Translations proofread by EDPB Members.
This language version has not yet been proofread.

Препоръки 01/2020 относно мерките, които допълват инструментите за предаване, за да се гарантира спазването на защита на личните данни на равнище ЕС

Приети на 10 ноември 2020 г.

Кратко изложение

Общият регламент за защита на данните (ОРЗД) на ЕС беше приет с двойна цел: улесняване на свободното движение на лични данни в рамките на Европейския съюз, като същевременно се запазват основните права и свободи на физическите лица, по-специално правото им на защита на личните данни.

В неотдавнашното си решение по дело C-311/18 (Schrems II) Съдът на Европейския съюз (Съдът на ЕС) ни припомни, че защитата, осигурена за личните данни в Европейското икономическо пространство (ЕИП), трябва да съпътства данните, независимо къде се изпращат. Предаването на лични данни на трети държави не може да се използва като средство за подкопаване или отслабване на защитата, която се предоставя в ЕИП. Съдът също така утвърждава това, като пояснява, че не е необходимо нивото на защита в трети държави да бъде еднакво с гарантираното в рамките на ЕИП, а по същество равностойно. Съдът потвърждава и валидността на стандартните договорни клаузи като инструмент за предаване, който може да гарантира равностойно по същество равнище на защита на данните, предавани на трети държави по договор.

Стандартните договорни клаузи и другите инструменти за предаване, посочени в член 46 от ОРЗД, не функционират изолирано. Съдът посочва, че администраторите или обработващите лични данни, които действат в качество на износители, отговарят за проверката във всеки отделен случай и, когато е целесъобразно, си сътрудничат с вносителя в третата държава, ако правото или практиката на третата държава нарушава ефективността на подходящите гаранции, съдържащи се в инструментите за предаване на данни по член 46 от ОРЗД. По тези дела Съдът все пак оставя открита възможността износителите да прилагат допълнителни мерки, които запълват тези пропуски в защитата и я повишават до равнището, изисквано от правото на Съюза. Съдът не уточнява какви биха могли да бъдат тези мерки. Съдът подчертава обаче, че износителите ще трябва да ги идентифицират във всеки отделен случай. Това е в съответствие с принципа на отчетност от член 5, параграф 2 от ОРЗД, в който се изисква администраторите да носят отговорност и да са в състояние да докажат, че принципите на ОРЗД, свързани с обработването на лични данни, се спазват.

За да помогне на износителите (независимо дали са администратори или обработващи лични данни, частни субекти или публични органи, обработващи лични данни в рамките на приложното поле на ОРЗД) в сложната задача да правят оценка на трети държави и да определят подходящи допълнителни мерки, когато е необходимо, Европейският комитет по защита на данните (ЕКЗД) прие настоящите препоръки. С настоящите препоръки на износителите се посочват поредица от стъпки, които да следват, потенциални източници на информация, както и примери за допълнителни мерки, които биха могли да бъдат въведени.

Като **първа стъпка** ЕКЗД Ви препоръчва, като износители, да **познавате предаването, което извършвате**. Картографирането на всяко предаване на лични данни на трети държави може да бъде трудно. Въпреки това е необходимо да се знае къде се предават личните данни, за да се гарантира, че са обект на равностойно по същество ниво на защита, независимо от мястото, където се обработват. Трябва също така да се уверите, че данните, които предавате, са подходящи, актуални и ограничени до необходимото за целите, за които се предават и обработват в третата държава.

Втората стъпка е да се **провери инструментът за предаване, от който зависи предаването**, сред изброените в глава V от ОРЗД. Ако Европейската комисия вече е обявила държавата, региона или сектора, на който предавате данните, за подходящ в свое решение относно адекватното ниво на защита съгласно член 45 от ОРЗД или съгласно предходната Директива 95/46, докато решението все още е в сила, няма да е необходимо да предприемате други стъпки, освен да следите дали решението относно адекватното ниво на защита остава валидно. При липса на решение относно адекватното ниво на защита трябва да разчитате на някой от инструментите за предаване, изброени в член 46 от ОРЗД, при предаване на данни, което е редовно или повтарящо се. Само в някои случаи на случайно и еднократно предаване на данни можете да се позовете на някоя от дерогациите, предвидени в член 49 от ОРЗД, ако отговаряте на условията.

Третата стъпка е да се **прецени** дали има нещо в **правото или практиката на третата държава**, което може да засегне ефективността на подходящите гаранции по отношение на инструментите за предаване, на които разчитате, в контекста на конкретното предаване. Вашата оценка следва да бъде съсредоточена основно върху законодателството на трети държави, което има отношение към Вашето предаване, и върху инструмента за предаване по член 46 от ОРЗД, на който разчитате, и което може да подкопае неговото ниво на защита. За оценка на елементите, които трябва да бъдат взети предвид при оценката на правото на трета държава, засягащо достъпа до данни от страна на публичните органи за целите на надзора, направете справка с препоръките на ЕКЗД относно основните европейски гаранции. По-специално това следва да се разгледа внимателно, когато законодателството, уреждащо достъпа на публичните органи до данни, е двусмислено или не е публично достъпно. При липса на законодателство, уреждащо обстоятелствата, при които публичните органи могат да получат достъп до лични данни, ако все още желаете да продължите с предаването, следва да разгледате други относими и обективни фактори, а не да разчитате на субективни фактори, например вероятността публичните органи да имат достъп до Вашите данни по начин, който не е в съответствие със стандартите на ЕС. Тази оценка следва да извършите с дължимата грижа и да я документирате задълбочено, тъй като ще носите отговорност за решението, което можете да вземете на тази база.

Четвъртата стъпка е **да се определят и приемат допълнителни мерки**, необходими за привеждане на нивото на защита на предаваните данни в съответствие със стандарта на ЕС за равностойност по същество. Тази стъпка е необходима само ако според Вашата оценка законодателството на третата държава засяга ефективността на инструмента за предаване по член 46 от ОРЗД, на който разчитате или на който възнамерявате да разчитате в контекста на предаването. В настоящите препоръки се съдържа (в Приложение 2) неизчерпателен списък с примери за допълнителни мерки с някои от условията, които те ще изискват, за да бъдат ефективни. Както в случая с подходящите гаранции, съдържащи се в инструментите за предаване по член 46, някои допълнителни мерки могат да бъдат ефективни в някои държави, но не непременно в други. Вие отговаряте за оценката на ефективността им в контекста на предаването, както и с оглед на правото на третата държава и инструмента за предаване, на който разчитате, и ще носите отговорност за взетото от Вас решение. Може да е необходимо също така да комбинирате няколко допълнителни мерки. В крайна сметка може да установите, че никоя допълнителна мярка не може да гарантира равностойно по същество ниво на защита за Вашето конкретно предаване. В случаите, когато не е подходяща допълнителна мярка, трябва да избегнете, преустановите или прекратите предаването, за да не бъде компрометирано нивото на защита на личните данни. Също така трябва да извършите тази оценка на допълнителните мерки с необходимата грижа и да я документирате.

Петата стъпка е да се **предприемат** всички **формални процедурни стъпки**, които може да са необходими за приемането на Вашата допълнителна мярка, в зависимост от инструмента за предаване по член 46 от ОРЗД, на който разчитате. Тези формалности са уточнени в настоящите препоръки. Може да е необходимо да се консултирате с Вашите компетентни надзорни органи относно някои от тях.

Шестата и последна стъпка ще бъде да правите преоценка през подходящи интервали на нивото на защита на данните, които предавате на трети държави, и да следите дали е имало или ще има развитие, което може да ги засегне. Принципът на отчетност изисква постоянна бдителност по отношение на нивото на защита на личните данни.

Надзорните органи ще продължат да упражняват своите правомощия за наблюдение на спазването на ОРЗД и ще го прилагат. Надзорните органи ще обърнат дължимото внимание на действията, които износителите предприемат, за да гарантират, че данните, които предават, получават по същество равностойно ниво на защита. Както припомня Съдът, надзорните органи спират или забраняват предаването на данни в случаите, когато след разследване или жалба установят, че не може да се гарантира равностойно по същество ниво на защита.

Надзорните органи ще продължат да разработват насоки за износителите и да координират действията си в рамките на ЕКЗД, за да се гарантира последователност в прилагането на законодателството на ЕС за защита на данните.

Съдържание

Европейският комитет по защита на данните,

като взе предвид член 70, параграф 1, буква д) от 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 и за отмяна на Директива 95/46/ЕО (по-нататък „ОРЗД“),

като взе предвид Споразумението за Европейското икономическо пространство (ЕИП), и по-специално Приложение XI и протокол 37 към него, изменени с Решение на Съвместния комитет на ЕИП № 154/2018 от 6 юли 2018 г.[1],

като взе предвид членове 12 и 22 от своя процедурен правилник,

като има предвид, че:

(1) В решението си от 16 юли 2020 г. по делото *Data Protection Commissioner/Facebook Ireland LTD, Maximillian Schrems,* C-311/18, Съдът на Европейския съюз стига до заключението, че член 46, параграф 1 и член 46, параграф 2, буква в) от ОРЗД трябва да се тълкуват в смисъл, че чрез подходящите гаранции, приложимите права и ефективните правни средства за защита, изисквани от тези разпоредби, трябва да се гарантира, че субектите на данни, чиито лични данни се предават на трета държава по силата на стандартни клаузи за защита на данните, се ползват със степен на защита, която по същество е равностойна на гарантираната в Европейския съюз от този регламент, разглеждана в светлината на Хартата на основните права на Европейския съюз[2].

(2) Както подчертава Съдът, независимо от разпоредбата на глава V, въз основа на която се извършва предаването на лични данни на трета държава, трябва да се гарантира ниво защита на физическите лица, което по същество е равностойно на гарантираното в рамките на Европейския съюз от ОРЗД, тълкуван в светлината на Хартата. Разпоредбите на глава V имат за цел да се гарантира непрекъснатостта на тази висока степен на защита, когато личните данни се предават на трета държава[3].

(3) В съображение 108 и член 46, параграф 1 от ОРЗД се предвижда, че при липса на решение на ЕС относно адекватното ниво на защита администраторът или обработващият лични данни следва да предприеме мерки за компенсиране на липсата на защита на данните в трета държава чрез подходящи гаранции за субекта на данните. Администраторът или обработващият лични данни може да предостави подходящи гаранции, без да се изисква специално разрешение от надзорен орган, чрез използването от негова страна на някой от инструментите за предаване, изброени в член 46, параграф 2 от ОРЗД, например стандартни клаузи за защита на данните.

[1] Позоваванията на „държави членки“ в настоящия документ следва да се разбират като позовавания на „държавите — членки на ЕИП“.
[2] Решение на Съда на ЕС от 16 юли 2020 г., Data Protection Commissioner/Facebook Ireland Ltd, Maximillian Schrems, (наричано по-нататък C-311/18 (Schrems II), втора констатация.
[3] Дело C-311/18 (Schrems II), точки 92 и 93.

(4) Съдът пояснява, че стандартните клаузи за защита на данните, приети от Комисията, имат за цел единствено да се предоставят договорни гаранции, които се прилагат еднакво във всички трети държави за администраторите и обработващите лични данни, установени в Европейския съюз. Поради договорния си характер стандартните клаузи за защита на данните не могат да обвързват публичните органи на трети държави, тъй като те не са страна по договора. Ето защо може да се наложи износителите на данни да допълнят гаранциите, съдържащи се в тези стандартни клаузи за защита на данните, с допълнителни мерки, за да се гарантира спазването на нивото на защита в конкретна трета държава, изисквано съгласно правото на ЕС. Съдът се позовава на съображение 109 от ОРЗД, в което се споменава тази възможност и администраторите и обработващите лични данни се насърчават да я използват[4].

(5) Съдът уточнява, че преди всичко износителят на данни е длъжен да провери във всеки отделен случай и евентуално в сътрудничество с вносителя на данните дали с правото на третата страна по местоназначение се гарантира по същество равностойно ниво на защита съгласно правото на ЕС на личните данни, предавани по силата на стандартни клаузи за защита на данните, като при необходимост включва допълнителни мерки към предвидените в тези клаузи[5].

(6) Ако администраторът или обработващият лични данни, установен в Европейския съюз, не е в състояние да предприеме подходящи допълнителни мерки, за да гарантира равностойно по същество ниво на защита съгласно правото на ЕС, от администратора или обработващия лични данни или, ако това не е възможно, от компетентния надзорен орган, се изисква да спре или да прекрати предаването на лични данни на съответната трета държава[6].

(7) ОРЗД или Съдът не определят, нито уточняват „допълнителни гаранции“, „допълнителни мерки“ или „допълващи мерки“ към гаранциите на инструментите за предаване, изброени в член 46, параграф 2 от ОРЗД, които администраторите и обработващите лични данни могат да приемат, за да се гарантира спазването на нивото на защита в дадена трета държава, изисквано съгласно правото на ЕС.

(8) ЕКЗД реши по собствена инициатива да разгледа този въпрос и да предостави на администраторите и обработващите лични данни, действащи като износители, препоръки относно процеса, които те могат да следват за идентифициране и приемане на допълнителни мерки. Настоящите препоръки имат за цел да се осигури методология, чрез която износителите да определят дали и какви допълнителни мерки ще трябва да бъдат въведени за тяхното предаване на данни. Основната отговорност на износителите е да гарантират, че предадените данни се предоставят в третата държава с ниво на защита, което по същество е равностойно на гарантираното в рамките на ЕС. Чрез настоящите препоръки ЕКЗД се стреми да насърчава последователното прилагане на ОРЗД и решението на Съда в съответствие с мандата на ЕКЗД[7].

ПРИЕ СЛЕДНАТА ПРЕПОРЪКА:

[4] Дело C-311/18 (Schrems II), точки 132 и 133.
[5] Дело C-311/18 (Schrems II), точка 134.
[6] Дело C-311/18 (Schrems II), точка 135.
[7] Член 70, параграф 1 от ОРЗД.

1 ОТЧЕТНОСТ ПРИ ПРЕДАВАНЕТО НА ДАННИ

1. В първичното право на ЕС правото на защита на данните се счита за основно право[8]. Съответно правото на защита на данните се ползва с висока степен на защита и ограничения могат да бъдат налагани само ако са предвидени по закон, с тях се зачита основното съдържание на правото му, ако са пропорционални, необходими и действително отговарят на признатите от Съюза цели от общ интерес или на необходимостта да се защитят правата и свободите на други хора[9]. Правото на защита на личните данни не е абсолютно право. То трябва да бъде разглеждано във връзка с функцията му в обществото и да бъде в равновесие с другите основни права съгласно принципа на пропорционалност[10].

2. При пренасянето им до трети държави извън ЕИП данните трябва да получават ниво на защита, което по същество е равностойно на гарантираното в рамките на ЕС, за да се гарантира, че се спазва нивото на защита, гарантирано от ОРЗД.

3. Правото на защита на данните има активен характер. От износителите и вносителите (независимо дали са администратори и/или обработващи лични данни) се изисква да излязат извън рамките на признаването или пасивното спазване на това право[11]. Администраторите и обработващите лични данни трябва да се стремят да спазват правото на защита на данните по активен и непрекъснат начин, като прилагат правни, технически и организационни мерки, които гарантират неговата ефективност. Администраторите и обработващите лични данни трябва също така да могат да докажат тези усилия пред субектите на данни, широката общественост и надзорните органи за защита на данните. Това е т.нар. принцип на отчетност[12].

4. Принципът на отчетност, който е необходим, за да се гарантира ефективното прилагане на нивото на защита, предвидено в ОРЗД, се прилага и за предаването на данни на трети държави[13], тъй като само по себе си то представлява форма на обработване на данни[14]. Както подчерта Съдът в своето решение, независимо от разпоредбата на тази глава, въз основа на която се извършва предаването на лични данни на трета държава, трябва да се гарантира ниво на защита, което по същество е равностойно на гарантираното в рамките на Европейския съюз от ОРЗД, тълкуван в светлината на Хартата[15].

5. В решението по делото Schrems II Съдът изтъква отговорностите на износителите и вносителите да гарантират, че обработването на лични данни се извършва и ще продължи да се извършва в съответствие с нивото на защита, определено от правото на ЕС в областта на защитата на данните, и да спрат предаването и/или да прекратят договора, когато вносителят на данните не е в състояние или вече не е в състояние да спазва стандартните клаузи за защита на данните,

[8] Член 8, параграф 1 от Хартата на основните права и член 16, параграф 1 от ДФЕС, преамбюл 1, член 1, параграф 2 от ОРЗД.
[9] Член 52, параграф 1 от Хартата на основните права на ЕС.
[10] Съображение 4 от ОРЗД и дело C-507/17 Google LLC, правоприемник на Google Inc./Commission nationale de l'informatique et des libertés (CNIL), точка 60.
[11] Дела C-92/09 и C-93/02, Volker und Markus Schecke GbR v. Land Hessen, Заключение на генерален адвокат Sharpston, 17 юни 2010 г., точка 71.
[12] Член 5, параграф 2 и член 28, параграф 3, буква з) от ОРЗД.
[13] Член 44 и съображение 101 от ОРЗД, както и член 47, параграф 2, буква г) от ОРЗД.
[14] Решение на Съда на ЕС от 6 октомври 2015 г., *Maximillian Schrems/Data Protection Commissioner, (наричано по-нататък* C-362/14 (Schrems I), точка 45.
[15] Дело C-311/18 (Schrems II), точки 92 и 93.

включени в съответния договор между износителя и вносителя[16]. Администраторът или обработващият лични данни, действащ като износител, трябва да гарантира, че вносителите си сътрудничат с износителя, когато е целесъобразно, при изпълнението на тези отговорности, като го информира, например, за всяко развитие, засягащо нивото на защита на личните данни, получени в държавата на вносителя[17]. Тези отговорности са прилагане на принципа на ОРЗД за отчетност при предаването на данни[18].

2 ПЪТНА КАРТА: ПРИЛАГАНЕ НА ПРИНЦИПА НА ОТЧЕТНОСТ КЪМ ПРЕДАВАНЕТО НА ДАННИ НА ПРАКТИКА

6. Следва пътна карта на стъпките, които трябва да предприемете, за да разберете дали Вие (износителят на данни) трябва да предприемете допълващи мерки, за да можете законно да предавате данни извън ЕИП. „Вие“ в настоящия документ означава администратор или обработващ лични данни, действащ като износител на данни, който обработва лични данни в рамките на приложното поле на ОРЗД — включително обработването от частни субекти и публични органи при предаването на данни на частни органи[19]. Що се отнася до предаването на лични данни между публични органи, в *Насоки 2/2020 относно член 46, параграф 2, буква а) и член 46, параграф 3, буква б) от Регламент (ЕО) № 2016/679 са предвидени специални насоки за предаването на лични данни между публични органи от ЕИП и извън ЕИП*[20].

7. Вие ще трябва да документирате по подходящ начин тази оценка и допълващите мерки, които избирате и прилагате, и да предоставите тази документация на компетентния надзорен орган при поискване[21].

2.1 Стъпка 1: Бъдете запознати с предаването на данни, което извършвате

8. За да знаете какво може да се изисква, за да можете (като износител на данни) да продължите да извършвате или да извършвате ново предаване на лични данни[22], първата стъпка е да се уверите, че сте напълно запознати с предаването на данни (знаете какви данни предавате). Регистрирането и картографирането на всяко предаване може да бъде сложен процес за субектите, участващи в многобройно, разнообразно и редовно предаване на трети държави и използващи редица от обработващи лични данни и подизпълнители. Познаването на предаваните данни е важна първа стъпка за изпълнението на задълженията Ви съгласно принципа на отчетност.

[16] Дело C-311/18 (Schrems II), точки 134, 135, 139, 140, 141, 142.
[17] Дело C-311/18 (Schrems II), точка 134.
[18] Член 5, параграф 2 и член 28, параграф 3, буква з) от ОРЗД.
[19] Вж. Насоки 3/2018 на ЕКЗД относно териториалния обхват на ОРЗД (член 3) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en
[20] Насоки 2/2020 на ЕКЗД относно член 46, параграф 2, буква а) и член 46, параграф 3, буква б) от Регламент (ЕО) № 2016/679 за предаването на лични данни между публични органи от ЕИП и извън ЕИП; вж. https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_en
[21] Член 5, параграф 2 от ОРЗД и член 24, параграф 1 от ОРЗД.
[22] Имайте предвид, че дистанционният достъп на субект от трета държава до данни, намиращи се в ЕИП, също се счита за предаване.

9. За да се запознаете изцяло с предаваните данни, можете да използвате записите на дейностите по обработване, които може да сте задължени да поддържате като администратор или обработващ лични данни съгласно член 30 от ОРЗД[23]. От полза могат да Ви бъдат и предишни действия за изпълнение на задълженията за информиране на субектите на данни относно предаването от Ваша страна на техните лични данни на трети държави съгласно член 13, параграф 1, буква е) и член 14, параграф 1, буква е) от ОРЗД[24].

10. При картографирането на предаване на данни не забравяйте да вземете предвид и последващото предаване, например дали обработващите лични данни извън ЕИП, с които работите, предават поверените личните данни, които сте им поверили, на подизпълнител в друга трета държава или в същата трета държава[25].

11. С оглед на спазването на принципа от ОРЗД за „свеждане на данните до минимум“[26] трябва също така да се уверите, че данните, които предавате, са подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се предават и обработват в третата държава.

12. Тези дейности трябва да се извършват преди всяко предаване на данни и да се актуализират преди възобновяването на предаването след преустановяване на операциите по предаване на данни: трябва да знаете къде могат да се намират или обработват от вносителите личните данни, които сте изнесли (карта на местоназначенията).

13. Имайте предвид, че достъп от разстояние от трета държава (например в ситуации на подкрепа) и/или съхранението в облак, намиращ се извън ЕИП, също се счита за предаване[27]. По-конкретно, ако използвате международна инфраструктура за компютърни услуги в облак, трябва да прецените дали Вашите данни ще бъдат предадени на трети държави и къде, освен ако доставчикът на услуги в облак ясно е посочил в договора си, че данните изобщо няма да бъдат обработвани в трети държави.

---

[23] Вж. член 30 от ОРЗД, и по-специално параграф 1, буква д) и параграф 2, буква в). Освен това Вашите записи на обработването следва да съдържат описание на дейностите Ви по обработване (които включват, но не се ограничават до категориите субекти на данни, категориите лични данни и целите на обработването, както и конкретна информация относно предаването на данни). Някои администратори и обработващи лични данни са освободени от задължението да поддържат документация за дейностите по обработване (член 30, параграф 5 от ОРЗД). За насоки относно това изключение вж. Позиция на Работната група по член 29 относно изключенията от задължението за поддържане на регистри по дейностите по обработване, съгласно член 30, параграф 5 от ОРЗД (одобрена от ЕКЗД на 25 май 2018 г.).

[24] Съгласно правилата за прозрачност на ОРЗД трябва да информирате субектите на данни за предаването на лични данни на трети държави (член 13, параграф 1, буква е) и член 14, параграф 1, буква е) от ОРЗД). Необходимо е да ги информирате по-конкретно за наличието или липсата на решение на Европейската комисия относно адекватното ниво на защита или, в случай на предаване на данни, посочено в членове 46 или 47 от ОРЗД, или в член 49, параграф 1, втора алинея от ОРЗД, да посочите целесъобразни или подходящи гаранции и средствата, чрез които да получите копие от тях или информация къде са били предоставени. Информацията, предоставена на субекта на данните, трябва да бъде точна и актуална, особено с оглед на съдебната практика на Съда относно предаването на данни.

[25] Когато администраторът е дал своето предварително конкретно или общо писмено разрешение в съответствие с член 28, параграф 2 от ОРЗД.

[26] Член 5, параграф 1, буква в) от ОРЗД.

[27] Вж. Често задавани въпроси (ЧЗВ) № 11 *„следва да се има предвид, че дори предоставянето на достъп до данни от трета държава, например за административни цели, също представлява предаване“*, ЕКЗД, Често задавани въпроси относно решението на Съда на Европейския съюз по дело C-311/18 — Data Protection Commissioner/Facebook Ireland Ltd и Maximillian Schrems, 23 юли 2020 г.

2.2 Стъпка 2: Определяне на инструментите за предаване, на които разчитате

14. Втората стъпка, която трябва да предприемете, е да определите инструментите за предаване, на които разчитате, въз основа на списъците по глава V от ОРЗД.

Решения относно адекватното ниво на защита

15. Европейската комисия може да признае чрез своите **решения относно адекватното ниво на защита**, отнасящи се до някои или всички трети държави, на които предавате лични данни, че те предлагат адекватно ниво на защита на личните данни[28].

16. В резултат на такова решение относно адекватното ниво на защита личните данни могат да се предават от ЕИП към тази трета държава, без да е необходим инструмент за предаване на данни по член 46 от ОРЗД.

17. Решенията относно адекватното ниво на защита могат да обхващат дадена държава като цяло или да бъдат ограничени до част от нея. Решенията относно адекватното ниво на защита могат да обхващат всяко предаване на данни към дадена държава или да бъдат ограничени до някои видове предаване (например в един сектор)[29].

18. Европейската комисия публикува списъка на своите решения относно адекватното ниво на защита на данните на своя уебсайт[30].

19. Ако предавате лични данни на трети държави, региони или сектори, обхванати от решение на Комисията относно адекватното ниво на защита (доколкото е приложимо), **не е необходимо да предприемате по-нататъшни стъпки, както е описано в настоящите препоръки[31]**. Въпреки това трябва да следите дали решенията относно адекватното ниво на защита, които са от значение за Вашето предаване, са отменени или обявени за недействителни[32].

[28] Въз основа на член 45 от ОРЗД Европейската комисия има правомощието да определя дали държава извън ЕС предлага адекватно ниво на защита на данните. По същия начин Европейската комисия има правомощието да определи, че дадена международна организация предлага адекватно ниво на защита.
[29] Член 45, параграф 1 от ОРЗД.
[30] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
[31] При условие че Вие и вносителят на данни сте въвели мерки за спазване на другите задължения съгласно ОРЗД, в противен случай прилагате посочените мерки.
[32] Европейската комисия трябва периодично да преразглежда всички решения относно адекватното ниво на защита и да следи дали третите държави, които се ползват от решенията относно адекватното ниво на защита, продължават да гарантират адекватно ниво на защита (вж. член 45, параграф 3 и член 45, параграф 4 от ОРЗД). Освен това Съдът на ЕС може да обяви за недействителни решенията относно адекватното ниво на защита (вж. неговите решения по дела C-362/14 (Schrems I) и C-311/18 (Schrems II).

20. Решенията относно адекватното ниво на защита обаче не възпрепятстват субектите на данни да подадат жалба. Те не възпрепятстват и надзорните органи да сезират национален съд, ако се съмняват във валидността на дадено решение, така че националният съд може да отправи преюдициално запитване до Съда на ЕС, за да провери тази валидност[33].

Пример: Гражданин на ЕС, г-н Schrems, е подал жалба през юни 2013 г. в Ирландската комисия за защита на данните (КЗД) и е поискал от този надзорен орган да забрани или да спре предаването на негови лични данни от Facebook Ireland към Съединените щати, тъй като счита, че правото и практиката на Съединените щати не гарантират адекватна защита на личните данни, съхранявани на тяхна територия, срещу дейностите по наблюдение, извършвани там от публичните органи. Ирландската КЗД отхвърля жалбата, по-специално с довода, че в Решение 2000/520 Комисията е приела, че в рамките на т.нар. принцип „сфера на неприкосновеност на личния живот“ САЩ гарантират достатъчна степен на защита на предаваните лични данни (Решение относно сферата на неприкосновеност на личния живот). Г-н Schrems обжалва решението на КЗД и ирландският High Court (Висш съд на Ирландия) отправя до Съда на Европейския съюз (Съда на ЕС) въпрос относно валидността на Решение 2000/520. Впоследствие Съдът на ЕС реши да обяви за недействително Решение 2000/520 на Комисията относно адекватността на защитата, осигурявана от принципите за сферата на неприкосновеност на личния живот[34].

Инструменти за предаване съгласно член 46 от ОРЗД

21. В член 46 от ОРЗД са изброени редица инструменти за предаване, съдържащи *„подходящи гаранции“*, които износителите могат да използват, за да предават лични данни на трети държави при липса на решения относно адекватното ниво на защита. Основните видове инструменти за предаване на данни по член 46 от ОРЗД са:

- стандартни клаузи за защита на данните (СДК);
- задължителни фирмени правила (ЗФП);
- кодекси за поведение;
- механизми за сертифициране;
- ad hoc договорни клаузи.

22. Независимо от избрания от Вас инструмент за предаване на данни по член 46 от ОРЗД, Вие трябва да гарантирате, че като цяло предадените лични данни ще получат равностойно по същество ниво на защита.

[33] C-311/18 (Schrems II), точки 118—120. Надзорните органи нямат право да пренебрегват решение относно адекватното ниво на защита и да преустановяват или забраняват предаването на лични данни на такива държави, като се позовават единствено на недостатъчното ниво на защита. Те могат да упражняват правомощието си да преустановят или забранят предаването на лични данни на тази трета държава единствено на други основания (например поради недостатъчни мерки за сигурност в нарушение на член 32 от ОРЗД, липсата на правно основание, което валидно да подкрепя обработването на лични данни като такова, представляващо нарушение на член 6 от ОРЗД). Надзорните органи могат да проучат напълно независимо дали предаването на тези данни отговаря на изискванията, определени в ОРЗД, и, когато е приложимо, да сезират националните съдилища, за да могат, ако имат съмнения относно валидността на решението на Комисията относно адекватното ниво на защита, да отправят преюдициално запитване до Съда на Европейския съюз с цел проверка на неговата валидност.

[34] Дело C-362/14 (Schrems I).

23. В инструментите за предаване на данни съгласно член 46 от ОРЗД се съдържат главно подходящи гаранции от договорно естество, които могат да се прилагат при предаването на данни на всички трети държави. Ситуацията в третата страна, на която предавате данни, може все пак да изисква от Вас да допълните тези инструменти за предаване и съдържащите се в тях гаранции с допълнителни мерки („допълващи мерки“), за да се гарантира равностойно по същество ниво на защита[35].

Дерогации

24. Освен решенията относно адекватното ниво на защита и инструментите за предаване на данни по член 46 от ОРЗД, ОРЗД съдържа и трето средство, което позволява предаване на лични данни в определени ситуации. Като спазвате определени условия, можете да предадете лични данни въз основа на дерогация, посочена в член 49 от ОРЗД.

25. Член 49 от ОРЗД има изключителен характер. Дерогациите, които се съдържат в него, трябва да се тълкуват ограничително и да се отнасят главно за дейности по обработване, които засягат само отделни случаи и не се повтарят. ЕКЗД публикува своите Насоки 2/2018 относно дерогациите по член 49 съгласно Регламент (ЕО) № 2016/679. [36]

26. Преди да се позовете на дерогация по член 49 от ОРЗД, трябва да проверите дали предаването Ви отговаря на строгите условия, определени в посочената разпоредба за всяка от тях.

***

27. Ако Вашето предаване на данни не може да се основава нито на решение относно адекватното ниво на защита, нито на дерогация по член 49, трябва да продължите със стъпка 3.

2.3 Стъпка 3: Преценете дали инструментът за предаване на данни по член 46 от ОРЗД е ефективен с оглед на всички обстоятелства в процеса на предаването

28. Изборът на инструмент за предаване по член 46 от ОРЗД може да се окаже недостатъчен. Инструментът за предаване трябва да гарантира, че нивото на защита, осигурено от ОРЗД, не е засегнато от предаването[37]. С други думи, Вашият инструмент за предаване трябва да функционира по ефективен начин на практика.

29. „Ефективен“ означава, че предадените лични данни получават степен на защита в третата държава, която по същество е равностойна на гарантираната в ЕИП[38]. Случаят не е такъв, ако вносителят на данни е възпрепятстван да изпълни задълженията си съгласно избрания инструмент за предаване по член 46 от ОРЗД поради законодателството и практиките на третата държава, приложими към предаването.

30. Третата стъпка е да се прецени дали е налице фактор в правото или практиката на третата държава, който може да засегне ефективността на подходящите гаранции, осигурени в член 46 от ОРЗД по отношение на инструментите за предаване, на които разчитате, в контекста на конкретното предаване. Когато е целесъобразно, Вашият вносител на данни следва да Ви

[35] Дело C-311/18 (Schrems II), точки 130 и 133. Вж. също точка 2.3 по-долу.
[36] За допълнителни насоки по този въпрос вж. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_en.
[37] Член 44 от ОРЗД.
[38] Дело C-311/18 (Schrems II), точка 105 и втора констатация.

запознае със съответните източници и информация, свързани с третата държава, в която е установен, както и с приложимото към предаването законодателство. Можете да се позовете и на други източници на информация, например онези, които са изброени неизчерпателно в Приложение 3[39].

31. Когато извършвате преценка, следва да вземете предвид всички участници в предаването (например администратори, обработващи лични данни и подизпълнители, обработващи данни в третата държава), както са определени при картографирането на предаването. Колкото повече администратори, обработващи лични данни или вносители участват, толкова по-сложна ще бъде Вашата оценка. При тази оценка ще трябва също така да вземете под внимание всяко последващо предаване, което евентуално ще възникне.

32. За тази цел ще трябва да разгледате характеристиките на всяко Ваше предаване на данни и да определите как се прилага вътрешният правен ред на държавата, на която се предават (или предават впоследствие) данните.

33. Приложимият правен контекст ще зависи от обстоятелствата на предаването им, по-специално:

- Целите, за които се предават и обработват данните (например маркетинг, човешки ресурси, съхранение, ИТ поддръжка, клинични изпитвания);
- Видове субекти, участващи в обработването (публични/частни; администратор/обработващ данните);
- Сектор, в който се извършва предаването (например рекламни технологии, телекомуникации, финанси и др.);
- Категории предавани лични данни (например личните данни, свързани с деца, могат да попаднат в обхвата на специфично законодателство в третата държава);
- Дали данните ще се съхраняват в третата държава или ще има само дистанционен достъп до данните, съхранявани в ЕС/ЕИП;
- Формат на данните, които ще бъдат предавани (т.е. в обикновен текст/псевдонимизирани или криптирани[40]);
- Вероятност данните да подлежат на последващо предаване от третата държава на друга трета държава[41].

34. Като имате предвид приложимите закони ще трябва да прецените дали е налице засягане на ангажиментите, съдържащи се в избрания от Вас инструмент за предаване на данни по член 46 от ОРЗД. Трябва да проверите дали ангажиментите, които дават възможност на субектите на данни да упражняват правата си в контекста на международното предаване на данни (например искания за достъп, поправка и заличаване на предадени данни), могат да бъдат ефективно приложени на практика и не са възпрепятствани от правото в третата държава на местоназначение.

35. Ще трябва да направите оценка на съответните правила от общ характер, доколкото те влияят върху ефективното прилагане на гаранциите, съдържащи се в инструмента за предаване на данни по член 46 от ОРЗД, и основните права на физическите лица (по-специално правото на

[39] Вж. също точка 43 по-долу.

[40] Някои трети държави не разрешават вноса на криптирани данни.

[41] Когато администраторът е дал своето предварително конкретно или общо писмено разрешение в съответствие с член 28, параграф 2 от ОРЗД.

защита, предоставено на субекта на данните в случай на достъп на публични органи на трети държави до предаваните данни).

36. Във всеки случай трябва да обръщате специално внимание на съответните закони, и по-конкретно на законите, с които се определят изисквания за разкриване на лични данни пред публични органи или се предоставят правомощия на тези публични органи за достъп до лични данни (например за целите на наказателното правоприлагане, регулаторния надзор и националната сигурност). Ако тези изисквания или правомощия са ограничени до това, което е необходимо и пропорционално в едно демократично общество[42], те не могат да засегнат ангажиментите, съдържащи се в инструмента за предаване по член 46 от ОРЗД, на който разчитате.

37. Стандартите на ЕС, например членове 47 и 52 от Хартата на основните права на ЕС, трябва да се използват като отправна точка, за да се прецени дали този достъп на публичните органи е ограничен до това, което е необходимо и пропорционално в едно демократично общество, и дали субектите на данни разполагат с ефективни средства за правна защита.

38. При извършването на тази оценка от значение са и различните аспекти на правната система на тази трета държава, например елементите, изброени в член 45, параграф 2 от ОРЗД[43]. Например положението с принципите на правовата държава в трета държава може да бъде от значение за оценката на ефективността на наличните механизми, чрез които физическите лица могат да получат (съдебна) защита срещу незаконен достъп на правителството до лични данни. Съществуването на всеобхватен закон за защита на данните или независим орган за защита на данните, както и придържането към международни инструменти, в които се предвиждат гаранции за защита на данните, могат да допринесат за гарантиране на пропорционалността на намесата на правителствата[44].

***

39. В препоръките на ЕКЗД относно основните европейски гаранции (EEG) се съдържат елементи, които трябва да бъдат оценени, за да се определи дали правната рамка, уреждаща достъпа до лични данни от страна на публичните органи в трета държава, които са национални агенции за сигурност или правоприлагащи органи, може да се разглежда като оправдана намеса (и следователно като незасягаща ангажиментите, поети в инструмента за предаване на данни по член 46 от ОРЗД) или като неоправдана намеса. По-специално това следва да се разгледа внимателно, когато законодателството, уреждащо достъпа на публичните органи до данни, е двусмислено или не е публично достъпно.

[42] Вж. членове 47 и 52 от Хартата на основните права на ЕС, член 23, параграф 1 от ОРЗД и Препоръки 02/2020 на ЕКЗД относно европейските съществени гаранции за мерките за наблюдение, 10 ноември 2020 г., https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

[43] Дело C-311/18 (Schrems II), точка 104.

[44] Например: В Конвенция 108 (Конвенция за защита на лицата при автоматизираната обработка на лични данни, ETS № 108) или Конвенция № 108+ (осъвременена Конвенция за защита на лицата при обработката на лични данни, CETS № 223) се предвиждат приложими международни средства за правна защита в случай на нарушения на защитата на данните и с тях се допринася за осигуряване на минимално равнище на защита на личните данни и зачитане на личния живот.

40. Приложени към случая на предаване на данни въз основа на инструментите за предаване по член 46, препоръките на ЕКЗД относно основните европейски гаранции могат да насочват износителя на данни и вносителя на данни при оценката дали тези правомощия неоправдано засягат задълженията на вносителя на данни за гарантиране на равностойност по същество.

41. Липсата на равностойно по същество ниво на защита ще бъде особено явна, когато законодателството или практиката на третата държава, свързана с Вашето предаване, не отговаря на изискванията на европейските основни гаранции.

42. Вашата оценка трябва да се основава преди всичко на законодателството, което е публично достъпно. В някои ситуации обаче това няма да е достатъчно, тъй като може да липсва законодателство на третите държави по този въпрос. В този случай, ако все още желаете да планирате предаването, трябва да разгледате други важни и обективни фактори[45] и да не разчитате на субективни фактори, например вероятността публичните органи да имат достъп до Вашите данни по начин, който не е в съответствие със стандартите на ЕС. Тази оценка следва да извършите с дължимата грижа и да я документирате задълбочено, тъй като ще носите отговорност за решението, което можете да вземете на тази база[46].

43. Можете да допълните оценката си с информация, получена от други източници[47], например:

> - Елементи, доказващи, че орган на трета държава ще се стреми да получи достъп до данните със или без знанието на вносителя на данни, като се имат предвид докладваните прецеденти, законодателство и практика;
> - Елементи, доказващи, че орган на трета държава ще има достъп до данните чрез вносителя на данни или чрез пряко прихващане на канала за комуникация с оглед на докладваните прецеденти, законовите правомощия и техническите, финансовите и човешките ресурси, с които разполага.

44. В крайна сметка оценката Ви може да разкрие, че инструментът за предаване по член 46 от ОРЗД, на който разчитате, и подходящите гаранции, които той съдържа:

> - Гарантира по ефективен начин, че предадените лични данни получават степен на защита в третата държава, която по същество е равностойна на гарантираната в ЕИП. Законодателството и практиките на третата държава, приложими към предаването, дават възможност на вносителя на данни да изпълни задълженията си съгласно избрания инструмент за предаване. Вие следва да правите нови оценки на подходящи интервали от време или когато възникнат значителни промени (вж. стъпка 6).
> - Не гарантира по ефективен начин равностойно по същество ниво на защита. Вносителят на данни не може да изпълни задълженията си поради законодателството и/или практиките на третата държава, приложими към предаването. Съдът на ЕС подчерта, че когато инструментите за предаване на данни по член 46 от ОРЗД са недостатъчни, отговорност на износителя на данни е да въведе ефективни допълващи мерки или да не предава лични данни[48].

[45] Вж. точка 43 по-долу, както и Приложение 3.
[46] Член 5, параграф 2 от ОРЗД.
[47] Вж. също Приложение 3.
[48] Съд на ЕС, дело C-311/18 (Schrems II), точки 134—135.

Съдът на ЕС например постанови, че в член 702 от Закона на САЩ за наблюдение на чуждите разузнавателни служби (ЗНЧРС на САЩ) не се зачитат минималните гаранции, произтичащи от принципа на пропорционалност съгласно правото на ЕС, и не може да се счита за ограничен до строго необходимото. Това означава, че нивото на защита на програмите, разрешени от член 702 г. от ЗНЧРС, по същество не е равностойно на гаранциите, изисквани от правото на ЕС. В резултат на това, ако вносителят на данни или друг получател, пред който вносителят на данни може да разкрие данните, попада в обхвата на член 702 г. от ЗНЧРС[49], СДК или други инструменти за предаване по член 46 от ОРЗД, на него може да се разчита за такова предаване само ако допълващи технически мерки правят достъпа до предадените данни невъзможен или неефективен.

2.4 Стъпка 4: Приемане на допълващи мерки

45. Ако съгласно оценката Ви по стъпка 3 Вашият инструмент за предаване на данни по член 46 от ОРЗД не е ефективен, ще трябва да разгледате, когато е целесъобразно в сътрудничество с вносителя, дали съществуват допълващите мерки, които, ако бъдат добавени към гаранциите, съдържащи се в инструментите за предаване, биха могли да гарантират, че на предадените данни се осигурява в третата държава степен на защита, която по същество е равностойна на гарантираната в рамките на ЕС[50]. Съгласно определението „допълващите мерки“ допълват гаранциите, които инструментът за предаване на данни по член 46 от ОРЗД вече осигурява[51].

46. Когато използвате конкретен инструмент за предаване по член 46 от ОРЗД, трябва да определите за всеки отделен случай какви допълващи мерки биха могли да бъдат ефективни за набор от предавания на данни към конкретна трета държава. Ще можете да се основавате на предишните си оценки по стъпките (1, 2 и 3 по-горе) и да проверите въз основа на констатациите от оценките потенциалната ефективност на допълващите мерки, за да гарантирате необходимото ниво на защита.

47. По принцип допълващите мерки могат да имат договорен, технически или организационен характер. Съчетаването на различни мерки по начин, при който те взаимно се подкрепят и надграждат една друга, може да повиши нивото на защита и така да допринесе за постигането на стандартите на ЕС.

48. Само чрез договорните и организационните мерки по принцип няма да бъде преодолян достъпът до личните данни от страна на публичните органи на третата държава (когато това необосновано засяга задълженията на вносителя на данни за гарантиране на равностойност по същество). Действително ще има ситуации, при които само технически мерки биха могли да възпрепятстват или да направят неефективен достъпа на публичните органи в трети държави до

[49] Член 702 г. от ЗНЧРС е приложим, ако данните са получени „от или с помощта на доставчик на електронни съобщителни услуги“ (член 702 от ЗНЧРС = раздел 50 от Кодекса на САЩ, член 1881a, буква з), точка 2, (A), подточка vi), което от своя страна е определено в раздел 50 от Кодекса на САЩ, член 1881 параграф б), точка 4 като
„А) доставчик на телекомуникационни услуги, както е определен терминът в член 153 от дял 47;
Б) доставчик на електронни съобщителни услуги, както е определен терминът в член 2510 от дял 18;
В) доставчик на дистанционна изчислителна услуга, както е определен терминът в член 2711 от дял 18;
Г) всеки друг доставчик на съобщителни услуги, който има достъп до жични или електронни съобщителни услуги, независимо дали такива съобщения се предават или се съхраняват;
Д) длъжностно лице, служител или представител на субект, описан в букви А), Б), В) или Г).“
[50] Дело C-311/18 (Schrems II), точка 96.
[51] Съображение 109 от ОРЗД и дело C-311/18 (Schrems II), точка 133.

личните данни, по-специално за целите на наблюдението[52]. В такива ситуации договорните или организационните мерки могат да допълват техническите мерки и да укрепват общото равнище на защита на данните, например като създават пречки пред опитите на публичните органи да получат достъп до данни по начин, който не съответства на стандартите на ЕС.

49. Когато е целесъобразно, можете да разгледате, в сътрудничество с вносителя на данни, следния (неизчерпателен) списък с фактори, за да определите кои допълващи мерки биха били най-ефективни за защитата на предаваните данни:

- Формат на данните, които ще бъдат предавани (т.е. в обикновен текст/псевдонимизирани или криптирани);
- Естество на данните;
- Продължителност и сложност на работния процес при обработването на данни, брой на участниците в обработването и връзката между тях (например дали предаването включва множество администратори или едновременно администратори и обработващи лични данни, или участие на обработващи лични данни, които ще предават данните от Вас на Вашия вносител на данни (като се имат предвид съответните разпоредби, приложими за тях съгласно законодателството на третата държава на местоназначение)[53];
- Възможно е данните да бъдат предмет на последващо предаване в рамките на същата трета държава или дори на други трети държави (например участие на подизпълнители на вносителя на данни[54]).

Примери за допълващи мерки

50. Примери за технически, договорни и организационни мерки, които могат да бъдат обмислени, могат да бъдат намерени в неизчерпателните списъци, описани в Приложение 2.

***

51. Ако сте въвели ефективни допълващи мерки, които заедно с избрания от Вас инструмент за предаване на данни по член 46 от ОРЗД достигат ниво на защита, което понастоящем е равностойно по същество на равнището на защита, гарантирано в рамките на ЕИП: Вашето предаване може да бъде извършено.

[52] Когато този достъп надхвърля необходимото и пропорционалното в демократичното общество. Вж. членове 47 и 52 от Хартата на основните права на ЕС, член 23, параграф 1 от ОРЗД и Препоръки 02/2020 на ЕКЗД относно европейските съществени гаранции за мерките за наблюдение, 10 ноември 2020 г., https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en .

[53] В ОРЗД са определени отделни задължения за администраторите и за обработващите лични данни. Предаването на данни може да бъде от администратор към администратор, между съвместни администратори, от администратор към обработващ лични данни и, с разрешение от администратора, от обработващ лични данни до администратор или от обработващ лични данни до обработващ лични данни.

[54] Вж. бележка под линия 25.

52. Когато не можете да намерите или да приложите ефективни допълващи мерки, които да гарантират, че предадените лични данни се ползват с равностойно по същество ниво на защита[55], не трябва да започвате да предавате лични данни на съответната трета държава въз основа на инструмента за предаване по член 46 от ОРЗД, на който разчитате. Ако вече извършвате предаване, от Вас се изисква да преустановите или прекратите предаването на лични данни[56] . В съответствие с гаранциите, съдържащи се в инструмента за предаване на данни по член 46 от ОРЗД, данните, които вече сте предали на тази трета държава, и копията от тях следва да Ви бъдат върнати или унищожени изцяло от вносителя[57].

Пример: в правото на третата държава се забраняват допълващите мерки, които сте определили (например забранява се използването на криптиране), или по друг начин се възпрепятства тяхната ефективност. Не трябва да започвате да предавате лични данни към тази държава или трябва да преустановите текущото предаване към нея.

53. Ако решите да продължите предаването, независимо от факта, че вносителят не е в състояние да спази ангажиментите, поети по инструмента за предаване на данни по член 46 от ОРЗД, следва да уведомите компетентния надзорен орган съгласно конкретните разпоредби, въведени в съответния инструмент за предаване на данни по член 46 от ОРЗД[58]. Компетентният надзорен орган спира или забранява предаването на данни в случаите, когато установи, че не може да се гарантира равностойно по същество ниво на защита[59].

54. Компетентният надзорен орган може да наложи други корективни мерки (например глоба), ако въпреки факта, че не можете да докажете равностойно по същество ниво на защита в третата държава, започнете или продължите предаването.

2.5 Стъпка 5: Процедурни стъпки, ако сте набелязали ефективни допълващи мерки

55. Процедурните стъпки, които може да се наложи да следвате, в случай че сте определили ефективни допълващи мерки, които да бъдат въведени, може да се различават в зависимост от инструмента за предаване по член 46 от ОРЗД, който използвате или възнамерявате да използвате.

[55] Когато този достъп надхвърля необходимото и пропорционалното в демократичното общество. Вж. членове 47 и 52 от Хартата на основните права на ЕС, член 23, параграф 1 от ОРЗД и Препоръки 02/2020 на ЕКЗД относно европейските съществени гаранции за мерките за наблюдение, 10 ноември 2020 г., https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en .

[56] Дело C-311/18 (Schrems II), точка 135.

[57] Вж. клауза 12 в приложението към Решение 87/2010 относно СДК; вж. (незадължителната) клауза за допълнително прекратяване в Приложение Б SCC 2004/915/ЕО.

[58] Вж. ЕКЗД, Често задавани въпроси относно решението на Съда на Европейския съюз по дело C-311/18 — Data Protection Commissioner/Facebook Ireland Ltd и Maximillian Schrems, 23 юли 2020 г. и по-специално ЧЗД 5, 6 и 9. Вж. също клауза 4, буква ж) от Решение 2010/87/ЕС на Комисията; клауза 5, буква а) от Решение 2001/497/ЕО на Комисията и клауза II, буква в), „комплект II“ от приложението към Решение 2004/915/ЕО на Комисията.

[59] Дело C-311/18 (Schrems II), точки 113 и 121.

2.5.1 Стандартни клаузи за защита на данните („СДК“) (член 46, параграф 2, букви в) и г) от ОРЗД)

56. Когато възнамерявате да въвеждате допълващи мерки в допълнение към СДК, не е необходимо да искате разрешение от компетентния НО, за да добавите такива клаузи или допълнителни гаранции, стига установените допълващи мерки да не противоречат пряко или косвено на СДК и да са достатъчни, за да се гарантира, че нивото на защита, гарантирано от ОРЗД, не е застрашено[60]. Износителят на данни и вносителят на данни трябва да гарантират, че допълнителните клаузи не могат да се тълкуват по начин, по който да бъдат ограничени правата и задълженията в СДК, или по друг начин, за да бъде понижено нивото на защита на данните. Вие следва да сте в състояние да докажете това, включително недвусмисления характер на всички клаузи, в съответствие с принципа на отчетност и задължението си да осигурите достатъчна степен на защита на данните. Компетентните надзорни органи имат правомощия да преразглеждат тези допълнителни клаузи, когато това е необходимо (например в случай на жалба или разследване по собствена инициатива).

57. Когато възнамерявате да промените самите стандартни клаузи за защита на данните или когато добавените допълващи мерки „противоречат“ пряко или косвено на СДК, вече не се счита, че разчитате на стандартните договорни клаузи[61] и трябва да поискате разрешение от компетентния надзорен орган в съответствие с член 46, параграф 3, буква а) от ОРЗД.

2.5.2 ЗФП (член 46, параграф 2, буква б) от ОРЗД)

58. Мотивите, изложени в решението по делото Schrems II, се прилагат и за други инструменти за предаване на данни съгласно член 46, параграф 2 от ОРЗД, и тъй като всички тези инструменти имат основно договорен характер, то предвидените гаранции и поетите от страните ангажименти в тях не могат да обвързват публичните органи на трети държави[62].

59. Решението по делото Schrems II е от значение за предаването на лични данни въз основа на ЗФП, тъй като законите на трети държави могат да засегнат защитата, предоставяна от тези инструменти. Точното въздействие на решението по дело Schrems II върху ЗФП все още се обсъжда. ЕКЗД ще предостави във възможно най-кратък срок повече подробности за това дали

[60] Съображение 109 от ОРЗД гласи: „Възможността администраторът или обработващият лични данни да използва стандартни клаузи за защита на данните, приети от Комисията или от надзорен орган, не следва да възпрепятства администраторите или обработващите лични данни да включат стандартни клаузи за защита на данните в договор с по-голям обхват, като договор между обработващия лични данни и друг обработващ лични данни, нито да добавят други клаузи или допълнителни гаранции, при условие че същите не противоречат пряко или косвено на стандартните договорни клаузи, приети от Комисията или от надзорен орган, нито засягат основните права или свободи на субектите на данни.“ Подобни разпоредби са предвидени в редица СДК, приети от Европейската комисия съгласно Директива 95/45/ЕО.
[61] Вж. по аналогия Становище 17/2020 на ЕКЗД относно проекта на стандартни договорни клаузи, внесен от словенския надзорен орган (член 28, параграф 8 от ОРЗД), във връзка с вече приетите СДК по член 28, което съдържа подобна разпоредба („Освен това Комитетът припомня, че възможността за използване на приети от надзорен орган стандартни договорни клаузи не възпрепятства страните да добавят други клаузи или допълнителни гаранции, при условие че те не противоречат пряко или косвено на приетите стандартни договорни клаузи и не засягат основните права или свободи на субектите на данни. Освен това, ако стандартните клаузи за защита на данните бъдат изменени, вече няма да се счита, че страните са приложили приетите стандартни договорни клаузи“), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_202017_art28sccs_si_en.pdf.
[62] Съд на ЕС, C-311/18 (Schrems II), точка 132.

може да се наложи включването на допълнителни ангажименти в ЗФП в референтните документи WP256/257[63].

60. Съдът изтъква, че износителят на данни и вносителят на данни са длъжни да извършат оценка на спазването в съответната трета държава на изискването от правото на ЕС ниво на защита, за да установят дали предвидените в СДК или в ЗФП гаранции могат да бъдат спазени на практика. Ако това не е така, трябва да прецените дали можете да предвидите допълнителни мерки, за да осигурите ниво на защита, което по същество е равностойно на осигуреното в ЕИП, и дали правото или практиката на третата държава няма да засегне тези допълнителни мерки по начин, който нарушава ефективността им.

2.5.3 Ad hoc договорни клаузи (член 46.3, буква а) от ОРЗД)

61. Мотивите, изложени в решението по делото Schrems II, се прилагат и за други инструменти за предаване на данни съгласно член 46, параграф 2 от ОРЗД, и тъй като всички тези инструменти имат основно договорен характер, то предвидените гаранции и поетите от страните ангажименти в тях не могат да обвързват публичните органи на трети държави[64]. Ето защо решението по делото Schrems II е от значение за предаването на лични данни въз основа на ad hoc договорните клаузи, тъй като законите на трети държави могат да засегнат защитата, предоставяна от тези инструменти. Точното въздействие на решението по дело Schrems II върху ad hoc клаузите все още се обсъжда. ЕКЗД ще предостави повече подробности възможно най-скоро.

2.6 Стъпка 6: Преоценка на подходящи интервали от време

62. Трябва да следите постоянно, ако е необходимо в сътрудничество с вносителите на данни, промените в третата държава, на която сте предали лични данни, тъй като тези промени биха могли да повлияят на Вашата първоначална оценка на нивото на защита и на решенията, които евентуално сте взели по отношение на предаването на данни. Поддържането на отчетност е постоянно задължение (член 5, параграф 2 от ОРЗД).

63. Желателно е да въведете достатъчно стабилни механизми, за да се гарантира, че незабавно преустановявате или прекратявате предаване, когато:

- вносителят е нарушил или не е в състояние да изпълни ангажиментите, които е поел в инструмента за предаване по член 46 от ОРЗД;
- допълващите мерки вече не са ефективни в тази трета държава.

[63]Работна група по член 29, Работен документ за съставяне на таблица с елементите и принципите, които трябва да бъдат включени в задължителните фирмени правила, последно преработен и приет на 6 февруари 2018 г., WP 256 рев.01; Работна група по член 29, Работен документ за съставяне на таблица с елементите и принципите, които трябва да бъдат включени в задължителните фирмени правила, последно преработен и приет на 6 февруари 2018 г., WP 257 рев.01

[64] Съд на ЕС, C-311/18 (Schrems II), точка 132.

ЗАКЛЮЧЕНИЕ

64. В ОРЗД се определят правила относно обработването на лични данни в ЕИП и по този начин се дава възможност за свободно движение на лични данни в рамките на ЕИП. В глава V от ОРЗД се урежда предаването на лични данни към трети страни и се поставя високо изискване: предаването не трябва да подкопава нивото на защита на физическите лица, гарантирано от ОРЗД (член 44 от ОРЗД). В решението на Съда на ЕС по дело C-311/18 (Schrems II) се подчертава необходимостта да не се прекъсва нивото на защита, предоставено съгласно ОРЗД по отношение на личните данни, предавани на трета държава[65].

65. За да гарантирате еднакво по същество ниво на защита на Вашите данни, трябва преди всичко да сте внимателно запознати с предаването на Вашите данни. Трябва също така да се уверите, че данните, които предавате, са подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се предават и обработват в третата държава.

66. Трябва също така да идентифицирате инструмента за предаване, на който разчитате за предаването. Ако инструментът за предаване не включва решение относно адекватното ниво на защита, трябва да проверите във всеки отделен случай дали правото или практиката на третата държава на местоназначение не нарушава гаранциите, съдържащи се в инструмента за предаване на данни по член 46 от ОРЗД в контекста на Вашето предаване на данни. Когато инструментът за предаване на лични данни по член 46 от ОРЗД сам по себе си не осигурява по същество равностойно ниво на защита, то чрез допълващите мерки могат да бъдат отстранени пропуските.

67. Когато не можете да намерите или да приложите ефективни допълващи мерки, които да гарантират, че предадените лични данни се ползват с равностойно по същество ниво на защита, не трябва да започвате да предавате лични данни на съответната трета държава въз основа на избрания от Вас инструмент за предаване. Ако вече извършвате предаване, от Вас се изисква своевременно да преустановите или прекратите предаването на лични данни.

68. Компетентният надзорен орган има правомощието да спре или прекрати предаването на лични данни на трета държава, ако защитата на прехвърлените данни не е гарантирана съгласно правото на ЕС, по-специално по силата на членове 45 и 46 от ОРЗД и Хартата на основните права.

За Европейския комитет по защита на данните

Председател

(Андреа Йелинек)

[65] Дело C-311/18 (Schrems II), точка 93.

ПРИЛОЖЕНИЕ 1: ОПРЕДЕЛЕНИЯ

- „Трета държава“ означава всяка държава, която не е държава — членка на ЕИП.
- „ЕИП“ означава Европейското икономическо пространство и включва държавите — членки на Европейския съюз, и Исландия, Норвегия и Лихтенщайн. ОРЗД се прилага за последните по силата на Споразумението за ЕИП, по-специално Приложение XI към него и Протокол 37 към него.
- „ОРЗД“ означава Регламент (ЕС) № 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година 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).
- „Хартата“ означава Харта на основните права на Европейския съюз, ОВ C 326, 26.10.2012 г., стр. 391—407.
- „Съд на ЕС“ или „Съдът“ означава Съдът на Европейския съюз. Той е съдебният орган на Съюза и осигурява еднаквото прилагане и тълкуване на правото на Съюза в сътрудничество със съдилищата и юрисдикциите на държавите членки,.
- „Износител на данни“ означава администратор или обработващ лични данни в рамките на ЕИП, който предава лични данни на администратор или обработващ лични данни в трета държава.
- „Вносител на данни“ означава администратор или обработващ лични данни в трета държава, който получава или придобива достъп до лични данни, предавани от ЕИП.
- „Инструмент за предаване съгласно член 46 от ОРЗД“ означава подходящите гаранции съгласно член 46 от ОРЗД, които износителите на данни трябва да въведат при предаването на лични данни на трета държава, при липса на решение относно адекватното ниво на защита съгласно член 45, параграф 3 от ОРЗД. В член 46, параграфи 2 и 3 от ОРЗД се съдържа списъкът на инструментите за предаване на данни по член 46 от ОРЗД, които администраторите и обработващите лични данни могат да използват.
- „СДК“ означава стандартни клаузи за защита на данните (или „стандартни договорни клаузи“), приети от Европейската комисия за предаването на лични данни между администратори или обработващи лични данни в ЕИП и администратори или обработващи лични данни извън ЕИП. Стандартните договорни клаузи, приети от Европейската комисия, са инструмент за предаване на данни съгласно ОРЗД, според член 46, параграф 2, буква в) и параграф 5 от ОРЗД.

ПРИЛОЖЕНИЕ 2: ПРИМЕРИ ЗА ДОПЪЛВАЩИ МЕРКИ

69. Следните мерки са примери за допълващи мерки, които бихте могли да обмислите, когато достигнете стъпка 4 „Приемане на допълващи мерки“. Този списък не е изчерпателен. Изборът и прилагането на една или няколко от тези мерки няма непременно и систематично да гарантират, че Вашето предаване на данни отговаря на основния стандарт за гарантиране на равностойност по същество, изискван от законодателството на ЕС. Трябва да изберете такива допълващи мерки, които могат ефективно да гарантират това ниво на защита за Вашето предаване.

70. Всяка допълваща мярка може да се счита за ефективна по смисъла на решението на Съда на ЕС по делото „Schrems II“ само ако и доколкото с нея се отстраняват конкретните недостатъци, установени във Вашата оценка на правното положение в третата държава. Ако в крайна сметка не можете да гарантирате равностойно по същество ниво на защита, не трябва да предавате личните данни.

71. Като администратор или обработващ лични данни от Вас вече може да се изисква да прилагате някои от мерките, описани в настоящото приложение, дори ако Вашият вносител на данни е обхванат от решение относно адекватното ниво на защита, като е възможно от Вас да се изисква да ги прилагате, когато обработвате данни в рамките на ЕИП[66].

Технически мерки

72. В настоящия раздел са описани по неизчерпателен начин примери за технически мерки, които могат да допълват гаранциите, посочени в член 46 от ОРЗД, за да се гарантира спазването на нивото на защита, изисквано съгласно правото на ЕС в контекста на предаването на лични данни на трета държава. Тези мерки ще бъдат особено необходими, когато правото на тази държава налага на вносителя на данни задължения, които противоречат на гаранциите, предвидени в член 46 от ОРЗД, и по-специално могат да засегнат договорната гаранция за равностойно по същество ниво на защита срещу достъп на публичните органи на тази трета държава до тези данни[67].

73. За по-голяма яснота в този раздел първо се посочват техническите мерки, които биха могли да бъдат ефективни при определени сценарии/случаи на използване, за да се гарантира по същество равностойно ниво на защита. Разделът продължава с някои сценарии/случаи на употреба, при които не могат да бъдат намерени технически мерки за гарантиране на такова ниво на защита.

Сценарии, при които *могат* да бъдат намерени ефективни мерки

74. Мерките, изброени по-долу, имат за цел да се гарантира, че достъпът до предаваните данни от страна на публичните органи в трети държави не засяга ефективността на подходящите гаранции, съдържащи се в инструментите за предаване на данни по член 46 от ОРЗД. Тези мерки

[66] Член 5 , параграф 2 от ОРЗД, член 32 от ОРЗД.
[67] Дело C-311/18 (Schrems II), точка 135.

се прилагат дори ако достъпът на публичните органи е в съответствие с правото на държавата на вносителя, когато този достъп надхвърля необходимото и пропорционалното в едно демократично общество[68]. Тези мерки имат за цел да не се допусне възможността за нарушаване на достъпа, като органите бъдат възпрепятствани да идентифицират субектите на данни, да извличат информация за тях, да ги разграничават в друг контекст или да свързват предадените данни с други набори от данни, които могат да съдържат, наред с други данни, онлайн идентификатори, осигурени от устройствата, приложенията, инструментите и протоколите, използвани от субектите на данни в друг контекст.

75. Публичните органи в трети държави могат да се стремят да получат достъп до предадените данни

a) При транзитно преминаване чрез достъп до линиите за комуникация, използвани за предаване на данните на държавата получател. Този достъп може да бъде пасивен, като в този случай съдържанието на съобщението, евентуално след процес на подбор, просто се копира. Достъпът обаче може да бъде активен, в смисъл че публичните органи се намесват в процеса на предаване на съобщението не само чрез прочитане на съдържанието, но и чрез манипулиране или потискане на части от него.

b) Докато се държат от предвидения получател на данните — чрез получаване на достъп до самите средства за обработка или чрез изискване от получателя на данните да установи местонахождението и да извлече данните, които представляват интерес, и да ги предаде на органите.

76. В настоящия раздел се разглеждат сценарии, при които се прилагат мерки, които са ефективни и в двата случая. Могат да се прилагат различни допълващи мерки и те да бъдат достатъчни в конкретния случай на предаване, ако в правото на държавата получател се предвижда само един вид достъп. Поради това е необходимо износителят на данни да анализира внимателно, с подкрепата на вносителя на данни, задълженията, наложени на вносителя.

Например вносителите на данни от САЩ, които попадат в обхвата на раздел 50 от Кодекса на САЩ, член 1881a (FISA 702), имат пряко задължение да предоставят достъп до внесени лични данни или да предадат внесени лични данни, които притежават, съхраняват или контролират. Това задължение може да обхваща всички криптографски ключове, необходими за осигуряване на разбираемостта на данните.

77. В сценариите се описват конкретните обстоятелства и предприетите мерки. Различните промени в сценариите могат да доведат до различни заключения.

78. Администраторите могат да бъдат задължени да прилагат някои или всички мерки, описани тук, независимо от степента на защита, осигурена в законодателството, приложимо за вносителя на данни, тъй като тези мерки са необходими за спазване на членове 25 и 32 от ОРЗД при конкретните обстоятелства на предаването. С други думи, от износителите може да се изисква да прилагат мерките, описани в настоящия документ, дори ако техните вносители на данни са обхванати от решение относно адекватното ниво на защита, точно както администраторите и обработващите лични данни могат да бъдат задължени да ги прилагат, когато данните се обработват в рамките на ЕИП.

[68] Вж. членове 47 и 52 от Хартата на основните права на ЕС, член 23, параграф 1 от ОРЗД и Препоръките на ЕКЗД относно европейските съществени гаранции за мерките за наблюдение.

Случай на употреба 1: Съхранение на данни за резервни копия и други цели, за които не се изисква достъп до данните в чист вид

79. Износителят на данни използва доставчик на хостинг услуги в трета държава, за да съхранява лични данни, например с цел създаване на резервни копия.

Ако

1. личните данни се обработват чрез силно криптиране преди предаването,
2. алгоритъмът за криптиране и неговата параметризация (например дължина на ключа, режим на работа, ако е приложимо) съответстват на съвременното техническо равнище и могат да се считат за надеждни срещу криптоанализ, извършен от публичните органи в държавата получател, като се вземат предвид ресурсите и техническите възможности (например изчислителна мощност за посрещане на атаки с груба сила), с които разполагат,
3. в силата на криптирането се отчита конкретният период от време, през който трябва да се запази поверителността на криптираните лични данни,
4. алгоритъмът за криптиране се прилага безпогрешно чрез правилно поддържан софтуер, чието съответствие със спецификацията на избрания алгоритъм е проверено, например чрез сертифициране,
5. ключовете се управляват по надежден начин (те се генерират, администрират, съхраняват, ако е приложимо, във връзка със самоличността на предвидения получател, и се отменят), и
6. ключовете се пазят единствено под контрола на износителя на данни или на други субекти, натоварени с тази задача, които пребивават в ЕИП или в трета държава, на територията или в един или повече определени сектори на трета държава, или в международна организация, за която Комисията е установила в съответствие с член 45 от ОРЗД, че е осигурено адекватно ниво на защита,

тогава ЕКЗД счита, че извършеното криптиране представлява ефективна допълваща мярка.

Случай на употреба 2: Предаване на псевдонимизирани данни

80. Износителят на данни първо псевдонимизира данните, които притежава, и след това ги предава на трета държава за анализ, например за изследователски цели.

Ако

1. износителят на данни предава лични данни, които са обработени така, че вече не могат да бъдат свързани с конкретен субект на данни, нито да се използват за идентифициране на субекта на данни в по-голяма група, без да се използва допълнителна информация[69],
2. тази допълнителна информация се държи изключително от износителя на данни и се съхранява отделно в държава членка или в трета държава, на територията или в един или повече определени сектори на трета държава, или в международна организация, за която Комисията е установила в съответствие с член 45 от ОРЗД, че е осигурено адекватно ниво на защита,

[69] В съответствие с член 4, параграф 5 от ОРЗД: „псевдонимизация“ означава обработването на лични данни по такъв начин, че личните данни не могат повече да бъдат свързвани с конкретен субект на данни, без да се използва допълнителна информация, при условие че тя се съхранява отделно и е предмет на технически и организационни мерки с цел да се гарантира, че личните данни не са свързани с идентифицирано физическо лице или с физическо лице, което може да бъде идентифицирано“.

3. разкриването или неразрешеното използване на тази допълнителна информация се предотвратява чрез подходящи технически и организационни гаранции, като се гарантира, че износителят на данни запазва едноличен контрол върху алгоритъма или регистъра, който дава възможност за повторна идентификация чрез използване на допълнителната информация, и
4. администраторът е установил чрез задълбочен анализ на въпросните данни, като е взел предвид всяка информация, с която публичните органи на държавата получател може да разполагат, че псевдонимизираните лични данни не могат да бъдат приписани на идентифицирано или подлежащо на идентификация физическо лице, дори ако са съпоставени с такава информация,

тогава ЕКЗД счита, че извършеното псевдонимизиране представлява ефективна допълваща мярка.

81. Следва да се отбележи, че в много случаи факторите, които са специфични за физическата, физиологичната, генетичната, психическата, икономическата, културната или социалната идентичност на дадено физическо лице, неговото физическо местоположение или взаимодействието му с интернет услуга в определени моменти във времето[70], могат да позволят идентифицирането на това лице, дори ако неговото име, адрес или други обикновени данни за идентификация са пропуснати.

82. Това е особено вярно, когато данните се отнасят до използването на информационни услуги (време на достъп, последователност на елементите, до които е получен достъп, характеристики на използваното устройство и т.н.). Както и при вносителя на лични данни, по отношение на тези услуги може да има задължение да се предостави достъп на същите публични органи в тяхната юрисдикция, като те вероятно ще притежават данни за използването на тези информационни услуги от лицето (лицата), към което (които) са насочени.

83. Освен това, като се има предвид, че използването на някои информационни услуги е публично по своя характер или че те могат да бъдат експлоатирани от страни със значителни ресурси, администраторите трябва да бъдат по-внимателни, като се има предвид, че публичните органи в тяхната юрисдикция вероятно притежават данни за използването на информационни услуги от лице, към което са насочени.

Случай на употреба 3: Криптирани данни, които само преминават транзитно през трети държави

84. Износителят на данни желае да предаде данни до местоназначение, което е признато като предоставящо адекватно ниво на защита в съответствие с член 45 от ОРЗД. Данните се насочват през трета държава.

[70] Член 4, параграф 1 от ОРЗД: „лични данни“ означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице;“.

Ако

1. износителят на данни предава лични данни на вносител на данни в юрисдикция, осигуряваща адекватна защита, данните се пренасят по интернет и данните могат да бъдат географски маршрутизирани през трета държава, която не осигурява равностойно по същество ниво на защита,
2. използва се транзитно криптиране на транспортно равнище, по отношение на което се гарантира, че използваните протоколи за криптиране са съвременни и осигуряват ефективна защита срещу активни и пасивни атаки с ресурси, за които е известно, че са достъпни за публичните органи на третата държава,
3. декриптиране може да се извърши само извън въпросната трета държава,
4. страните, участващи в комуникацията, се споразумяват да използват надежден орган или инфраструктура за сертифициране на публичен ключ,
5. се използват специфични защитни и най-съвременни мерки срещу активни и пасивни атаки срещу транзитно криптиране на транспортно равнище,
6. в случай че транзитното криптиране на транспортно равнище само по себе си не осигурява подходяща сигурност поради наличието на уязвимост на инфраструктурата или използвания софтуер, личните данни също се криптират „от край до край“ на нивото на приложението, като се използват най-съвременни методи за криптиране,
7. алгоритъмът за криптиране и неговата параметризация (например дължина на ключа, режим на работа, ако е приложимо) съответстват на съвременното техническо равнище и могат да се считат за надеждни срещу криптоанализ, извършен от публичните органи в транзитната държава, като се вземат предвид ресурсите и техническите възможности (например изчислителна мощност за посрещане на атаки с груба сила), с които разполагат,
8. в силата на криптирането се отчита конкретният период от време, през който трябва да се запази поверителността на криптираните лични данни,
9. алгоритъмът за криптиране се прилага безпогрешно чрез правилно поддържан софтуер, чието съответствие със спецификацията на избрания алгоритъм е проверено, например чрез сертифициране,
10. изключено е наличието на задни вратички (в хардуер или софтуер),
11. ключовете се управляват по надежден начин (те се генерират, администрират, съхраняват, ако е приложимо, във връзка със самоличността на предвидения получател, и се отменят) от износителя или от субект, на когато износителят има доверие в юрисдикция, предлагаща по същество равностойно ниво на защита,

тогава ЕКЗД счита, че транзитното криптиране на транспортно равнище, ако е необходимо в съчетание с криптиране на съдържание от край до край, представлява ефективна допълваща мярка.

Случай на употреба 4: Защитен получател

85. Износителят на данни предава лични данни на вносител на данни в трета държава, които са специално защитени от правото на тази държава, например с цел съвместно предоставяне на медицинско лечение на пациент или правни услуги на клиент.

Ако

1. правото на трета държава освобождава местен вносител на данни от потенциално нарушаване на достъпа до данни, съхранявани от този получател за дадената цел, например по силата на задължение за опазване на професионалната тайна, което се прилага по отношение на вносителя на данни,
2. това освобождаване обхваща цялата информация, с която разполага вносителят на данни, която може да се използва за заобикаляне на защитата на привилегирована информация (криптографски ключове, пароли, други данни за самоличност и др.),
3. вносителят на данни не използва услугите на обработващ лични данни по начин, който позволява на публичните органи да получат достъп до данните, съхранявани от обработващия лични данни, нито пък вносителят на данни препраща данните на друг субект, който не е защитен, въз основа на инструментите за предаване на данни по член 46 от ОРЗД,
4. личните данни са криптирани преди предаването им по метод, съответстващ на съвременното техническо равнище, който гарантира, че няма да бъде възможно декриптиране без да се познава ключът за декриптиране (криптиране от край до край) за целия период от време, през който данните трябва да бъдат защитени,
5. ключът за декриптиране се съхранява единствено от вносителя на защитени данни и е защитен по подходящ начин срещу неразрешено използване или разкриване посредством технически и организационни мерки, съобразени с достиженията на техническия прогрес, и
6. износителят на данни е установил по надежден начин, че ключът за криптиране, който възнамерява да използва, съответства на ключа за декриптиране, с който разполага получателят,

тогава ЕКЗД счита, че извършеното транзитно криптиране на транспортно равнище представлява ефективна допълваща мярка.

Случай на употреба 5: Разделена обработка или обработка от няколко страни

86. Износителят на данни желае личните данни да бъдат обработвани съвместно от двама или повече независими обработващи лични данни, намиращи се в различни юрисдикции, без да им бъде разкрито съдържанието на данните. Преди предаването той разделя данните така, че никоя част, която отделният обработващ лични данни получава, да не е достатъчна за цялостното или частичното възстановяване на личните данни. Износителят на данни получава резултата от обработката от всеки от обработващите лични данни отделно и обединява получените части, за да се постигне крайният резултат, който може да представлява лични или обобщени данни.

Ако

1. износител на данни обработва лични данни по начин, при който те се разделят на две или повече части, всяка от които не може вече да се тълкува или приписва на конкретен субект на данни, без да се използва допълнителна информация,
2. всяка от частите се предава на отделен обработващ лични данни, който се намира в различна юрисдикция,
3. обработващите лични данни могат да изберат да обработват данните съвместно, например като използват сигурни изчисления, включващи множество страни по начин, по който на никой от тях не се разкрива информация, която те не притежават преди изчислението,
4. алгоритъмът, използван за споделеното изчисление, е защитен срещу активни злонамерени страни,

5. няма доказателства за сътрудничество между публичните органи, намиращи се в юрисдикциите, в които се намира всеки от обработващите лични данни, което би им позволило достъп до всички набори от лични данни, съхранявани от обработващите лични данни, както и да възстановят и използват съдържанието на личните данни в ясна форма при обстоятелства, при които това използване не би било съобразено със същността на основните права и свободи на субектите на данни. По същия начин публичните органи на която и да е държава не следва да имат правомощия да получават достъп до лични данни, съхранявани от обработващите лични данни във всички съответни юрисдикции.
6. администраторът е установил чрез задълбочен анализ на въпросните данни, като е взел предвид всяка информация, с която публичните органи на държавите получатели може да разполагат, че частите от лични данни, които той предава на обработващите лични данни, не могат да бъдат приписани на идентифицирано или подлежащо на идентификация физическо лице, дори ако са съпоставени с такава информация,

тогава ЕКЗД счита, че извършената разделена обработка представлява ефективна допълваща мярка.

Сценарии, при които *не могат* да бъдат намерени ефективни мерки

87. Описаните по-долу мерки при определени сценарии не биха били ефективни за осигуряване на равностойно по същество ниво на защита на данните, предавани на трета държава. Ето защо те не биха могли да се квалифицират като допълващи мерки.

Случай на употреба 6: Предаване към доставчици на компютърни услуги в облак или други обработващи лични данни, които се нуждаят от достъп до данните в чист вид

88. Износителят на данни използва доставчик на услуги в облак или друг обработващ лични данни, за да могат личните данни да бъдат обработвани в съответствие с неговите инструкции в трета държава.

Ако

1. администратор предава данни на доставчик на услуги в облак или на друг обработващ лични данни,
2. доставчикът на услуги в облак или друг обработващ лични данни се нуждае от достъп до данните в чист вид, за да изпълни възложената задача, и
3. правомощията, предоставени на публичните органи в държавата получател за достъп до предадените данни, излизат от рамките на това, което е необходимо и пропорционално в едно демократично общество[71],

тогава, като се има предвид съвременното технологично равнище, ЕКЗД не е в състояние да предвиди ефективна техническа мярка за предотвратяване на нарушаването на правата на субектите на данни. ЕКЗД не изключва възможността в резултат на по-нататъшното технологично

[71] Вж. членове 47 и 52 от Хартата на основните права на ЕС, член 23, параграф 1 от ОРЗД и Препоръките на ЕКЗД относно европейските съществени гаранции за мерките за наблюдение.

развитие да бъдат осигурени мерки, с които да бъдат постигнати планираните стопански цели, без да се изисква достъп до данни в чист вид.

89. При дадените сценарии, когато некриптираните лични данни са технически необходими за предоставянето на услугата от обработващия лични данни, транзитното криптиране на транспортно равнище и криптирането на данни в покой, дори взети заедно, не представляват допълваща мярка, която гарантира равностойно по същество ниво на защита, ако вносителят на данни притежава криптографските ключове.

Случай на употреба 7: Дистанционен достъп до данни за стопански цели

90. Износителят на данни предоставя лични данни на субекти в трета държава, за да се използват за споделени стопански цели. Обичайната конфигурация може да се състои от администратор или обработващ лични данни, установен на територията на държава членка, който предава лични данни на администратор или обработващ лични данни в трета държава, принадлежащ към същата група предприятия или група предприятия, извършващи съвместна икономическа дейност. Вносителят на данни може например да използва данните, които получава, за да предоставя услуги за персонала на износителя на данни, за които се нуждае от данни за човешки ресурси, или да общува по телефона или електронната поща с клиенти на износителя на данни, които живеят в Европейския съюз.

Ако

1. износителят на данни предава лични данни на вносител на данни в трета държава, като ги предоставя в широко използвана информационна система по начин, който му осигурява пряк достъп до данни по негов избор, или като ги предава пряко, индивидуално или в насипно състояние, чрез използване на комуникационна услуга,
2. вносителят използва данните за свои собствени цели,
3. правомощията, предоставени на публичните органи в държавата получател за достъп до предадените данни, излизат извън рамките на това, което е необходимо и пропорционално в едно демократично общество,

тогава ЕКЗД не може да предвиди ефективна техническа мярка, с която да бъде предотвратено нарушаването на правата на субектите на данни.

91. При дадените сценарии, когато некриптираните лични данни са технически необходими за предоставянето на услугата от обработващия лични данни, транзитното криптиране на транспортно равнище и криптирането на данни в покой, дори взети заедно, не представляват допълваща мярка, която гарантира равностойно по същество ниво на защита, ако вносителят на данни притежава криптографските ключове.

Допълнителни договорни мерки

92. Тези мерки обикновено се състоят от едностранни, двустранни или многостранни [72] договорни ангажименти[73] . Ако се използва инструмент за предаване на данни по член 46 от ОРЗД, в повечето случаи той вече ще съдържа редица (предимно договорни) ангажименти за износителя на данни и вносителя на данни, които имат за цел да послужат като гаранции за личните данни[74].

93. В някои случаи тези мерки могат да допълнят и укрепят гаранциите, които инструментът за предаване и съответното законодателство на третата държава могат да предоставят, когато, като се вземат предвид обстоятелствата по предаването, те не отговарят на всички условия, необходими за осигуряване на ниво на защита, което по същество е равностойно на гарантираното в рамките на ЕС. Като се има предвид естеството на договорните мерки, които по принцип не обвързват органите на тази трета държава, когато те не са страна по договора[75], тези мерки следва да бъдат съчетани с други технически и организационни мерки, за да се осигури необходимото ниво на защита на данните. Изборът и прилагането на една или няколко от тези мерки няма непременно и систематично да гарантират, че Вашето предаване на данни отговаря на основния стандарт за гарантиране на равностойност по същество, изискван от законодателството на ЕС.

94. В зависимост от това какви договорни мерки са включени вече в инструмента за предаване на данни по член 46 от ОРЗД, на който се разчита, допълнителните договорни мерки също могат да бъдат полезни, за да могат установените в ЕИП износители на данни да се запознаят с новостите, засягащи защитата на данните, предавани на трети държави.

95. Както беше посочено, с договорните мерки не се изключва прилагането на законодателството на трета държава, което не отговаря на стандарта за европейските основни гаранции на ЕКЗД, в случаите, когато законодателството задължава вносителите да спазват заповедите за разкриване на данни, които получават от публичните органи[76].

96. Някои примери за тези потенциални договорни мерки са изброени по-долу и са класифицирани в съответствие с тяхното естество:

[72] Например в рамките на ЗФП, които при всички случаи следва да регулират някои от мерките, изброени по-долу.

[73] Те ще имат частен характер и няма да се считат за международни споразумения съгласно международното публично право. Освен това те обикновено не са обвързващи за публичните органи на третата държава, които не са страни по договора, когато е сключен с частни организации в трети държави, както подчертава Съдът в решението си по дело C-311/18 (Schrems II), точка 125.

[74] Вж. решение C-311/18 (Schrems II), точка 137, в което Съдът призна, че СДК съдържа *„ефективни механизми, позволяващи на практика да се осигури спазването на изискването от правото на Съюза ниво на защита и предаването на лични данни, основаващо се на такива клаузи, да бъде спряно или забранено в случай на нарушение на тези клаузи или при невъзможност за спазването им“* (вж. също точка 148).

[75] Дело C-311/18 (Schrems II), точка 125.

[76] Решение на Съда на ЕС по дело C-311/18 (Schrems II), точка 132.

Предвиждане на договорно задължение за използване на специфични технически мерки

97. ***В зависимост от конкретните обстоятелства на предаването, в договора може да се наложи да се посочи, че за осъществяването на предаването ще бъде необходимо въвеждането на специални технически мерки (вж. по-горе предложените технически мерки).***

98. ***Условия за ефективност:***

- Тази клауза би могла да бъде ефективна в ситуации, при които износителят е установил необходимост от технически мерки. В такъв случай трябва да се предвиди в правна форма, че вносителят също се ангажира да въведе необходимите технически мерки, ако е необходимо.

Задължения за прозрачност:

99. ***Износителят може да добави приложения към договора с информация, която вносителят би предоставил, като положи максимални усилия, по отношение на достъпа на публичните органи до данни, включително в областта на разузнаването, при условие че законодателството е в съответствие с европейските съществени гаранции на ЕКЗД в държавата по местоназначение. Това може да помогне на износителя на данни да изпълни задължението си да документира своята оценка за нивото на защита в третата държава.***

100. Вносителят може да бъде задължен например:

(1) да посочи законовите и подзаконовите разпоредби в държавата по местоназначение, приложими за него или неговите подизпълнители, които биха позволили достъп на публичните органи до личните данни, които подлежат на предаване, по-специално в областта на разузнаването, правоприлагането, административния и регулаторния надзор, приложим към предадените данни;

(2) при липсата на закони, уреждащи достъпа на публичните органи до данни, да предостави информация и статистически данни въз основа на своя опит или доклади от различни източници (например партньори, отворени източници, национална съдебна практика и решения на надзорни органи) относно достъпа на публичните органи до лични данни в конкретни случаи на предаване на данни (т.е. в конкретната регулаторна област; относно типа на субектите, към които принадлежи вносител;...)

(3) да посочи какви мерки са предприети за предотвратяване на достъпа до предадените данни (ако има такива);

(4) да предостави достатъчно подробна информация относно всички искания за достъп до лични данни от страна на публичните органи, които е получил през определен период от време[77], по-специално в областите, посочени в точка 1 по-горе, които включват информация за получените искания, исканите данни, органа, подаващ искането, и

[77] Продължителността на периода следва да зависи от риска за правата и свободите на субектите на данни, чиито данни са предмет на въпросното предаване — например последната година преди закриването на инструмента за износ на данни при износителя на данни.

правното основание за разкриване, както и до каква степен вносителят е оповестил искането за данни[78];

(5) да посочи дали и до каква степен на вносителя е законно забранено да предоставя информацията, посочена в точки 1—5 по-горе.

101. Тази информация може да бъде предоставена чрез структурирани въпросници, които вносителят следва да попълни и подпише, както и да бъде допълнена от договорното задължение вносителят да декларира в рамките на определен период от време всяка евентуална промяна в тази информация, каквато е настоящата практика при процедурите за надлежна проверка.

102. ***Условия за ефективност:***

- Вносителят трябва да е в състояние да предостави на износителя тези видове информация, доколкото му е известна и след като е положил всички усилия за получаването ѝ[79].

- Това задължение, наложено на вносителя, е средство да се гарантира, че износителят е запознат с рисковете, свързани с предаването на данни на трета държава. По този начин износителят ще може да откаже да сключи договора или, ако информацията се промени след сключването му, да изпълни задължението си да спре предаването и/или да прекрати договора, ако правото на третата държава, използваните гаранции, съдържащи се в инструмента за предаване по член 46 от ОРЗД, и всички допълнителни гаранции, които евентуално е приел, вече не могат да осигурят ниво на защита, което по същество е равностойно на това в ЕС. Това задължение обаче не може да оправдае разкриването на лични данни от страна на вносителя, нито да породи очакването, че няма да има допълнителни искания за достъп.

***

103. ***Износителят би могъл също така да добави клаузи, в които се изисква вносителят да удостовери, че (1) не е създал целенасочено задни врати или подобни програми, които биха могли да се използват за достъп до системата и/или личните данни, (2) че не е създал или изменил целенасочено своите бизнес процеси по начин, който улеснява достъпа до лични данни или системи, и (3) че националното законодателство или правителствената политика не изисква вносителят да създава или поддържа задни врати или да улеснява достъпа до лични данни или системи, или да притежава или предава ключа за криптиране[80].***

[78] Спазването на това задължение само по себе си не е равнозначно на предоставяне на подходящо ниво на защита. В същото време всяко неподходящо оповестяване, което действително е осъществено, води до необходимостта от прилагане на допълващи мерки.

[79] Вж. точка 32.5 по-горе.

[80] Тази клауза е важна, за да се гарантира адекватно ниво на защита на предаваните лични данни, и обикновено следва да се изисква наличието ѝ.

104. ***Условия за ефективност:***

- Съществуването на законодателство или държавни политики, които не позволяват на вносителите да разкриват тази информация, може да направи тази клауза неефективна. Ето защо вносителят няма да може да сключи договора или ще трябва да уведоми износителя за невъзможността си да продължи да спазва договорните си задължения[81].
- В договора трябва да се посочват санкции и/или възможността на износителя да прекрати договора с кратко предизвестие в случаите, когато вносителят не разкрие наличието на задна вратичка или подобна програмна схема, или манипулирани бизнес процеси, или изискване за изпълнение на някое от тях, или не информира своевременно износителя след като узнае за съществуването им.

***

105. ***Износителят би могъл да засили правомощията си да извършва одити[82] или проверки на оборудването на вносителя за обработването на данни, на място и/или от разстояние, да проверява дали данните са били разкрити пред публичните органи и при какви условия (достъп, който не надхвърля това, което е необходимо и пропорционално в едно демократично общество), например чрез осигуряване на кратко предизвестие и механизми за бърза намеса на контролните органи и засилване на автономността на износителя при подбора на контролните органи.***

106. ***Условия за ефективност:***

- За да бъде напълно ефективен, одитът следва да обхваща от правна и техническа гледна точка всяко обработване на личните данни, предадени в третата държава, извършвано от обработващите лични данни или подизпълнителите на вносителя.
- Записите за достъпа и други подобни следи е желателно да бъдат защитени срещу подправяне, така че одиторите да могат да намерят доказателства за разкриване. В записите за достъпа и други подобни следи следва също да се прави разграничение между достъп в резултат на редовни работни операции, и достъп, дължащ се на нареждания или искания за достъп.

***

107. ***Когато правото и практиката на третата държава на вносителя първоначално са били оценени и се е считало, че осигуряват по същество равностойно ниво на защита, както е предвидено в ЕС за предаваните от износителя данни, износителят все пак би могъл да направи по-строго задължението на вносителя на данни да информира своевременно износителя на данни за невъзможността си да изпълни договорните задължения и в резултат на това да спази изисквания стандарт за „равностойно по същество ниво на защита на данните“.[83]..***

[81] Вж. точка 32.5 по-горе.

[82] Вж. например клауза 5, буква е) от СДК между администраторите и обработващите лични данни (Решение № 2010/87/ЕС), одитите могат да се извършват и в рамките на кодекс за поведение или чрез сертифициране.

[83] Клауза 5, буква а) и буква г), подточка i) от Решение № 2010/87/ЕС.

108. Тази невъзможност за спазване може да се дължи на промени в законодателството или практиката на третата държава[84]. В клаузите биха могли да бъдат определени конкретни и строги срокове и процедури за бързото спиране на предаването на данни и/или прекратяването на договора и връщането или заличаването на получените данни от вносителя. Проследяването на получените искания, техният обхват и ефективността на приетите мерки срещу тях следва да осигуряват на износителя достатъчно данни, за да изпълни задължението си за спиране или прекратяване на предаването и/или прекратяване на договора.

109. ***Условия за ефективност:***

- Уведомяването трябва да се извърши преди да бъде предоставен достъп до данните. В противен случай към момента, в който износителят получи уведомлението, правата на физическото лице може вече да са били нарушени, ако искането се основава на закони на тази трета държава, които надхвърлят това, което е допустимо съгласно нивото на защита на данните според правото на ЕС. Уведомлението може все пак да послужи за предотвратяване на бъдещи нарушения и да позволи на износителя да изпълни задължението си да спре предаването на лични данни на третата държава и/или да прекрати договора.
- Вносителят на данни трябва да наблюдава всички промени в правото или в политиката, които биха могли да го направят неспособен да изпълнява задълженията си, и своевременно да информира износителя на данни за всякакви такива промени и развития и, ако е възможно, преди тяхното прилагане, за да може износителят на данни да получи обратно данните от вносителя на данни.
- В клаузите следва да е предвиден бързодействащ механизъм, чрез който износителят на данни разрешава на вносителя на данни да осигури своевременно сигурността на данните или да ги върне на износителя на данни, или ако това не е осъществимо, да изтрие или да криптира по сигурен начин данните, без непременно да изчаква инструкциите на износителя, ако е спазен конкретен праг, договорен между износителя на данни и вносителя на данни. Вносителят следва да прилага този механизъм от самото начало на предаването на данни и да го проверява редовно, за да се увери, че той може да се приложи в кратък срок.
- В други клаузи на износителя може да се предостави възможност да наблюдава спазването на тези задължения от страна на вносителя чрез одити, проверки и други мерки за проверка и да ги прилага със санкции по отношение на вносителя и/или възможността на износителя да спре предаването и/или незабавно да прекрати договора.

***

[84] Вж. C-311/18 (Schrems II), точка 139, в която Съдът заявява, че *„макар същата клауза 5, буква г), подточка i) да позволява на получателя на лични данни в случай на законодателство, което му налага забрана, като например наказателноправна забрана за разкриване на информация с цел запазване на тайната на разследване от страна на правоприлагащ орган, да не съобщава на установения в Съюза администратор правнообвързващо искане за разкриване на личните данни от правоприлагащ орган, той все пак е длъжен в съответствие с клауза 5, буква а) от приложението към решението СК да информира администратора за невъзможността си да осигури съответствие със стандартните клаузи за защита на данните.“*

110. ***Доколкото това се допуска от националното право на третата държава, в договора могат да бъдат засилени задълженията на вносителя за осигуряване на прозрачност, като се предвиди метод на „Warrant Canary“, при който вносителят се задължава редовно да публикува (например най-малко на всеки 24 часа) криптографично подписано съобщение, с което да информира износителя, че към определена дата и час не е получил нареждане за разкриване на лични данни или друго подобно. Липсата на актуализация на това уведомление ще покаже на износителя, че вносителят вероятно е получил поръчка.***

111. ***Условия за ефективност:***

- Разпоредбите на третата държава трябва да позволяват на вносителя на данни да издаде тази такъв формуляр за пасивно уведомяване на износителя.
- Износителят на данни трябва автоматично да наблюдава уведомленията от типа Warrant Canary.
- Вносителят на данни трябва да гарантира, че неговият частен ключ за подписване на уведомление Warrant Canary се съхранява по сигурен начин и че не може да бъде принуден да издава фалшиви уведомления Warrant Canary по силата на разпоредбите на третата държава. За тази цел вносителят може да използва, ако са необходими, няколко подписа от различни лица и/или ако уведомлението Warrant Canary е издадено от лице извън юрисдикцията на третата държава.

Задължения за предприемане на конкретни действия

112. ***Вносителят може да се ангажира да преразгледа, съгласно законодателството на държавата по местоназначение, законността на всяко нареждане за разкриване на данни, по-специално дали то е в рамките на правомощията, предоставени на отправилия искането публичен орган, и да оспори нареждането, ако след внимателна оценка стигне до заключението, че съгласно законодателството на държавата по местоназначение са налице основания за това. Когато оспорва нареждане, вносителят на данни следва да поиска временни мерки за спиране на действието на нареждането, докато съдът не се произнесе по същество. Вносителят ще бъде задължен да не разкрива исканите лични данни, докато това не бъде изискано съгласно приложимите процедурни правила. Вносителят на данни ще се ангажира също така да предостави минимално допустимото количество информация, когато отговаря на нареждането, въз основа на разумното му тълкуване***

113. ***Условия за ефективност:***

- Правният ред на третата държава трябва да осигурява правни възможности за ефективно оспорване на нарежданията за разкриване на данни.
- В тази клауза винаги ще се предлага много ограничена допълнителна защита, тъй като нареждането за разкриване на данни може да бъде законно съгласно правния ред на третата държава, но този правен ред може да не отговаря на стандартите на ЕС. Тази договорна мярка задължително ще трябва да допълва други допълващи мерки.
- Оспорването на заповедите трябва да има суспензивно действие съгласно правото на третата държава. В противен случай публичните органи ще продължат да имат достъп до данните на физическите лица и всяко последващо действие в полза на лицето би

ограничило възможността му да предяви иск за обезщетение за отрицателни последици, произтичащи от разкриването на данни.

- Вносителят ще трябва да може да документира и да докаже пред износителя действията, които е предприел, като полага максимални усилия, за да изпълни този ангажимент.

***

114. ***В ситуацията, описана по-горе, вносителят може да се ангажира да информира отправилия искането публичен орган за несъвместимостта на нареждането с гаранциите, съдържащи се в инструмента за предаване на данни по член 46 от ОРЗД[85], и за произтичащия от това конфликт на задължения за вносителя. Вносителят уведомява едновременно и възможно най-бързо износителя и/или компетентния надзорен орган от ЕИП, доколкото това е възможно съгласно правния ред на третата държава.***

115. ***Условия за ефективност:***

- Тази информация относно защитата, предоставена от правото на ЕС, и конфликта на задължения следва да има някои правни последици в правния ред на третата държава, като съдебен или административен контрол върху нареждането или искането за достъп, изискването за съдебна заповед и/или временното спиране на изпълнението на заповедта, за да се добави известна защита на данните.
- Правната система на държавата не трябва да възпрепятства вносителя да уведоми износителя или поне компетентния надзорен орган от ЕИП за полученото нареждане или искане за достъп.
- Вносителят ще трябва да може да документира и да докаже пред износителя действията, които е предприел, като полага максимални усилия, за да изпълни този ангажимент.

Оправомощаване на субектите на данни да упражняват правата си

116. ***В договора може да бъде предвидено, че достъп до личните данни, предавани под формата на обикновен текст в хода на обичайната стопанска дейност (включително в съпътстващи случаи), може да се осъществява само с изричното или мълчаливото съгласие на износителя и/или субекта на данните.***

117. ***Условия за ефективност:***

- Тази клауза би могла да бъде ефективна в ситуации, в които вносителите получават искания от публични органи да си сътрудничат на доброволна основа, за разлика

[85] В СДК се предвижда например, че обработването на данни, включително предаването им, се е извършвало и ще продължи да се извършва в съответствие с *„приложимото право за защита на данните“*. Това право се определя като *„законодателството, защитаващо основните права и свободи на лицата, и по-специално правото на личен живот при обработването на лични данни, приложимо към администратор на данни в държавата членка, в която е установен износителят на данни“.* Съдът на ЕС потвърждава, че разпоредбите на ОРЗД, тълкувани в светлината на Хартата на основните права на ЕС, са част от това законодателство, вж. Съд на ЕС C-311/18 (Schrems II), точка 138.

например от достъпа на публичните органи до данни, който се осъществява без знанието на вносителя на данни или против неговата воля.

- В някои ситуации субектът на данни може да не е в състояние да се противопостави на достъпа или да даде съгласие, което отговаря на всички условия, определени в правото на ЕС (свободно изразено, конкретно, информирано и недвусмислено) (например в случай на служители)[86].

- В националните разпоредби или политики, с които вносителят се задължава да не разкрива нареждането за достъп, тази клауза може да бъде обезсилена, освен ако не е подкрепена с технически методи, които изискват намесата на износителя или на субекта на данни, за да могат данните под формата на обикновен текст да бъдат достъпни. Такива технически мерки за ограничаване на достъпа могат да бъдат предвидени по-специално, ако достъпът се предоставя само при специфични случаи на подкрепа или услуги, но самите данни се съхраняват в ЕИП.

***

118. ***Чрез договора вносителят и/или износителят може да бъде задължен да уведоми своевременно субекта на данните за искането или нареждането, получено от публичните органи на третата държава, или за невъзможността на вносителя да спази договорните задължения, за да се даде възможност на субекта на данни да потърси информация и ефективна правна защита (например чрез подаване на иск до неговия компетентен надзорен орган и/или съдебен орган и да докаже своята процесуална легитимация пред съдилищата на третата държава).***

119. ***Условия за ефективност:***

- С това уведомление субектът на данните може да бъде уведомен за потенциален достъп на публични органи в трети държави до неговите данни. След като го получи, субектът на данните има възможност да потърси допълнителна информация от износителите и да подаде иск до своя компетентен надзорен орган. С тази клауза би могло да бъде намерено решение на някои от трудностите, с които дадено лице може да се сблъска при доказването на своята процесуална легитимация *(locus standi)* пред съдилищата на трети държави, за да оспори достъпа на публичните органи до неговите данни.

- Националните разпоредби и политики могат да възпрепятстват това уведомяване на субекта на данните. Въпреки това износителят и вносителят биха могли да се ангажират да информират субекта на данните веднага след отмяната на ограниченията за разкриване на данни и да положат всички усилия, за да бъдат освободени от забраната за разкриване. Като минимум износителят или компетентният надзорен орган може да уведоми субекта на данните за спирането или прекратяването на предаването на неговите лични данни поради невъзможността на вносителя да спази договорните си задължения вследствие на получаването на искане за достъп.

***

[86] Член 4, параграф 11 от ОРЗД.

120. ***Договорът може да задължи износителя и вносителя да съдействат на субекта на данни при упражняването на правата му в юрисдикцията на третата държава чрез ad hoc механизми за правна защита и правни консултации.***

121. ***Условия за ефективност***

- В националните разпоредби и политики могат да се определят условия, които е възможно да намалят ефективността на предвидените ad hoc механизми за правна защита.
- Правните консултации биха могли да бъдат от полза за субекта на данни, особено като се има предвид колко сложно и скъпо е за субекта на данни да разбира правната система на трета държава и да извършва правни действия от чужбина, евентуално на чужд език. Тази клауза обаче винаги ще предлага ограничена допълнителна защита, тъй като предоставянето на помощ и правни консултации на субектите на данни само по себе си не може да отстрани неуспеха на правния ред на трета държава да осигури ниво на защита, което по същество е равностойно на гарантираното в рамките на ЕС. Тази договорна мярка задължително ще трябва да допълва други допълващи мерки.

Тази допълнителна мярка би била ефективна само при условие че правото на третата държава предвижда правна защита пред нейните национални съдилища или че съществува ad hoc механизъм за правна защита. Във всеки случай обаче това не би било ефективна допълнителна мярка срещу мерките за наблюдение, ако не съществува механизъм за правна защита.

Организационни мерки

122. Допълнителните организационни мерки могат да включват вътрешни политики, организационни методи и стандарти, които администраторите и обработващите лични данни могат да прилагат за себе си и да налагат на вносителите на данни в трети държави. Те могат да допринесат за осигуряване на последователност в защитата на личните данни по време на пълния цикъл на обработването. Организационните мерки могат също така да подобрят осведомеността на износителите относно риска и опитите за получаване на достъп до данните в трети държави, както и способността им да реагират на тях. Изборът и прилагането на една или няколко от тези мерки няма непременно и систематично да гарантират, че Вашето предаване на данни отговаря на основния стандарт за гарантиране на равностойност по същество, изискван от законодателството на ЕС. В зависимост от конкретните обстоятелства на предаването и оценката, извършена въз основа на законодателството на третата държава, са необходими организационни мерки за допълване на договорните и/или техническите мерки, за да се гарантира ниво на защита на личните данни, което по същество е равностойно на гарантираното в рамките на ЕС.

123. Оценката на най-подходящите мерки трябва да се извършва за всеки отделен случай, като се има предвид необходимостта администраторите и обработващите лични данни да спазват принципа на отчетност. По-долу ЕКЗД изброява някои примери за организационни мерки, които износителите могат да прилагат, въпреки че списъкът не е изчерпателен, а други мерки също могат да бъдат подходящи:

Вътрешни политики за управление на предаванията, особено по отношение на групи от предприятия

124. ***Приемане на подходящи вътрешни политики с ясно разпределение на отговорностите за предаване на данни, канали за докладване и стандартни оперативни процедури за случаи на скрити или официални искания от публични органи за достъп до данните. Особено в случай на предаване на данни между групи предприятия, тези политики могат да включват, наред с другото, назначаването на специален екип, който следва да бъде установен в ЕИП, да се състои от експерти по законодателството в областта на информационните технологии, защитата на данните и неприкосновеността на личния живот, който да разглежда искания, които включват лични данни, предавани от ЕС; уведомяването на висшето юридическо и корпоративно ръководство и на износителя на данни при получаване на такива искания; процедурните стъпки за оспорване на непропорционални или незаконни искания и предоставяне на прозрачна информация на субектите на данни.***

125. Разработване на специални процедури за обучение на персонала, отговарящ за управлението на исканията за достъп до лични данни от публични органи, които следва да се актуализират периодично, за да отразяват новите законодателни и съдебни развития в третата държава и в ЕИП. Процедурите за обучение следва да включват изискванията на правото на ЕС по отношение на достъпа на публичните органи до лични данни, по-специално съгласно член 52, параграф 1 от Хартата на основните права. Осведомеността на персонала следва да се повиши по-специално чрез оценка на практически примери за искания на публичните органи за достъп до данни и чрез прилагане на стандарта съгласно член 52, параграф 1 от Хартата на основните права към такива практически примери. Това обучение следва да отчита конкретното положение на вносителя на данни, например законодателството и разпоредбите на третата държава, на която е подчинен вносителят на данни, и следва да бъде разработено, когато е възможно, в сътрудничество с износителя на данни.

126. ***Условия за ефективност:***

- Тези политики могат да бъдат предвидени само в случаите, когато искането от страна на публичните органи в третата държава е съвместимо с правото на ЕС[87]. Когато искането е несъвместимо, тези политики не няма да са достатъчни, за да се гарантира равностойно ниво на защита на личните данни, и, както беше посочено по-горе, предаването на данни трябва да бъде спряно или да бъдат въведени подходящи допълващи мерки, за да бъде избегнат достъпът.

Мерки за прозрачност и отчетност

127. ***Документиране и записване на получените от публичните органи искания за достъп и предоставения отговор, заедно с правната обосновка и участниците (напр. ако износителят е бил уведомен и неговият отговор, оценката на екипа, отговарящ за разглеждането на тези искания, и т.н.). Тези записи следва да се предоставят на износителя на данни, който от своя страна следва да ги предостави на съответните субекти на данни, когато това е необходимо.***

[87] Вж. дело C-362/14 (Schrems I), точка 94; C-311/18 (Schrems II), точки 168, 174, 175 и 176.

128. ***Условия за ефективност:***

- В националното законодателство на третата държава може да не се допуска разкриването на исканията или на съществена информация за тях и така тази практика да бъде направена неефективна. Вносителят на данни следва да информира износителя за невъзможността да предостави такива документи и записи и така да му предложи възможност да спре предаването на данни, ако тази невъзможност би довела до понижаване на нивото на защита.

***

129. ***Редовно публикуване на доклади или резюмета за прозрачност във връзка с искания на държавни органи за достъп до данни и вида на предоставения отговор, доколкото публикуването е разрешено от местното законодателство.***

130. ***Условия за ефективност:***

- Предоставената информация следва да бъде уместна, ясна и възможно най-подробна. В националното законодателство на третата държава може да не се допуска разкриването на подробна информация. В тези случаи вносителят на данни следва да положи максимални усилия, за да публикува статистическа информация или подобен вид обобщена информация.

Организационни методи и мерки за свеждане на данните до минимум

131. ***Полезни в контекста на предаване на данни могат да бъдат и вече съществуващите организационни изисквания съгласно принципа на отчетност, като приемането на стриктен и подробен достъп до данни и политики за поверителност и най-добри практики, стриктно основани на принципа „необходимост да се знае“, наблюдавани чрез редовни одити и прилагани чрез дисциплинарни мерки. В това отношение следва да се обмисли свеждането на данните до минимум, за да се ограничи излагането на лични данни на неразрешен достъп. В някои случаи може да не е необходимо например да се предават определени данни (например в случай на дистанционен достъп до данни на ЕИП, както при случаи на подкрепа, когато се предоставя ограничен вместо пълен достъп, или когато предоставянето само на услуга изисква предаване на ограничен набор от данни, а не на цяла база данни).***

132. ***Условия за ефективност:***

- За да се наблюдава и налага спазването на мерките за свеждане на данните до минимум и в контекста на предаването, следва да бъдат въведени редовни одити и строги дисциплинарни мерки.
- Износителят на данни извършва оценка на личните данни, с които разполага, преди да се осъществи предаването, за да установи кои набори от данни не са необходими за целите на предаването и следователно няма да бъдат споделяни с вносителя на данни.
- Мерките за свеждане на данните до минимум следва да бъдат придружени от технически мерки, за да се гарантира, че данните не са обект на неразрешен достъп. Например прилагането на механизми за сигурни изчисления, включващи множество страни, и разпространението на криптирани набори от данни сред различни доверени

субекти могат да послужат за предотвратяване на ситуации, при които всеки едностранен достъп води до разкриване на данни, които могат да бъдат идентифицирани.

***

133. ***Разработване на най-добри практики с цел подходящо и навременно включване и предоставяне на достъп до информация на длъжностното лице по защита на данните, ако има такова, както и на правните служби и службите за вътрешен одит, по въпроси, свързани с международното предаване на лични данни.***

134. ***Условия за ефективност:***

- Длъжностното лице по защита на данните, ако има такова, и правният екип, както и екипът за вътрешен одит, получават цялата необходима информация преди предаването и с тях се прави консултация относно необходимостта от предаването и допълнителните гаранции, ако има такива.
- Съответната информация следва да включва например оценка на необходимостта от предаване на конкретните лични данни, преглед на приложимото законодателство на третата държава и гаранциите, които вносителят се е задължил да прилага.

Приемане на стандарти и най-добри практики

135. ***Приемане на строги политики в областта на сигурността и неприкосновеността на данните, основани на сертифициране от ЕС или кодекси за поведение, или на международни стандарти (например нормите на ISO) и най-добри практики (например Агенцията на Европейския съюз за киберсигурност (ENISA), като се взема предвид съвременното технологично равнище, в съответствие с риска, свързан с категориите обработвани данни, и вероятността публичните органи да получат достъп до тях.***

Други

136. ***Приемане и редовен преглед на вътрешните политики, за да се оцени пригодността на приложените допълващи мерки и да се набележат и приложат допълнителни или алтернативни решения, когато е необходимо, за да се гарантира, че се поддържа ниво на защита на предадените лични данни, равностойно на гарантираното в рамките на ЕС.***

***

137. ***Ангажименти от страна на вносителя на данни да не се пристъпва към по-нататъшно предаване на лични данни в рамките на същата или друга трета държава или да бъде спряно текущото предаване на данни, когато в третата държава не може да бъде гарантирано ниво на защита на личните данни, равностойно на осигуреното в ЕС[88].***

[88] Дело C-311/18 (Schrems II), точки 135 и 137.

ПРИЛОЖЕНИЕ 3: ВЪЗМОЖНИ ИЗТОЧНИЦИ НА ИНФОРМАЦИЯ ЗА ОЦЕНКА НА ТРЕТА ДЪРЖАВА

138. Вашият вносител на данни следва да бъде в състояние да Ви предостави съответните източници и информация, свързани с третата държава, в която е установен, и приложимото законодателство. Можете да се позовете и на няколко източника на информация, например онези, които не са изброени изчерпателно по-долу:

- Съдебната практика на Съда на Европейския съюз (Съда на ЕС) и на Европейския съд по правата на човека (ЕСПЧ)[89], посочена в препоръките относно европейските съществени гаранции[90];
- Решения относно адекватното ниво на защита в държавата по местоназначение, ако предаването се базира на различно правно основание[91];
- Резолюции и доклади от междуправителствени организации като Съвета на Европа[92], други регионални органи[93] и органи и агенции на ООН (например Съвет на ООН по правата на човека[94], Комитет по правата на човека[95]);
- Национална съдебна практика или решения, взети от независими съдебни или административни органи, компетентни в областта на неприкосновеността на данните и защитата на данните на трети държави;
- Доклади от академични институции и организации на гражданското общество (напр. НПО и търговски сдружения).

[89] Вж. фактологична справка за съдебната практика на ЕСПЧ относно масовото наблюдение: https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf

[90] https://www.coe.int/en/web/data-protection/reports-studies-and-opinions

[91] C-311/18 (Schrems II), точка 141; вж. решения относно адекватното ниво на защита https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[92] https://www.coe.int/en/web/data-protection/reports-studies-and-opinions

[93] Вж. например докладите по държави на Междуамериканската комисия по правата на човека (IACHR), https://www.oas.org/en/iachr/reports/country.asp.

[94] Вж. https://www.ohchr.org/EN/HRBodies/UPR/Pages/Documentation.aspx

[95] Вж.: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=5