401 Constitution
Ave., NW Washington, DC 20230

Уважаема г-жо Kiernan,

На 7 октомври 2022 г. президентът Байдън подписа Указ 14086, *Enhancing Safeguards for United States Signals Intelligence Activities* [Засилване на гаранциите за дейностите на САЩ за радиоелектронно разузнаване], който укрепва строгия набор от гаранции за неприкосновеността на личния живот и гражданските свободи, които се прилагат по отношение на дейностите на САЩ за радиоелектронно разузнаване. Тези гаранции включват: изискване дейностите за радиоелектронно разузнаване да отговарят на изброени законни цели; изрично изключване на такива дейности за постигане на конкретни забранени цели; въвеждане на нови процедури, с които да се гарантира, че дейностите за радиоелектронно разузнаване допринасят за постигането на тези законни цели и не спомагат за постигането на забранени цели; изискване дейностите за радиоелектронно разузнаване да се извършват само след като въз основа на разумна оценка на всички съответни фактори бъде установено, че дейностите са необходими за постигане на напредък по утвърден приоритет на разузнаването, и само до степен и по начин, които са пропорционални на утвърдения приоритет на разузнаването, за който са били разрешени; и указване на разузнавателните структури да актуализират своите политики и процедури, за да включват изискваните съгласно изпълнителния указ гаранции за радиоелектронното разузнаване. Най-важното е, че с изпълнителния указ се въвежда също независим и обвързващ механизъм, който дава възможност на лица от „отговарящи на условията щати“, определени съгласно указа, да търсят правна защита, ако смятат, че са били обект на незаконни дейности на САЩ за радиоелектронно разузнаване, включително дейности, нарушаващи защитата, предвидена в изпълнителния указ.

Издаването на Указ 14086 от президента Байдън бележи кулминацията на продължилите повече от година подробни преговори между представители на Европейската комисия (ЕК) и Съединените щати и определя стъпките, които САЩ ще предприемат за изпълнение на ангажиментите си съгласно Рамката за личните данни в отношенията между ЕС и САЩ. В унисон с духа на сътрудничество, който доведе до създаването на рамката, разбирам, че сте получили два набора от въпроси от ЕК относно начина, по който разузнавателните структури ще прилагат изпълнителния указ. Имам удоволствието да отговоря на тези въпроси с настоящото писмо.

Раздел 702 от Закона за упражняване на надзор върху външното разузнаване от 1978 г. (член 702 от ЗУНВР)

Първият набор от въпроси се отнася до член 702 от ЗУНВР, с който се разрешава придобиването на външно разузнавателна информация чрез целево събиране от лица, които не са граждани на САЩ и са с местонахождение извън Съединените щати, при задължително съдействие от страна на доставчиците на електронни далекосъобщителни услуги. По-конкретно въпросите се отнасят до взаимодействието между тази разпоредба и Указ 14086, както и другите гаранции, които се прилагат за дейностите, извършвани съгласно член 702 от ЗУНВР.

Като начало можем да потвърдим, че разузнавателните структури ще прилагат гаранциите, предвидени в Указ 14086, по отношение на дейностите, извършвани съгласно член 702 от ЗУНВР.

Освен това при използването от страна на правителството на член 702 от ЗУНВР се прилагат редица други гаранции. Например всички сертифицирани по член 702 от ЗУНВР трябва да бъдат подписани както от главния прокурор, така и от директора на Националното разузнаване, а правителството трябва да представи всички тези сертифицирани за одобрение от Съда по надзора върху външното разузнаване (СНВР), който е съставен от независими пожизнени съдии, които изпълняват седемгодишни мандати без право на подновяване. В сертифицираните се определят какви категории външноразузнавателна информация, която трябва да отговаря на законоустановеното определение за външноразузнавателна информация, ще се събира чрез целенасочени действия спрямо лица, които не са граждани на САЩ и са с местонахождение извън Съединените щати. Сертифицираните включват информация относно международния тероризъм и други теми, като например придобиването на информация относно оръжия за масово унищожение. Всяко годишно сертифициране трябва да бъде представено на СНВР за одобрение в пакет от заявление за сертифициране, който включва сертифицираните на главния прокурор и на директора на Националното разузнаване, клетвените декларации на някои ръководители на разузнавателни агенции, както и процедурите за целево събиране, процедурите за свеждане до минимум и процедурите за търсене, които са задължителни за правителството. Процедурите за целево събиране налагат наред с другото разузнавателните структури да направят обоснована оценка въз основа на всички обстоятелства дали има вероятност целевото събиране да доведе до придобиване на външноразузнавателна информация, посочена в сертифициране по член 702 от ЗУНВР.

Освен това, когато събират информация съгласно член 702 от ЗУНВР, разузнавателните структури трябва: да предоставят писмено обяснение на основанията за своята оценка към момента на целевото събиране, че се очаква обектът на разузнаване да притежава, да получи или да има вероятност да съобщи външноразузнавателна информация, посочена в сертифициране по член 702 от ЗУНВР; да потвърдят, че изискванията за целево събиране, посочени в процедурите за целево събиране съгласно член 702 от ЗУНВР, продължават да се спазват; и да прекратят събирането, ако изискванията вече не се спазват. Вж. U.S. Government Submission to Foreign Intelligence Surveillance Court, 2015 Summary of Notable Section 702 Requirements [Становище на правителството на САЩ до Съда по надзора върху външното разузнаване], *обобщение от 2015 г. във връзка с изискванията по член 702*, стр. 2—3 (15 юли 2015 г.).

Изискването разузнавателните структури да документират писмено и редовно да потвърждават валидността на своята оценка, че обектите на разузнаване по член 702 от ЗУНВР отговарят на приложимите стандарти за целево събиране, улеснява надзора на СНВР върху дейностите за целево събиране на разузнавателните структури. Всяка документирана оценка и обосновка на целево събиране се преглежда на всеки два месеца от прокурори по надзор на разузнаването в Министерството на правосъдието (МП), които изпълняват тази надзорна функция независимо от операциите на външното разузнаване. След това отделът на МП, изпълняващ тази функция, носи отговорност съгласно отдавна установено правило на СНВР да му докладва за всички нарушения на приложимите процедури. Това докладване заедно с редовните срещи между СНВР и този отдел на МП относно надзора на целевото събиране съгласно член 702 от ЗУНВР дава възможност на СНВР да наложи спазването на процедурите за целево събиране и други процедури съгласно член 702 от ЗУНВР и да гарантира по друг начин, че дейностите на правителството са законосъобразни. По-специално СНВР може да направи това по няколко начина, включително чрез постановяване на обвързващи коригиращи решения за прекратяване на правомощията на правителството да събира данни за конкретен обект на разузнаване или за изменение или забавяне на събирането на данни съгласно член 702 от ЗУНВР. СНВР може също така да изиска от правителството да предостави допълнителни доклади или информация относно спазването на процедурите за целево събиране и други процедури или да изиска промени в тези процедури.

Събирането на „масиви“ от информация от радиоелектронното разузнаване

Вторият набор от въпроси се отнася до събирането на „масиви“ от информация от радиоелектронното разузнаване, което се определя в Указ 14086 като „разрешеното събиране на големи количества данни от радиоелектронното разузнаване, които поради технически или оперативни съображения са придобити без използване на разграничителни критерии (например без използване на конкретни идентификатори или критерии за избор).“

По отношение на тези въпроси първо отбелязваме, че нито съгласно ЗУНВР, нито съгласно писмата във връзка с националната сигурност се разрешава събирането на масиви от данни. По отношение на ЗУНВР:

- В дялове I и III от ЗУНВР, в които се разрешават съответно електронното наблюдение и физическото претърсване, се изисква съдебно разпореждане (с ограничени изключения, като например при извънредни обстоятелства) и винаги се изисква обосновано предположение в уверение на това, че обектът на разузнаване е чужда сила или агент на чужда сила. Вж. 50 U.S.C. §§ 1805, 1824.
- Със Закона за свободата в САЩ от 2015 г. беше изменен дял IV от ЗУНВР, в който се разрешава използването на електронни устройства за регистриране и проследяване съгласно съдебно разпореждане (освен при извънредни обстоятелства), по такъв начин, че да се изисква от правителството да основава исканията си на „конкретен критерий за избор“. Вж. 50 U.S.C. § 1842(c)(3).

- В дял V от ЗУНВР, в който се разрешава на Федералното бюро за разследвания (ФБР) да получава определени видове търговска информация, се изисква издадено съдебно разпореждане въз основа на молба, в която се посочва, че „съществуват конкретни и доказуеми факти, които дават основание да се смята, че лицето, за което се отнася информацията, е чужда сила или агент на чужда сила.“ Вж. 50 U.S.C. § 1862(b)(2)(B). Вж. 50 U.S.C. § 1862(b)(2)(B) ⁽¹⁾.
- И накрая, съгласно член 702 от ЗУНВР се разрешава „за обект на разследване да се определят лица, за които има разумни основания да се счита, че се намират извън територията на Съединените щати, с цел събиране на външно Разузнавателна информация.“ Вж. 50 U.S.C. § 1881a. По този начин, както отбелязва Надзорният съвет по въпросите на неприкосновеността на личния живот и гражданските свободи, събирането на данни от страна на правителството съгласно член 702 от ЗУНВР „се изразява изцяло в целенасочено разследване на отделни лица и събиране на данни за съобщения, свързани с тези лица, от които правителството има основание да очаква, че ще получи определени видове външно Разузнавателна информация, така че „програмата не функционира чрез събиране на масиви от данни за съобщения.“ Надзорен съвет по въпросите на неприкосновеността на личния живот и гражданските свободи, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* [Доклад относно програмата за разузнаване, функционираща съгласно член 702 от Закона за упражняване на надзор върху външното разузнаване], стр. 103 (2 юли 2014 г.) ⁽²⁾.

Що се отнася до писмата във връзка с националната сигурност, съгласно Закона за свободата в САЩ от 2015 г. се налага изискване за „конкретен критерий за избор“ при използването на такива писма. Вж. 12 U.S.C. § 3414(a)(2); 15 U.S.C. § 1681u; 15 U.S.C. § 1681v(a); 18 U.S.C. § 2709(b).

Освен това в Указ 14086 се предвижда, че „се отдава приоритет на целевото събиране“ и че когато разузнавателните структури извършват събиране на масиви от данни, „събирането на масиви от радиоелектронна разузнавателна информация се разрешава само въз основа на констатация ... че информацията, необходима за постигане на напредък по утвърден приоритет на разузнаването, не може да бъде разумно придобита чрез целево събиране.“ Вж. Указ 14086, § 2(c)(ii)(A).

Освен това, когато разузнавателните структури установят, че събирането на масиви от данни отговаря на тези стандарти, Указ 14086 осигурява допълнителни гаранции. По-конкретно съгласно изпълнителния указ се изисква от разузнавателните структури, когато извършват събиране на масиви от данни, да „прилагат разумни методи и технически мерки, за да се ограничи събирането на данни само до това, което е необходимо за постигане на напредък по утвърден приоритет на разузнаването, като същевременно се сведе до минимум събирането на информация, която не е от значение.“ В указа също така се посочва, че „дейностите за радиоелектронно разузнаване,“ които включват търсене в радиоелектронна разузнавателна информация, получена чрез събиране на масиви от данни, „се извършват само след като въз основа на разумна оценка на всички съответни фактори бъде установено, че дейностите са необходими за постигане на напредък по утвърден приоритет на разузнаването.“ Вж. *пак там* § 2(a)(ii)(A). Освен това указът способства за прилагането на този принцип, като в него се посочва, че разузнавателните структури може да извършват търсения в необработена радиоелектронна разузнавателна информация, получена чрез събиране на масиви от данни, само за постигането на шест допустими цели и че тези търсения трябва да се извършват в съответствие с политики и процедури, които „отчитат по подходящ начин въздействието [на търсенията] върху неприкосновеността на личния живот и гражданските свободи на всички лица независимо от тяхната националност или място на пребиваване.“ Вж. *пак там* § 2(c)(iii)(D). И накрая, указът предвижда контрол на обработката, сигурността и достъпа до събраните данни. Вж. *пак там* § 2(c)(iii)(A) и § 2(c)(iii)(B).

* * * * *

Надяваме се тези разяснения да бъдат от полза. Не се колебайте да се свържете с нас, ако имате допълнителни въпроси относно начина, по който разузнавателните структури на САЩ планират да приложат Указ 14086.

⁽¹⁾ От 2001 г. до 2020 г. в дял V от ЗУНВР се позволяваше на ФБР да иска разрешение от СНВР за получаване на „материални вещи“, които са от значение за някои разрешени разследвания. Вж. Закона за обединяване и укрепване на САЩ, Pub. L. No. 107-56, 115 Stat. 272, § 215 (2001). Тази формулировка, чийто срок на действие е изтекъл и следователно вече не е закон, осигуряваше правомощието, съгласно което правителството събираше в определен момент масиви от метаданни за телефония. Още преди изтичането на срока на действие на разпоредбата обаче тя беше изменена със Закона за свободата в САЩ така, че да се изисква от правителството да основава молбите си до СНВР на „конкретен критерий за избор“. Вж. Закона за свободата в САЩ, Pub. L. No. 114-23, 129 Stat. 268, § 03 (2015).

⁽²⁾ В членове 703 и 704, в които се разрешава на разузнавателните структури да предприемат целево събиране на данни за лица от САЩ, намиращи се в чужбина, се изисква съдебно разпореждане (освен при извънредни обстоятелства) и винаги се изисква обосновано предположение в уверение на това, че обектът на разузнаване е чужда сила, агент на чужда сила или длъжностно лице или служител на чужда сила. Вж. 50 U.S.C. §§ 1881b, 1881c.

Sincerely,

A handwritten signature in black ink, appearing to read 'C. FONZONE', followed by a horizontal line extending to the right and ending at a vertical line.

Christopher C. FONZONE
Главен юрисконсулт

ПРИЛОЖЕНИЕ VIII

Списък на съкращенията

В настоящото решение се съдържат следните съкращения:

AAA	Американска арбитражна асоциация
Правило на IKE на ООН	Регламент на главния прокурор относно Съда за преглед на защитата на данните
AGG-DOM	Насоки на главния прокурор за вътрешни операции на ФБР
APA	Закон за административното производство
ЦРУ	Централно разузнавателно управление
CNSS	Комитет по националните системи за сигурност
Съд	Съд на Европейския съюз
Решение	Решение за изпълнение на Комисията съгласно Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета относно адекватното ниво на защита на личните данни в Рамката за защита на личните данни в отношенията между ЕС и САЩ
DHS	Министерство на вътрешната сигурност
DNI	Директор на Националното разузнаване
DoC	Министерство на търговията на САЩ
DoJ	Министерство на правосъдието на САЩ
DoT	Министерство на търговията на САЩ
ОЗД	Орган за защита на данните
Списък на РЛД	Списък по рамката за защита на личните данни между ЕС и САЩ
DPRC	Апелативен съд по въпросите на защитата на личните данни
Европейска сметна палата	Закон за равните възможности за кредитиране
ЗНЕС	Законът за неприкосновеност на електронните съобщения
ЕИП	Европейско икономическо пространство
Указ 12333	Указ 12333 „Разузнавателни дейности на Съединените щати“
Указ 14086	Указ 14086 „Засилване на гаранциите за дейностите на САЩ за радиоелектронно разузнаване“
РЛД в отношенията между ЕС и САЩ или РЛД	Рамка за личните данни в отношенията между ЕС и САЩ
Панел по РЛД между ЕС и САЩ	Панел по рамката за защита на личните данни между ЕС и САЩ
ФБР	Федерално бюро за разследване
FCRA	Закона за оповестяване на информация за кредити
FISA	Закона за упражняване на надзор върху външното разузнаване
FISC	Съд за надзор на външното разузнаване
FISCR	Апелативен съд за надзор на външното разузнаване
FOIA	Закон за свобода на информацията
FRA	Закон за федералните архиви

ФТК	Федералната търговска комисия
HIPAA	Закон за преносимост и отчетност при здравното осигуряване
ICDR	Международен център за разрешаване на спорове
IOB	Надзорен съвет по въпросите на разузнаването
NIST	Национален институт по стандарти и технологии
АНС	Агенция по национална сигурност
NSL	Писмо (а), свързано (и) с националната сигурност
ODNI	Служба на директора на Националното разузнаване
ODNI CLPO, CLPO	Длъжностно лице по защита на гражданските свободи към Службата на директора на Националното разузнаване
OMB	Служба за управление и бюджет
OPCL	Служба за неприкосновеност на личния живот и граждански свободи към Министерството на правосъдието
PCLOB	Надзорен съвет по въпросите на неприкосновеността на личния живот и гражданските свободи
PIAB	Консултативен съвет на президента по въпросите на разузнаването
PPD 28	Президентска политическа директива № 28
Регламент (ЕС) 2016/679	Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО.
SAOP	Висш служител на Агенцията по въпросите на неприкосновеността на личния живот
Принципите	Принципи на Рамката за защита на личните данни между ЕС и САЩ
САЩ	Съединени щати
Съюз	Европейски съюз