Насоки 7/2022 относно сертифицирането като инструмент за предаване на данни

Версия 2.0

Приети на 14 февруари 2023 г.

ХРОНОЛОГИЯ НА ВЕРСИИТЕ

Версия 1.0	14 юни 2022 г.	Приемане на насоките за обществена консултация
Версия 2.0	14 февруари 2023 г.	Приемане на насоките след обществена консултация

КРАТКО ИЗЛОЖЕНИЕ

В член 46 от ОРЗД е предвидено изискване за износителите на данни да въведат подходящи гаранции за предаване на лични данни на трети държави или международни организации. За тази цел в ОРЗД са предвидени разнообразни подходящи гаранции, които могат да бъдат използвани от износителите на данни съгласно член 46 за регулиране на предаването на данни на трети държави, като се въвежда, наред с другото, сертифициране като нов механизъм за предаване на данни (член 42, параграф 2 и член 46, параграф 2, буква е) от ОРЗД).

В настоящите насоки са предоставени указания за прилагането на член 46, параграф 2, буква е) от ОРЗД относно предаването на лични данни на трети държави или международни организации въз основа на сертифициране. Документът е структуриран в четири раздела с приложение.

В първата част на настоящия документ („ОБЩИ ПОЛОЖЕНИЯ“) се пояснява, че насоките допълват вече съществуващите общи Насоки 1/2018 относно сертифицирането и разглеждат специфични изисквания от глава V от ОРЗД, когато сертифицирането се използва като инструмент за предаване на данни. Съгласно член 44 от ОРЗД всеки трансфер на лични данни на трети държави или международни организации трябва да отговаря на условията на другите разпоредби на ОРЗД в допълнение към спазването на глава V от ОРЗД. Ето защо на първо място трябва да се гарантира спазването на общите разпоредби на ОРЗД, а на второ място трябва да се спазват разпоредбите на глава V. В тази връзка са описани основните роли на участниците, като се обръща специално внимание на вносителя на данни, на когото ще бъде издаден сертификат, и на износителя на данни, който ще го използва като инструмент за регулиране на предаването на данни (като се има предвид, че отговорността за съответствието на обработването на данни остава за износителя на данни). В този смисъл сертифицирането може да включва и мерки, които допълват инструментите за предаване на данни, за да се гарантира спазването на нивото на защита на личните данни в ЕС. Първата част на насоките съдържа и информация относно процеса на получаване на сертификат, който да се използва като инструмент за предоставяне на данни.

Във втората част на настоящите насоки („УКАЗАНИЯ ЗА ПРИЛАГАНЕ НА ИЗИСКВАНИЯТА ЗА АКРЕДИТАЦИЯ“) се припомня, че изискванията за акредитация на сертифициращ орган са изложени в ISO 17065 и чрез тълкуване на Насоки 4/2018 относно акредитацията на сертифициращи органи съгласно член 43 от ОРЗД и приложението към него с оглед на глава V. По отношение на предаването на данни обаче в настоящите насоки допълнително са обяснени някои от изискванията за акредитация, приложими към сертифициращия орган.

Третата част на настоящите насоки („СПЕЦИФИЧНИ КРИТЕРИИ ЗА СЕРТИФИЦИРАНЕ“) съдържа указания относно критериите за сертифициране, които вече са посочени в Насоки 1/2018, и определя допълнителни специфични критерии, които следва да бъдат включени в механизъм за сертифициране, предназначен за използване като инструмент за предаване на данни на трети държави. Тези критерии обхващат оценката на законодателството на третата държава, общите задължения на износителите и вносителите, правилата за последващо предаване на данни, средствата за правна защита и правоприлагането, процеса и действията в случаи, в които националното законодателство и практики възпрепятстват спазването на ангажиментите, поети в рамките на сертифицирането, и исканията за достъп до данни от страна на органите на третата държава.

В четвъртата част на настоящите насоки („ЗАДЪЛЖИТЕЛНИ И ИЗПЪЛНИМИ АНГАЖИМЕНТИ КОИТО ТРЯБВА ДА БЪДАТ ВЪВЕДЕНИ“) са посочени елементите, които следва да бъдат разгледани в задължителните и изпълними ангажименти, които администраторите или обработващите лични данни, непопадащи в обхвата на ОРЗД, следва да поемат с цел осигуряване на подходящи гаранции за данните, предавани на трети държави. Тези ангажименти, които могат да бъдат определени в различни инструменти, включително договори, включват по-специално гаранция, че вносителят няма причина да смята, че законодателството и практиките в третата държава, приложими към съответното обработване, включително всякакви изисквания за разкриване на лични данни или мерки, разрешаващи достъп на публични органи, му пречат да изпълни ангажиментите си по сертифицирането.

ПРИЛОЖЕНИЕТО към настоящите насоки съдържа някои примери за допълващи мерки в съответствие с посочените в приложение II към Препоръки 01/2020 (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) по отношение на използването на сертификат като инструмент за трансфер на данни. Примерите са съставени с цел да се привлече вниманието към критични ситуации.

СЪДЪРЖАНИЕ

Европейският комитет по защита на данните,

като взе предвид член 70, параграф 1, буква д) от Регламент (ЕС) 2016/679 на Европейския парламент и Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (наричан по-нататък ОРЗД),

като взе предвид Споразумението за ЕИП, и по-специално приложение XI и Протокол 37 към него, изменени с Решение № 154/2018 на Съвместния комитет на ЕИП от 6 юли 2018 г.[1],

като взе предвид членове 12 и 22 от своя Правилник за дейността,

ПРИЕ СЛЕДНИТЕ НАСОКИ:

1 ОБЩИ ПОЛОЖЕНИЯ

1.1 Цел и обхват

1. Целта на настоящия документ е да се предоставят насоки относно прилагането на член 46, параграф 2, буква е) от ОРЗД за предаването на лични данни на трети държави или международни организации въз основа на сертифициране. ЕКЗД вече публикува общи насоки относно сертифицирането[2] и акредитацията[3] съгласно ОРЗД. Следователно, настоящите нови насоки отразяват само специфичните аспекти, свързани със сертифицирането като инструмент за предаване на данни. В тях се уточнява прилагането на член 46, параграф 2, буква е) и член 42, параграф 2 от ОРЗД, като се предоставят практически насоки в това отношение и се въвеждат нови елементи към вече публикуваните насоки.

2. ЕКЗД ще оцени функционирането на тези насоки с оглед на опита, натрупан при тяхното прилагане в практиката, и ще предостави допълнителни указания за изясняване на прилагането на посочените по-долу елементи, включително ролята на споразумението за сертифициране по отношение на задължителните и изпълними ангажименти, посочени в член 46, параграф 2, буква е) от ОРЗД.

1.2 Общи правила, приложими за международното предаване на данни

3. Съгласно член 44 от ОРЗД всяко предаване на лични данни на трети държави[4] или международни организации трябва да се осъществява само при условие че са спазени другите разпоредби на ОРЗД в допълнение към спазването на глава V. Поради това всяко предоставяне на данни трябва да отговаря, наред с другото, на принципите за защита на данните в член 5 от ОРЗД, да бъде законосъобразно в съответствие с член 6 от ОРЗД и да е в съответствие с член 9 от ОРЗД в случай на специални категории данни. Следователно трябва да се извърши проверка,

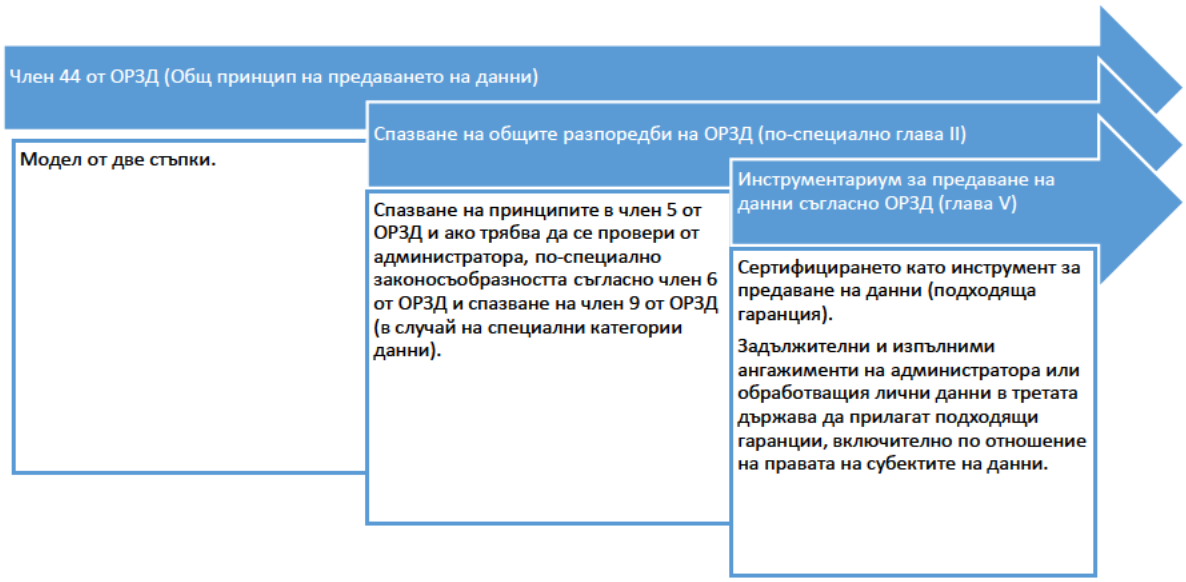
[1] Позоваването на „държави членки“ в настоящия документ следва да се разбира като позоваване на „държавите — членки на ЕИП“.

[2] Насоки 1/2018 относно сертифицирането и определянето на критериите за сертифициране в съответствие с членове 42 и 43 от Регламент 2016/679.

[3] Насоки 4/2018 относно акредитацията на сертифициращи органи съгласно член 43 от Общия регламент относно защитата на данните (2016/679).

[4] Насоки 5/2021 относно взаимодействието между прилагането на член 3 и разпоредбите относно международното предаване на данни съгласно глава V от ОРЗД, стр. 4.

която се състои от два етапа. На първо място трябва да се гарантира спазването на общите разпоредби на ОРЗД, а на второ място трябва да се спазват разпоредбите на глава V.



4. В член 46 от ОРЗД е посочено, че „при липса на решение съгласно член 45, параграф 3, администраторът или обработващият лични данни може да предава лични данни на трета държава или международна организация само ако е предвидил подходящи гаранции и при условие че са налице приложими права на субектите на данни и ефективни правни средства за защита“. Съгласно член 46, параграф 2, буква е) от ОРЗД такива подходящи гаранции могат да бъдат предвидени посредством одобрен механизъм за сертифициране, заедно със задължителни и изпълними ангажименти на администратора или обработващия лични данни в третата държава да прилагат подходящите гаранции, включително по отношение на правата на субектите на данни.

5. В резултат на това износителят на данни може да реши да разчита на сертификата, получен от вносителя на данни, като елемент за доказване на спазването на неговите задължения, например съгласно член 24, параграф 3 или член 28, параграф 5 от ОРЗД. Вносителят на данни може да реши да подаде заявление за сертифициране, за да докаже, че са въведени подходящи гаранции.

6. Както износителят, така и вносителятна данни могат да изпълняват различни роли (например на администратор или обработващ данни)[5] в зависимост от обработването в рамките на глава V, което води до различни отговорности:

[5] Вж. по-долу УКАЗАНИЯ ЗА ПРИЛАГАНЕ НА КРИТЕРИИТЕ ЗА СЕРТИФИЦИРАНЕ.

7. Освен използването на сертифициране или на някой от другите инструменти или механизми за предаване на данни, посочени в членове 45 и 46, в член 49 от ОРЗД е предвидено, че в ограничен брой особени случаи може да се извършва международно предаване на данни, когато не е спазен нито един друг механизъм в глава V[6]. Въпреки това, както е обяснено в предходните насоки, издадени от ЕКЗД, дерогациите, предвидени в член 49 от ОРЗД, трябва да се тълкуват ограничително и главно да се отнасят до дейности по обработване, които засягат отделни случаи и са неповторяеми[7].

1.3 Кои са участниците и каква е тяхната роля за сертифицирането като инструмент за предаване на данни?

8. **Европейският комитет по защита на данните (ЕКЗД)** е оправомощен да одобрява критериите за сертифициране в рамките на ЕИП (Европейски печат за защита на данните) и да предоставя становища по проекторешенията на надзорните органи относно критериите за сертифициране и изискванията за акредитация на сертифициращите органи, за да се осигури съгласуваност. Освен това той е компетентен да обединява всички механизми за сертифициране и всички печати и маркировки за защита на данните в регистър и да осигурява публичен достъп до тях[8].

9. **Надзорните органи** одобряват критериите за сертифициране, когато механизмът за сертифициране не е Европейски печат за защита на данните[9]. Те могат също така да акредитират сертифициращия орган, да изготвят критериите за сертифициране и да издават сертификати, ако това е предвидено в националното законодателство на тяхната държава членка[10].

10. **Националният орган по акредитация** може да акредитира сертифициращи органи на трети страни въз основа на ISO 17065 и допълнителните изисквания за акредитация на надзорните органи, които следва да са в съответствие с раздел 2 от настоящите насоки. В някои държави членки акредитацията може да се предлага както от компетентния надзорен орган, така и да се извършва от национален орган по акредитация или и от двата.

11. **Собственикът на схемата** е организация, която е създала критерии за сертифициране и изисквания за методологията, съгласно които трябва да се оцени съответствието. Организацията, извършваща оценяването, може да бъде същата организация, която е разработила схемата и е неин собственик, но може да съществуват договорености, съгласно които една организация да притежава схемата, а друга (или няколко други) да извършва (ват) оценяването като сертифициращ (и) орган (и).

12. В зависимост от националното законодателство **сертифициращият орган**, акредитиран съгласно посоченото по-горе, може да издава сертификати като алтернатива на надзорните органи[11]. Той може да разработи критерии за сертифициране и по този начин да бъде собственик на схемата (вж. точка 11 по-горе). Той трябва да е установен в ЕИП, по-специално, за да позволи ефективното упражняване на корективните правомощия, залегнали в член 58, параграф 2,

[6] За допълнителна информация относно член 49 и неговото взаимодействие с член 46 като цяло, вж. Насоки 2/2018 относно дерогациите по член 49 от Регламент 2016/679.
[7] Насоки 2/2018 относно дерогациите по член 49 от Регламент 2016/679, стр. 5.
[8] Член 42, параграф 8 от ОРЗД.
[9] Насоки 1/2018 относно сертифицирането и определянето на критериите за сертифициране в съответствие с членове 42 и 43 от Регламент 2016/679, точка 2.2.
[10] Член 42, параграф 5 и член 43, параграф 1 от ОРЗД.
[11] Член 42, параграф 5 от ОРЗД.

буква е) от ОРЗД. Сертифициращият орган обаче може да възлага дейности на подизпълнители — местни експерти или структури извън ЕИП, които да извършват одитни дейности от негово име[12]. Въпреки това сертифициращият орган не възлага на подизпълнители вземането на решение за издаване на сертификат или за отказ за издаване на сертификат.

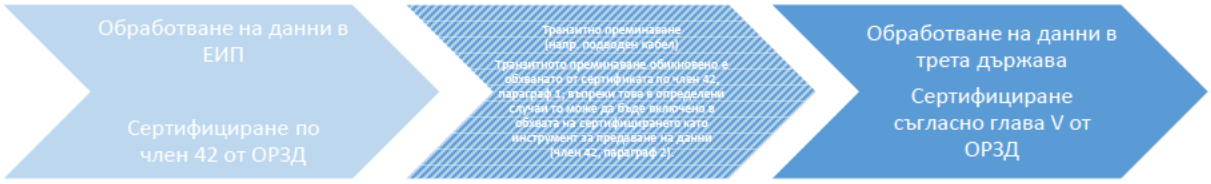
13. **Вносителят на данни** е субектът (администратор или обработващ лични данни) в третата държава, който получава данни от износител на данни.

14. **Износителят на данни** е субектът (администратор или обработващ лични данни), който предава данни от ЕИП на вносител на данни. Износителят на данни трябва да гарантира спазването на глава V.

1.4 Какви са обхватът и обектът на сертифицирането като инструмент за предаване на данни?

15. Механизмът за сертифициране като инструмент за предаване на данни съгласно член 42, параграф 2 трябва да има за цел да осигури подходящи гаранции за обработването на лични данни съгласно условията на член 46, параграф 2, буква е). Сертифицирането доказва наличието на подходящи гаранции, предоставени от администраторите или обработващите лични данни извън ЕИП или представляващи международна организация, която получава данни от администратори или обработващи лични данни от ЕИП, за да се противодейства на специфичните рискове, свързани с предаването на лични данни.

16. По принцип операцията по трансфер на лични данни от държава членка към трета държава сама по себе си представлява обработване на лични данни по смисъла на член 4, точка 2 от ОРЗД, извършвано на територията на държава членка[13], и следователно подлежи на сертифициране съгласно член 42, параграф 1 от ОРЗД. Въпреки това в някои случаи, в зависимост от контекста, транзитното преминаване може да бъде включено в обхвата на сертифицирането като инструмент за предаване на данни. Следователно обектът на сертифицирането, който съвпада с обекта на оценката (ОнО) по време на сертифицирането[14], обикновено следва да бъде обработването на данните, получени от ЕИП от вносителя на данни, в третата държава и транзитното преминаване, ако е под контрола на вносителя.



[12] Сертифициращите органи трябва да оценяват своите местни експерти в съответствие с ISO 17065 и с допълнителните изисквания за акредитация, определени от надзорния орган (член 43, параграф 1, буква б) от ОРЗД).

[13] Решение на Съда по дело C-311/18 — Data Protection Commissioner срещу Facebook Ireland Ltd и Maximillian Schrems, т. 83.

[14] Насоки 1/2018 относно сертифицирането и определянето на критериите за сертифициране в съответствие с членове 42 и 43 от Регламент 2016/679, стр. 17.

17. Обектът на сертифициране може да бъде отделна операция по обработване на данни или набор от операции. Те могат да включват процеси на управление в смисъл на организационни мерки, следователно като неразделна част от операцията по обработване на данни[15].

18. Следователно субектът, който подава заявлението, ще бъде вносителят на данни в третата държава по отношение на обекта на сертифициране.

1.5 Каква следва да бъде ролята на износителя на данни при използването на сертифицирането като инструмент за предаване на данни?

19. Самото предаване на данни от износителя на данни по принцип попада пряко в обхвата на ОРЗД. Това означава, че износителят на данни е длъжен да изпълни задълженията си по ОРЗД и по-специално да осигури предаването на данните по сигурен начин в съответствие с член 32 и глава V, за да се гарантира, че необходимото ниво на защита на физическите лица, осигурено от посочения регламент, не се излага на риск (член 44 от ОРЗД)[16]. Това, разбира се, може да бъде сертифицирано съгласно член 42, параграф 1.

20. Освен това износителят на данни, който иска да използва сертификат като подходяща гаранция съгласно член 46, параграф 2, буква е) от ОРЗД, е длъжен да провери дали сертификатът, на който възнамерява да се основава, е ефективен с оглед на характеристиките на планираното обработване. За тази цел износителят трябва да провери валидността и срока на действие на издадения сертификат, дали той обхваща конкретното предаване на данни, което трябва да се извърши, и дали транзитното преминаване на лични данни попада в обхвата на сертификата, както и дали става въпрос за последващи предавания и дали за тях е предоставена подходяща документация. Освен това трябва да провери дали сертифициращият орган, който издава сертификата, е акредитиран от национален орган по акредитация или от компетентен надзорен орган. Също така следва да посочи използването на сертифицирането като инструмент за предаване на данни в договора за обработване на данни по член 28 от ОРЗД в случай на предаване на данни от администратор на обработващ лични данни или в договора за обмен на данни с вносителя на данни в случай на предаване на данни от администратор на администратор.

21. Като се има предвид, че износителят на данни е отговорен за прилагането на всички разпоредби на глава V, той трябва също така да прецени дали сертификатът, на който възнамерява да се основава като инструмент за предаване на данни, е ефективен с оглед на действащото законодателство и практики в третата държава, които са от значение за въпросното предаване.

---

[15] Насоки 1/2018 относно сертифицирането и определянето на критериите за сертифициране в съответствие с членове 42 и 43 от Регламент 2016/679, стр. 16 (напр. механизъм за обработване на жалби).

[16] В това отношение е важно да се отбележи, че в член 44 от ОРЗД е ясно предвидено, че предаването на данни може да бъде извършено не само от администратор, но и от обработващ лични данни. Следователно ще е налице случай на предаване на данни, при който обработващ лични данни изпраща данни на друг обработващ лични данни или дори на администратор в трета държава по нареждане на своя администратор (член 28, параграф 3, буква а) от ОРЗД). В тези случаи обработващият лични данни действа като износител на данни от името на администратора и трябва да гарантира, че разпоредбите на глава V са спазени за въпросното предаване на данни в съответствие с нареждането на администратора, включително че се използва подходящ инструмент за предаване на данни. Като се има предвид, че предаването на данни е дейност по обработване, извършвана от името на администратора, администраторът също носи отговорност и може да бъде подведен под отговорност съгласно глава V, а също така трябва да гарантира, че обработващият лични данни предоставя достатъчни гаранции съгласно член 28.

За целите на тази оценка и като важен елемент, чрез който доказва изпълнението на своята отговорност, износителят на данни може да се основава на извършената от сертифициращия орган проверка на документираната от вносителя оценка на законодателството и практиките на третата държава.

22. В случай че оценката на вносителя е показала, че той и/или износителят на данни могат да се нуждаят от предоставяне на допълващи мерки, предвидени в сертификата, за да се осигури по същество равностойно ниво на защита, каквото се предоставя в ЕИП, износителят на данни трябва да провери допълващите мерки, предоставени от вносителя, притежаващ сертификат, и дали той е в състояние да отговори на техническите и (ако има такива) допълващи мерки, поискани от вносителя на данни.

23. Ако тези разпоредби не са изпълнени, износителят на данни ще трябва да поиска от вносителя да въведе адаптирани допълващи мерки или да ги установи сам.

1.6 Какво представлява процесът на сертифициране като инструмент за предаване на данни?

24. Сертифицирането е доброволно, но когато е поискано, то трябва да бъде предоставено чрез прозрачен процес, основан на задължителни правила. ОРЗД разчита до голяма степен на частните механизми за сертифициране като „регулирано саморегулиране“. Съответно тези механизми трябва да гарантират, че сертификатите отговарят по същество на изискванията за подходящи гаранции, както е определено в член 46 от ОРЗД.

25. Следователно сертифицирането трябва да се основава на оценка на критериите за сертифициране съгласно задължителна методология за одит. Тези критерии ще бъдат одобрени от националните надзорни органи или от ЕКЗД, както е описано в член 42, параграф 5 от ОРЗД. Критериите за сертифициране включват изисквания за оценка на обработването, извършвано от вносителя на данни, включително последващи предавания на данни, и на съответната правна рамка на третата държава, за да се избегне възможността правилата и практиките на третата държава да попречат на вносителя да изпълни задълженията си по сертифицирането.

26. По време на процеса на сертифициране обектът на оценката се проверява съгласно критериите за сертифициране от сертифициращ орган, акредитиран от националния орган по акредитация или от компетентния надзорен орган[17].

27. Съгласно член 43, параграф 1 от ОРЗД сертифициращите органи, притежаващи подходящ опит в областта на защитата на данните, издават и подновяват сертификати, след уведомяване на надзорния орган с цел той да може да упражни правомощията си съгласно член 58, параграф 2, буква з) от ОРЗД, когато е необходимо.

28. В съответствие с член 43, параграф 5 от ОРЗД сертифициращите органи представят на компетентните надзорни органи мотивите за издаване или отнемане на исканията сертификат. Това не означава, че сертифициращият орган се нуждае от разрешението на надзорния орган, за да издаде сертификат. Сертифициращият орган ще следи дали неговите клиенти спазват критериите за сертифициране.

[17] Насоки 4/2018 относно акредитацията на сертифициращи органи съгласно член 43 от Общия регламент относно защитата на данните (2016/679), стр. 9.

29. Надзорният орган разполага с корективно правомощие да отнема сертификат или да разпореди отнемането му съгласно членове 42 и 43 от ОРЗД, или да нареди на сертифициращия орган да не издава сертификат, ако изискванията за сертифицирането вече не се изпълняват.

30. Европейският печат за защита на данните за международно предаване на данни може да послужи като инструмент за обхващане на предаването на данни на трети държави заедно със задължителните и изпълними ангажименти[18].

31. Въпреки това сертификатите, които се използват като инструмент за предаване на данни, могат да бъдат издавани и в съответствие с одобрени национални схеми за сертифициране в държавите от ЕИП. В този смисъл те са валидни само за предаване на трети държави от износители в държавата — членка на ЕИП, в която е одобрена схемата за сертифициране, тъй като няма взаимно признаване на сертификати от различни държави. Надзорните органи в различни държави от ЕИП обаче могат да одобрят един и същ механизъм за сертифициране на предаване на данни[19].

2 УКАЗАНИЯ ЗА ПРИЛАГАНЕ НА ИЗИСКВАНИЯТА ЗА АКРЕДИТАЦИЯ

32. Изискванията за акредитация на сертифициращ орган по отношение на сертифицирането като инструмент за предаване на данни са посочени в ISO 17065 и чрез тълкуване на Насоки 4/2018[20] във връзка с глава V, както е обяснено по-долу.

33. ЕКЗД счита, че допълнителните изисквания за акредитация, изготвени въз основа на Насоки 4/2018 и ISO 17065 и приети в съответствие с член 64, параграф 1, буква в) от ОРЗД, вече обхващат специфичните изисквания, необходими за акредитацията на сертифициращ орган по отношение на сертифицирането като инструмент за предаване на данни. Обаче, при определни случаи на трансфер на данни някои изисквания може да се нуждаят от уточнения по отношение на обяснителните бележки и тълкуването.

34. По отношение на изискванията за ресурсите (вж. изискване 6 от приложение 1 към Насоки 4/2018) сертифициращият орган гарантира, че разполага с необходимите ресурси, за да може да провери дали, както се изисква от критериите за сертифициране, вносителят на данни надлежно и правилно е извършил необходимата оценка на правното положение и практиките на третата държава или държави, в които е установен или извършва дейност[21]. Тази оценка следва да бъде извършена по отношение на дейностите по обработване, които трябва да бъдат

[18] Вж. член 42, параграф 5 от ОРЗД и точка 35 от Насоки 1/2018 на ЕКЗД относно сертифицирането и определянето на критериите за сертифициране в съответствие с членове 42 и 43 от регламента.
[19] Ако надзорен орган отговаря за приемането на критериите за сертифициране X в рамките на своя национална инициатива и след това, като се вземат предвид критериите на схемата и приложимите специфични национални разпоредби, други държави искат да приемат същите критерии за сертифициране, те могат да ги приемат, без да задействат становище на ЕКЗД по член 64 от ОРЗД, и да се основат на становището, дадено на първия надзорен орган по член 64, параграф 3 от ОРЗД (вж. в тази връзка препратка към насоки — допълнение (приложение към Насоки 1/2018 относно сертифицирането и определянето на критериите за сертифициране в съответствие с членове 42 и 43 от регламента, точка 66).
[20] Насоки 4/2018 относно акредитацията на сертифициращи органи съгласно член 43 от ОРЗД и приложението към него.
[21] Вж. точка 12 по-горе.

сертифицирани като част от ОнО, с оглед на подходящите гаранции от член 46 от ОРЗД, и включва допълващите мерки, определени и прилагани от вносителя на данни, когато е необходимо. Това включва също така например всеобхватно познаване на съответните местни закони и практики и адекватни езикови умения по отношение на третата държава или държави.

35. Що се отнася до изискванията към процеса (вж. изискване 7 от приложение 1 към Насоки 4/2018) сертифициращият орган гарантира, че процесът на сертифициране може да бъде подкрепен от евентуални одити на място, чесе извършва по отношение на обработването на данни, което ще се състои в третата държава или държави, и че оценката обхваща и прилагането на практика на съществуващите закони и политики в третата държава или държави.

36. По отношение на изискванията към промените, засягащи сертифицирането (вж. изискване 7.10 от приложение 1 към Насоки 4/2018), сертифициращият орган следи за промени в законодателството и/или съдебната практика на трети държави, които могат да окажат въздействие върху обработването, попадащо в обхвата на ОнО.

3 СПЕЦИФИЧНИ КРИТЕРИИ ЗА СЕРТИФИЦИРАНЕ

37. При разглеждането на специфичните критерии за сертифициране настоящите насоки се основават на Насоки 1/2018 относно сертифицирането и определянето на критериите за сертифициране в съответствие с членове 42 и 43 от Регламента (версия 3.0), приложение 2 към тях относно прегледа и оценката на критериите за сертифициране в съответствие с член 42, параграф 5 и допълнението към Насоките за оценяване на критериите за сертифициране.

38. ЕКЗД счита, че критериите за сертифициране, изготвени въз основа на приложение 2 към Насоки 1/2018 и допълнението към Насоките за оценяване на критериите за сертифициране, вече обхващат по-голямата част от критериите за сертифициране, които трябва да бъдат взети предвид при изготвянето на схема за сертифициране, която да се използва като инструмент за предаване на данни. Възможно е обаче да е необходимо допълнително уточняване на някои от тези съществуващи критерии, за да бъдат адаптирани към конкретен случай на трансфер на данни (вж. точка 3.1). Освен това може да е необходимо да се формулират допълнителни критерии за целите на прилагането на подходящи гаранции, включително по отношение на правата на субектите на данни (вж. точка 3.2).

3.1 УКАЗАНИЯ ЗА ПРИЛАГАНЕ НА КРИТЕРИИТЕ ЗА СЕРТИФИЦИРАНЕ

39. По отношение на обхвата на механизма за сертифициране и обекта на оценката (ОнО) (вж. приложение 2, раздел 2.а), той следва да бъде ясно описан в съответната документация, включително по отношение на предаването на лични данни на трета държава или дали се предвижда да обхване и тяхното транзитно преминаване.

40. По отношение на обхвата на механизма за сертифициране и обекта на оценката (ОнО) (вж. приложение 2, раздел 2.б) в съответната документация следва да е описано конкретно за кой тип субект (напр. администратор и/или обработващ лични данни) е приложим механизмът за сертифициране.

41. По отношение на обхвата на механизма за сертифициране и обекта на оценката (ОнО) (вж. приложение 2, раздел 2.е) критериите следва да изискват конкретното определяне на ОнО, за да се избегнат недоразумения. Това следва да включва най-малко:

42. операцията(ите) по обработване на данни, включително в случай че се предвижда последващо предаване:

    а) целта;

    б) вида на субекта (напр. администратор и/или обработващ личните данни);

    в) вида на предаваните данни, като се отчита дали става въпрос за специални категории лични данни, както е определено в член 9 от ОРЗД;

    г) категориите субекти на данни;

    д) държавите, в които се извършва обработването на данни.

43. По отношение на прозрачността и правата на субектите на данни (вж. приложение 2, раздел 8) съгласно критериите за сертифициране следва:

    а) да се изисква предоставяне на информация на субектите на данни относно дейностите по обработване на данни, включително, когато е приложимо, относно предаването на лични данни на трета държава или международна организация (вж. членове 12, 13, 14 от ОРЗД);

    б) да се изисква гарантирането на субектите на данни на техните права за достъп, коригиране, изтриване, ограничаване, уведомяване относно коригиране или изтриване или ограничаване, възражение срещу обработването, на правото да не бъдат обект на решения единствено въз основа на автоматизирано обработване, включително профилиране, които по същество са равностойни на предвидените в членове 15—19, 21 и 22 от ОРЗД;

    в) да се изисква от вносителя на данни, притежаващ сертификат, да създаде подходяща процедура за разглеждане на жалби, за да се гарантира ефективното прилагане на правата на субекта на данните;

    г) да се изисква да се прецени, дали и до каква степен тези права са приложими за субектите на данни в съответната трета държава, както и да се оценят всякакви допълващи подходящи мерки, които може да се наложи да бъдат въведени, за да бъдат приложени, например изискване вносителят да приеме да подлежи на юрисдикцията на надзорния орган, компетентен за износителя(ите), и да си сътрудничи с него във всички процедури, целящи да гарантират спазването на тези права, и по-специално, да се съгласи да отговаря на запитвания, да се подлага на одити и да спазва мерките, приети от горепосочения надзорен орган, включително коригиращи, и компенсаторни мерки.

44. По отношение на техническите и организационните мерки, гарантиращи защита (приложение 2, раздел 10.р), съгласно критериите за сертифициране следва да се изисква от вносителя на данни да информира износителя на данни и, ако вносителят на данни действа като администратор на данни, да уведоми надзорния орган в ЕИП, компетентен за износителя(ите) на данни, при нарушения на сигурността на данните и да ги съобщи на субектите на данни, когато има вероятност нарушението да доведе до висок риск за техните права и свободи, в съответствие с изискванията на член 34 от ОРЗД.

3.2 ДОПЪЛНИТЕЛНИ СПЕЦИФИЧНИ КРИТЕРИИ ЗА СЕРТИФИЦИРАНЕ

45. С оглед на гаранциите, определени за други инструменти за предаване на данни съгласно член 46 от ОРЗД (като задължителни фирмени правила или кодекси за поведение), и с цел да се осигури последователно ниво на защита, както и като се вземе предвид решението Schrems II на

Съда на ЕС, ЕКЗД счита, че механизмът за сертифициране, който ще се използва като инструмент за предаване на данни на трети държави, следва да включва и изброените по-долу критерии.

1. Оценка на законодателството на третата държава

а) Съгласно критериите от вносителя на данни изисква ли се да е оценил правилата и практиките на третата държава, в която извършва дейност, и дали те не пречат на вносителя на данни да изпълнява ангажиментите си по сертифицирането?

б) Съгласно критериите от вносителя на данни изисква ли се да документира оценката на правилата и практиките на третата държава, в която извършва дейност, и да съхранява документацията на разположение на сертифициращия орган и при поискване на надзорния орган, компетентен за износителя на данни в ЕИП, и на износителя на данни?

в) Съгласно критериите от вносителя на данни изисква ли се да е определил и приложил организационните и техническите мерки за осигуряване на подходящи гаранции съгласно член 46 от ОРЗД, като се вземат предвид 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?

г) Съгласно критериите от вносителя на данни изисква ли се да документира организационните и техническите мерки, които ефективно прилага, за да осигури подходящите гаранции по член 46 от ОРЗД, и да съхранява документацията, за да е на разположение на сертифициращия орган и при поискване на компетентните органи за защита на данните и на износителя на данни?

д) Съгласно критериите от вносителя на данни изисква ли се да е определил и приложил организационните и техническите мерки за гарантиране на сигурността на предадените лични данни, като се вземат предвид Препоръки 01/2020 относно мерките, които допълват инструментите за предаване на данни, за да се гарантира спазването на нивото на защита на личните данни, заложено в ЕС, ако транзитното преминаване е включено в обхвата на сертифицирането като инструмент за предаване?

е) Съгласно критериите изисква ли се гаранция пред сертифициращия орган и износителя на данни, че вносителят на данни няма причина да смята, че приложимото към него законодателство и практики могат да му попречат да изпълнява задълженията си в рамките на сертифицирането?

2. Общи задължения на износителите и вносителите на данни

а) Съгласно критериите изисква ли се в договорните споразумения (напр. в съществуващ договор за услуги) между износителите и вносителите на данни да се съдържа описание на конкретното предаване на данни, за което се прилага сертифицирането, и да се признаят правата на третата страна бенефициент на съответните субекти на данни?

б) Доколкото съгласно критериите се изисква специфично съдържание за тези договорни споразумения или инструменти и е предоставен образец, изисква ли се самите критерии също да бъдат предмет на оценка?

3. Правила за последващи предавания на данни

а) Съгласно критериите изисква ли се последващите предавания на данни да подлежат на специфични гаранции в съответствие с изискванията на глава V от ОРЗД, така че да се гарантира, че нивото на защита на личните данни в ЕИП няма да бъде изложено на риск, и съгласно критериите изисква ли се съответната документация да бъде на разположение на сертифициращия орган и на надзорния орган в ЕИП за износителя (ите) на данни, както и на износителя на данни при поискване?

4. Правни средства за защита и правоприлагане

а) Съгласно критериите предвижда ли се субектите на данни да могат да упражняват правата си като трети страни бенефициенти срещу вносителя на данни пред съда на ЕИП по обичайното местопребиваване или пред международна организация, включително за обезщетение за вреди, претърпени от субектите в случай на неспазване от страна на вносителя на съответната схема за сертифициране?

б) Позволяват ли критериите да се прецени по подходящ начин, че даден вносител на данни носи отговорност в ЕИП за вредите, понесени от субекта на данните, в случай на неспазване на съответната схема за сертифициране?

в) Съгласно критериите изисква ли се субектите на данни да могат да подадат жалба срещу вносителя на данни до надзорен орган в ЕИП, по-специално в държавата от ЕИП, в която е обичайното им местопребиваване или мястото им на работа или която е компетентна за износителя (ите) на данни?

г) Съгласно критериите изисква ли се вносителят на данни да си сътрудничи с надзорния орган в ЕИП, компетентен за износителя (ите) на данни, и да приеме да бъде одитиран и проверяван от него**,** да се съобразява с неговите съвети и да спазва неговите решения?

5. Процес и действия в случаи, в които националното законодателство възпрепятства спазването на ангажиментите, поети в рамките на сертифицирането

а) Съгласно критериите има ли заложено изискване, когато вносителят на данни в трета държава или международна организация има основания да смята, че промени в приложимото към него законодателство и практики могат да му попречат да изпълни задълженията си по сертифицирането, той незабавно да уведоми за това сертифициращия орган и износителя на данни, за да може износителят да прецени дали да спре незабавно предаването на данни?

б) Съгласно критериите изисква ли се описание на стъпките, които трябва да бъдат предприети (включително уведомяване на износителя на данни в ЕИП и предприемане на подходящи допълващи мерки), ако вносителят на данни узнае за законодателство или практики на трета държава, които възпрепятстват спазването на задълженията по сертифицирането, както и мерките, които трябва да бъдат предприети в случай на искания за информация от органи на трета държава (включително задължението за преглед и, когато е необходимо, оспорване на законосъобразността на искането и свеждане до минимум на всяка разкрита информация)?

6. Разглеждане на искания за достъп до данни от органи на трети държави

а) Съгласно критериите изисква ли се вносителят на данни незабавно да информира износителя в случай на искания за достъп от органи на трета държава и да предприеме подходящи допълнителни мерки?

б) Съгласно критериите изисква ли се да не се извършва предаване на данни в резултат на непропорционални искания за достъп от публични органи на трети държави, по-специално искания, които изискват предаване на огромно и неизбирателно количество лични данни?

7. Допълнителни гаранции по отношение на износителя на данни

46. Съгласно критериите изисква ли се, когато това е предвидено, вносителят на данни да гарантира, също и чрез задължителни изисквания към износителя на данни, че определените от него допълващи мерки са съчетани със съответни допълващи мерки от страна на износителя, като се вземат предвид Препоръки 01/2020 на ЕКЗД и случаите на употреба, за да се гарантира ефективното прилагане на допълващите мерки на вносителя?

4. ЗАДЪЛЖИТЕЛНИ И ИЗПЪЛНИМИ АНГАЖИМЕНТИ, КОИТО ТРЯБВА ДА БЪДАТ ВЪВЕДЕНИ

47. В член 42, параграф 2 от ОРЗД се изисква администраторите и обработващите лични данни, които не попадат в обхвата на ОРЗД и към които се прилага механизмът за сертифициране, предназначен за предаване на данни, да поемат задължителни и изпълними ангажименти чрез договорни или други правно обвързващи инструменти[22] да прилагат подходящите гаранции, включително по отношение на правата на субектите на данни.

48. Както е посочено в ОРЗД, такива ангажименти могат да бъдат поети чрез използване на договор, което изглежда най-лесното решение. Могат да се използват и други инструменти, при условие че администраторът/обработващият лични данни, който се придържа към механизма за сертифициране, е в състояние да демонстрира задължителния характер и изпълнителната сила на другите средства.

49. Във всеки случай задължителният характер и изпълнителната сила трябва бъдат гарантирани в съответствие със законодателството на ЕС и ангажиментите също така следва да имат задължителен характер и изпълнителна сила за субектите на данните като трети страни бенефициенти.

50. Вариант за лесно решение би било задължителните и изпълними ангажиментида се включат в договора между износителя и вносителя на данни. На практика страните могат да използват съществуващ договор (напр. споразумение за услуги между износителя и вносителя на данни, договор за обработване на данни в съответствие с член 28 от ОРЗД между администратори и обработващи лични данни или споразумение за обмен на данни между отделни администратори), в който да се включат задължителните и изпълними ангажименти. Тези ангажименти следва да бъдат ясно разграничени от всички други клаузи. Друг вариант може да бъде да се използва, например, отделен договор, като към механизма за сертифициране,

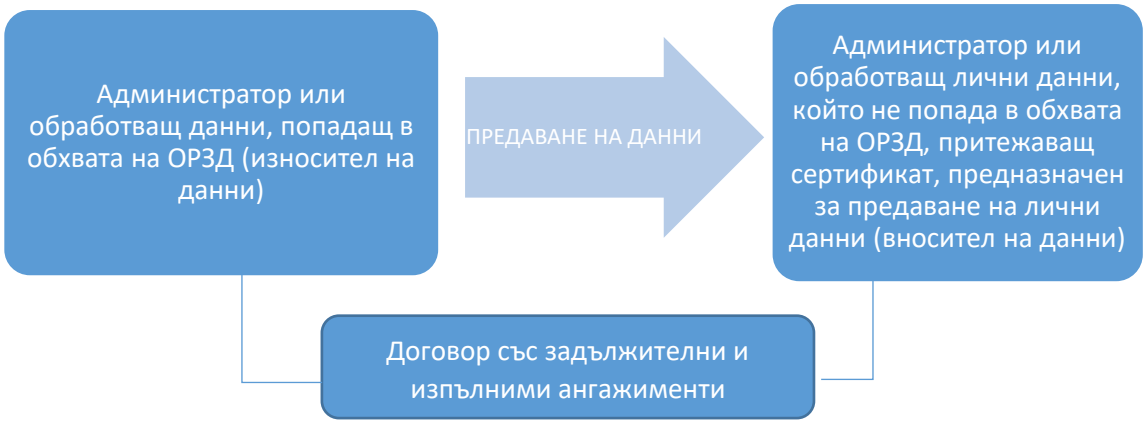
[22] Този правно обвързващ инструмент не може да бъде друг инструмент по глава V (като например СДК), тъй като тези задължителни и изпълними ангажименти, посочени в член 46, параграф 2, буква е), трябва да бъдат разработени така, че да гарантират, че вносителят ще спазва критериите за сертифициране.

предназначен за предаване на лични данни, се добави образец на договор, който след това трябва да бъде подписан от администратори/обработващи лични данни в третата държава и всички нейни износители на данни.

51. Трябва да е налице гъвкавост за избор на най-подходящия вариант в зависимост от конкретната ситуация.

52. Когато механизмът за сертифициране трябва да се използва за предаване на данни и последващ трансфер на данни от обработващ лични данни на обработващ лични данни подизпълнител, в споразумението с обработващия лични данни, подписано между обработващия лични данни и неговия администратор, следва да се направи препратка към механизма за сертифициране и средството, предвиждащо задължителни и изпълними ангажименти.

Пример за задължителни и изпълними ангажименти, включени в договора между износителя и вносителя на данни:



53. По принцип в договора или в друг правно обвързващ инструмент трябва да се посочи, че администраторът/обработващият лични данни, притежаващ сертификат и действащ като вносител на данни, се задължава да спазва правилата, посочени в сертификата, предназначен за предаване на данни, при обработването на съответните данни, получени от ЕИП, и гарантира, че няма причина да смята, че законодателството и практиките в третата държава, приложими към съответното обработване, включително всякакви изисквания за разкриване на лични данни или мерки, разрешаващи достъп на публични органи, му пречат да изпълни ангажиментите си по сертифицирането.

54. В договора или в другия инструмент също така се предвиждат механизми, позволяващи на администратора/обработващия лични данни, действащ като вносител на данни, да изиска принудителното изпълнение на такива ангажименти в случай на неспазване на правилата, свързани със сертифицирането, по-специално по отношение на правата на субектите на данните, чиито данни ще бъдат предадени в рамките на сертифицирането.

55. По-конкретно договорът или другият инструмент следва да включва:

- Наличието на право за субектите на данните, чиито данни се предават в рамките на сертифицирането, да приложат като трета страна бенефициент ангажиментите, поети от сертифицирания вносител на данни в рамките на сертифицирането.

- Въпросът за отговорността в случай на неспазване на правилата за сертифициране от страна на вносител на данни, притежаващ сертификат извън ЕИП. Субектите на данните имат възможност в случай на неспазване на правилата в рамките на сертифицирането от вносител на данни, притежаващ сертификат извън ЕИП, да предявят иск, като се позоват на правото си

на трета страна бенефициент, включително иск за обезщетение, срещу този субект пред надзорен орган в ЕИП и съд в ЕИП по обичайното местопребиваване. Вносителят, притежаващ сертификат, приема решението на субекта на данните да предприеме такива действия. Физическите лица също имат възможността, в случай че неспазването на изискванията от страна на вносителя на данни може да доведе до отговорност на износителя на данни, да предявят иск срещу износителя на данни пред надзорния орган или съда по мястото на установяване на износителя на данни или по обичайното местопребиваване на субекта на данните[23]. Вносителят и износителят на данни следва също да приемат, че субектът на данните може да бъде представляван от структура, организация или сдружение с нестопанска цел при условията, посочени в член 80, параграф 1 от ОРЗД.

- Наличието на право на износителя да прилага спрямо вносителя на данни, притежаващ сертификат, правилата, свързани със сертифицирането, като трета страна бенефициент.
- Наличието на задължение на вносителя на данни, притежаващ сертификат, да уведоми износителя на данни и надзорния орган на износителя на данни за всякакви мерки, предприети от сертифициращия орган в отговор на установено неспазване на правилата, свързани със сертифицирането, от страна на същия вносител на данни.

[23] Тази отговорност следва да не засяга механизмите, които трябва да се прилагат в рамките на сертифицирането от сертифициращия орган, който може също да предприеме действия срещу сертифицираните администратори/обработващи лични данни в съответствие със сертифицирането, чрез налагане на корективни мерки.

ПРИЛОЖЕНИЕ

А. ПРИМЕРИ ЗА ДОПЪЛВАЩИ МЕРКИ, КОИТО ВНОСИТЕЛЯТ ТРЯБВА ДА ПРИЛОЖИ, В СЛУЧАЙ ЧЕ ТРАНЗИТНОТО ПРЕМИНАВАНЕ Е ВКЛЮЧЕНО В ОБХВАТА НА СЕРТИФИЦИРАНЕТО

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

Трябва да се установят критерии, свързани със стандартите за криптиране и сигурността на ключа за декриптиране, и по-специално такива, свързани с правното положение в третата държава. Ако вносителят може да бъде принуден да предаде ключовете за декриптиране, допълващата мярка не може да се счита за ефективна[24].

Случай на употреба 2: Предаване на псевдонимизирани данни

В случай на псевдонимизирани данни се установяват критерии относно сигурността на допълнителната информация, необходима за свързване на предадените данни с идентифицирано лице или лице, което може да бъде идентифицирано, и по-специално:

— Критерии относно правното положение в третата държава. Ако вносителят може да бъде принуден да получи достъп до допълнителни данни или да използва допълнителни данни, за да свърже данните с идентифицирано лице или лице, което може да бъде идентифицирано, мярката не може да се счита за ефективна[25].

— Критерии, свързани с определянето на допълнителната информация, с която разполагат органите на трета държава и която може да е достатъчна, за да се свържат данните с идентифицирано лице или лице, което може да бъде идентифицирано.

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

В случай на криптирани данни се включват всички критерии за сигурност на транзитното преминаване. Ако вносителят може да бъде принуден да предаде криптографски ключове за декриптиране или удостоверяване на автентичността или да модифицира компонент, използван за транзитно преминаване, по такъв начин, че да се нарушат неговите характеристики за защитата на сигурността, допълващата мярка не може да се счита за ефективна[26].

Случай на употреба 4: Защитен получател

В случай на защитени получатели трябва да се определят критерии за границите на правото на защитата. Обработването на лични данни трябва да остане в рамките на правото за запазване на

[24] Приложение 2 към 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, Случай на употреба 1: Съхранение на данни за резервни копия и други цели, за които не се изисква достъп до данните в чист вид, т. 85; https://edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_bg_0.pdf

[25] Вж. по-горе точки 86—89.

[26] Вж. по-горе точка 90.

поверителността. Това се отнася и за обработването от администратори (подизпълнители) и последващите предавания на данни, чиито получатели също трябва да имат право на защита[27].

Б. ПРИМЕРИ ЗА ДОПЪЛВАЩИ МЕРКИ, В СЛУЧАЙ ЧЕ ТРАНЗИТНОТО ПРЕМИНАВАНЕ НЕ Е ОБХВАНАТО ОТ СЕРТИФИКАТА И ИЗНОСИТЕЛЯТ НА ДАННИ ТРЯБВА ДА ГИ ОСИГУРИ

Случай на употреба 2: Предаване на псевдонимизирани данни

Предвиждат се критерии, свързани с допълнителната информация, с която разполагат органите на третата държава и която може да е достатъчна, за да се свържат данните с идентифицирано лице или лице, което може да бъде идентифицирано.

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

Предвиждат се критерии, свързани с надеждността на използвания удостоверяващ орган или инфраструктура за публични ключове, сигурността на криптографските ключове, използвани за удостоверяване или декриптиране, и надеждността на управлението на ключовете, както и използването на правилно поддържан софтуер без известни уязвимости.

Ако вносителят може да бъде принуден да разкрие криптографски ключове, подходящи за декриптиране или удостоверяване на автентичност, или да модифицира компонент, използван за транзитно преминаване, за да изложи на риск неговите характеристики за защитата на сигурността, мярката не може да се счита за ефективна[28].

Случай на употреба 4: Защитен получател

В случай на защитени получатели трябва да се определят критерии за границите на правото на защитата. Обработването на лични данни трябва да остане в рамките на правото за запазване на поверителността. Това се отнася и за обработването от администратори (подизпълнители) и последващите предавания на данни, чиито получатели също трябва да имат право на защита[29].

[27] Вж. по-горе точка 91.
[28] Вж. посочените по-горе препоръки, точка 90.
[29] Вж. посочените по-горе препоръки, точка 91.