

Препоръки



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

Версия 2.0

Приети на 18 юни 2021 г.

История на версиите

Версия 2.0	18 юни 2021 г.	Приемане на препоръките след обществени консултации
Версия 1.0	10 ноември 2020 г.	Приемане на препоръките за обществена консултация

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 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 трансфер, който може да гарантира равностойно по същество равнище на защита на данните, предавани чрез договор на трети държави.

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 трансфер 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. Същевременно, Съдът подчертава, 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 тях 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 предоставят личните данни, за да се гарантира, че са обект на равностойно по същество ниво на защита, независимо от мястото, където се обработват. Трябва също да се уверите, че данните, които предавате, са подходящи, актуални и ограничени до необходимото за целите, за които се обработват.

Втората стъпка е да се **провери инструментът за предаване, от който зависи трансфера**, 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 това решение остава валидно. При липса на решение относно адекватното ниво на защита трябва да разчитате на един от инструментите за предаване, изброени в член 46 от ОРЗД. Само в някои случаи можете да се позовете на една от дерогациите, предвидени в член 49

от ОРЗД, ако отговаряте на условията. Дерогациите на практика не следва да се превръщат в „правило“, а трябва да се ограничават до конкретни ситуации.

Третата стъпка е да се **прецени** дали има нещо в действащото право и/или практики на третата държава, което може да засегне ефективността на подходящите гаранции по отношение на инструментите за предаване, на които разчитате, при конкретния трансфер. Вашата оценка следва да бъде съсредоточена преди всичко и най-вече върху законодателството на трети държави, което има отношение към вашето предоставяне и върху инструмента за предаване по член 46 от ОРЗД, на който разчитате. Проучването и на практиките на публичните органи на трети държави ще ви позволи да проверите дали гаранциите, съдържащи се в инструмента за трансфер, могат на практика да гарантират ефективна защита на предадените лични данни. Изследването на тези практики ще е от особено значение за оценката ви в случаите, когато:

(i.) законодателството на третата държава, която формално отговаря на стандартите на ЕС, очевидно не се прилага/спазва на практика;

(ii.) са налице практики, които са несъвместими с ангажиментите, съдържащи се в инструментите за предаване, когато в третата държава липсва съответното законодателство;

(iii.) вашите предадени данни и/или вносителят попадат или могат да попадат в обхвата на проблемно законодателство (напр. да засегнат съдържащата се в инструмента за трансфер договорна гаранция за равностойно по същество ниво на защита и да не отговарят на стандартите на ЕС за основните права, необходимостта и пропорционалността).

В първите два случая ще трябва да спрете предаването или да приложите адекватни допълнителни мерки, ако желаете да продължите с него.

В третия случай, предвид рисковете, свързани с потенциалното прилагане на проблемно законодателство при вашия трансфер, може да решите да: спрете предаването, да приложите допълнителни мерки, за да продължите с него, или евентуално да решите да продължите с трансфера, без да прилагате допълнителни мерки, ако считате и можете да докажете и документирате, че нямате никакви основания за тълкуването и/или прилагането на практика на съответното и проблемно законодателство по отношение на вашите предадени данни и вносител.

За преценката 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.

Тази оценка следва да извършите с дължимата грижа и да я документирате задълбочено. Вашите компетентни надзорни и/или съдебни органи е възможно да поискат такава оценка и да ви държат отговорни за всяко решение, което 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 използвате при 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 при трансфера, както и с оглед на правото и практиките на третата държава и инструмента за предаване, на който разчитате, тъй като ще носите отговорност за всяко решение, което вземете на тази база. Може да е необходимо също 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 преценка 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 допълнителната ви мярка, в зависимост от инструмента за предаване по член 46 от ОРЗД, на който разчитате. Някои формалности са уточнени в настоящите препоръки. Може да е необходимо да се консултирате с компетентните надзорни органи относно някои от тях.

Шестата и последна стъпка е да се направи **преоценка** през подходящи интервали на нивото на защита на личните данни, които предавате на трети държани, 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. Органите за защита на данните 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.

Компетентните 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

Съдържание	6
1 Отчетност при предаването на данни	9
2 Пътна карта: прилагане на принципа на отчетност при практическото предаване на данни 10	
2.1 Стъпка 1: Бъдете запознати с предаването на данни, което извършвате	10
2.2 Стъпка 2: Определяне на инструментите за предаване, на които разчитате	12
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 трансфер.....	15
2.4 Стъпка 4: Приемане на допълващи мерки	23
2.5 Стъпка 5: Процедурни стъпки, ако сте набелязали ефективни допълващи мерки	26
2.6 Стъпка 6: Преоценка на подходящи интервали от време	28
3 Заключение	28
ПРИЛОЖЕНИЕ 1: ОПРЕДЕЛЕНИЯ	30
ПРИЛОЖЕНИЕ 2: ПРИМЕРИ ЗА ДОПЪЛВАЩИ МЕРКИ	31
Технически мерки.....	31
2.2 Допълнителни договорни мерки	41
2.3 Организационни мерки	50
ПРИЛОЖЕНИЕ 3: ВЪЗМОЖНИ ИЗТОЧНИЦИ НА ИНФОРМАЦИЯ ЗА ОЦЕНКА на трета държава....	54

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 Правилник за дейността,

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 съюз².

(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 държава³.

(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 използват⁴.

(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 клаузи⁵.

(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 държава⁶.

(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 ЕКЗД⁷.

ПРИЕ СЛЕДНАТА ПРЕПОРЪКА:

⁴ Дело С-311/18 (Schrems II), точки 132 и 133.

⁵ Дело С-311/18 (Schrems II), точка 134.

⁶ Дело С-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 право⁸. 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 хора⁹. 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 пропорционалност¹⁰.
2. При пренасянето им до трети държави извън ЕИП данните трябва да получават ниво на защита, което по същество е равностойно на осигуреното в рамките на ЕС, за да се гарантира, че се спазва нивото на защита, заложено в ОРЗД, както по време на предаването, така и след него.
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 право¹¹. 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 да могат да докажат тези усилия пред субектите на данни и пред надзорните органи за защита на данните. Това е т.нар. принцип на отчетност¹².
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 държави¹³, тъй като само по себе си то представлява форма на обработване на данни¹⁴. 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 Хартата¹⁵.
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

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, правоприменик 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., Maximilian 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.

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, включени в съответния договор между износителя и вносителя¹⁶. 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 вносителя¹⁷. Тези отговорности са прилагане на принципа на ОРЗД за отчетност при предаването на данни¹⁸.

2 ПЪТНА КАРТА: ПРИЛАГАНЕ НА ПРИНЦИПА НА ОТЧЕТНОСТ ПРИ ПРАКТИЧЕСКОТО ПРЕДАВАНЕ НА ДАННИ

6. Следва пътна карта на стъпките, които трябва да предприемете, за да разберете дали вие (износителят на данни) трябва да въведете 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 данни¹⁹, 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 органи²⁰. 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*²¹.
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 поискване²².

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 осъществите ново предаване на лични данни²³, първата стъпка е да се уверите, че сте напълно запознати с предоставянето на данни (знаете какви

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 Следователно не се стичате за износител на данни, ако например сте субект на данни, който чрез онлайн анкета предоставя личните си данни на администратор на данни, установен в трета държава.

²⁰ 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

²¹ 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

²² Член 5, параграф 2 от ОРЗД и член 24, параграф 1 от ОРЗД.

²³ Имайте предвид, че дистанционният достъп на субект от трета държава до данни, намиращи се в ЕИП, също се счита за предаване.

данни предавате). Регистрирането и картографирането на всеки трансфер може да бъде сложен процес за субектите, участващи в многобройно, разнообразно и редовно предаване на трети държави и използващи множество обработващи лични данни и подизпълнители. Познаването на предаваните данни е важна първа стъпка за изпълнението на задълженията ви съгласно принципа на отчетност.

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 ОРЗД²⁴. 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 ОРЗД²⁵.
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, предоставят личните данни, които сте им поверили, на подизпълнител в друга трета държава или в същата трета държава²⁶.
11. С оглед на спазването на принципа от ОРЗД за „свеждане на данните до минимум“²⁷ трябва да се уверите, че данните, които предавате, са подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват.
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 трансфер на данни: трябва да знаете къде могат да се намират или обработват от вносителите личните данни, които сте изнесли (карта на местоназначенията).
13. Обърнете внимание, че достъп от разстояние от трета държава (напр. в ситуации на техническа поддръжка) и/или съхранението в предложен от доставчик на услуги облак,

²⁴ 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.).

²⁵ 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 трансфера на данни.

²⁶ Когато администраторът е дал своето предварително конкретно или общо писмено разрешение в съответствие с член 28, параграф 2 от ОРЗД.

²⁷ Член 5, параграф 1, буква в) от ОРЗД.

намиращ се извън ЕИП, също се счита за предаване²⁸. 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 е установен в ЕИП и ясно е посочил в договора си, че данните изобщо няма да бъдат обработвани в трети държави.

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 данни²⁹.
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 (напр. в един сектор)³⁰.
18. Европейската комисия публикува списъка на своите решения относно адекватното ниво на защита на данните на своя уебсайт³¹.
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**³². Въпреки това трябва да следите дали решенията относно адекватното ниво на защита, които са от значение за вашето предаване, са отменени или обявени за недействителни³³.

²⁸ 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.

²⁹ 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.

³⁰ Член 45, параграф 1 от ОРЗД.

³¹ https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

³² При условие че вие и вносителят на данни сте въвели мерки за спазване на другите задължения съгласно ОРЗД, в противен случай прилагате посочените мерки.

³³ 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

20. Същевременно решенията относно адекватното ниво на защита 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 валидност³⁴.

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 живот³⁵.

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 трансфер на данни по член 46 от ОРЗД са:

- стандартни договорни клаузи за защита на данните (СДК);
- задължителни фирмени правила (ЗФП);
- кодекси за поведение;

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)).

³⁴ 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 (напр. 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.

³⁵ Дело C-362/14 (Schrems I).

- механизми за сертифициране;
 - специфични договорни клаузи.
22. Независимо от избора от вас инструмент за предаване на данни по член 46 от ОРЗД, трябва да гарантирате, че предадените лични данни ще се ползват с равностойно по същество ниво на защита.
23. В инструментите за трансфер 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 защита³⁶.

Дерогации

24. Освен решенията относно адекватното ниво на защита и инструментите за предаване на данни по член 46 от ОРЗД, в ОРЗД се съдържа и трето средство, което позволява трансфер 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. Съдържащите се в него дерогации трябва да се тълкуват по начин, който не противоречи на самото естество на дерогациите като изключения от правилото личните данни да не могат да бъдат предавани на трета държава, освен ако тази държава не осигури адекватно ниво на защита на данните или ако вместо това не бъдат въведени подходящи гаранции. Дерогациите на практика не се превръщат в „правило“, а трябва да се ограничават до конкретни ситуации. ЕКЗД публикува своите Насоки 2/2018 относно дерогациите по член 49 от Регламент (ЕО) № 2016/679.³⁷
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.

³⁶ Дело C-311/18 (Schrems II), точки 130 и 133. Вж. също подточка 2.3 по-долу.

³⁷ 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.

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 трансфер

28. Избраният инструмент за предаване по член 46 от ОРЗД трябва да гарантира ефективно, че нивото на защита, осигурено от ОРЗД, не е засегнато от предаването на практика³⁸.
29. По-специално защитата на личните данни, предадени в третата държава, трябва да бъде по същество равностойна на гарантираната в ЕИП от ОРЗД, тълкувана в светлината на Хартата на основните права на ЕС.³⁹ 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, включително по време на предаването на данни от администратора към държавата на вносителя⁴⁰.
30. Първо трябва да прецените, когато е целесъобразно в сътрудничество с вносителя, дали е налице фактор в действащото право и/или практики⁴¹ в третата държава, който може да засегне ефективността на подходящите гаранции, осигурени в член 46 от ОРЗД по отношение на инструментите за трансфер, на които разчитате, при конкретното предаване. Това означава да определите дали вашия трансфер попада в обхвата на законодателството и/или практиките, които може да засегнат ефективността на вашия инструмент за предаване по член 46 от ОРЗД. Необходимата оценка трябва да се основава преди всичко на законодателството, което е публично достъпно.
31. Тази оценка трябва да съдържа елементи относно достъпа до данни от страна на публичните органи на третата държава на вашия вносител, например:
 - елементи за това дали публичните органи на третата държава на вашия вносител може да се стремят да получат достъп до данните със или без знанието на вносителя на данни, като се имат предвид законодателството, практиката и докладваните прецеденти;
 - елементи за това дали публичните органи на третата държава на вашия вносител могат да имат достъп до данните чрез вносителя на данни или чрез доставчиците на телекомуникационни услуги или каналите за комуникация с оглед на законодателството, законовите правомощия, техническите, финансовите и човешките ресурси, с които разполагат, и на докладваните прецеденти.

Определяне на законите и практиките, които са от значение с оглед на всички обстоятелства на предаването

32. Трябва да разгледате характеристиките на всяко ваше предаване на данни и да определите дали действащият вътрешен правен ред и/или практики на държавата, на която се предават (или предоставят впоследствие) данните, повлияват на предаването, което извършвате.

³⁸ Член 44 от ОРЗД и точки 126, 137 и 148 от C-311/18 (Schrems II).

³⁹ Дело C-311/18 (Schrems II), точка 105 и втора констатация.

⁴⁰ Вж. C-311/18 (Schrems II), точка 183 във връзка с точка 184.

⁴¹ Вж. точка 126 от решението по дело C-311/18 (Schrems II), в което Съдът изрично се позовава на „действащото право и практики в съответната трета държава“ и изисква „(...) осигуряване на практика на ефективна защита на личните данни, предавани на съответната трета държава.“ (курсивът е добавен) и точка 158.

Поради това обхватът на оценката ви е ограничен до законодателството и практиките, които са от значение за защитата на конкретните данни, които трансферирате, в сравнение с общите и широкообхватни преценки на адекватното ниво на защита, които Европейската комисия извършва в съответствие с член 45 от ОРЗД.

33. Приложимият правен характер и/или практики ще зависят от конкретните обстоятелства на вашето предаване на данни, по-специално:

- целите, за които се предават и обработват данните (напр. маркетинг, човешки ресурси, съхранение, ИТ поддръжка, клинични изпитвания);
- видове субекти, участващи в обработването (публични/частни; администратор/обработващ данните);
- сектор, в който се извършва предаването (напр. рекламни технологии, телекомуникации, финанси и др.);
- категории предавани лични данни (напр. личните данни, свързани с деца, могат да попаднат в обхвата на специфично законодателство в третата държава);⁴²
- 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 криптирани⁴³);
- вероятност данните да подлежат на последващо предаване от третата държава на друга трета държава⁴⁴.

34. Когато извършвате преценка, следва да вземете предвид всички участници в предаването (напр. 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 оценката ви. При тази преценка ще трябва също да вземете под внимание всяко предвидено последващо предаване.

35. Във всеки случай трябва да обръщате специално внимание на съответните закони, и по-конкретно на тези, 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 (напр. за целите на наказателното правоприлагане, регулаторния надзор и националната сигурност). Ако тези изисквания или правомощия ограничават основните

⁴² Предаването на лични данни е операция по обработване (член 4.2 от ОРЗД). Ако желаете да предадете чувствителни данни, попадащи в обхвата на членове 9 и 10 от ОРЗД, можете да извършите предаване само ако то попада в обхвата на една от дерогациите и условията, посочени в членове 9 и 10 от ОРЗД и правото на държавата — членка на ЕС. В съответствие с член 32 от ОРЗД ще трябва също да приложите, като вносителят действа в качеството си на администратор или обработващ лични данни, подходящи технически и организационни мерки за осигуряване на ниво на сигурност, съобразено с рисковете за правата и свободите на субектите на данни, породени от нарушаване на сигурността на личните данни на предаваните данни (член 4.12 от ОРЗД). Категориите предавани данни и тяхната чувствителност ще са от значение за оценката на риска и целесъобразността на мерките.

⁴³ Някои трети държави не разрешават вноса на криптирани данни.

⁴⁴ Когато администраторът е дал своето предварително конкретно или общо писмено разрешение в съответствие с член 28, параграф 2 от ОРЗД.

права на субекта на данни, но същевременно с това зачитат основното съдържание на тези права и са необходими и пропорционални мерки в едно демократично общество, за да се защитят важните цели, признати и в правото на Съюза или на държавата — членка на ЕС,⁴⁵ те не могат да засегнат ангажиментите, съдържащи се в инструмента за предаване по член 46 от ОРЗД, на който разчитате.

36. Ще трябва да направите оценка на съответните правила и практики от общ характер, доколкото те влияят върху ефективното прилагане на гаранциите, съдържащи се в инструмента за предаване по член 46 от ОРЗД.
37. 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. Например, ситуацията, свързана със спазването на 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 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.
38. Задълженията или правомощията, произтичащи от такива закони и практики, ще се считат за засягащи/несъвместими с ангажиментите, съдържащи се в инструмента за предаване по член 46 от ОРЗД, ако те⁴⁶:
 -)] не зачитат основното съдържание на основните права и свободи на Хартата на основните права на ЕС или
 -)] надхвърлят това, което е необходимо и пропорционално в едно демократично общество, за да се защитят важните цели, признати и в правото на Съюза или на държавата — членка, като изброените в член 23, точка 1 от ОРЗД.
39. Трябва да проверите дали ангажиментите на вносителя на данни, които дават възможност на субектите на данни да упражняват правата, предвидени в инструмента за предаване по член 46 от ОРЗД (напр. искания за достъп, поправка и заличаване на предадени данни, както и (съдебна) защита), могат да бъдат ефективно приложени на практика и не са възпрепятствани от правото и/или практиките в третата държава на местоназначение.
40. 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, по-конкретно, дали този достъп на публичните органи е ограничен до това, което е необходимо и пропорционално в едно

⁴⁵ 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 основни гаранции при прилагане на мерки за наблюдение, 10 ноември 2020 г. - https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

⁴⁶ Вж. членове 47 и 52 от Хартата на основните права на ЕС, член 23, параграф 1 от ОРЗД, C-311/18 (Schrems II), точки 174 и 187, и Препоръки 02/2020 на ЕКЗД относно основни гаранции при прилагане на мерки за наблюдение, 10 ноември 2020 г.

демократично общество, и дали субектите на данни разполагат с ефективни средства за защита.

41. В препоръките на ЕКЗД относно основните европейски гаранции⁴⁷ се съдържат разяснения по елементите, 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 оправдана⁴⁸ 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. Първото изискване на основните европейски гаранции е наличието на правна рамка, която да осигурява такъв достъп, когато е предвидено, и която да е публично достъпна и достатъчно ясна.
42. 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 при оценката дали тези правомощия неоправдано засягат задълженията на вносителя и на износителя на данни за гарантиране на равностойност по същество съгласно ОРЗД или ангажиментите, съдържащи се в инструмента за предаване на данни. 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 основните гаранции. ЕКЗД отново изтъква, че тези гаранции са референтен стандарт при оценката на намесата, произтичаща от мерките за наблюдение на трети държави, при международното предаване на данни. Тези стандарти произтичат от правото на ЕС и от съдебната практика на Съда на ЕС и ЕСПЧ, която е задължителна за държавите — членки на ЕС.
43. Вашата оценка трябва да се основава преди всичко на законодателството, което е публично достъпно. Проучването и на практиките на публичните органи на трети държави ще ви позволи да проверите дали гаранциите, съдържащи се в инструмента за предаване на данни по член 46 от ОРЗД, могат да бъдат на практика достатъчно средство за гарантиране на ефективна защита на предадените лични данни.⁴⁹ Проучването на действащите в третата държава практики ще бъде от особено значение за оценката ви в описаните по-долу ситуации.
- 43.1 **Съответното законодателство в третата държава може формално да отговаря на стандартите на ЕС за основните права и свободи и на необходимостта и пропорционалността на ограниченията към тях.** Същевременно практиките на нейните публични органи (напр. достъп до личните данни, с които разполага частният сектор, или когато налага или не законодателство в качеството си на надзорен или правен орган) могат ясно да посочват, че те обикновено не прилагат/спазват законодателството, което на практика урежда техните дейности. В този случай в оценката ви трябва да се вземат предвид тези практики, както и да приемете, че инструментът по член 46 от ОРЗД няма да може сам по себе си да гарантира по ефективен начин (т.е. без допълнителни мерки)

⁴⁷ [Препоръки 2/2020 относно европейските основни гаранции при прилагане на мерки за наблюдение, 10 ноември 2020 г.](#)

⁴⁸ И следователно като не засягаща ангажиментите, поети в инструмента за предаване на данни по член 46 от ОРЗД.

⁴⁹ Дело C-311/18 (Schrems II), точка 126.

равностойно по същество ниво на защита. В тази връзка, ако искате да продължите с предаването, ще трябва да приложите адекватни допълнителни мерки.

43.2 Съответно законодателство в третата държава (напр. за достъп до лични данни, с които разполага частният сектор) може да липсва. В този случай вие не можете автоматично да направите извод от тази липса на съответно законодателство, че вашият инструмент за предаване на данни по член 46 от ОРЗД може да бъде ефективно приложен. Ще трябва да проверите дали са налице достатъчно данни за действащи в държавата практики, които са несъвместими с правото на ЕС и с ангажиментите, съдържащи се в инструмента за предаване на данни по член 46 от ОРЗД. Ако са налице несъвместими практики, инструментът за предаване на данни по член 46 от ОРЗД няма да може сам по себе си да гарантира по ефективен начин (т.е. без адекватни допълнителни мерки) равностойно по същество ниво на защита. В такъв случай, ако искате да продължите с предаването, ще трябва да приложите адекватни допълнителни мерки.

43.3 Оценката може да разкрие, че съответното законодателство в третата държава може да е проблемно⁵⁰ и че предадените данни и/или вносителят попадат или могат да попадат в обхвата на това проблемно законодателство⁵¹.

Предвид опасностите, свързани с потенциалното прилагане на проблемното законодателство към вашето предаване, може да решите да:

-) спрете предаването;
-) да приложите допълнителни мерки⁵² за избягване на риска от потенциално прилагане към вашия вносител и/или предадени данни на закони и/или практики на третата държава на вносителя на данни, които могат да засегнат съдържащите се в инструмента за предаване договорни гаранции за ниво на защита, което е равностойно по същество на гарантираното в ЕИП; или
-) вместо това можете да решите да продължите с предаването, без да е необходимо да прилагате допълнителни мерки, ако нямате никакви основания да считате, че съответното и проблемно законодателство ще бъде на практика приложено към вашите предадени данни и/или вносител. Ще е необходимо да докажете и документирате чрез оценката си, когато е целесъобразно в сътрудничество с вносителя, че на практика правото не се тълкува и/или прилага така, че да обхване вашите предадени данни и вносител, като се вземе предвид, и опита на другите

⁵⁰ „Проблемно законодателство“ се разбира като законодателство, което 1) налага на получателя на лични данни от Европейския съюз задължения и/или засяга предадените данни по начин, който може да засегне съдържащата се в инструмента за предаване договорна гаранция за равностойно по същество ниво на защита и 2) не зачита основното съдържание на основните права и свободи, признати от Хартата на основните права на ЕС, или надхвърля това, което е необходимо и пропорционално в едно демократично общество, за да се защитят важните цели, признати и в правото на Съюза или на държавата — членка на ЕС, като изброените в член 23, точка 1 от ОРЗД.

⁵¹ Може да не е ясно дали вносителят и/или прехвърлените данни попадат в обхвата на общите термини, често използвани в законодателството в областта на националната сигурност, за да се ограничи техният обхват на прилагане, например „доставчик на електронни съобщителни услуги“ и „външно разузнавателна информация“.

⁵² Вж. съображение 109 от ОРЗД и дело C-311/18 (Schrems II), точка 132.

участници, работещи в същия сектор, и/или имащи отношение към подобни предадени лични данни, и допълнителни източници на информация, описани по-долу⁵³.

Ето защо ще е необходимо да докажете и документирате с подробен доклад⁵⁴, че проблемното законодателство няма да бъде на практика прилагано към вашите предадени данни и/или вносител, и следователно няма да попречи на вносителя да изпълни задълженията си съгласно инструмента за предаване по член 46 от ОРЗД⁵⁵.

Възможни източници на информация

44. Вашият вносител на данни следва да ви предостави съответните източници и информация, свързани с третата държава, в която е установен, както и с приложимото към предаването действащо законодателство.
45. Вие и вашият вносител можете да допълните оценката си с информация, получена от източници като тези, изброени като примери в Приложение 3.
46. В допълнение към правната рамка на третата държава, приложима към предаването, източниците и информацията следва да бъдат уместни, обективни, надеждни, доказуеми и публично или по друг начин достъпни, за да се определи дали вашият инструмент за предаване по член 46 може да бъде ефективно приложен⁵⁶, и ще трябва да оцените и да документирате, че те са такива.

Уместност: информацията трябва да има отношение към конкретното предаване и/или вносител и да съответства на изискванията на правото на ЕС, и на инструмента за предаване по член 46 от ОРЗД, както и да не бъде прекалено обща или абстрактна.

Обективна информация: е информация, която е подкрепена от емпирични доказателства, основаващи се на знания, получени от миналото, а не на предположения за потенциални събития и рискове.

⁵³ Вж. точки 45 до 47.

⁵⁴ Докладите, които ще представите като доказателство, трябва да включват пълна информация относно правната оценка на законодателството и практиките, и на тяхното приложение към конкретно предаване, вътрешната процедура за представяне на оценката (вкл. информация за участниците, включени в оценката, напр. адвокатски кантори, консултанти или вътрешни отдели) и датите на проверките. Докладите следва да бъдат одобрени от законния представител на износителя.

⁵⁵ Демонстрирането, че проблемното законодателство не се прилага на практика към вашите предадени данни и вносител, като се вземе предвид и опита на другите участници, работещи в същия сектор и/или имащи отношение към подобни предадени лични данни, не ви освобождава от осигуряването на необходимите допълнителни мерки за защита на личните данни по време на техния трансфер и обработване в третата държава на местоназначение (напр. криптиране от край до край на данни — вж. примери за технически допълнителни мерки в Приложение 2), ако анализът ви на приложимото законодателство на третата държава на местоназначение посочва, че достъп до данни може да се осъществи дори и без намеса от страна на вносителя в този момент на предаването. Може вече да сте предвидили такива мерки, при които вносителят действа като администратор или обработващ лични данни в съответствие с член 32 от ОРЗД.

⁵⁶ Вж. Приложение 3 за неизчерпателния списък с източниците на информация, които вие и вносителят можете да използвате.

Надеждност: износителят и вносителят трябва да направят обективна оценка на надеждността на източника на информация и на самата информация, както и преценка на тях двете поотделно.

Доказуемост: информацията и заключенията следва да могат да бъдат доказани или съпоставени с други видове информация или източници като част от една обща оценка, както и да позволят на компетентния надзорен или съдебен орган да извършат проверка на обективността и надеждността на тази информация при необходимост.

Публично или по друг начин достъпна информация: за предпочитане е информацията да бъде публична или поне достъпна, за да улесни проверката на посочените по-горе критерии и да гарантира нейния възможен обмен с надзорни и съдебни органи и в крайна сметка със субекти на данни.

47. Можете да вземете под внимание и документирания практически опит на вносителя със съответни предишни случаи на искания за достъп, постъпили от публични органи в третата държава. Ще можете да използвате опита на вносителя само като допълнителен източник на информация, ако правната рамка на третата държава не забранява на вносителя да предоставя информация по искания за разкриване на данни от публични органи или при липса на такива искания (като следва да документирате и тази оценка). Същевременно, трябва да отбележите, че липсата на предишни случаи на искания, постъпили от вносителя, не може никога да се счита само по себе си за решаващ фактор за ефективността на инструмента за предаване по член 46 от ОРЗД, който да позволява на предаването да продължи без допълнителни мерки. Ще можете да разгледате тази информация заедно с други видове информация, получена от други източници, като част от цялостната ви оценка на законите и практиките на третата държава във връзка с вашето предаване. Подходящият и документиран опит на вносителя следва да бъде потвърден и да не противоречи на уместната, обективна, надеждна, доказуема и публично или по друг начин достъпна информация за практическото приложение на съответното право (напр. съществуването или отсъствието на искания за достъп, постъпили от други участници, работещи в същия сектор и/или имащи отношение към подобни предадени лични данни⁵⁷, и/или за практическото прилагане на закона, като съдебна практика и доклади от независими надзорни органи).

Резултати от оценката ви

48. Тази цялостна оценка на закона и практиката на третата държава на вашия вносител, приложими към вашето предаване, следва да извършите с дължимата грижа и да я документирате задълбочено. Вашите компетентни надзорни и/или съдебни органи е възможно да поискат такава оценка и да ви държат отговорни за всяко решение, което вземете на тази база⁵⁸.

⁵⁷ Опитът може да бъде опитът на други субекти, които познавате директно от предишно предаване от същия вид, което сте извършвали, или което е докладвано в съответната съдебна практика, доклади на НПО и др. (вж. Приложение 3).

⁵⁸ Член 5, параграф 2 от ОРЗД.

49. В крайна сметка преценката ви може да разкрие, че инструментът за предаване по член 46 от ОРЗД, на който разчитате:

- 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 б).
- Не гарантира по ефективен начин равностойно по същество ниво на защита. Вносителят на данни не може да изпълни задълженията си, защото законодателството и/или практиките на третата държава, приложими към предаването, не отговарят на стандартите на ЕС за основните права и свободи, и на необходимостта, и пропорционалността на ограниченията към тях, за да се гарантират легитимни цели от общ интерес. 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 данни⁵⁹.

Пример:

Обосновка:

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.

Оценка:

Ако оценката ви на съответното законодателство на САЩ ви кара да считате, че вашето предаване може да попадне в обхвата на член 702 от ЗНЧРС, но не сте сигурни дали то попада в обхвата на приложението, можете да решите:

1. да спрете предаването;
2. да приемете подходящи мерки, които да гарантират ефективно ниво на защита на предадените данни, което да е равностойно по същество на гарантираното в ЕИП, или
3. да потърсите друга обективна, надеждна, уместна, доказуема и за предпочитане публично достъпна информация (което може да включва информацията, която ви е предоставена от вашия вносител на данни), която да разясни обхвата на приложение на практика на член 702 от ЗНЧРС към конкретното предаване. Тази информация следва да дава отговори на някои уместни въпроси, например следните:

- Показва ли публично достъпната информация, че съществува законова забрана за информиране относно постъпило конкретно искане за достъп до данни и конкретни ограничения върху предоставянето на обща информация относно постъпили искания за достъп до данни или липса на постъпили искания?

⁵⁹ Дело на Съда на ЕС C-311/18 (Schrems II), точки 134 и 135.

- Потвърдил ли е вашият вносител на данни, че в миналото при него са постъпили искания за достъп до данни от страна на публични органи в САЩ? Или потвърдил ли е вашият вносител на данни, че в миналото при него не са постъпвали искания за достъп до данни от страна на публични органи в САЩ и че не му е наложена забрана за предоставяне на информацията относно такива искания или за липса на такива?

- Разкрива ли получената от вас публично достъпна информация за съдебната практика на САЩ и докладите от надзорни органи, организации на гражданското общество и академични институции,⁶⁰ че при вносителите на данни от същия сектор като на вашия вносител са постъпвали искания за достъп до данни за подобни трансферирани данни в миналото?

Отговорите на тези въпроси, получени от вас в резултат на извършената обща оценка, ви водят до заключението, че:

- Член 702 от ЗНЧРС на практика се прилага към конкретното предаване и следователно засяга ефективността на вашия инструмент за предаване по член 46 от ОРЗД. В резултат на това, ако желаете да продължите с предаването, трябва да обмислите, когато е целесъобразно в сътрудничество с вносителя, дали е възможно да приемете допълващи мерки, които гарантират, че на предадените данни се осигурява степен на защита, която по същество е равностойна на гарантираната в рамките на ЕС. Ако не можете да откриете ефективни допълващи мерки, вие не трябва да предавате личните данни.

или

- Член 702 от ЗНЧРС на практика не се прилага към конкретното предаване и следователно не засяга ефективността на вашия инструмент за предаване по член 46 от ОРЗД. След това можете да продължите с предаването без каквито и да било допълващи мерки.

2.4 Стъпка 4: Приемане на допълващи мерки

50. 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 в третата държава се осигурява степен на защита, която по същество е

⁶⁰ Напр. разпоредбите на член 702 от ЗНЧРС; Процедурния правилник на Съда за наблюдение на чуждите разузнавателни служби (ЗНЧРС), разсекретените становища и решения на ЗНЧРС, съдебната практика на съдилищата на САЩ; доклади и протоколи от изслушванията на Надзорния съвет по въпросите на неприкосновеността на личния живот и гражданските свободи (НСНЛЖГС); доклади на Кабинета на главния инспектор, Министерство на правосъдието на САЩ; доклади на директора на Службата за гражданските свободи и неприкосновеността на личния живот към АНС; доклади, изготвени от Научноизследователската служба на Конгреса; доклади от Фондацията на американския съюз за защита на гражданските свободи (АСЗГС).

равностойна на гарантираната в рамките на ЕС⁶¹. Съгласно определението „допълващите мерки“ допълват гаранциите, които инструментът за предаване на данни по член 46 от ОЗРД вече осигурява, както и всички останали приложими изисквания за сигурност (напр. технически мерки за сигурност), установени в ОРЗД.⁶²

51. 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 трансферите на данни към конкретна трета държава. Не е необходимо да повтаряте оценката всеки път, когато извършвате едно и също предаване на конкретен вид данни към една и съща трета държава. Някои от данните, планирани за предоставяне, може да изискват допълващи мерки, докато други данни — не (като се вземе предвид формалното и/или практическото приложение на законодателството на третата държава). Ще можете да се основавате на предишните си оценки по стъпките (1, 2 и 3 по-горе) и да проверите, въз основа на заключенията от оценките, потенциалната ефективност на допълващите мерки, за да гарантирате необходимото ниво на защита.
52. 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.
53. Само чрез договорните и организационните мерки по принцип няма да бъде преодолян достъпът до личните данни от страна на публичните органи на третата държава, основаващо се на проблемно законодателство и/или практики⁶³. 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 личните данни, по-специално за целите на наблюдението⁶⁴. В такива ситуации договорните или организационните мерки могат да допълват техническите мерки и да укрепват общото равнище на защита на данните (напр. чрез въвеждане на проверки и елиминиране на автоматичните опити на публичните органи да получат достъп до данни по начин, който не съответства на стандартите на ЕС).
54. Когато е целесъобразно, можете да разгледате, в сътрудничество с вносителя на данни, следния (неизчерпателен) списък с фактори, за да определите кои допълващи мерки биха

⁶¹ Дело C-311/18 (Schrems II), точка 96.

⁶² Съображение 109 от ОРЗД и дело C-311/18 (Schrems II), точка 133.

⁶³ „Проблемно законодателство“ се разбира като законодателство, което 1) налага на получателя на лични данни от Европейския съюз задължения и/или засяга предадените данни по начин, който може да засегне съдържащата се в инструмента за предаване договорна гаранция за равностойно по същество ниво на защита и 2) не зачита основното съдържание на основните права и свободи, признати от Хартата на основните права на ЕС, или надхвърля това, което е необходимо и пропорционално в едно демократично общество, за да се защитят важните цели, признати и в правото на Съюза или на държавата — членка на ЕС, като изброените в член 23, точка 1 от ОРЗД.

⁶⁴ 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 основни гаранции при прилагане на мерки за наблюдение, 10 ноември 2020 г., https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

били най-ефективни за защитата на предаваните данни при искания от публични органи за достъп до данни въз основа на прилагано на практика проблемно законодателство:

- формат на данните, които ще бъдат предоставени (т.е. в обикновен текст/псевдонимизирани или криптирани);
- естество на данните (напр. в ЕИП се осигурява по-високо ниво на защита на категориите данни, обхванати от членове 9 и 10 от ОРЗД)⁶⁵;
- продължителност и сложност на работния процес при обработването на данни, брой на участниците в обработването и връзката между тях (напр. 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)⁶⁶;
- техниката или параметрите на практическото приложение на законодателството на третата държава, които са изпълнени в стъпка 3;
- възможно е данните да бъдат предмет на последващо предаване в рамките на същата трета държава или дори на други трети страни (напр. участие на подизпълнители на вносителя на данни⁶⁷).

Примери за допълващи мерки

55. Някои от примерите за технически, договорни и организационни мерки, които могат да бъдат обмислени и които все още не са включени в използвания инструмент за предаване на данни по член 46 от ОРЗД, могат да бъдат намерени в неизчерпателните списъци, описани в Приложение 2.

56. Ако сте въвели ефективни допълващи мерки, които заедно с избория от вас инструмент за предаване на данни по член 46 от ОРЗД достигат ниво на защита, което понастоящем е равностойно по същество на нивото на защита, гарантирано в рамките на ЕИП: можете да продължите с вашето предаване.

57. Когато не можете да намерите или да приложите ефективни допълващи мерки, които да гарантират, че трансферираните лични данни се ползват с равностойно по същество ниво на защита⁶⁸, не трябва да започвате да предавате лични данни на съответната трета държава

⁶⁵ Вж. бележка под линия 42.

⁶⁶ 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.

⁶⁷ Вж. бележка под линия 26.

⁶⁸ 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 основни гаранции при прилагане на мерки за наблюдение, 10 ноември

въз основа на инструмента за предаване по член 46 от ОРЗД, на който разчитате. Ако вече извършвате предоставяне на лични данни, от вас се изисква да го преустановите или прекратите⁶⁹. В съответствие с гаранциите, съдържащи се в инструмента за предаване на данни по член 46 от ОРЗД, данните, които вече сте предоставили на тази трета държава, и копията от тях следва да ви бъдат върнати или унищожени изцяло от вносителя⁷⁰.

Пример:

Пример: в правото на третата държава се забраняват допълващите мерки, които сте определили (напр. 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 текущия трансфер към нея.

58. Компетентният надзорен орган може да наложи други корективни мерки (напр. 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

59. 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.

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

60. Когато възнамерявате да въведете 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 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 застрашено⁷¹. Износителят 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

2020 г., https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

⁶⁹ Дело C-311/18 (Schrems II), точка 135.

⁷⁰ Вж. клауза 12 в приложението към Решение 87/2010 относно СДК; вж. (незадължителната) клауза за допълнително прекратяване в Приложение Б SCC 2004/915/ЕО.

⁷¹ 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.

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 (напр. в случай на жалба или разследване по собствена инициатива).

61. 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 клаузи⁷² 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)

62. 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 ангажменти в тях не могат да обвързват публичните органи на трети държави⁷³.
63. 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.
64. Всички ангажменти, които е необходимо да бъдат включени, ще бъдат посочени в актуализираните референтни документи РД 256/257,⁷⁴ с които всички групи, разчитащи на ЗФП като инструменти за предаване, ще трябва да съобразят своите съществуващи и бъдещи ЗФП.
65. Съдът изтъква, че износителят и вносителят на данни са длъжни да извършат оценка на спазването в съответната трета държава на изискваното 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

⁷² 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.

⁷³ Съд на ЕС, С-311/18 (Schrems II), точка 132.

⁷⁴ 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., РД 256 ред.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., РД 257 ред.01

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 Специални договорни клаузи (член 46.3, буква а) от ОРЗД)

66. 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 държави⁷⁵. Ето защо решението по делото Schrems II е от значение за предаването на лични данни въз основа на специални договорните клаузи, тъй като законите на трети държави могат да засегнат защитата, предоставяна от тези инструменти.

2.6 Стъпка 6: Преоценка на подходящи интервали от време

67. 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 трансфера на данни. Поддържането на отчетност е постоянно задължение (член 5, параграф 2 от ОРЗД).

68. 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.

3 ЗАКЛЮЧЕНИЕ

69. В ОРЗД се определят правила относно обработването на лични данни в ЕИП и по този начин се дава възможност за свободно движение на тези данни в рамките на ЕИП. В глава V от ОРЗД се урежда предаването на лични данни към трети страни и се поставя високо изискване: предоставянето 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, трансферирани в трета държава⁷⁶.

70. 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 да проверите дали данните, които предавате, са подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват.

⁷⁵ Съд на ЕС, C-311/18 (Schrems II), точка 132.

⁷⁶ Дело C-311/18 (Schrems II), точка 93.

71. Трябва също да идентифицирате инструмента за предаване, на който разчитате за извършване на трансфера. Ако инструментът 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 по член 46 от ОРЗД по отношение на вашето предаване на данни. Когато инструментът сам по себе си не осигурява по същество равностойно ниво на защита, то чрез допълващите мерки могат да бъдат отстранени пропуските.
72. 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 предоставяте лични данни на съответната трета държава въз основа на избрания от вас инструмент за предаване. Ако вече извършвате трансфер, от вас се изисква своевременно да преустановите или прекратите предаването на лични данни.
73. 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
(Andrea Jelinek)

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 С 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, 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

74. 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. Можете да изследвате други допълващи мерки. Бъдещите технологични, правни или организационни промени могат да доведат до появата на нови допълващи мерки, които да обмислите. 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 осигуряват това ниво на защита за вашето предаване.
75. 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 или в комбинация с други се отстраняват конкретните недостатъци, установени при оценката на ситуацията в третата държава, свързана с нейното законодателство и практики, приложими към вашето предаване. Ако в крайна сметка не можете да гарантирате равностойно по същество ниво на защита, не трябва да трансферирате личните данни.
76. Като администратор или обработващ лични данни от вас вече може да се изисква да прилагате някои от мерките, описани в това приложение, за да се постигне съответствие с ОРЗД. Това означава, че може да възникне необходимост от въвеждане на подобни мерки за личните данни, обработени в ЕИП, които са предадени на вносител на данни и са обхванати от решение относно адекватно ниво на защита или на други трети държави.⁷⁷

Технически мерки

77. 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 данни⁷⁸.
78. За по-голяма яснота в този раздел първо се посочват техническите мерки, които биха могли да бъдат ефективни при определени сценарии, за да се осигури равностойно по същество ниво на защита. Разделът продължава с някои сценарии, при които не могат да бъдат определени технически мерки за гарантиране на такова ниво на защита.

⁷⁷ Член 5, параграф 2 от ОРЗД, член 32 от ОРЗД.

⁷⁸ Дело C-311/18 (Schrems II), точка 135.

Примери за сценарии, отнасящи се до случаи, при които са определени ефективни мерки

79. 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 биха били необходими за гарантиране на ниво на защита, равностойно по същество на гарантираното в ЕИП дори и ако достъпът на публичните органи е в съответствие с правото на държавата на вносителя, когато на практика този достъп надхвърля необходимото и пропорционалното в едно демократично общество⁷⁹. 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 другото, онлайн идентификатори, осигурени от устройствата, приложенията, инструментите и протоколите, използвани от субектите на данни с друга цел.
80. Публичните органи в трети държави могат да се стремят да получат достъп до предадените данни:
- а) 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.
 - б) 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.
81. В настоящия раздел се разглеждат сценарии, при които се прилагат ефективни мерки 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 1881а (ЗНЧРС 702), имат пряко задължение да предоставят достъп до 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.

⁷⁹ 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 основни гаранции при прилагане на мерки за наблюдение, 10 ноември 2020 г., https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

82. В сценариите се описват конкретните обстоятелства и предприетите мерки, които да служат за пример. Различните промени в сценариите могат да доведат до различни заключения. Сценариите се отнасят до ситуации, при които се е стигнало до заключението, че на първо място са необходими допълващи мерки, т.е. когато на практика към въпросното предаване се прилага проблемно законодателство.
83. 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 износителя 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.

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

84. 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, а идентичността на вносителя се проверява,
2. алгоритъмът за криптиране и неговата параметризация (напр. 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 (напр. изчислителна мощност за посрещане на атаки с груба сила), с които разполагат,⁸⁰
3. в силата на криптирането и дължината на ключа се отчита конкретният период от време, през който трябва да се запази поверителността на криптираните лични данни⁸¹,

⁸⁰ За оценката на алгоритмите за криптиране, тяхното съответствие със съвременното техническо равнище и тяхната надеждност срещу криптоанализ във времето износителят на данни могат да разчитат на технологични насоки, публикувани от официалните органи по киберсигурност на ЕС и неговите държави членки. Вж. напр. доклада на ENISA „What is „state of the art“ in IT security“, Агенция на ЕС за киберсигурност („Какво е „съременно техническо равнище“ в ИТ сигурността?“), 2019 г., <https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security>; Насоки, дадени от Немския федерален отдел за информационна сигурност в неговите Технически насоки от серията TR-02102 и „Algorithms, Key Size and Protocols Report (2018)“, („Алгоритми, дължина на ключа и доклади за протоколите“ (2018 г.)) H2020-ICT-2014 – Project 645421, D5.4, [ECRYPT-CSA, 02/2018](https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf)“ на <https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf>.

⁸¹ Защитната функция на криптографските алгоритми с времето намалява поради откриването на нови криптоаналитични техники, появата на нови изчислителни парадигми като квантово изчисляване и общото нарастване на наличната изчислителна мощ, освен ако не бъде доказано, че приложените алгоритми са информационно теоретично сигурни. Това опасение се прилага особено към публичните

4. алгоритмът за криптиране се прилага безпогрешно и чрез правилно поддържан софтуер без известни уязвимости, 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)⁸², и
6. ключовете се съхраняват единствено под контрола на износителя на данни или от субект, който се ползва с доверието на износителя в ЕИП, или под юрисдикция, предлагаща ниво на защита, еквивалентно по същество на гарантираното в рамките на ЕИП,

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

Случай на употреба 2: Предаване на псевдонимизирани данни

85. 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 информация⁸³,
2. тази допълнителна информация се държи изключително от износителя на данни и се съхранява отделно в държава членка или в трета държава, от субект, на когото износителят има доверие, в ЕИП или в юрисдикция, предлагаща ниво на защита, което е равностойно по същество на гарантираното в ЕИП,
3. разкриването или неразрешеното използване на тази допълнителна информация се предотвратява чрез подходящи технически и организационни мерки, като се гарантира,

ключови алгоритми, които към момента на изготвяне се използват широко. В резултат на това износителят на данните трябва да отчете факта, че публичните органи могат да предприемат достъп до криптирани данни при обстоятелствата, описани в точка № 80, и да ги съхраняват докато техните ресурси са достатъчни за дешифриране. Допълващите мерки могат да се считат за ефективни само ако дешифрирането и последващото допълнително обработване по това време няма повече да съставлява нарушаване на правата на субектите на данни, напр. защото данните не могат повече да се използват за тяхното директно или косвено определяне.

⁸² Специална публикация на NIST 800-57, „Препоръка за управление на ключове“ <https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final>

⁸³ 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 свързани с конкретен субект на данни, без да се използва допълнителна информация, при условие че тази допълнителна информация 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“. Допълнителните данни могат да се състоят от таблици, съпоставящи псевдоними с идентифициращите атрибути, които те заменят, криптографски ключове или други параметри за трансформиране на атрибути, или други данни, позволяващи приписването на псевдонимизираните данни на идентифицирани физически лица и физически лица, които може да бъдат идентифицирани.

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 и използват, че псевдонимизираните лични данни не могат да бъдат приписани на идентифицирано физическо лице или на физическо лице, което може да бъде идентифицирано, дори ако са съпоставени с такава информация,

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

86. 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 времето⁸⁴, могат да позволят идентифицирането на това лице, дори ако неговото име, адрес или други обикновени данни за идентификация са пропуснати.
87. 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.
88. 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.
89. Ако в хода на извършване на псевдонимизация атрибутите, съдържащи се в личните данни, са трансформирани чрез използване на криптографски алгоритъм и се прилагат насоките в бележки под линия 80 и 81. Оттук нататък се препоръчва да се спре изключителното ползване на криптография и да се прилагат трансформации, основаващи се на механизми за търсене в таблици.

⁸⁴ 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;“.

Случай на употреба 3: Криптиране на данни с цел тяхната защита срещу достъп от страна на публичните органи на третата държава на вносителя, когато тя се предава между износителя и нейния вносител

90. Износителят на данни желае да предаде данни до местоназначение, където правото и/или практиките позволяват достъп от страна на публични органи до данни, докато те се предават между държавата на износителя и държавата по местоназначение.

Ако

1. износител на данни предава лични данни до вносител на данни в юрисдикция, където правото и/или практиката позволяват на публичните органи достъп до данни, докато те се пренасят по интернет до тази трета държава, без да може да се използват европейските основни гаранции относно този достъп, като се използва транспортно криптиране, 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 тази трета държава,
2. страните, участващи в комуникацията, се споразумяват да използват надежден орган или инфраструктура за сертифициране на публичен ключ,
3. използват се конкретни защитни и съвременни мерки срещу активните и пасивните атаки срещу системите за изпращане и получаване, които предоставят транспортното криптиране, включително проверки за уязвимости на софтуера и възможни задни вратички,
4. в случай че транспортното криптиране 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,
5. алгоритъмът за криптиране и неговата параметризация (напр. 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, когато се предават данни до тази трета държава, като се вземат предвид ресурсите и техническите възможности (напр. изчислителна мощност за посрещане на атаки с груба сила), с които разполагат (вж. бележка под линия 80 по-горе),⁸⁵
6. в силата на криптирането се отчита конкретният период от време, през който трябва да се запази поверителността на криптираните лични данни,
7. алгоритъмът за криптиране се прилага безпогрешно и чрез правилно поддържан софтуер без известни уязвимости, чието съответствие със спецификацията на избрания алгоритъм е проверено, например чрез сертифициране,
8. 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,

⁸⁵ Вж. бележка под линия 80 за някои препратки към техническите насоки, публикувани от официалните органи по киберсигурност на ЕС и на неговите държави членки.

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

Случай на употреба 4: Защитен получател

91. 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 привилегирана 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 по възможност от самия износител или от друг субект, на когато износителят има доверие в ЕИП или в юрисдикция, предлагаща ниво на защита, което е равностойно по същество на гарантираното в ЕИП, и е защитен по подходящ начин срещу неразрешено използване или разкриване чрез 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 транспортно криптиране представлява ефективна допълваща мярка.

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

92. 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. администраторът е установил чрез задълбочен анализ на въпросните данни, като е взел предвид всяка липсваща част от информация, с която публичните органи на държавите получатели може да се очаква да разполагат и използват, че частите от лични данни, които той предава на обработващите лични данни, не могат да бъдат приписани на идентифицирано физическо лице или на физическо лице, което може да бъде идентифицирано, дори ако са съпоставени с такава информация,
6. 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.

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

Примери за сценарии, отнасящи се до случаи, при които не са определени ефективни мерки

93. 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 адекватни 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

94. Износителят на данни предава лични данни чрез електронно предаване или като ги предоставя на разположение на доставчик на услуги в облак или на друг обработващ лични данни, за да могат данните да бъдат обработвани в съответствие с неговите инструкции в трета държава (напр. с цел предоставяне на техническа подкрепа или всякакъв вид обработване в облак), и тези данни не са или не могат да бъдат псевдонимизирани, както е описано в Случай на употреба 2, или криптирани, както е описано в Случай на употреба 1, защото обработването изисква достъп до данни в чист вид,

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 въпросните предадени данни, излизат от рамките на това, което е необходимо и пропорционално в едно демократично общество, където на практика към въпросното предаване се прилага проблемното законодателство на третата държава (вж. стъпка 3).⁸⁶

тогава, като се има предвид съвременното технологично равнище, ЕКЗД не е в състояние да предвиди ефективна техническа мярка, за да попречи на този достъп да наруши основните права на субекта на данни. Комитетът не изключва възможността в резултат на по-нататъшното технологично развитие да бъдат осигурени мерки, с които да бъдат постигнати планираните стопански цели, без да се изисква достъп до данни в чист вид.

95. При дадените сценарии, когато некриптираните лични данни са технически необходими за предоставянето на услугата от обработващия лични данни, транспортното криптиране 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: Предаване на лични данни за стопански цели, включително чрез дистанционен достъп

96. Износителят на данни предава лични данни на субекти в трета държава, за да се използват за споделени стопански цели, по електронен път или като ги предоставя на разположение за дистанционен достъп от вносителя на данни, като тези данни не са или не могат да бъдат псевдонимизирани, както е описано в Случай на употреба 2, или криптирани, както е описано в Случай на употреба 1, защото обработването изисква достъп до данни в чист вид. Обичайната конфигурация може да се състои от администратор или обработващ

⁸⁶ 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 основни гаранции при прилагане на мерки за наблюдение, 10 ноември 2020 г., https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

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 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 носител 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. носителят⁸⁷ обработва данни в чист вид в третата държава (вкл. за свои собствени цели в случаите, когато носителят е администратор),
3. правомощията, предоставени на публичните органи в държавата получател за достъп до предадените данни, надхвърлят необходимото и пропорционалното в едно демократично общество, където на практика към въпросното предаване се прилага проблемното законодателство на третата държава (вж. Стъпка 3).

тогава ЕКЗД не може да предвиди ефективна техническа мярка, с която да се попречи на този достъп да наруши основните права на субекта на данни.

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

⁸⁷ Независимо дали става въпрос за администратор или обработващ лични данни в трета държава, който получава или придобива достъп до лични данни, предавани от ЕИП.

2.2 Допълнителни договорни мерки

98. Тези мерки обикновено се състоят от едностранни, двустранни или многостранни ⁸⁸ договорни ангажименти ⁸⁹. 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 и вносителя на данни, които имат за цел да послужат като гаранции за личните данни ⁹⁰.

99. В някои случаи тези мерки могат да допълнят и укрепят гаранциите, предоставени от инструментът за предаване и съответното законодателство на третата държава, когато, 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 ⁹¹, може често да се налага мерките 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.

100. 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.

101. 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 ⁹².

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

Предвиждане на договорно задължение за използване на специфични технически мерки

103. В зависимост от конкретните обстоятелства на предаването (вкл. практическото приложение на законодателството на третата държава), в договора може да се наложи да

⁸⁸ Например в рамките на ЗФП, които при всички случаи следва да регулират някои от мерките, изброени по-долу.

⁸⁹ 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.

⁹⁰ 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 изискваното 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).

⁹¹ Дело C-311/18 (Schrems II), точка 125.

⁹² Решение на Съда на ЕС по дело C-311/18 (Schrems II), точка 132.

се посочи, че за осъществяването на предаването ще бъде необходимо въвеждането на специални технически мерки (вж. по-горе предложените технически мерки).

104. 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:

105. Износителят може да добави приложения към договора с информация, която вносителят би предоставил преди сключването на договора, 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. То може също да подчертае задължението на вносителя да оказва съдействие на износителя при неговата оценка и да поеме отговорност да му предоставя информация, която е обективна, надеждна, уместна, доказуема и достъпна публично или по друг начин.

106. 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, подлежащи на предаване, по-специално в областта на разузнаването, правоприлагането, административния и регулаторния надзор, приложим към трансферираните 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 (напр. 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 време⁹³, по-специално в областите, посочени в точка 1 по-горе, които

⁹³ 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.

включват информация за получените искания, изисканите данни, органа, подаващ искането, и правното основание за разкриване, както и до каква степен вносителят е оповестил искането за данни⁹⁴;

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

107. 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.

108. 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.
- 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 предоставянето 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 мерки, които евентуално е приел, вече не могат да осигурят ниво на защита, което по същество е равностойно на това в ЕС. Същевременно това задължение не може да оправдае разкриването на лични данни от страна на вносителя, нито да породя очакването, че няма да има допълнителни искания за достъп.

109. Износителят би могъл също да добави клаузи, в които се изисква вносителят да удостовери, че (1) не е създавал целенасочено задни врати или подобни програми, които биха могли да се използват за достъп до системата и/или личните данни, (2) че не е създавал 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 тайни процедури или да улеснява достъпа до лични данни или системи, или да притежава, или предава ключа за криптиране⁹⁵.

110. Условия за ефективност:

- Съществуването на законодателство или държавни политики, които не позволяват на вносителите да разкриват тази информация, може да направи тази клауза неефективна.

⁹⁴ 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.

⁹⁵ Тази клауза е важна, за да се гарантира адекватно ниво на защита на предаваните лични данни, и обикновено следва да се изисква наличието ѝ.

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.

- 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 тайни процедури 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.
- В случаите, когато вносителят на данни разкрива лични данни в нарушение на ангажиментите, съдържащи се в избрания инструмент за предаване, договорът може да включва и компенсация от вносителя на данни към физическото лице за понесени материални и нематериални щети.

111. Износителят би могъл да засили правомощията си да извършва одити⁹⁶ 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.

112. 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 достъп и други подобни следи следва да бъдат защитени срещу подправяне (напр. те трябва да бъдат направени така, че да не могат да се променят с помощта на най-съвременни техники за криптиране, например хеширане, както и да бъдат систематично предавани на износителя на периодична основа), 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 такъв, дължащ се на нареждания или искания за достъп.

113. Когато правото и практиката на третата държава на вносителя първоначално са били оценени и се е считало, че осигуряват ниво на защита, което е равностойно по същество на предвиденото в ЕС за предаването от износителя данни, износителят все пак би могъл да направи по-строго задължението на вносителя на данни да информира своевременно, в случай на промяна в ситуацията, за невъзможността си да изпълни договорните задължения

⁹⁶ 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.

и в резултат на това да спази изисквания стандарт за „равностойно по същество ниво на защита на данните“.^{97.}

114. Тази невъзможност за спазване може да се дължи на промени в законодателството или практиката на третата държава^{98.} 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.

115. 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.
- В клаузите следва да е предвиден бързодействащ механизъм, чрез който износителят на данни разрешава на вносителя да осигури своевременно сигурността на данните или да ги върне на износителя, 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^{99.} договорен между износителя и вносителя. 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 могат да предоставят възможност на износителя да наблюдава спазването на тези задължения от страна на вносителя чрез одити, проверки и други

⁹⁷ Клауза 5, буква а) и буква г), подточка i) от Решение № 2010/87/ЕС.

⁹⁸ Вж. С-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, 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.“

⁹⁹ Този праг следва да гарантира, че на субектите на данни продължава да се осигурява ниво на защита, еквивалентно на осигуряването в рамките на ЕИП.

мерки за проверка и да ги наложи под формата на санкции на вносителя , както и/или да спре предаването и/или незабавно да прекрати договора.

116. 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 (напр. 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.

117. Условия за ефективност:

- Разпоредбите на третата държава трябва да позволяват на вносителя на данни да издаде 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 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

118. 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 отправилния 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 да предостави минимално допустимото количество информация, когато отговаря на нареждането, въз основа на разумното му тълкуване.

119. 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 това законодателство може да не отговаря на стандартите на ЕС. Тази договорна мярка задължително ще трябва да допълва други допълващи мерки.

- Оспорването на заповедите трябва временно да прекрати действията по трансфера 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.

120. В ситуацията, описана по-горе, вносителят може да се ангажира да информира отправилния искането публичен орган за несъвместимостта на нареждането с гаранциите, съдържащи се в инструмента за предаване на данни по член 46 от ОРЗД¹⁰⁰, 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.

121. 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.
- Законодателството на държавата не трябва да възпрепятства вносителя да уведоми износителя или поне компетентния надзорен орган от ЕИП относно 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

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

123. Условия за ефективност:

¹⁰⁰ 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.

- 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 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) (напр. в случай на служители)¹⁰¹.
- 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 той се предоставя само при специфични случаи на подкрепа или услуги, но самите данни се съхраняват в ЕИП.

124. 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 физическото лице да потърси информация и ефективна защита (напр. чрез подаване на иск до неговия компетентен надзорен орган и/или съдебен орган и да докаже своята процесуална легитимация пред съдилищата на третата държава), включително компенсация от вносителя на данни за понесени материални и нематериални щети вследствие на разкриването на неговите лични данни, предадени чрез избрания инструмент за предаване в нарушение на съдържащите се в него ангажменти.

125. Условия за ефективност:

- С това уведомление субектът на данните може да бъде информиран 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

¹⁰¹ Член 4, параграф 11 от ОРЗД.

уведоми субекта на данните за спирането или прекратяването на предаването на неговите лични данни поради невъзможността на вносителя да спазва договорните си задължения вследствие на получаването на искане за достъп.

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

127. Условия за ефективност

- Някои национални разпоредби може да не дават право на вносителя на данни да предоставя този вид съдействие директно на субектите на данни, а по-скоро да дават възможност на вносителя на данни индиректно да осигури това съдействие на физическите лица.
- В националните разпоредби и политики могат да се определят условия, които е възможно да намалят ефективността на предвидените специални 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 физическото лице да разбира правната система на трета държава и да извършва правни действия от чужбина, евентуално на чужд език. Същевременно тази клауза 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 провала 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 допълваща мярка би била ефективна само при условие че правото на третата държава предвижда правна защита пред нейните национални съдилища или че съществува специален механизъм, включително срещу мерки за наблюдение.

2.3 Организационни мерки

128. 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 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 вашия трансфер 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.
129. 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

130. 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 трансфер на данни между групи предприятия, тези политики могат да включват, наред с другото, назначаването на специален екип, състоящ се от експерти в областта на защита на ИТ данните и неприкосновеността на личния живот, който да разглежда искания, които включват лични данни, предавани от ЕИП; 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.
131. 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 развиятия 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.

132. 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 ЕС¹⁰². 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, трансферът на данни трябва да бъде спрял или да бъдат въведени подходящи допълващи мерки, за да бъде избегнат достъпът.

Мерки за прозрачност и отчетност

133. 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 трябва да ги представи на съответните физически лица.

134. 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 си да предостави такива документи и записи, и така да предложи на износителя възможност да спре предаването на данни, ако не може да се осигури адекватно ниво на защита.

135. 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.

136. 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.

¹⁰² Вж. дело C-362/14 (Schrems I), точка 94; C-311/18 (Schrems II), точки 168, 174, 175 и 176.

Организационни методи и мерки за свеждане на данните до минимум

137. Полезни при предаване на данни могат да бъдат и вече съществуващите организационни изисквания съгласно принципа на отчетност, като приемането на ограничен и подробен достъп до данни и политики за поверителност и най-добри практики, строго 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 да се предават определени данни (напр. 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).

138. Условия за ефективност:

- За да се наблюдава и налага спазването на мерките за свеждане на данните до минимум при 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 трансфера 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.

139. 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 такава, както и на правните служби и службите за вътрешен одит, по въпроси, свързани с международното предаване на лични данни.

140. Условия за ефективност:

- Длъжностното лице по защита на данните, ако има такава, и правният екип, както и екипът за вътрешен одит, получават цялата необходима информация преди предаването и с тях се прави консултация относно необходимостта от трансфера 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

141. 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 (напр. нормите на ISO) и най-добри практики (напр. Агенцията на Европейския съюз за киберсигурност (ENISA), като се взема предвид съвременното технологично равнище, в съответствие с риска, свързан с категориите обработвани данни.

Други

142. Приемане и редовен преглед на вътрешните политики, за да се оцени пригодността на използваните 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.

143. 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 ЕС¹⁰³.

¹⁰³ Дело C-311/18 (Schrems II), точки 135 и 137.

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

144. Вашият вносител на данни следва да бъде в състояние да ви предостави съответните източници и информация, свързани с третата държава, в която е установен, включително и законите и практиките, приложими към вносителя и предаваните данни. Вие и вносителят можете да се позовете на няколко източници на информация като тези, които са неизчерпателно изброени по-долу и представени по реда на предпочитание:

- съдебната практика на Съда на Европейския съюз (Съда на ЕС) и на Европейския съд по правата на човека (ЕСПЧ)¹⁰⁴, посочена в препоръките относно европейските основни гаранции¹⁰⁵;
- решения относно адекватното ниво на защита в държавата по местоназначение, ако предаването се базира на различно правно основание¹⁰⁶;
- резолюции и доклади от междуправителствени организации като Съвета на Европа¹⁰⁷, други регионални органи¹⁰⁸ и органи и агенции на ООН (напр. Съвет на ООН по правата на човека,¹⁰⁹ Комитет по правата на човека¹¹⁰);
- доклади и анализ от компетентни регулаторни мрежи като Глобалната асамблея по правото на неприкосновеност на личния живот (GPA);¹¹¹
- 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 на независими надзорни или парламентарни органи;
- доклади, изготвени въз основа на практически опит, в които са включени предишни случаи на искания за разкриване на данни от публични органи или липса на такива искания от субекти, работещи в същия сектор като вносителя;
- известия за получени искания за достъп до данни до други субекти, обработващи данни в същата област като вносителя ;
- доклади, изготвени или поръчани от търговски камари, бизнес, професионални и търговски асоциации, правителствени, дипломатически, търговски и инвестиционни

¹⁰⁴ Вж. фактологична справка за съдебната практика на ЕСПЧ относно масовото наблюдение:

¹⁰⁵ Вж. Препоръки 2/2020 на ЕКЗД относно европейските основни гаранции при прилагане на мерки за наблюдение, 10 ноември 2020 г. https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

¹⁰⁶ 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

¹⁰⁷ <https://www.coe.int/en/web/data-protection/reports-studies-and-opinions>

¹⁰⁸ Вж. например докладите по държави на Интер-американската комисия по правата на човека (ИАКПЧ), <https://www.oas.org/en/iachr/reports/country.asp>.

¹⁰⁹ Вж. <https://www.ohchr.org/EN/HRBodies/UPR/Pages/Documentation.aspx>

¹¹⁰ Вж.:

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

¹¹¹ Вж. напр. https://globalprivacyassembly.org/wp-content/uploads/2020/10/Day-1-1_2a-Day-3-3_2b-v1_0-Policy-Strategy-Working-Group-WS1-Global-frameworks-and-standards-Report-Final.pdf

агенции на износителя или други трети страни, изнасящи за третата страна, към която се извършва предаването;

- доклади от академични институции и организации на гражданското общество (напр. НПО);
- доклади от частни доставчици на услуги, предлагащи търговско разузнаване относно рисковете за дружествата, свързани с финансите, регулацията и репутацията;
- известия за получени искания от публични органи за достъп до данни, обработвани от самия вносител ; ¹¹²
- доклади за прозрачност, при условие че те изрично упоменават факта, че не са получени никакви искания за достъп. Доклади за прозрачност, в които това не е застъпено, няма да се считат за достатъчно доказателство, тъй като те в по-голямата част от случаите се фокусират върху исканията за достъп, получени от правоприлагащи органи, и предоставят данни само във връзка с този аспект, като запазват мълчание по отношение на получените искания за достъп за целите на националната сигурност. Това не означава, че не са получени никакви искания за достъп, а по-скоро че тази информация не може да бъде обменена; ¹¹³
- вътрешни изявления или доклади на вносителя, в които изрично се посочва, че за един достатъчно дълъг период от време не са получавани никакви искания за достъп, и с предпочитание към изявления и доклади, ангажиращи отговорността на вносителя и/или издадени от лица, заемащи вътрешни позиции с известна автономност като вътрешни одитори, длъжностни лица за защита на данните и др. ¹¹⁴

¹¹² Вж. условията за разглеждане на документирания практически опит на вносителя със съответни предишни случаи на искания за достъп, получени от публични органи в третата държава в точка 47.

¹¹³ *Пак там.*

¹¹⁴ *Пак там.*