18/BG

WP 254 rev.01

Работна група по член 29

Референтен документ относно адекватното ниво на защита

Приет на 28 ноември 2017 г.

Последно преработен и приет на 6 февруари 2018 г.

Въведение

Работната група на органите за защита на личните данни в ЕС[1] (Работната група по член 29) вече е публикувала Работен документ относно предаването на лични данни на трети държави (наричан по-нататък „WP12“)[2]. След като Директивата беше заменена от Общия регламент на ЕС относно защитата на данните (ОРЗД)[3], Работната група по член 29 преразгледа по-ранните си насоки, предоставени с WP12, за да ги актуализира в контекста на новото законодателство и скорошната съдебна практика на Съда на Европейския съюз[4].

Целта на настоящия работен документ е да се актуализира първата глава от WP12, отнасяща се до основния въпрос за адекватното ниво на защита на данните в трета държава, територия или един или повече конкретни сектори в тази трета държава, или в международна организация (наричани по-долу „трети държави или международни организации“). Настоящият документ ще се преразглежда редовно и, ако е необходимо, ще се актуализира през следващите години въз основа на придобития практически опит при прилагането на ОРЗД. На по-късен етап следва да бъдат актуализирани глава 2 (*Прилагане на подхода към държави, които са ратифицирали Конвенция 108*) и глава 3 (*Прилагане на подхода към отрасловите правила за саморегулиране*) от документ WP12.

Настоящият работен документ е съсредоточен единствено върху решенията относно адекватното ниво на защита, които представляват актове за изпълнение[5] на Европейската комисия в съответствие с член 45 от ОРЗД. Други аспекти на предаването на лични данни на трети държави и международни организации ще бъдат разгледани в следващи работни документи, които ще бъдат публикувани отделно (задължителни корпоративни правила, дерогации).

Целта на настоящия документ е да даде насоки съгласно ОРЗД на Европейската комисия и Работната група по член 29 за оценка на нивото на защита на данните в трети държави и международни организации, като установи основните принципи за защита на данните, които трябва да присъстват в правната уредба на третата държава или международната организация, за да се гарантира равностойност по същество с уредбата на ЕС. Освен това документът може да предостави насоки и на трети държави и международни организации, които са заинтересовани от получаването на статут на трета държава или международна организация с адекватно ниво на защита. Все пак принципите, посочени в настоящия работен документ, не са насочени пряко към администраторите на данни или обработващите лични данни.

Настоящият документ се състои от 4 глави:

Глава 1: Обща информация във връзка с понятието „адекватно ниво на защита“

Глава 2: Процедурни аспекти на констатациите, отнасящи се до адекватното ниво на защита съгласно ОРЗД

Глава 3: Общи принципи за защита на данните. Тази глава включва основните общи принципи на защита на данните, за да се гарантира, че нивото на защита на данните в трета държава или международна организация по същество е равностойно на установеното със законодателството на ЕС.

---

[1] Създадена съгласно член 29 от Директивата на ЕС за защита на личните данни (Директива 95/46/ЕО).

[2] WP12 , „Работен документ: предаване на лични данни на трети държави: прилагане на членове 25 и 26 от Директивата на ЕС за защита на личните данни“, приет от Работната група на 24 юли 1998 г.

[3] 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) (текст от значение за ЕИП).

[4] Включително дело C-362/14, Maximillian Schrems срещу Data Protection Commissioner, 6 октомври 2015 г.

[5] За допълнителна информация относно актовете за изпълнение вж. съответно член 45, параграф 3 и член 93, параграф 2 от ОРЗД.

Глава 4: Основни гаранции за достъпа до данни с цел правоприлагане и национална сигурност с оглед на ограничаването на намесите в основните права. Тази глава включва основните гаранции за достъпа до данни с цел правоприлагане и национална сигурност с отчитане на решението на Съда по делото Schrems от 2015 г. и въз основа на работния документ на Работната група по член 29 относно основните гаранции, приет през 2016 г.

Глава 1: Обща информация във връзка с понятието „адекватно ниво на защита“

В член 45, параграф 1 от ОРЗД е установен принципът, че предаването на данни на трета държава или международна организация се извършва само ако третата държава, територия или един или повече конкретни сектори в тази трета държава, или въпросната международна организация осигуряват адекватно ниво на защита.

Това понятие за „адекватно ниво на защита“, което съществуваше и според Директива 95/46/ЕО, бе доразвито от Съда на ЕС. В тази връзка е важно да се припомни стандартът, установен от Съда по делото Schrems, а именно че докато „*степента на защита*“ в третата държава трябва да бъде *„по същество [...] равностойна*“ на гарантираната в ЕС, то е възможно *„средствата, до които третата страна прибягва в това отношение, за да гарантира такава степен на защита, да са различни от прилаганите вътре в [ЕС]“*[6]. Ето защо целта не е да се отрази точка по точка европейското законодателство, а да се установят съществените, основните изисквания на това законодателство.

Целта на решенията относно адекватното ниво на защита, които се вземат от Европейската комисия, е официално да се потвърди с обвързващи последици за държавите членки[7], че нивото на защита на данните в дадена трета държава или международна организация е по същество равностойно на нивото на защита на данните в Европейския съюз[8]. Адекватно ниво на защита може да се постигне чрез комбинация от права за субектите на данни и задължения за лицата, които обработват данните или които упражняват контрол върху това обработване и надзор от страна на независими органи. Правилата за защита на данните обаче са ефективни само ако се прилагат и се спазват на практика. Поради това е необходимо да се разгледа не само съдържанието на правилата, които са приложими за предаването на лични данни на трета държава или международна организация, но също така въведената система за гарантиране на ефективността на тези правила. Ефикасните механизми за правоприлагане са от съществена важност за ефективността на правилата за защита на данните.

В член 45, параграф 2 от ОРЗД са установени елементите, които Европейската комисия взема предвид при оценяването на адекватността на нивото на защита в трета държава или международна организация.

Например Комисията взема предвид върховенството на закона, спазването на правата на човека и основните свободи, съответното законодателство, наличието и ефективното функциониране на един или повече независими надзорни органи и международните ангажименти, които съответната трета държава или международна организация е поела.

Затова е ясно, че всеки значим анализ на адекватната защита трябва да включва двата основни елемента: съдържанието на приложимите правила и средствата за осигуряване на тяхното ефективно прилагане. Европейската комисия следва редовно да проверява дали въведените правила са ефективни на практика.

Основната част от принципите, отнасящи се до „съдържанието“ на правилата за защита на данните, и от изискванията за „процедурите/правоприлагането“, които може да се разглеждат като минимално изискване, за да се приеме, че защитата е адекватна, произтичат от Хартата на основните права на ЕС и от ОРЗД. Освен това следва да се вземат предвид и други международни споразумения относно защитата на данните, напр. Конвенция 108[9].

Необходимо е също така да се обърне внимание на правната уредба за достъпа на публичните органи до лични данни. Допълнителни насоки в тази връзка са предоставени в работен

[6] Дело C-362/14, Maximillian Schrems срещу Data Protection Commissioner, 6 октомври 2015 г. (точки 73, 74).

[7] Член 288, параграф 2 от ДФЕС.

[8] Дело C-362/14, Maximillian Schrems срещу Data Protection Commissioner, 6 октомври 2015 г. (точка 52).

[9] Съображение 105 от ОРЗД.

документ WP 237 (т.е. документа относно основните гаранции)[10] по отношение на гаранциите в контекста на надзора.

Не е достатъчно да са налице общи разпоредби за защита на данните и неприкосновеността на личния живот в третата държава. Напротив, в правната уредба на третата държава или международната организация трябва да бъдат включени специфични разпоредби относно конкретни потребности, свързани с практически значими аспекти на правото на защита на данните. Изпълнението на тези разпоредби трябва да може да бъде осигурявано.

Глава 2: Процедурни аспекти на констатациите, отнасящи се до адекватното ниво на защита съгласно ОРЗД

За да може Европейският комитет по защита на данните да изпълнява задачата си за даване на консултации на Европейската комисия в съответствие с член 70, параграф 1, буква т) от ОРЗД, на Комитета следва да се предоставя съответната документация, включително свързаната кореспонденция и констатациите, направени от Европейската комисия. Когато правната уредба е сложна, предоставената документация следва да включва всеки един изготвен доклад относно нивото на защита на данните в третата държава или международната организация. Във всеки случай предоставената от Европейската комисия информация следва да бъде изчерпателна и да дава възможност на Европейския комитет по защита на данните да извърши собствена оценка на нивото на защита на данните в третата държава. Комитетът ще представя своевременно своето становище по констатациите на Европейската комисия и ще посочва недостатъците в рамката за осигуряване на адекватно ниво на защита, ако има такива. Комитетът ще се стреми също така да предлага поправки или изменения с оглед на преодоляването на възможни недостатъци.

Според член 45, параграф 4 от ОРЗД Европейската комисия осъществява постоянно наблюдение на развитието, което би могло да повлияе на действието на решение относно адекватното ниво на защита.

В член 45, параграф 3 от ОРЗД се предвижда, че трябва да се извършва периодичен преглед най-малко веднъж на четири години. Това обаче е общ срок, който трябва да се адаптира за всяка трета държава или международна организация, за която е прието решение относно адекватното ниво на защита. В зависимост от конкретните обстоятелства в дадения случай, може да е обосновано прилагането на по-кратък цикъл за прегледа. Освен това инциденти или друга информация относно правната уредба в дадената трета държава или международна организация, както и промени в тази правна уредба, биха могли да породят необходимост от предсрочен преглед. Също така изглежда целесъобразно първият преглед на напълно ново решение относно адекватното ниво на защита да се извършва по-скоро и цикълът на прегледите да се коригира постепенно в зависимост от резултата.

Предвид мандата на Европейския комитет по защита на данните да представя на Европейската комисия становище дали дадена трета държава, територия, или един или повече конкретни сектори в трета държава, или дадена международна организация е престанала да осигурява адекватно ниво на защита, Комитетът трябва своевременно да получава важната информация от мониторинга на съответните развития в дадената трета държава или международна организация от страна на Европейската комисия. Съответно Комитетът следва да бъде информиран за всички процеси по преглед на правната уредба или за всички възложени задачи за такъв преглед в третата държава или международната организация. Комитетът би приветствал отправянето до него на покани за участие в тези процеси и задачи за преглед.

Следва да се отбележи също така, че съгласно член 45, параграф 5 от ОРЗД Европейската комисия има право да отменя, изменя или спира прилагането на съществуващи решения относно адекватното ниво на защита. В такива случаи процедурата за отмяна, изменение или спиране на прилагането следва да включва Европейския комитет по защита на данните, като се иска неговото становище в съответствие с член 70, параграф 1, буква т).

[10] Работен документ 01/2016 относно обосновка на намесите в основните права на неприкосновеност на личния живот и защита на данните чрез мерките за надзор, когато се предават лични данни (Европейски основни гаранции), 16/EN WP 237, 13 април 2016 г.

Освен това, както вече се предвижда в член 58, параграф 5 от ОРЗД и в съответствие с решението на Съда по делото Schrems, органите за защита на данните трябва да имат възможност да участват в съдебни производства, ако считат, че искът, предявен от дадено лице срещу решение относно адекватното ниво на защита, е основателен: *„В това отношение националният законодател трябва да предвиди правни способи, позволяващи на съответния национален надзорен орган да изложи твърденията за нарушения, които счита 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“*[11].

[11] Дело C-362/14, Maximillian Schrems срещу Data Protection Commissioner, 6 октомври 2015 г. (точка 65).

Глава 3: Общи принципи за защита на данните, с които се гарантира, че нивото на защита в дадена трета държава, територия или един или повече конкретни сектори в тази трета държава, или в международна организация по същество е равностойно на нивото на защита, гарантирано от законодателството на ЕС

Системата на третата държава или на международната организация трябва да включва следните основни принципи и механизми, отнасящи се до съдържанието и процедурите/прилагането в областта на защитата на данните:

A. <u>Принципи, отнасящи се до съдържанието:</u>

1) Понятия

Трябва да съществуват основните понятия и/или принципи за защита на данните. Не е необходимо те да съвпадат с терминологията според ОРЗД, но следва да отразяват понятията, заложени в европейското право в областта на защитата на данните и да съответстват на тях. Например ОРЗД включва следните важни понятия: „лични данни“, „обработване на лични данни“, „администратор на данни“, „обработващ лични данни“, „получател“ и „чувствителни данни“.

2) Основания за законосъобразно и добросъвестно обработване за легитимни цели

Данните трябва да се обработват законосъобразно, добросъвестно и легитимно.

Легитимните основания, според които личните данни може да бъдат обработвани законосъобразно, добросъвестно и легитимно, следва да бъдат установени достатъчно ясно. Европейската рамка признава няколко такива легитимни основания, включително например разпоредби в националното право, съгласието на субекта на данни, изпълнението на договор или законен интерес на администратора на данни или на трета страна, който няма преимущество пред интересите на физическото лице.

3) Принцип на ограничаване до предвидената цел

Данните трябва да се обработват с конкретна цел и впоследствие да се използват само дотолкова, доколкото употребата не е несъвместима с целта на обработването.

4) Принцип на качеството и пропорционалността на данните

Данните трябва да бъдат точни и при необходимост редовно да се актуализират. Данните трябва да са подходящи, релевантни и да не превишават по обем необходимото във връзка с целите, за които се обработват.

5) Принцип на запазване на данни

Като общо правило данните трябва да се съхраняват не повече от необходимото за целите, за които личните данни се обработват.

6) Принцип на сигурност и поверителност

Всяко образувание, което обработва лични данни, следва да гарантира, че данните се обработват по начин, който гарантира сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки. При определянето на степента на сигурност следва да се вземат предвид достиженията на техническия прогрес и свързаните разходи.

7) Принцип на прозрачността

Всяко физическо лице следва да бъде информирано за всички основни елементи по обработването на неговите/нейните лични данни в ясна, лесно достъпна, кратка, прозрачна и разбираема форма. Тази информация следва да включва целта на обработването, идентичността на администратора на данни, правата, които са му предоставени, и друга информация, доколкото това е необходимо, за да се гарантира добросъвестността. При определени условия може да съществуват някои изключения от това право на информиране, например за защита на разследването на престъпления, националната сигурност, независимостта на съдебната власт, съдебните производства или други важни цели от широк обществен интерес, както е предвидено в член 23 от ОРЗД.

8) Правото на достъп, коригиране, изтриване и възражение

Субектът на данни следва да има право да получи потвърждение относно това дали се обработват данни за него/нея или не, както и достъп до неговите/нейните данни, включително да получи копие на всички обработвани данни, които са свързани с него/нея.

Субектът на данни следва да има право да поиска коригиране на неговите/нейните данни, когато е целесъобразно, поради определени причини, като например когато се окаже, че те са неточни или непълни, както и право на изтриване на неговите/нейните лични данни, когато например обработването им повече не е необходимо или е незаконосъобразно.

Субектът на данните следва също така да има право да възрази във всеки един момент и на базата на неоспорими легитимни основания, свързани с конкретната му/ѝ ситуация, срещу обработването на неговите/нейните данни, при спазване на конкретните условия, определени в правната уредба на третата държава. В ОРЗД например тези условия включват случаите, когато обработването е необходимо за изпълнението на задача от обществен интерес или когато е необходимо за упражняването на официални правомощия, предоставени на администратора, или когато обработването е необходимо за целите на легитимните интереси на администратора на данни или на трета страна.

Упражняването на тези права не следва да бъде прекалено трудно за субекта на данни. Възможно е да има известни ограничения на тези права, например с цел защита на разследването на престъпления, националната сигурност, независимостта на съдебната власт, съдебните производства или други важни цели от широк обществен интерес, както е предвидено в член 23 от ОРЗД.

9) Ограничения на последващи предавания на данни

Последващи предавания на личните данни от първоначалния получател на първоначалното предаване на данни следва да бъдат разрешени само когато следващият получател (т.е. получателят на последващото предаване на данни) също е обвързан с правила (включително договорни правила), осигуряващи подходящо ниво на защита, и при спазване на съответните указания, когато данните се обработват от името на администратора на данни. Нивото на защита на физическите лица, чиито данни се предават, не трябва да бъде понижено вследствие на последващото предаване. Първоначалният получател на данните, които се предават от ЕС, следва да носи отговорност за осигуряването на подходящи гаранции за последващите предавания на данните, ако не е издадено решение относно адекватното ниво

на защита. Такива последващи предавания на данни следва да се извършват само за ограничени и определени цели и доколкото са налице правни основания за такова обработване.

Б. Примери за допълнителни принципи във връзка със съдържанието, които трябва да се прилагат при специфични видове обработване:

1) Специални категории данни

Когато се касае за „специални категории данни“[12], трябва да има специфични гаранции. Тези категории данни трябва да отразяват категориите, заложени в членове 9 и 10 от ОРЗД. Защитата трябва да се осигури или чрез по-строги изисквания към обработването на данните, като например субектът на данни да дава своето изрично съгласие за обработването, или чрез допълнителни мерки за сигурност.

2) Директен маркетинг

Когато данните се обработват за целите на директния маркетинг, субектът на данни следва да може по всяко време да направи възражение срещу обработването на неговите/нейните данни, без за целта да му/ѝ се начисляват каквито и да било такси.

3) Автоматизирано вземане на решения и профилиране

Решения, основани единствено на автоматизирано обработване (автоматизирано вземане на индивидуални решения), включително профилиране, които пораждат правни последици или сериозно засягат субекта на данните, може да се вземат само при определени условия, установени в правната уредба на третата държава. Според европейската уредба тези условия включват например необходимостта да се получи изричното съгласие на субекта на данните или приемането на такова решение да е необходимо за сключването на договор. Ако решението не отговаря на условията, предвидени в правната уредба на третата държава, субектът на данни следва да има право да бъде освободен от неговото действие. Във всеки случай правото на третата държава трябва да предвижда необходимите гаранции, включително правото на уведомяване за конкретните съображения, на които почива решението, и следваната в него логика, правото на поправяне на неточна или непълна информация, както и правото на възражение срещу решението, когато е било прието въз основа на неточни факти.

В. Процедурни механизми и механизми за правоприлагане:

Въпреки че средствата, до които третата държава има достъп, за да гарантира адекватно ниво на защита, може да се различават от използваните в рамките на Европейския съюз[13], за да отговаря системата на европейската, тя трябва да се характеризира с наличието на следните елементи:

1) Компетентен независим надзорен орган

[12] Тези специални категории данни са наречени също така „чувствителни данни“ в съображение 10 от ОРЗД.

[13] Дело C-362/14, Maximillian Schrems срещу Data Protection Commissioner, 6 октомври 2015 г., точка 74.

Следва да съществуват един или повече независими надзорни органи, натоварени с наблюдение, гарантиране и осигуряване на спазването на разпоредбите за защита на данните и неприкосновеността на личния живот в третата държава. Надзорният орган следва да действа изцяло независимо и безпристрастно при изпълнението на задачите и упражняването на правомощията си, като в тази връзка няма нито да търси, нито да приема инструкции. В този контекст надзорният орган следва да разполага с всички необходими и налични правомощия и да е натоварен със съответните мисии, за да се гарантира спазването на правата за защита на данните и да се насърчава осведомеността. Следва да се обърне внимание също и на персонала и на бюджета на надзорния орган. Надзорният орган трябва да може също така да извършва проучвания по собствена инициатива.

2) **Системата за защита на данните трябва да гарантира добро равнище на съответствие**

Системата на третата държава следва да гарантира висока степен на отчетност и осведоменост на администраторите на данни и обработващите лични данни от тяхно име, що се отнася до техните задължения, задачи и отговорности, както и на субектите на данни относно техните права и средствата за упражняването им. Наличието на ефективни и възпиращи санкции може да има важна роля за осигуряването на спазването на правилата, като разбира се такава роля могат да имат и системите за пряка проверка от органи, одитори или независими длъжностни лица, отговарящи за защитата на данните.

3) **Отчетност**

Рамката за защита на данните на третата държава следва да задължава администраторите на данни и/или обработващите лични данни от тяхно име да я спазват и да могат да докажат, че я спазват, по-специално пред компетентния надзорен орган. Тези мерки може да включват например оценки на въздействието на защитата на данните, воденето на записи или регистри на дейностите по обработване на данни за определен период от време, назначаването на длъжностно лице по защита на данните или защитата на данните на етапа на проектирането и по подразбиране.

4) **Системата за защита на данните трябва да осигурява подпомагане и помощ за отделните субекти на данни при упражняването на техните права, както и подходящи механизми за съдебна защита**

Физическото лице следва да може да използва средства за правна защита, за да упражни правата си бързо и ефективно и без възпиращи разходи, както и за да се гарантира спазване на правилата. За тази цел трябва да има механизми за надзор, позволяващи независимо разследване по жалбите и установяване и реално санкциониране на всяко нарушение на правото на защита на данните и на зачитане на неприкосновеността на личния живот.

Когато правилата не се спазват, субектът на данни следва да разполага също така с ефективни административни и съдебни средства за защита, включително за обезщетение за вреди в резултат на незаконосъобразно обработване на неговите/нейните лични данни. Това е ключов елемент, който трябва да включва система за независимо отсъждане или арбитраж, даваща възможност за изплащането на компенсация и, по целесъобразност, налагането на санкции.

Глава 4: Основни гаранции в третите държави за достъпа до данни с цел правоприлагане и национална сигурност с оглед на ограничаването на намесите в основните права

При оценяването на адекватността на нивото на защита по член 45, параграф 2, буква а) се изисква Комисията да взема предвид „съответното законодателство — както общо, така и секторно, включително в областта на обществената сигурност, отбраната, националната сигурност и наказателното право и достъпа на публичните органи до лични данни, а също и прилагането на такова законодателство*…“*.

В решението си по дело Schrems Съдът е отбелязал, че *„изразът „достатъчна степен на защита“ трябва да се разбира в смисъл, че от съответната трета страна се изисква ефективно да гарантира, по силата на вътрешното си законодателство или на международните си споразумения, степен на защита на основните права и свободи, която по същество е равностойна на гарантираната в Съюза по силата на Директива 95/46, разглеждана във връзка с Хартата“*. Макар да е възможно средствата, до които третата държава прибягва в тази връзка, да са различни от прилаганите вътре в Европейския съюз, все пак е необходимо на практика тези средства да се окажат ефективни[14].

В този контекст Съдът също така отбелязва критично, че предходното решение за „сферата на неприкосновеност на личния живот“ *„не съдържа каквато и да било констатация относно наличието в Съединените щати на правила с етичен характер, предназначени за ограничаване на евентуалната намеса, засягаща основните права на лицата, чиито данни се прехвърлят от Съюза към Съединените щати, която намеса държавните структури на тази страна имат право да извършват, ако преследват законосъобразни цели, като например осигуряването на националната сигурност“.*

В своето становище WP237, прието на 13 април 2016 г., Работната група по член 29 е установила основни гаранции, отразяващи практиката на Съда и на Европейската конвенция за правата на човека в областта на надзора. Въпреки че препоръките, които са описани подробно в WP237, продължават да бъдат валидни и следва да се вземат предвид при оценяването на адекватността в областта на надзора в дадена трета държава, прилагането на тези гаранции може да се различава в областта на достъпа до данни с цел правоприлагане и национална сигурност. При все това, посочените четири гаранции трябва да се спазват от всички трети държави, за да може по отношение на достъпа до данни, независимо дали за целите на националната сигурност или за целите на правоприлагането, да се счита, че е налице адекватно ниво на защита:

1) **обработването трябва да се основава на ясни, точни и достъпни правила (правно основание);**

2) **трябва да се докаже необходимост и пропорционалност по отношение на преследваните легитимни цели;**

3) **обработването трябва да бъде обект на независим надзор;**

4) **физическите лица трябва да разполагат с ефективни средства за защита.**

[14] Дело C-362/14, Maximillian Schrems срещу Data Protection Commissioner, 6 октомври 2015 г., точка 74.