Становище на Комитета (член 64)

Становище 22/2024 относно някои задължения, произтичащи от разчитането на обработващ(и) лични данни и обработващ(и) лични данни подизпълнител(и)

Прието на 7 октомври 2024 г.

Резюме

Надзорният орган (НО) на Дания поиска от ЕКЗД да издаде становище по въпроси с общо приложение съгласно член 64, параграф 2 от ОРЗД. Становището допринася за хармонизирано тълкуване от страна на националните надзорни органи на някои аспекти на член 28 от ОРЗД, когато е целесъобразно във връзка с глава V от ОРЗД. В становището се разглеждат, по-специално, въпроси относно тълкуването на някои задължения на администраторите, които разчитат на обработващи лични данни и обработващи лични данни подизпълнители, произтичащи от член 28 от ОРЗД, както и относно формулировката на договорите между администратори и обработващи лични данни. Въпросите засягат обработването на лични данни в ЕИП, както и обработването след предаване на данни на трета държава.

В настоящото становище Комитетът стига до заключението, че администраторите следва да имат на разположение по всяко време информацията относно самоличността (т.е. име, адрес, лице за контакт) на всички обработващи лични данни, обработващи лични данни подизпълнители и т.н., за да могат да изпълняват в най-голяма степен задълженията си съгласно член 28 от ОРЗД, независимо от риска, свързан с дейността по обработване. За тази цел обработващият лични данни следва активно да предоставя на администратора цялата тази информация и постоянно да я актуализира.

В член 28, параграф 1 от ОРЗД се предвижда, че администраторите са длъжни да включат обработващи лични данни, които предоставят „достатъчни“ гаранции за прилагането на „подходящи“ мерки по такъв начин, че обработването да протича в съответствие с изискванията на ОРЗД и да осигурява защита на правата на субектите на данни. В становището си ЕКЗД изразява мнение, че когато оценяват как администраторите спазват това задължение и принципа на отчетност (член 24, параграф 1 от ОРЗД), надзорните органи следва да имат предвид, че включването на обработващите лични данни не следва да понижава равнището на защита на правата на субектите на данни. *Задължението* на администратора да проверява дали обработващите лични данни (подизпълнители) предоставят „достатъчни гаранции“ за прилагане на подходящите мерки, определени от администратора, следва да се прилага независимо от риска за правата и свободите на субектите на данни. Въпреки това *обхватът* на такава проверка на практика ще варира в зависимост от естеството на тези технически и организационни мерки, които могат да бъдат по-строги или по-широкообхватни в зависимост от нивото на този риск.

В становището ЕКЗД допълнително уточнява, че макар първоначалният обработващ лични данни да следва да гарантира, че той предлага обработващи лични данни подизпълнители, предоставящи достатъчни гаранции, крайното решение дали да се включи конкретен подизпълнител и свързаната с това отговорност, включително по отношение на проверката на гаранциите, се взема от администратора. НО следва да преценят дали администраторът е в състояние да докаже, че проверката на това доколко достатъчни са гаранциите, предоставени от неговите обработващи лични данни (подизпълнители), е извършена по удовлетворителен за администратора начин. Администраторът може да избере да се довери на информацията, получена от неговия обработващ лични данни, и да я допълни, ако е необходимо (например когато тя изглежда непълна, неточна или възникват въпроси). По-конкретно, при обработване,

което представлява висок риск за правата и свободите на субектите на данни, администраторът следва да разшири степента на проверката си, като провери предоставената информация. В това отношение ЕКЗД счита, че съгласно ОРЗД администраторът не е длъжен систематично да изисква договорите за подизпълнение, за да проверява дали задълженията за защита на данните, предвидени в първоначалния договор, са били предоставени надолу по веригата на обработване. Администраторът следва да преценява за всеки отделен случай дали е необходимо да поиска копие от такива договори или да ги прегледа по всяко време, за да може да докаже, че се спазва принципът на отчетност.

Когато предаването на лични данни извън ЕИП се извършва между двама обработващи лични данни (подизпълнители) в съответствие с указанията на администратора, той продължава да се подчинява на задълженията, произтичащи от член 28, параграф 1 от ОРЗД относно „достатъчните гаранции“, в допълнение към задълженията съгласно член 44, за да гарантира, че нивото на защита, осигурено от ОРЗД не се подкопава от трансфера на лични данни. В съответствие със съдебната практика и както е обяснено в Препоръки на ЕКЗД 1/2020, обработващият лични данни/износителят трябва да подготви необходимата документация. Администраторът следва да оцени и да може да представи на компетентния НО такава документация. Администраторът може да разчита на документацията или информацията, получени от обработващия лични данни/износителя, и ако е необходимо, да я допълва. Степента и естеството на задължението на администратора да оцени тази документация може да зависи от основанието, използвано за предаването, и от това дали предаването е първоначално или последващо.

В становището си ЕКЗД разгледа също така въпроса относно текста на договорите между администратора и обработващия лични данни. В това отношение основен елемент е задължението обработващият лични данни да обработва лични данни само въз основа на документирано нареждане от администратора, освен когато обработващият лични данни е *„длъжен да [обработи личните данни] по силата на правото на Съюза или правото на държава членка, което се прилага спрямо обработващия лични данни“* (член 28, параграф 3, буква а) от ОРЗД) — като се припомня общият принцип, че договорите не могат да отменят законите. С оглед на свободата на договаряне, предоставена на страните, за да приспособят договора си между администратор и обработващ лични данни към конкретните обстоятелства, спазвайки обхвата на член 28, параграф 3 от ОРЗД, ЕКЗД горещо препоръчва да се включва фразата *„освен когато е длъжен да направи това по силата на правото на Съюза или правото на държава членка, което се прилага спрямо обработващия лични данни“* (дословно или чрез много подобни изрази), без да е задължително.

Що се отнася до вариантите, подобни на *„освен когато е длъжен да направи това по силата на правото или обвързващо разпореждане на държавен орган“*, ЕКЗД счита, че този въпрос остава в прерогативите на свободата на договаряне на страните и сам по себе си не нарушава член 28, параграф 3, буква а) от ОРЗД. Същевременно в становището си ЕКЗД посочва редица нередности, тъй като такава клауза не освобождава обработващия лични данни от спазването на задълженията му съгласно ОРЗД.

За лични данни, предавани извън ЕИП, ЕКЗД счита, че е съмнително формулировката *„освен когато е длъжен да направи това по силата на правото или обвързващо разпореждане на*

държавен орган“ да е достатъчна сама по себе си, за да се постигне спазване на член 28, параграф 3, буква а) от ОРЗД във връзка с глава V. Както е посочено в стандартните договорни клаузи за международни предавания на Европейската комисия и в препоръките относно задължителните фирмени правила за администраторите, по принцип член 28, параграф 3, буква а) от ОРЗД не възпрепятства включването в договора на разпоредби, които се отнасят до законодателните изисквания на трети държави за обработване на предадените лични данни. Въпреки това, както е в случая с тези документи, следва да се прави разграничение между законите на трети държави, които биха изложили на риск нивото на защита, осигурено от ОРЗД, и законите, които не биха го изложили на риск. И накрая, ЕКЗД напомня, че възможността законодателството на трета държава да възпрепятства спазването на ОРЗД следва да бъде фактор, който страните трябва да вземат предвид, преди да сключат договора (между администратора и обработващия лични данни или между обработващия лични данни и обработващия лични данни подизпълнител).

Когато обработващият лични данни обработва лични данни в рамките на ЕИП, при определени обстоятелства той все пак може да бъде засегнат от законодателството на трета държава. ЕКЗД изтъква, че добавянето в договора на формулировка, подобна на „*освен когато е длъжен да направи това по силата на правото или обвързващо разпореждане на държавен орган*“, не освобождава обработващия лични данни от задълженията му съгласно ОРЗД.

И накрая, ЕКЗД е на мнение, че последващото поемане на ангажимент от обработващия лични данни да обработва само въз основа на документирано нареждане с „*освен когато е длъжен да направи това по силата на закон или от задължителна заповед на правителствен орган*“ (дословно или чрез много подобни изрази) не може да се тълкува като писмена инструкция от администратора.

Съдържание

Европейският комитет по защита на данните,

като взе предвид член 63 и член 64, параграф 2 от Регламент 2016/679/ЕС 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 (наричан по-нататък „ОРЗД“),

като взеха предвид Споразумението за Европейското икономическо пространство, и по-специално приложение XI и протокол 37 към него, както е изменено с Решение на Съвместния комитет на ЕИП 154/2018 от 6 юли 2018 г.[1],

като взе предвид членове 10 и 22 от своя Правилник за дейността,

като има предвид, че:

(1) Главната роля на Европейския комитет по защита на данните (наричан по-нататък „Комитетът“) е да гарантира съгласуваното прилагане на ОРЗД в цялото Европейско икономическо пространство (ЕИП). В член 64, параграф 2 от ОРЗД се предвижда, че всеки надзорен орган (НО), председателят на Комитета или Комисията може да поиска всеки въпрос с общо приложение или с последици в повече от една държава членка на ЕИП, да бъде разгледан от Комитета с цел получаване на становище. Целта на настоящото становище е да се проучи въпрос с общо приложение или с последици в повече от една държава членка на ЕИП.

(2) Становището на Комитета следва да се приеме съгласно член 64, параграф 3 от ОРЗД във връзка с член 10, параграф 2 от Правилника за дейността на ЕКЗД в рамките на осем седмици от първия работен ден, след като председателят и компетентните надзорни органи установят, че досието е пълно. По решение на председателя този срок може да бъде удължен с още шест седмици поради сложното естество на въпроса.

ПРИЕ СЛЕДНОТО СТАНОВИЩЕ:

1 ВЪВЕДЕНИЕ

1.1 Кратко изложение на фактите

1. На 5 юли 2024 г. Датският надзорен орган (наричан по-нататък „НО на Дания“) поиска от Европейския комитет по защита на данните (наричан по-нататък „ЕКЗД“ или „Комитетът“) да издаде становище във връзка със задълженията на администраторите за отчетност по отношение на веригата на обработване и отношенията между администраторите и техните обработващи лични данни (подизпълнители) (наричано по-нататък „искането“).

[1] Позоваванията на „държави членки“ в настоящото становище следва да се разбират като позовавания на „държавите — членки на ЕИП“. Позоваванията на „Съюза“ в настоящото становище следва да се разбират като позовавания на „ЕИП“.

2. На 8 юли 2024 г. НО на Дания потвърди, че досието е пълно. На 9 юли 2024 г. председателят на Комитета прие, че досието е пълно. Секретариатът на ЕКЗД публикува досието на същата дата. Като взе предвид сложността на въпроса, председателят реши да удължи законоустановения срок в съответствие с член 64, параграф 3 от ОРЗД и член 10, параграф 4 от Правилника за дейността.

3. В искането си НО на Дания също така се позовава на доклада, приет от ЕКЗД през януари 2023 г., относно констатациите от първото си координирано действие по правоприлагане[2] в рамките на рамката за координирано правоприлагане (РКП)[3]. Това координирано действие беше съсредоточено върху използването на услуги в облак от страна на публичния сектор. В доклада на ЕКЗД надзорните органи, участващи в координираното действие, набелязаха осем предизвикателства, по-специално във връзка с използването на услуги в облак от страна на публичните органи, и предоставиха списък с въпроси, на които съответните заинтересовани страни да обърнат внимание, когато оценяват услугите „в облак“ и взаимодействат с доставчиците на услуги в облак[4]. Въпреки че за повечето от тези точки обхватът на задълженията, наложени от ОРЗД, е ясен както за администраторите, така и за обработващите лични данни, според НО на Дания точният обхват на някои задължения съгласно ОРЗД остава неясен[5].

НО на Дания зададе следните въпроси:

4. <u>Въпрос 1.1</u>: Като се вземат предвид член 5, параграф 2 и член 24, параграф 1 от ОРЗД, когато обработващият лични данни се ангажира да извършва обработване от името на администратора, за да документира спазването, *наред с другото*, на член 28, параграфи 1 и 2 (включително при предоставянето на документация на надзорния орган при проверка):

   а. Трябва ли администраторът да идентифицира всички подизпълнители на обработващия лични данни, техните обработващи лични данни подизпълнители и т.н. по цялата верига на обработване или да идентифицира само първата линия на обработващите лични данни подизпълнители, включени от обработващия лични данни?

   б. До каква степен и колко подробно администраторът трябва да проверява и документира:

      i. наличието на достатъчни гаранции, предоставени от обработващите лични данни, техните обработващи лични данни подизпълнители и т.н.;
      ii. съдържанието на договорите между първоначалния обработващ лични данни и допълнителните обработващи лични данни, за да се установи дали същите задължения са наложени на допълнителните обработващи лични данни съгласно член 28, параграф 4 от ОРЗД; и
      iii. дали обработващите лични данни, техните обработващи лични данни подизпълнители и т.н. отговарят на изискванията на администратора съгласно член 28, параграф 1?

[2] Доклад за координираните действия по правоприлагане от 2022 г. — Използване на услуги в облак от страна на публичния сектор, 17 януари 2023 г. (наричан по-долу „Доклад за рамката за координирано правоприлагане относно услугите в облак“).

[3] Рамката за координирано правоприлагане беше създадена от ЕКЗД през октомври 2020 г. с цел рационализиране на правоприлагането и сътрудничество между надзорните органи. Вж. Документ на ЕКЗД относно рамката за координирано правоприлагане съгласно Регламент 2016/679, приет на 20 октомври 2020 г., версия 1.1.

[4] Доклад за рамката за координирано правоприлагане относно услугите в облак, стр. 10—20.

[5] Искане, стр. 1.

5. Въпрос 1.2: В случаите на предавания или последващи предавания от обработващ лични данни (подизпълнител) на друг обработващ лични данни (подизпълнител) в съответствие с указанията на администратора: До каква степен администраторът, като част от задължението си по член 28, параграф 1 от ОРЗД във връзка с член 44 от ОРЗД трябва да оценява и да е в състояние да покаже документация от обработващите лични данни (подизпълнители), че нивото на защита на личните данни не е изложено на риск от (последващите) предавания на лични данни?

6. Въпрос 1.3: Обхватът на задълженията съгласно член 28, параграфи 1 и 2 от ОРЗД във връзка с член 5, параграф 2 и член 24 от ОРЗД, както е посочено във въпрос 1.1 и въпрос 1.2, варира ли в зависимост от риска, свързан с дейността по обработване? Ако е така, какъв е обхватът на такива задължения за дейности по обработване с нисък риск и за дейности по обработване с висок риск?

7. Въпрос 2: Трябва ли договор или друг правен акт съгласно правото на Съюза или на държава членка съгласно член 28, параграф 3 от ОРЗД да съдържа предвиденото в член 28, параграф 3, буква а) изключение „*освен когато е длъжен да направи това по силата на правото на Съюза или правото на държава членка, което се прилага спрямо обработващия лични данни*“ ((дословно или чрез много подобни изрази), за да е в съответствие с ОРЗД?

8. Въпрос 2а: Ако отговорът на въпрос 2 е отрицателен, когато договор или друг правен акт съгласно правото на Съюза или на държава членка, разширява изключението, заложено в член 28, параграф 3, буква а) от ОРЗД, така че да обхваща като цяло и правото на трета държава (например „освен когато е длъжен да направи това по силата на закон или от задължителна заповед на правителствен орган“), представлява ли това само по себе си нарушение на член 28, параграф 3, буква а) от ОРЗД?

9. Въпрос 2б: Ако отговорът на въпрос 2а е отрицателен, следва ли такова разширено изключение вместо това да се тълкува като документирано указание от администратора по смисъла на член 28, параграф 3, буква а) от ОРЗД?

1.2 Допустимост на искането за становище по член 64, параграф 2 от ОРЗД

10. В член 64, параграф 2 от ОРЗД се предвижда по-специално, че всеки надзорен орган може да поиска всеки въпрос с общо приложение или с последици в повече от една държава членка на ЕИП, да бъде разгледан от Комитета с цел получаване на становище.

11. Първите въпроси, поставени от НО на Дания, се отнасят до задълженията на администраторите за отчетност съгласно член 28 от ОРЗД (въпроси 1.1, 1.2 и 1.3), а последният се отнася до конкретното съдържание на договора между администратора и обработващия лични данни или правния акт съгласно член 28, параграф 3, буква а) от ОРЗД (въпрос 2).

12. Комитетът счита, че тези въпроси са свързани с тълкуването на ОРЗД, по-специално по отношение на отношенията между администраторите и техните обработващи лични данни (подизпълнители), както и с тълкуването на член 5, параграф 2, член 24 и член 28 от ОРЗД. От една страна, искането е свързано със задълженията за отчетност на администраторите и нивото на документацията, която надзорните органи следва да очакват от всички администратори, чиито обработващи лични данни (подизпълнители) се ангажират да извършват дейности по обработване от тяхно име, и от друга страна, със съдържанието на договорите между администраторите и обработващите лични данни или правните актове. Поради това настоящото искане се отнася до „*въпрос с общо приложение*“ по смисъла на член 64, параграф 2 от ОРЗД.

13. Освен това Комитетът счита, че искането на НО на Дания е обосновано в съответствие с член 10, параграф 3 от Правилника за дейността на ЕКЗД, тъй като НО на Дания е представил аргументи в подкрепа на необходимостта от последователно тълкуване на въпросите, разгледани в искането.

14. В съответствие с член 64, параграф 3 от ОРЗД ЕКЗД не издава становище, ако вече е издавал становище по въпроса[6]. ЕКЗД все още не е предоставял отговори на въпросите, възникнали в резултат на искането на НО на Дания. Освен това наличните насоки на ЕКЗД, включително по-специално Насоки на ЕКЗД 7/2020 относно понятията „администратор“ и „обработващ лични данни“[7] (наричани по-долу „Насоки на ЕКЗД 7/2020“), предоставят някои насоки относно обхвата на задълженията на администратора за отчетност съгласно член 28 от ОРЗД, но съществуващите насоки не отговарят изцяло на всички въпроси, изложени в искането[8]. По-конкретно, например в съществуващите насоки относно член 28, параграф 3, буква а) от ОРЗД не се разглежда конкретно въпросът, включен в искането на НО на Дания, дали клаузата *„освен когато е длъжен да направи това по силата на правото на Съюза или правото на държава членка, което се прилага спрямо обработващия лични данни“* следва да бъде включена в договорите между администратора и обработващия лични данни или в правните актове.

15. Поради тези причини Комитетът счита, че искането на НО на Дания е допустимо, и въпросите, произтичащи от него, следва да бъдат анализирани в становище, прието съгласно член 64, параграф 2 от ОРЗД.

2 ПО СЪЩЕСТВОТО НА ИСКАНЕТО

2.1 Относно тълкуването на член 28, параграфи 1, 2 и 4 от ОРЗД във връзка с член 5, параграф 2 и член 24, параграф 1 (въпроси 1.1 и 1.3)

16. В този раздел се разглеждат въпроси 1.1 и 1.3, отправени към Комитета, както е посочено в раздел „Допустимост“ по-горе.

17. В член 28 от ОРЗД се определят отношенията между администратора и обработващия лични данни и се възлагат преки задължения на администраторите и обработващите лични данни. Като предварителна забележка следва да се отбележи, че понятието „обработващ лични данни“ се определя в ОРЗД в член 4, параграф 8 по общ начин, като включва както първоначалния обработващ лични данни, включен пряко от администратора, така и обработващия лични данни подизпълнител и т.н. по веригата на обработване.

18. ЕКЗД изтъква, че оценката на ролята на страните (и дали те действат като самостоятелни или съвместни администратори или като обработващи лични данни) не попада в обхвата на искането. ЕКЗД припомня, че основно страните са тези, които трябва да оценят конкретната си

[6] Член 64, параграф 3 от ОРЗД и член 10, параграф 4 от Процедурния правилник на ЕКЗД.

[7] Насоки на ЕКЗД 7/2020 относно понятията „администратор“ и „обработващ лични данни“ в ОРЗД, версия 2.1, приети на 7 юли 2021 г. (наричани по-нататък „Насоки 7/2020“).

[8] Вж. по-специално Насоки на ЕКЗД 7/2020, раздел 1.1 „Избор на обработващ лични данни“ на страница 36, раздел 1.3.4 *„Обработващият лични данни трябва да спазва условията, по член 28, параграфи 2 и 4, за включване на друг обработващ лични данни (член 28, параграф 3, буква г) от ОРЗД)“* на страница 44, раздел 1.6 „Подизпълнители, които обработват лични данни“, на страница 50.

роля в зависимост от фактическите елементи или обстоятелства по случая[9], без да се засяга правомощието на НО да провери дали оценката им е вярна.

19. С оглед на горните въпроси настоящото становище се съсредоточава единствено върху обхвата и степента на задълженията на администратора съгласно член 28, параграф 1 от ОРЗД, за да провери дали обработващите лични данни (подизпълнители) предоставят „достатъчни гаранции“ съгласно член 28, параграф 2 и свързаните с това задължения на администратора за отчетност съгласно член 5, параграф 2 и член 24, параграф 1 от ОРЗД[10].

20. Освен това Комитетът отбелязва, че горепосочените въпроси не се отнасят до отговорността на администратора спрямо субектите на данни за дейностите по обработване, извършвани от негово име, например по отношение на правото на субектите на данни на обезщетение съгласно член 82 от ОРЗД. Поради това настоящият раздел ще се съсредоточи върху предоставянето на разяснения за НО относно тълкуването на член 28, параграфи 1 и 2 от ОРЗД във връзка с член 5, параграф 2 и член 24 от ОРЗД във връзка с определени задължения, произтичащи от доверието в обработващия(ите) лични данни и подизпълнителите, обработващи лични данни. С цел да отговори на тези въпроси, Комитетът ще извърши анализ, съсредоточен върху ситуации, в които няма предаване на лични данни извън ЕИП. За разлика от това, в раздела по-долу относно въпрос 1.2 се оценяват ситуациите, в които се извършват предавания по веригата на обработване.

2.1.1 Идентифициране на участниците във веригата на обработване

21. По отношение на въпроса дали, по същество, администраторът следва да идентифицира всички подизпълнители на обработващия лични данни, техните подизпълнители и т.н. по цялата верига на обработване или да идентифицира само първата линия от подизпълнители, включени от обработващия лични данни, ЕКЗД припомня, на първо място, че *„въпреки че веригата [на обработване] може да бъде твърде дълга, администраторът запазва основната си роля при определянето на целта и средствата на обработването“*[11].

22. С цел да отговори на тези въпроси, ЕКЗД тълкува термините „идентифицира“ и „информация за идентичността“ като отнасящи се до името, адреса, лицето за контакт (име, длъжност, данни за контакт) на обработващия лични данни и описанието на обработването (включително ясно разграничаване на отговорностите, в случай че са упълномощени няколко подизпълнители)[12].

23. Що се отнася до избора на обработващи лични данни, администраторите следва да са в състояние ефективно да определят целите и средствата на обработването съгласно член 4,

[9] Насоки на ЕКЗД 7/2020, точка 12.

[10] Този въпрос е различен и независим от всички други задължения на администратора (или обработващите лични данни (подизпълнители)) за осигуряване на съответствие с ОРЗД, напр. с принципа на законосъобразност, с член 32 или задълженията по глава V от ОРЗД. Администраторът все още може да бъде отговорен за обработване под негов контрол, което не е в съответствие с тези разпоредби на ОРЗД, дори ако е изпълнил задълженията си да провери своите обработващи лични данни (подизпълнители) в съответствие с член 28, параграф 1 от ОРЗД, подробно описани в настоящото становище, и в настоящото становище не се разглежда отговорността на администратора да спазва разпоредбите на ОРЗД, различни от член 24, параграф 1, член 28, параграфи 1 и 2 от ОРЗД.

[11] Насоки на ЕКЗД 7/2020, точка 152.

[12] Това отразява информацията, която се изисква за идентифициране на обработващите лични данни в приложение IV от стандартните договорни клаузи между администратор и обработващ лични данни на Европейската комисия (Решение за изпълнение 2021/915 на Комисията от 4 юни 2021 година) и приложение III от стандартните договорни клаузи при международно предаване на лични данни на Европейската комисия (Решение за изпълнение 2021/914 на Комисията от 4 юни 2021 година).

параграф 7 от ОРЗД. Във връзка с това определянето на получателите (включително обработващите лични данни) се счита за „основно средство“ на обработването, въз основа на което администраторът взема решение[13].

24. За тази цел, по отношение на включването на **допълнителни обработващи лични данни** от първоначалния обработващ лични данни, предварителното специално или общо писмено разрешение на администратора е необходимо съгласно член 28, параграф 2 от ОРЗД. В Насоки на ЕКЗД 7/2020 се пояснява, че задълженията, предвидени в член 28, параграф 2 се *„задействат, когато даден обработващ лични данни (обработващ лични данни подизпълнител) възнамерява да включи друг участник, като по този начин добавя друго звено към веригата, възлагайки му дейности, налагащи обработването на лични данни“*[14].

25. В случаите, в които администраторът реши да приеме определени обработващи лични данни подизпълнители към момента на подписване на договора, в договора или в приложение към него следва да бъде включен списък с одобрените обработващи лични данни подизпълнители. След това списъкът следва да се актуализира в съответствие с общото или конкретното разрешение, предоставено от администратора[15].

26. Що се отнася до включването на обработващи лични данни подизпълнители, в ОРЗД се предвижда възможността за общо и специално разрешение. **В случай на специално разрешение** администраторът следва да посочи в писмен вид кой обработващ лични данни подизпълнител е упълномощен и за каква конкретна дейност по обработване и срок[16]. Ако на искането на обработващия лични данни за специално разрешение не бъде отговорено в рамките на определения срок, следва да се счита, че искането е отхвърлено[17].

27. **В случай на общо разрешение**, обработващият лични данни следва да предостави на администратора възможността да одобри списъка на обработващите лични данни подизпълнители към момента на подписване на общото разрешение и възможността — включително в рамките на разумен срок — да възрази срещу всякакви последващи промени в обработващите лични подизпълнители[18]. Комитетът припомня, че следва да зависи от

---

[13] Насоки на ЕКЗД 7/2020, точка 40.

[14] Насоки на ЕКЗД 7/2020, точка 151 гласи: *„Дейностите по обработване на данни често се извършват от голям брой участници, като веригите от подизпълнители стават все по-сложни. С ОРЗД се въвеждат специфични задължения, които биват задействани, когато даден обработващ лични данни (подизпълнител) възнамерява да включи друг участник, като по този начин добавя друго звено към веригата, възлагайки му дейности, налагащи обработването на лични данни. Анализът на това дали доставчикът на услуги действа като обработващ лични данни подизпълнител следва да се извърши в съответствие с описанието по-горе относно понятието „обработващ лични данни“*.

[15] Насоки на ЕКЗД 7/2020, точка 154.

[16] Насоки на ЕКЗД 7/2020, точки 153 и 155. Съгласно клауза 7.7, вариант 1, от стандартните договорни клаузи между администратор и обработващ лични данни на Европейската комисия, списъкът на обработващите лични данни подизпълнители, специално упълномощени от администратора, се намира в приложение IV, което следва да се поддържа в актуално състояние.

[17] Насоки на ЕКЗД 7/2020, точка 155.

[18] Вж. също Насоки 1/2020 на ЕКЗД, точка 156. *„Като алтернативна възможност администраторът може да предостави своето общо разрешение за използване на подизпълнители (в договора, включително списък с подизпълнителите в приложение към договора*) *(...)*“. В този смисъл от значение е също така Становище на ЕКЗД 14/2019 относно проектите на стандартни договорни клаузи, представени от НО на Дания (член 28, параграф 8 от ОРЗД). Съгласно клауза 7.7, вариант 2 от стандартните договорни клаузи между администратор и обработващ лични данни на Европейската комисия, обработващият лични данни има общото разрешение на администратора за включване на обработващи лични данни

първоначалния **обработващ лични данни проактивно да предоставя определена информация** на администратора, а „задължението на обработващия лични данни да информира администратора за всяка промяна, касаеща подизпълнителите, означава, че обработващият лични данни **по активен начин** уведомява администратора или му сигнализира за тези промени“[19].

28. Това означава, че информацията, свързана с идентифицирането на всички обработващи лични данни подизпълнители на обработващия следва да бъде лесно достъпна за администратора. Идентифицирането на тези участници е от особено значение, за да може администраторът да има контрол върху дейностите си по обработване, за които носи отговорност, и в случай на нарушение на ОРЗД може да бъде подведен под отговорност.

29. Поради това обработващият лични данни следва да предостави цялата информация за това как ще се извършва дейността по обработване от името на администратора, включително информация за използвания обработващ лични данни подизпълнител[20] и описание на обработването, което е поверено на обработващия лични данни подизпълнител[21].

30. Изискването администраторът да идентифицира всички обработващи лични данни и всички обработващи лични данни подизпълнители се обосновава с други правни съображения. Обработващите лични данни, пред които се разкриват или предават данни, се считат за „получатели“[22].

    - За да спазят изискванията за прозрачност съгласно член 13, параграф 1, буква д) и член 14, параграф 1, буква д) от ОРЗД, администраторите следва да информират субектите на данни за получателите или категориите получатели на личните данни, като са възможно най-конкретни и подробни[23]. Информацията за

подизпълнители от съгласуван списък и изрично уведомява писмено администратора за всички планирани промени в този списък, като предварително добавя или заменя обработващи лични данни подизпълнители.

[19] Насоки на ЕКЗД 7/2020, точка 128 (удебеляването е добавено). Вж. също бележка под линия 14.

[20] Насоки на ЕКЗД 7/2020, точка 143.

[21] Вж. например приложение IV от стандартните договорни клаузи между администратор и обработващ лични данни на Европейската комисия и приложение II от стандартните договорни клаузи при международното предаване на лични данни на Европейската комисия.

[22] Член 4, параграф 9 от ОРЗД; Насоки на Работната група по член 29 относно прозрачността съгласно Регламент 2016/679, приети на 29 ноември 2017 г., последно преразгледани и приети на 11 април 2018 г., РД 260 ред.01, одобрени от ЕКЗД (наричани по-долу „Насоки на Работната група по член 29 относно прозрачността“), стр. 37.

[23] Насоки на Работната група по член 29 относно прозрачността, стр. 37 („*В съответствие с принципа на добросъвестност администраторите трябва да предоставят на субектите на данни най-съществената информация за получателите*. *На практика обикновено това са получателите, изброени поименно, така че субектите на данни да знаят кой точно разполага с техните лични данни. Ако администраторите изберат да посочат категориите получатели, информацията следва да бъде възможно най-конкретна, като се посочи видът на получателя (т.е. като се посочат дейностите, които той извършва), отрасълът, секторът и подсекторът и местоположението на получателите*“); Насоки на ЕКЗД 1/2022 относно правата на субектите на данни — право на достъп, версия 2.1, приети на 28 март 2023 г. (наричани по-долу „Насоки на ЕКЗД 1/2022 (право на достъп)), параграф 117 („*вече съгласно членове 13 и 14 от ОРЗД информацията относно получателите или категориите получатели следва да бъде възможно най-конкретна съгласно принципите на прозрачност и добросъвестност*“); вж. Съд на ЕС, решение от 12 януари 2023 г., *RW срещу Österreichische Post AG*, C-154/21, точка 25; становище на консултативната група относно СЕС C-154/21, параграф 36 („*В членове 13 и 14 от ОРЗД [...] се предвижда задължение за администратора да предостави на субекта*

„категориите получатели“ също трябва да бъде включена в регистрите на дейностите по обработване (член 30, параграф 1, буква г).

- В член 15 от ОРЗД е предвидено правото на достъп, наред с другото, до информация относно получателите или категориите получатели, пред които са или ще бъдат разкрити личните данни[24]. Съдът на ЕС уточни, че тази разпоредба налага на администратора задължение да предостави на субекта на данните самоличността на получателите[25]. Извън видовете случаи, в които администраторът може да посочва на субекта на данните само категориите получатели, по принцип следва винаги да е възможно администраторът да извлича имената на получателите и да предоставя без ненужно забавяне необходимата информация на субектите на данни.

- В член 19 от ОРЗД се предвижда, че администраторът съобщава за съобщава за всяко коригиране, изтриване или ограничаване на обработване на всеки получател, на когото личните данни са били разкрити, освен ако това е невъзможно или изисква несъразмерно големи усилия. Съдът на ЕС уточни, че второто изречение на член 19 изрично предоставя на субекта на данните правото да бъде информиран за конкретните получатели[26].

31. Въпреки че това не е изрично посочено в тези разпоредби, Комитетът счита, че за целите на член 28, параграфи 1 и 2 от ОРЗД администраторите следва да разполагат с информацията за самоличността на всички обработващи данни, обработващи данни подизпълнители и т.н., която да е лесно достъпна по всяко време[27], за да могат да изпълняват най-добре задълженията си съгласно горепосочените разпоредби. Тази достъпност е необходима също така, за да могат администраторите да събират и оценяват цялата необходима информация, за да изпълнят изискванията съгласно ОРЗД, включително за да могат да отговарят на исканията за достъп съгласно член 15 от ОРЗД без ненужно забавяне и да реагират бързо на нарушения на сигурността на данните, възникнали по веригата на обработване. Това ще се прилага независимо от риска, свързан с дейността по обработване.

на данните информация относно категориите получатели или конкретните получатели на свързаните с него лични данни, когато тези данни се събират или не се събират от субекта на данните“).

[24] Член 5, параграф 1, буква в) от ОРЗД. Насоки на ЕКЗД 1/2022 (право на достъп), точки 116—117.

[25] Решение на Съда от 12 януари 2023 г., *RW срещу Österreichische Post AG*, C-154/21, точка 51: „*Член 15, параграф 1, буква в) от ОРЗД трябва да се тълкува в смисъл, че предвиденото в тази разпоредба право на достъп на субекта на данните до свързаните с него лични данни включва — когато тези данни са или ще бъдат разкрити пред получатели — задължението на администратора да уведоми това лице за самоличността на тези получатели, освен ако е невъзможно да се установят получателите или администраторът докаже, че исканията за достъп на субекта на данните са явно неоснователни или прекомерни по смисъла на член 12, параграф 5 от ОРЗД, като в тези случаи администраторът може да посочи на субекта на данните само категориите получатели, за които става въпрос*“.

Съдът прие, че субектът на данни може също така „*да избере да се ограничи до това да поиска информация относно категориите получатели*“. Решение на СЕС от 12 януари 2023 г., *RW срещу Österreichische Post AG*, C-154/21, точка 43.

Насоки на ЕКЗД 1/2022 (право на достъп), точка 117.

[26] Решение на Съда на ЕС от 12 януари 2023 г., *RW срещу Österreichische Post AG*, C-154/21, точка 41.

[27] Тази информация е необходима на администратора, за да може да изпълнява задълженията си и в случай че веригата на обработване на обработващ лични данни подизпълнител е прекъсната, тъй като един обработващ лични данни (подизпълнител) е недостъпен, не желае или е неплатежоспособен и трябва да се осъществи връзка с друг обработващ лични данни (подизпълнител).

32. За тази цел обработващият лични данни следва активно да предоставя[28] на администратора цялата информация относно самоличността на всички обработващи лични данни, обработващи лични данни подизпълнители и т.н., които обработват лични данни от името на администратора, и трябва постоянно да актуализира тази информация относно всички включени обработващи лични данни подизпълнители. Администраторът и обработващият лични данни могат да включат в договора допълнително уточнение за това как и в какъв формат обработващият лични данни трябва да предостави тази информация, тъй като администраторът може да има специфични изисквания за формат с оглед извличането и подреждането на информацията.

2.1.2 Проверка и документиране от страна на администратора доколко достатъчни са гаранциите, предоставени от всички обработващи лични данни във веригата на обработване

33. Въпроси 1.1.б.i, 1.1.б.iii и 1.3 имат за цел да дадат разяснения до каква степен и колко подробно администраторът следва да проверява и документира доколко достатъчни са гаранциите, предоставени от всички обработващи лични данни във веригата на обработване, и до каква степен задълженията по член 28, параграфи 1 и 2 от ОРЗД във връзка с член 5, параграф 2 и член 24 от ОРЗД се различават в зависимост от риска, свързан с дейността по обработване. Във връзка с тези въпроси Комитетът изтъква следните елементи.

34. В член 5, параграф 2 от ОРЗД е заложен принципът на отчетност, като на администратора е възложена отговорност да спазва принципите за защита на данните по член 5, параграф 1 от ОРЗД и да е в състояние да докаже, че ги спазва. Член 5, параграф 2 от ОРЗД се прилага към всички общи принципи, изброени в член 5, параграф 1 от ОРЗД.

35. В член 24, параграф 1 от ОРЗД се включва задължението на администратора да докаже, че обработването се извършва в съответствие с ОРЗД, но се доразвива едно от задълженията, по отношение на които се прилага принципът на отчетност: въвеждането на „подходящи технически и организационни мерки“[29]. В член 24, параграф 1 от ОРЗД се посочва понятието „риск“[30], което е от значение за прилагането му, като един от критериите, които администраторът трябва да вземе предвид при оценката на целесъобразността на такива

[28] С цел спазване на член 28, параграф 2 от ОРЗД, за да се даде възможност на администратора да вземе решение относно добавянето на обработващи лични данни подизпълнители, както и да спазва член 28, параграф 1 от ОРЗД, за да може администраторът да провери дали обработващите лични данни (подизпълнители) предоставят достатъчно гаранции за прилагането на техническите и организационните мерки.

[29] Решение от 25 януари 2024 г., *BL срещу MediaMarktSaturn Hagen-Iserlohn GmbH*, C-687/21, ECLI:EU:C:2024:72, точка 36: *„Член 24 от ОРЗД предвижда общо задължение за администратора на лични данни да въведе подходящи технически и организационни мерки, за да гарантира и да е в състояние да докаже, че посоченото обработване се извършва в съответствие с този регламент“*.

[30] В съображение 75 от ОРЗД са изброени някои примери за рискове: *„обработването може да породи дискриминация, кражба на самоличност или измама с фалшива самоличност, финансови загуби, накърняване на репутацията, нарушаване на поверителността на лични данни, защитени от професионална тайна, неразрешено премахване на псевдонимизация, или други значителни икономически или социални неблагоприятни последствия*; в съображение 76 се уточнява: *„Вероятността и тежестта на риска за правата и свободите на субекта на данни следва да се определят с оглед на естеството, обхвата, контекста и целта на обработването. Рискът следва да се оценява въз основа на обективна оценка, с която се определя дали операцията по обработването на данни води до риск или до висок риск*“. Както е обобщено от Съда на ЕС „*съгласно съображение 76 от този регламент вероятността и тежестта на риска зависят от особеностите на разглежданото обработване и този риск следва да се оценява въз основа на обективна оценка*.“ (Съд на ЕС, решение от 14 декември 2023 г. *VB срещу Национална агенция за приходите*, C-340/21, EU:C:2023:986, точка 36).

мерки[31]. В член 24, параграф 1 от ОРЗД също така се добавя, че тези мерки се преразглеждат и при необходимост се актуализират.

36. Както е посочено от Съда на ЕС, *„член 5, параграф 2 и член 24 от ОРЗД налагат на администраторите общи изисквания за отчетност и съответствие*. *По-специално тези разпоредби изискват администраторът да приеме подходящи мерки, насочени към предотвратяване на евентуални нарушения на предвидените в ОРЗД правила за гарантиране на правото на защита на данните“ [32].*

37. Принципът на отчетност е насочен към администратора, включително когато администраторът е възложил на обработващи лични данни или на обработващи лични данни подизпълнители обработването на лични данни от негово име.

38. Съгласно член 28, параграф 1 от ОРЗД, когато администратор включва обработващ лични данни да извършва обработване от негово име, администраторът трябва д използва само обработващ лични данни, който може да предостави *„достатъчно гаранции за прилагане на подходящи технически и организационни мерки, така че обработването да отговаря на изискванията“* на ОРЗД *„и да осигурява защита на правата на субектите на данните“*[33]. Както е посочено в Насоки на ЕКЗД 7/2020, принципът на отчетност е отразен и в член 28 от ОРЗД[34].

39. В тази връзка ЕКЗД изтъква, че за целите на оценката на съответствието с член 24, параграф 1 и член 28, параграф 1 от ОРЗД надзорните органи следва да вземат предвид, че **включването на обработващи лични данни не следва да понижава нивото на защита на правата на субектите на данни** в сравнение със ситуацията, в която обработването се извършва пряко от администратора. Това се отнася до включването на първоначалния обработващ лични данни, но също така и до включването на допълнителни обработващи лични данни във веригата на обработване, например обработващи лични данни подизпълнители и обработващи лични данни подподизпълнители. Член 24, параграф 1 и член 28, параграф 1 от ОРЗД следва да се тълкуват в смисъл, че изискват от администратора да гарантира, че веригата на обработване се състои само от обработващи лични данни, обработващи лични данни подизпълнители, обработващи лични данни подподизпълнители (и др.), които предоставят „достатъчни гаранции

[31] Както посочва Съдът на ЕС, "*В член 24, параграф 1 са изброени редица критерии, които трябва да се вземат предвид при оценката на целесъобразността на такива мерки, а именно естеството, обхватът, контекстът и целта на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица*", решение от 14 декември 2023 г., *VB срещу Национална агенция за приходите*, C-340/21, EU:C:2023:986, точка 25. В същото решение Съдът на ЕС уточнява, че *„дали тези мерки са подходящи трябва да се оцени конкретно, като се провери дали те са приложени от администратора при отчитане на различните визирани критерии (...) и на нуждите от защита на данните, специфично присъщи на съответното обработване, както и свързаните с него рискове*“, точка 30; също така се припомня в Решение от 25 януари 2024 г., *BL срещу, MediaMarktSaturn Hagen-Iserlohn GmbH*, C-687/21, ECLI:EU:C:2024:72, точка 38: *„Така от текста на членове 24 и 32 от ОРЗД следва, че трябва конкретно да се преценява дали приложените от администратора мерки са подходящи, при отчитане на различните критерии, визирани в тези членове, и на нуждите от защита на данните, специфично присъщи на съответното обработване, както и на свързаните с него рискове, още повече че посоченият администратор трябва да е в състояние да докаже съответствието с този регламент на посочените мерки — възможност, от която ще бъде лишен, ако бъде приета необорима презумпция*“. Трябва да се отбележи, че анализът на Съда на ЕС се отнася също до член 32 от ОРЗД.

[32] Решение от 27 октомври 2022 г., *Proximus NV срещу Gegevensbeschermingsautoriteit*, C-129/21, ECLI:EU:C:2022:833, точка 81. Вж. също Насоки на ЕКЗД 7/2020, точка 9.

[33] Насоки на ЕКЗД 7/2020, точка 94.

[34] Насоки на ЕКЗД 7/2020, точка 8.

за прилагането на подходящи технически и организационни мерки“. Освен това администраторът следва да може да докаже, че е взел под сериозно внимание всички елементи, предвидени в ОРЗД[35]. Тези съображения са валидни дори в случаи, когато веригата на обработване е дълга и сложна с различни обработващи лични данни, обработващи лични данни подизпълнители и др., участващи на различни етапи от дейностите по обработване. Администраторът следва да полага дължимата грижа при избора и надзора на своите обработващи лични данни.

40. По отношение на избора на **първоначалния обработващ лични данни**, администраторът следва да провери дали гаранциите са достатъчни за всеки отделен случай, като се вземат предвид естеството, обхвата, контекста и целите на обработването, както и рисковете за правата и свободите на физическите лица, въз основа на вида на обработването, възложено на обработващия лични данни[36]. Съгласно член 28, параграф 5 от ОРЗД придържането на обработващия лични данни към одобрен кодекс за поведение съгласно член 40 от ОРЗД или одобрен механизъм за сертифициране съгласно член 42 от ОРЗД може да се използва като елемент, чрез който да се докаже че са налице достатъчни гаранции.

41. Както беше посочено по-горе от ЕКЗД, когато проверява гаранциите, предоставени от обработващите лични данни[37], администраторът следва да вземе предвид няколко елемента, като често ще се изисква обмен на съответната документация[38]. Във всички случаи *[г]аранциите, „предоставени“ от обработващия лични данни, са тези, които обработващият лични данни е в състояние да докаже по удовлетворителен за администратора начин, тъй като това са единствените гаранции, които могат ефективно да бъдат взети предвид от администратора при оценката на изпълнението на неговите задължения*“[39]. Нито член 28, параграф 1 от ОРЗД, нито предишни документи на ЕКЗД предоставят изчерпателен списък на документите или действията, които обработващият лични данни следва да покаже или да докаже, тъй като това до голяма степен зависи от конкретните обстоятелства на обработването[40]. Например, администраторът може да избере да изготви въпросник като средство за събиране на информация от своя обработващ лични данни, за да провери съответните гаранции, да поиска необходимата документация, да разчита на публично достъпна информация и/или сертификати или одитни доклади от надеждни трети страни и/или да извърши одити на място.

[35] Насоки на ЕКЗД 7/2020, точка 94.

[36] Насоки на ЕКЗД 7/2020, точка 96.

[37] Насоки на ЕКЗД 7/2020, точки 97—98 (позовавайки се на експертните познания, надеждността и ресурсите, както и на репутацията на обработващия лични данни на пазара, и на придържането към одобрен кодекс за поведение или механизъм за сертифициране).

[38] Насоки на ЕКЗД 7/2020, точка 95 (в която се споменават някои примери: политиката за поверителност, условията на предоставяне, регистър на дейностите по обработване, политика за управление на документите, политика за информационна сигурност, доклади от извършени външни одити на защитата на данните, международно признати сертификати, например от серията ISO 27000).

[39] Насоки на ЕКЗД 7/2020, точка 95.

[40] Насоки на ЕКЗД 7/2020, точка 96 („*Оценката на администратора по отношение на това дали гаранциите са достатъчни е форма на оценка на риска, която ще зависи до голяма степен от вида обработване, възложено на обработващия лични данни, и трябва да се извършва за всеки отделен случай, като се вземат предвид естеството, обхватът, същността и целите на обработването, както и рисковете за правата и свободите на физическите лица. В резултат на това ЕКЗД не може да предостави изчерпателен списък с документите или действията, които обработващият лични данни трябва да покаже или да докаже при даден сценарий, тъй като това зависи до голяма степен от конкретните обстоятелства, при които се обработват данните*“).

42. ЕКЗД вече уточни, че задължението да се използват само обработващи лични данни, „които предоставят достатъчни гаранции“, съдържащо се в член 28, параграф 1 от ОРЗД, е постоянно задължение и че администраторът следва, на подходящи интервали от време, да проверява гаранциите на обработващия лични данни[41].

43. В светлината на въпрос 1.3, повдигнат от НО на Дания в искането му, относно риска, свързан с обработването, ЕКЗД изтъква, че понятието „риск“ играе важна роля в редица разпоредби от ОРЗД, по-специално разпоредбите, свързани с глава IV от ОРЗД[42].

44. Важно е да се изтъкне, че споменаването на „риска“ в член 24, параграф 1 и съображение 74 от ОРЗД не следва да се тълкува в смисъл, че администраторът може да пренебрегне или да се отклони от задълженията си по ОРЗД въз основа на самия факт, че счита риска за правата и свободите на субектите на данни за „нисък“. Задължението за прилагане на „подходящи технически и организационни мерки“, за да се осигури спазване на ОРЗД в съответствие с член 24, параграф 1 от ОРЗД, се прилага винаги, но мерките, които са необходими за постигането на този резултат, могат да варират в зависимост от риска[43].

45. Въпреки че в член 28, параграф 1 от ОРЗД не се съдържат конкретни позовавания на „риска“, той предполага необходимостта да се вземе предвид равнището на риска за правата и свободите на субектите на данни. Изискването в член 28, параграф 1 да се използват само обработващи лични данни, които предоставят „достатъчни гаранции“ за прилагането на подходящи технически и организационни мерки“, следва да се тълкува в смисъл, че е необходимо да се прецени дали обработващите лични данни предоставят достатъчни гаранции за прилагането на такива мерки с оглед на рисковете, свързани с обработването, тъй като например нивото на мерките за сигурност, които трябва да се прилагат, също зависи от рисковете.

46. Рискът, свързан с дейността по обработване, играе важна роля при определянето доколко са подходящи техническите и организационните мерки, наред с другите критерии, посочени в член 24, параграф 1 от ОРЗД**[44]**. В зависимост от нивото на риска, свързан с дейността по обработване (например, ако се обработват специални категории лични данни), администраторът може да определи по-строги или по-обширни технически и организационни мерки. Поради това всеки обработващ лични данни следва да предостави достатъчни гаранции за ефективното прилагане на „подходящите“ мерки, определени от администратора.

47. Комитетът счита, че ***задължението*** **на администратора да проверява дали обработващите лични данни (подизпълнители) предоставят достатъчни гаранции, за да изпълнят мерките, определени от администратора, следва да се прилага независимо от риска за правата и свободите на субектите на данни.**

48. **Въпреки това на практика *степента* на такава проверка ще варира в зависимост от естеството на тези организационни и технически мерки, определени от администратора въз основа,**

[41] Насоки на ЕКЗД 7/2020, точка 99: „*включително чрез одити и проверки, когато това е целесъобразно*“.
[42] Терминът „риск“ се споменава в членове 24, 25, 27, 30, 32, 33, 34, 35, 36 и 39 от ОРЗД.
[43] Съд на ЕС, решение от 14 декември 2023 г., *VB срещу Национална агенция за приходите*, C-340/21, EU:C:2023:986, точка 35: „*съображение 74 от ОРЗД подчертава, че е важно администраторът да е длъжен да прилага подходящи и ефективни мерки и да е в състояние да докаже, че дейностите по обработването са в съответствие с този регламент, включително ефективността на мерките, които следва да отчитат критерии, свързани с характеристиките на съответното обработване, и с риска, който то представлява, които са изброени в тези членове 24 и 32*“.
[44] Член 24, параграф 1 се отнася до „*естеството, обхвата, контекста и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица*“.

наред с други критерии, на риска, свързан с обработването. Например, когато дейностите по обработване представляват по-малък риск за правата и свободите на субектите на данни, съответстващите „подходящи мерки“ ще бъдат по-малко строги. Поради това обхватът на проверката на администратора може на практика да не е толкова обширен. Обратно, в случай на по-високи рискове, произтичащи от конкретното обработване, нивото на проверка от страна на администратора може да бъде по-важно от гледна точка на проверката на достатъчните гаранции, предоставени от цялата верига на обработване, като се има предвид, че „подходящите мерки„, които трябва да се приложат, са по-обширни и надеждни, за да се преодолеят рисковете за субектите на данни.

49. В това отношение, в зависимост от нивото на риска, свързан с дейността по обработване, администраторът може да увеличи нивото на проверката си, като провери договорите за подизпълнение самостоятелно и/или също така да задължи първоначалния обработващ лични данни да извърши разширена проверка и изготви документация.

50. В съответствие с принципа на отчетност администраторът следва надлежно да документира всяка мярка, за която се счита, че е необходима за спазването на ОРЗД, включително въз основа на риска, свързан с обработването[45]. Това задължение се улеснява, от една страна, от **задълженията за съдействие и одит**, наложени на обработващите лични данни, и от друга страна, от **информацията, предоставена от първоначалния обработващ лични данни** на администратора преди включването на допълнителни обработващи лични данни.

51. На първо място, Комитетът отбелязва, че обработващите лични данни са обвързани от задължението да подпомагат администратора за спазването на определени изисквания на ОРЗД (съгласно член 28, параграф 3, букви д) и е))[46]. В по-общ план обработващият лични данни е обвързан от задължението да предостави на администратора цялата информация, необходима за доказване на спазването на член 28 (член 28, параграф 3, буква з))[47]. Администраторът следва да бъде напълно информиран относно подробностите за обработването, които са от значение за доказване на спазването на задълженията, предвидени в член 28 от ОРЗД, а обработващият лични данни следва да предостави цялата информация за това как се извършва дейността по обработване от името на администратора[48]. В договора следва да се посочва колко често и как следва да се осъществява този поток от информация[49].

---

[45] По отношение на тежестта на доказване на администратора на данни вж. решение на Съда на ЕС от 14 декември 2023 г., *VB срещу Национална агенция за приходите*, C-340/21, EU:C:2023:986, точка 52 : „*От текстовете на член 5, параграф 2, член 24, параграф 1 и член 32, параграф 1 от ОРЗД недвусмислено следва, че съответният администратор носи тежестта да докаже, че личните данни се обработват така, че да се гарантира подходяща сигурност на същите по смисъла на член 5, параграф 1, буква е) и член 32 от този регламент*“, вж. също решение на Съда на ЕС от 25 януари 2024 г., BL срещу MediaMarktSaturn Hagen-Iserlohn GmbH, C-687/21, ECLI:EU:C:2024:72, точка 42 „*в това отношение е важно да се подчертае, че от прочита на членове 5, 24 и 32 от ОРЗД във връзка със съображение 74 от него следва, че при иск за обезщетение по член 82 от този регламент съответният администратор носи тежестта да докаже, че личните данни се обработват по начин, че да се гарантира подходящо ниво на сигурност на същите по смисъла на член 5, параграф 1, буква е) и на член 32 от посочения регламент. Подобно разпределение на доказателствената тежест е от естество не само да насърчи администраторите на тези данни да приемат изискваните от ОРЗД мерки за сигурност, но и да запази полезното действие на правото на обезщетение, предвидено в член 82 от този регламент, и да спази намеренията на законодателя на Съюза, посочени в съображение 11 от него*“.

[46] Вж. Насоки 7/2020 на EDPB, точки 130—138.

[47] Вж. Насоки 7/2020 на EDPB, точки 143—145.

[48] Насоки на ЕКЗД 7/2020, точка 143.

[49] Насоки на ЕКЗД 7/2020, точка 143.

52. Поради това администраторът може да разчита на информацията, предоставена от обработващия лични данни, съгласно член 28, параграф 3, буква з) от ОРЗД, при изпълнение на задължението си за документиране на приетите мерки, при условие че информацията, предоставена от обработващия лични данни, действително доказва спазването на изискванията. Тъй като обработващият лични данни е добре запознат с подробностите за обработването, което извършва, и за обработването, извършвано от обработващите лични данни подизпълнители, той следва проактивно да предоставя на администратора цялата необходима информация[50].

53. Горното се прилага и за обработващите лични данни подизпълнители. Всъщност от обработващите лични данни се изисква да прехвърлят задълженията за съдействие надолу по веригата на обработване (член 28, параграф 4 от ОРЗД).

54. Второ, **включването на обработващи лични данни подизпълнители**, както беше припомнено по-горе, е възможно само с предварителното писмено разрешение на администратора, което би могло да бъде специално или общо. Ако администраторът избере да даде общо разрешение, то *„следва да бъде допълнено с критерии, които да насочват избора на обработващия лични данни (например гаранции по отношение на техническите и организационните мерки, експертни познания, надеждност и ресурси)“*[51].

55. Както ЕКЗД пояснява, [з]*а да извърши оценка и да вземе решение дали да разреши възлагането на подизпълнители, администраторът трябва да получи от обработващия лични данни списък с предвидените обработващи лични данни подизпълнители (включително за всеки от тях: местоположенията им, какво ще извършват и доказателство за това какви гаранции са били използвани)“*[52]. Тази информация е необходима на администратора, за да спази принципа на отчетност, определен в член 5, параграф 2 и член 24, и разпоредбите на член 28, параграф 1, член 32 и глава V от ОРЗД[53]. Що се отнася до предаването на лични данни извън ЕИП, Комитетът се позовава на предоставения по-долу отговор на въпрос 1.2, зададен от НО на Дания.

56. Както припомня ЕКЗД, първоначалният обработващ лични данни следва да гарантира, че предлага обработващи лични данни подизпълнители, предоставящи достатъчни гаранции[54]. Необходимостта първоначалният обработващ лични данни да предостави горепосочената информация свидетелства, че **обработващият лични данни има своята роля при избора на обработващи лични данни подизпълнители и при проверката на гаранциите, които те предоставят, и следва да предоставя на администратора достатъчно информация**. Това е в съответствие и с факта, че независимо от посочените от администратора критерии за избор на

[50] Насоки на ЕКЗД 7/2020, точка 143, във връзка с член 28, параграф 3, буква з): *„Например обработващият лични данни може да споделя с администратора съответни части от своите регистри на дейностите по обработване. Обработващият лични данни следва да предостави цялата информация за това как ще се извършва дейността по обработването от името на администратора. Тази информация следва да включва информация относно функционирането на използваните системи, мерките за сигурност, начина, по който се изпълняват изискванията по отношение на съхраняването на данните, местонахождението на данните, предаването на данните, кой има достъп до данните и кои са получателите на данните, включените обработващи лични данни подизпълнители и т.н.“*. Възможността администраторът да извършва одит е посочена и в точка 144: *„Целта на такъв одит е да се гарантира, че администраторът разполага с цялата информация относно дейността по обработване, извършвана от негово име, и относно гаранциите, предоставени от обработващия лични данни*.“

[51] Насоки на ЕКЗД 7/2020, точка 156.

[52] Насоки на ЕКЗД 7/2020, точка 152.

[53] Насоки на ЕКЗД 7/2020, бележка под линия 69.

[54] Насоки на ЕКЗД 7/2020, точка 159.

допълнителни обработващи лични данни, първоначалният обработващ лични данни остава изцяло отговорен пред администратора за изпълнението на задълженията от страна на обработващите лични данни подизпълнители (член 28, параграф 4 от ОРЗД).

57. В това отношение, дори ако съгласно член 28, параграф 4 от ОРЗД обработващият лични данни, който ангажира обработващ лични данни подизпълнител, е пряко отговорен да гарантира, че на този друг обработващ лични данни са възложени същите задължения за защита на данните, които са определени в първоначалния договор между администратора и обработващия лични данни, това не отменя отговорността на администратора да гарантира спазването на изискванията на член 28, параграф 1 и член 24, параграф 1 от ОРЗД и да може да докаже това спазване.

58. **В правомощията на администратора остава крайното решение дали да включи конкретен обработващ лични данни подизпълнител (подподизпълнител) и свързаната с това отговорност, включително по отношение на проверката на това доколко достатъчни са гаранциите, предоставени от обработващия лични данни (подизпълнител).** Както вече беше припомнено, в случай на общо или специално разрешение винаги зависи от администратора дали да одобри включването на този обработващ лични данни подизпълнител или да възрази срещу него.

59. Когато оценяват съответствието с член 24, параграф 1 и член 28, параграф 1 от ОРЗД, НО следва да преценят дали администраторът е в състояние да докаже, че проверката на това доколко достатъчни са гаранциите, предоставени от неговите обработващи лични данни подизпълнители, е извършена по удовлетворителен начин. Това означава, че администраторът може да реши да се базира на информацията, получена от обработващия лични данни, и ако е необходимо, да я допълни. Например, в случай че получената информация изглежда непълна, неточна или поражда въпроси или когато е целесъобразно въз основа на преценка на обстоятелствата по случая, включително риска, свързан с обработването, администраторът следва да поиска допълнителна информация и/или да провери предоставената такава и да я допълни/коригира, ако е необходимо.

60. По-конкретно, за обработването на данни, което представлява висок риск за правата и свободите на субектите на данни, администраторът следва да повиши нивото си на проверка при сверяването на информацията, предоставена във връзка с гаранциите, представени от различните обработващи лични данни във веригата на обработване.

2.1.3 Проверка на договора между първоначалния обработващ лични данни и допълнителните обработващи лични данни

61. НО на Дания пита, по същество, дали и до каква степен администраторът има задължението да провери и документира, че договорите за подизпълнение възлагат същите задължения на допълнителните обработващи лични данни.

62. В това отношение в член 28, параграф 4[55] се налага пряко задължение на обработващите лични данни. Освен това член 28, параграф 3, буква г) изисква от администратора и обработващия

[55] Член 28, параграф 4 от ОРЗД. *„Когато обработващ лични данни включва друг обработващ лични данни за извършването на специфични дейности по обработване от името на администратора, чрез договор или друг правен акт съгласно правото на Съюза или правото на държава членка на това друго лице се налагат същите задължения за защита на данните, както задълженията, предвидени в договора или друг правен акт между администратора и обработващия лични данни, както е посочено*

лични данни да „предвидят“ задължението на обработващия лични данни да спазва условията, посочени в член 28, параграф 4, в своя договор, като по този начин това изискване се превръща в договорно задължение, наложено на обработващия лични данни. С други думи, **първоначалният обработващ лични данни е законово и договорно задължен да прехвърли същите задължения за защита на данните в договорите за подизпълнение, които сключва с допълнителни обработващи лични данни.**

в параграф 3, по-специално да предостави достатъчно гаранции за прилагане на подходящи технически и организационни мерки, така че обработването да отговаря на изискванията на настоящия регламент.“

63. По подобен начин допълнителните обработващи лични данни ще бъдат договорно задължени (от първоначалния обработващ лични данни) да налагат същите задължения за защита на данните на своите собствени обработващи лични данни и т.н. по веригата на обработване[56]. Не е необходимо договорът за подизпълнение да бъде идентичен по съдържание с договора за обработване на данни, сключен с първоначалния обработващ лични данни[57].

64. Комитетът припомня, че ако обработващ лични данни подизпълнител не изпълни задълженията си, крайната отговорност за изпълнението на задълженията на този друг обработващ лични данни подизпълнител е на администратора. Въпреки това първоначалният обработващ лични данни ще продължи да носи отговорност пред администратора, така че администраторът да има възможност да предяви договорен иск срещу първоначалния си обработващ лични данни, ако този обработващ лични данни не прехвърли същите задължения за защита на данните в договорите за подизпълнение.

65. Обработващите лични данни са длъжни да предоставят на администратора цялата информация, необходима за доказване на спазването на член 28, параграф 3, буква з) от ОРЗД. Така, по искане на администратора, първоначалният обработващ лични данни ще трябва да предостави договорите за подизпълнение между първоначалния обработващ и допълнителните обработващи лични данни.

66. В тази връзка стандартните договорни клаузи между администратор и обработващ лични данни на Европейската комисия[58] и стандартните договорни клаузи при международно предаване на лични данни на Европейската комисия[59] предоставят на администратора възможността да

[56] В съвместното становище на ЕКЗД и ЕНОЗД 2/2021 относно Решението за изпълнение на Европейската комисия относно стандартните договорни клаузи за предаване на лични данни на трети държави, ЕКЗД и ЕНОЗД изтъкнаха, че изискването на член 28, параграф 4 от ОРЗД трябва да бъде взето предвид от страните в отношенията между обработващите лични данни (параграф 66).

[57] Насоки на ЕКЗД 7/2020, точка 160: „*Налагането на „същите“ задължения следва да се тълкува от гледна точка на функционалността, а не на формулировката: не е необходимо договорът да включва точно същите думи като използваните в договора между администратора и обработващия лични данни, но следва да се гарантира, че задълженията по същество са едни и същи*“. ЕКЗД отбелязва също така, че когато двама обработващи лични данни разчитат на модул 3 (между обработващите лични данни) на стандартните договорни клаузи при международно предаване на лични данни на Европейската комисия, първоначалният обработващ лични данни предоставя допълнителна гаранция. Съгласно клауза 8.1.г от стандартните договорни клаузи при международно предаване на лични данни на Европейската комисия износителят на данни (първоначалният обработващ лични данни) гарантира, че е наложил на вносителя на данни (обработващ лични данни подизпълнител) същите задължения за защита на данните, каквито са определени в договора или друг правен акт съгласно правото на Съюза или правото на държава членка между администратора и износителя на данни.

[58] В раздел 7 относно използването на подизпълнители, в член 7, параграф 7, буква в) стандартните договорни клаузи между администратор и обработващ лични данни на Европейската комисия се предвижда: „*По искане на администратора обработващият лични данни предоставя на администратора копие от споразумението с обработващия лични данни подизпълнител и всички последващи изменения. В степента, необходима за защита на търговска тайна или друга поверителна информация, включително лични данни, обработващият лични данни може да редактира текста на споразумението, преди да сподели копието*“. Решение за изпълнение 2021/915 на Комисията от 4 юни 2021 година относно стандартни договорни клаузи между администратори и обработващи лични данни съгласно член 28, параграф 7 от Регламент (ЕС) 2016/679 и член 29, параграф 7 от Регламент (ЕС) 2018/1725 („стандартни договорни клаузи между администратори и обработващи лични данни на Европейската комисия“).

[59] В модул 2 (от администратор до обработващ лични данни), клауза 9, буква в) от стандартните договорни клаузи при международно предаване на лични данни на Европейската комисия се предвижда: „*По искане*

поиска копие от договора за подизпълнение между първоначалния и допълнителните обработващи лични данни. Тази възможност е предвидена и в трите стандартни договорни клаузи между администратор и обработващ лични данни, приети от надзорните органи[60]. Тази възможност е изражение на правото на администратора на одит съгласно член 28, параграф 3, буква з) от ОРЗД. Ако администраторът поиска, обработващият лични данни следва да предостави такова копие.

67. Въпреки това ЕКЗД отбелязва, че стандартните договорни клаузи не уреждат дали администраторът *трябва* да поиска такова копие, за да спази член 28, параграф 1 от ОРЗД.

68. В този смисъл отговорността на администратора не може да се определи от това дали администраторът е избрал да поиска такова копие или не. При всички случаи обработващият лични данни има също така правни и договорни задължения, изискващи от него да налага същите задължения за защита на данните, както в първоначалния договор.

69. Предвид това **администраторът не е длъжен систематично да изисква договорите за подизпълнение, за да проверява дали задълженията за защита на данните, предвидени в първоначалния договор, са прехвърлени надолу по веригата на обработване**. Администраторът следва да преценява за всеки отделен случай дали е необходимо да поиска копие от такива договори или да ги прегледа по всяко време, за да може да докаже, че се спазва принципът на отчетност. В рамките на упражняването на правото си на одит съгласно 28, параграф 3, буква з), администраторът следва да разполага с процедура за извършване на одитни кампании, за да провери чрез проверки на извадки дали договорите с неговите подизпълнители съдържат необходимите задължения за защита на данните.

70. Поради това необходимостта да се поиска копие от договора за подизпълнение зависи от обстоятелствата по случая. Например в случай на съмнения дали обработващият лични данни или обработващият лични данни подизпълнител спазва изискванията на член 28, параграфи 1 и 4 или по искане на НО, администраторът следва да поиска договора за преглед (например в случай че допълнителният обработващ лични данни е пострадал от нарушение на сигурността на данните или в случай на друга публично достъпна информация или друга информация, с която разполага администраторът), например може да има образци на договора за обработване на данни на обработващия лични данни подизпълнител, които не отговарят на изискванията на член 28, параграф 3 от ОРЗД.

на износителя на данни вносителят на данни предоставя на износителя на данни копие от такова споразумение за обработващ лични данни подизпълнител и всички последващи изменения. В степента, необходима за защита на търговски тайни или друга поверителна информация, включително лични данни, вносителят на данни може да редактира текста на споразумението, преди да сподели копие“. Освен това в модул 3 (между обработващи лични данни) се предвижда, че „*по искане на износителя на данни или на администратора, вносителят на данни предоставя копие от такова споразумение с подизпълнител и всички последващи изменения. В степента, необходима за защита на търговски тайни или друга поверителна информация, включително лични данни, вносителят на данни може да редактира текста на споразумението, преди да сподели копие*“. Решение за изпълнение (ЕС) 2021/914 на Комисията от 4 юни 2021 година относно стандартни договорни клаузи за предаването на лични данни на трети държави съгласно Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета („стандартни договорни клаузи при международно предаване на лични данни на Европейската комисия“).

[60] НО на Дания — стандартни договорни клаузи за целите на спазването на член 28 от ОРЗД, по-специално клауза 7.5; стандартни договорни клаузи на НО на Литва за целите на спазването на член 28 от ОРЗД, по-специално клауза 18; стандартни договорни клаузи на НО на Словения за целите на спазването на член 28 от ОРЗД, по-специално клауза 6.5.

71. За да се осигури спазването на член 28, параграф 1 в светлината на принципа на отчетност, копие от договорите за подизпълнение може да помогне на администратора да докаже, че неговите обработващи лични данни и обработващи лични данни подизпълнители предоставят достатъчни гаранции, включително че обработващият обработващи лични данни спазва член 28, параграф 4 от ОРЗД. ЕКЗД отбелязва, че администраторът може да не е в състояние да оцени дали гаранциите, предоставени във връзка с подизпълнител, са достатъчни или не, без да е получил достъп до съдържанието на договора за подизпълнение и да го е оценил. Въпреки че гаранциите могат да са предвидени в писмен вид в договора, договорните клаузи не могат сами по себе си да докажат, че страните по договора ефективно прилагат достатъчни гаранции.

2.2 Относно тълкуването на член 28, параграф 1 от ОРЗД във връзка с член 44 от ОРЗД (предавания във веригата на обработване — въпроси 1.2 и 1.3)

72. Въпрос 1.2 от искането има за цел да внесе разяснения в случаите на предаване или последващо предаване от обработващ лични данни (подизпълнител) към друг обработващ лични данни (подизпълнител), до каква степен администраторът следва, като част от задължението си съгласно член 28, параграф 1 от ОРЗД във връзка с член 44 от ОРЗД, да прецени съгласно предоставената документация от обработващите лични данни (подизпълнители), че нивото на защита на личните данни не е изложено на риск от първоначалното или последващото предаване на данни.

73. С въпрос 1.3 се цели да се изясни дали обхватът на задълженията по член 28, параграф 1 от ОРЗД във връзка с член 5, параграф 2 и член 24 от ОРЗД, както е отговорено във въпрос 1.2, варира в зависимост от риска, свързан с дейността по обработване. Ако това е така, НО на Дания поиска да знае каква е степента на тези задължения за „нискорискови“ и за „високорискови“ дейности по обработване.

Уводни разяснения

74. За по-голяма яснота, в рамките на настоящото становище са дадени някои уводни разяснения, свързани с тези въпроси.

75. На първо място, ЕКЗД разбира понятието „предаване“ в смисъла, заложен в Насоки на ЕКЗД 5/2021 относно взаимодействието между член 3 и глава V от ОРЗД[61] (наричани по-долу „Насоки на ЕКЗД 5/2021 (взаимодействие)“), които се позовават и на Насоки на ЕКЗД 3/2018 относно териториалния обхват на ОРЗД[62]. Както беше изтъкнато по-рано от ЕКЗД, дистанционният достъп от трета държава представлява предаване, ако отговаря на критериите, определени в Насоки на ЕКЗД 5/2021 (взаимодействие)[63]. Във всеки случай при наличието на предаване се прилага глава V от ОРЗД.

76. Второ, тъй като въпрос 1.2 се отнася до ситуация, при която обработващият лични данни (подизпълнител) извършва първоначално или последващо предаване на друг обработващ лични данни (подизпълнител), администраторът не е износителят на данни; износителят на данни е по-скоро обработващ лични данни, който предава личните данни на друг обработващ лични данни по веригата от името на администратора, а не на отделен администратор. По тази причина това изключва личните данни, предавани на отделни администратори, включително правораздавателни органи, съдилища или административни органи на трети държави. Поради това тълкуването на член 48 от ОРЗД не попада в обхвата на тези въпроси.

77. На трето място, ЕКЗД отбелязва, че въпрос 1.2 се отнася до предавания, които се извършват по веригата на обработване в съответствие с писмените инструкции на администратора съгласно член 28, параграф 3, буква а) от ОРЗД. Следва да се изтъкне, че от администратора зависи да реши дали предаването на лични данни извън ЕИП е възможно като част от дейностите по обработване, възложени на обработващите лични данни (подизпълнители). Обработващият лични данни трябва да се въздържа от извършване на всяко първоначално или последващо предаване извън обхвата на инструкциите на администратора[64]. Писмените инструкции на администратора по отношение на първоначалното или последващото предаване на лични данни трябва да се предават надолу по веригата на обработване[65].

78. Четвърто, ЕКЗД пояснява, че понятието за риск, посочено във въпрос 1.3, следва да се разбира като риск за правата и свободите на субектите на данни, чиито лични данни се обработват, по смисъла на съображения 75 и 76 от ОРЗД (както е посочено в точка 35 по-горе).

[61] Насоки на ЕКЗД 5/2021 относно взаимодействието между прилагането на член 3 и разпоредбите относно международното предаване на данни съгласно глава V от ОРЗД, версия 2.0, приета на 14 февруари 2023 г., в която в параграф 9 се определят трите кумулативни критерия за определяне на дадена операция по обработване като предаване, а в по-общ план раздел 2 се описват подробно тези критерии.

[62] Насоки на ЕКЗД 5/2021 (взаимодействие), точка 12, като се позовава на Насоки на ЕКЗД 3/2018 относно териториалния обхват на ОРЗД, версия 2.1, приети на 12 ноември 2019 г. (с поправка от 7 януари 2020 г.), стр. 5 и раздели 1—3. Вж. по-специално „г) Обработващо лице, което не е установено в Съюза“ в раздел 2.

[63] Насоки на ЕКЗД 5/2021 (взаимодействие), точка 16.

[64] Член 29 от ОРЗД. Както се припомня от ЕКЗД, *„в договора следва да се определят изискванията по отношение на предаване на данни на трети държави или международни организации, като се вземат предвид разпоредбите на глава V от ОРЗД*“ (Насоки на ЕКЗД 7/2020, точка 119). Например администраторът може да избере да забрани предаването на данни или да го позволи само на определени държави.

[65] Член 28, параграф 4 от ОРЗД.

Отговорността на администратора се запазва дори ако обработващите лични данни (подизпълнители) извършват първоначалното или последващото предаване

79. Що се отнася до същността на искането, ЕКЗД вече посочи, че „(*...) ще има ситуация на предаване, при която обработващият лични данни (съгласно член 3, параграф 1 или съгласно член 3, параграф 2 според конкретното обработване (...)) изпраща данни на друг обработващ лични данни или дори на администратор в трета държава съгласно указанията на неговия администратор. В тези случаи обработващият лични данни действа като износител на данни от името на администратора и трябва да гарантира, че се спазват разпоредбите на глава V за въпросното предаване съгласно инструкциите на администратора, включително че се използва подходящ инструмент за предаване. Като се има предвид, че предаването 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****.*“[66]

80. С други думи, в случай на предаване, дори ако то не се извършва пряко от администратора, а по-скоро от обработващ лични данни от името на администратора, администраторът продължава да има задължения, произтичащи както от член 44 от ОРЗД, така и от член 28, параграф 1 от ОРЗД[67] [68].

Отговорността, произтичаща от член 44 от ОРЗД

81. Задълженията по член 44 от ОРЗД[69] са насочени както към обработващите лични данни (действащи като износители на данни в контекста на становището), така и към администраторите[70]. Поради това както обработващите лични данни, така и администраторите следва да гарантират, че нивото на защита на личните данни не е изложено на риск от първоначалното или последващото предаване, независимо от основанието, на което се извършва предаването[71]. Например както администраторът, така и обработващият лични данни по принцип продължават да носят отговорност съгласно глава V от ОРЗД за незаконно

[66] Насоки на ЕКЗД 5/2021 (взаимодействие), точка 19, подчертаването е добавено с получер шрифт.

[67] Също така е уместно да се отбележи, че член 28, параграф 1 от ОРЗД се отнася до изпълнението на изискванията на ОРЗД и поради това следва да се тълкува като включващ разпоредбите на глава V, свързани с първоначалното или последващото предаване на лични данни на трети държави. Това се отнася както до първоначалното, така и до последващото предаване на данни, вж. член 44 от ОРЗД.

[68] За целите на настоящия раздел от становището са разгледани задълженията, произтичащи от член 44 и член 28, параграф 1 от ОРЗД, като се уточнява, че администраторът продължава да подлежи на всички задължения, приложими към администраторите съгласно ОРЗД.

[69] Член 44 от ОРЗД се отнася до разпоредбите на глава V от ОРЗД.

[70] Член 44 от ОРЗД се отнася както до „администратора, така и до обработващия лични данни“ за спазване на глава V; вж. също съображение 101. Поради тази причина Препоръки на ЕКЗД 1/2020 относно мерките, които допълват инструментите за предаване на данни, за да се гарантира спазването на нивото на защита на личните данни в ЕС, версия 2.0, приети на 18 юни 2021 г. (наричани по-долу „Препоръки на ЕКЗД 1/2020“), се прилагат за „износителите на данни“ (независимо дали са администратори или обработващи лични данни (подизпълнители)).

[71] Решение на Съда на ЕС от 16 юли 2020 г. *Data Protection Commissioner срещу Facebook Ireland Ltd, Maximillian Schrems* (наричано по-долу „дело на Съда на ЕС Schrems II“), дело C-311/18, ECLI:EU:C:2020:559, точка 92.

първоначално или последващо предаване[72] и поради това в случай на нарушение могат да бъдат подведени под отговорност и двамата, и всеки поотделно.

Отговорността, произтичаща от член 28, параграф 1 от ОРЗД

82. Съгласно принципа на отчетност от администраторите се изисква да предприемат „подходящи мерки“ за предотвратяване на всякакви нарушения на правилата, установени в ОРЗД, за да се гарантира правото на защита на данните[73] и това включва предотвратяване на нарушения на глава V от ОРЗД. Тази отговорност има действие преди началото на предаването и докато предадените лични данни се обработват в третата държава.

83. Както е обяснено по-горе в точки 47—48, *задължението на администратора* да провери дали обработващите лични данни (подизпълнители) предоставят достатъчни гаранции за изпълнението на мерките, определени от администратора, съгласно член 28, параграф 1 от ОРЗД[74] следва да се прилага независимо от риска за правата и свободите на субектите на данни. Въпреки това *степента* на такава проверка на практика ще варира в зависимост от естеството на организационните и техническите мерки, определени от администратора въз основа, наред с други критерии, на риска, свързан с обработването[75]. В това отношение наличието на първоначално или последващо предаване на трети държави по веригата на обработване може да увеличи рисковете, произтичащи от обработването, и поради това оказва въздействие върху „подходящите“ мерки, определени от администратора[76].

84. При поискване администраторът — подпомаган от обработващия лични данни и обработващите лични данни подизпълнители — следва да може да докаже на компетентния НО, че спазва изискванията на член 28, параграф 1 от ОРЗД. Подходящата документация може да се основава, наред с другото, на информацията, получена от обработващите лични данни в контекста на включването на обработващи лични данни (подизпълнители)[77] (вж. точки 54—56), но също така

[72] Администраторът може да поиска от обработващия лични данни обезщетение, съответстващо на неговата част от отговорността, при условие че са изпълнени условията, посочени в член 82, параграф 5 от ОРЗД.

[73] Вижте раздела по-горе относно член 5, параграф 2 и член 24, параграф 1 във връзка с член 28, параграф 1 от ОРЗД.

[74] За да се избегнат съмнения, следва да се изясни, че „подходящите технически и организационни мерки“, посочени в член 24, параграф 1 и член 28, параграф 1 от ОРЗД, не трябва да се бъркат с „допълнителните мерки“, посочени в Препоръки на ЕКЗД 1/2020 (точка 50: *„По същество „допълнителните мерки“ допълват гаранциите, които инструментът за предаване на данни по член 46 от ОРЗД вече осигурява, и всички други приложими изисквания за сигурност (напр. технически мерки за сигурност), установени в ОРЗД*“, като се прави позоваване на съображение 109 от ОРЗД и решението на Съда на ЕС по делото Schrems II, точка 133).

[75] Вижте определението за риск, както е обяснено в точки 35 и 78.

[76] В съображение 116 от ОРЗД се предвижда: *„Трансграничното движение на лични данни извън Съюза може да увеличи риска физическите лица да не могат да упражнят правата на защита на данните, по-специално да се защитят срещу неправомерна употреба или разкриване на тези данни*.“

[77] Вж. също така клауза 9, буква а) от модул 3 (обработващ лични данни към обработващ лични данни) на стандартните договорни клаузи при международно предаване на лични данни на Европейската комисия и приложение III към него; вж. също така клауза 9, буква а) от модул 2 (от администратор към обработващ лични данни); и клауза 7.7, буква а) от стандартните договорни клаузи между администратор и обработващ лични данни на Европейската комисия и приложение IV към него „Списък на обработващите лични данни подизпълнители“. Както приложение II към стандартните договорни клаузи при международно предаване на лични данни на Европейската комисия, така и приложение IV към стандартните договорни клаузи между администратор и обработващ лични данни на Европейската комисия, трябва да бъдат попълнени със следната информация за обработващите данни подизпълнители

и с помощта на неговите обработващи лични данни в съответствие с член 28, параграф 3, буква з) от ОРЗД (вж. точки 51—52).

85. Администраторът също така се нуждае от цялата необходима информация, за да издаде необходимите инструкции за предаване на личните данни на съответните трети държави и за да може да спазва принципа на отчетност в член 5, параграф 2 и член 24 от ОРЗД, както и за да се съобрази с разпоредбите на член 28, параграф 1, член 32 и глава V от ОРЗД[78]. Администраторът може да възрази или да не разреши включването на допълнителен обработващ лични данни, когато това би довело до предаване на лични данни от първоначалния обработващ лични данни (като износител) към предвидения допълнителен обработващ лични данни (в качеството му на вносител) въз основа на получената информация.

86. В съответствие с точка 58 по-горе администраторът носи крайната отговорност за всяко нарушение на член 28, параграф 1 от ОРЗД, когато става въпрос за използване на обработващи лични данни (подизпълнители), и може да бъде подведен под отговорност за това нарушение. ЕКЗД изтъква, че практическите трудности, на които се позовават администраторите във връзка с контрола върху включването на обработващи лични данни подизпълнители от страна на техния обработващ лични данни — което може да затрудни проверката на „достатъчните гаранции“, особено по отношение на предаването на данни на трети държави — не освобождават администратора от неговите отговорности при обработването[79].

87. По-долу са изложени неизчерпателни примери за документацията, която администраторът трябва да оцени и да може да покаже на компетентния НО — описание на предаването, използвано основание за предаването и, когато е приложимо, „оценка на въздействието на предаването“ и допълнителни мерки.

Описание на предаването:

88. Като първа стъпка, когато ще се предават лични данни на трети държави във връзка с използването на обработващи лични данни (подизпълнители), администраторът следва да оцени и да бъде в състояние да покаже документация, свързана с описанието на предаването[80]. Администраторът следва да гарантира, че описанието на предаването се извършва от износителя (който обработва личните данни от негово име), като посочва кои лични данни се предават (включително достъп от разстояние), къде и за какви цели[81]. Администраторът може да разчита на такова описание и ако е необходимо, да го допълва. Например, когато описанието,

---

в случай на специално разрешение от администратора: име, адрес, име на лице за контакт, длъжност и данни за контакт, както и описание на обработването. Освен това, приложение I към стандартните договорни клаузи при международно предаване на лични данни на Европейската комисия, раздел Б „Описание на предаването“ включва „За предаването на данни на обработващи лични данни (подизпълнители), също така се посочват предметът, естеството и продължителността на обработването“. По същия начин приложение II към стандартните договорни клаузи между администратор и обработващ лични данни включва „За обработването от обработващи лични данни (подизпълнители), също така се посочват предметът, естеството и продължителността на обработването“.

[78] Насоки на ЕКЗД 7/2020, точка 152, бележка под линия 69.

[79] Доклад за рамката за координирано правоприлагане относно услугите в облак, стр. 16.

[80] „Описание“ се отнася до първата стъпка (т.нар. „Бъдете запознати с предаването на данни, което извършвате“) от Препоръки на ЕКЗД 1/2020, раздел 2.1 „Стъпка 1: Бъдете запознати с предаването на данни, което извършвате“. Тази първа стъпка се прилага независимо от основанието за предаването.

[81] Следва да се уточни, че целите се определят от администратора, заедно с „основните средства“ за обработването (вж. Насоки на ЕКЗД 7/2020, точка 40).

получено от администратора, изглежда непълно[82], неточно или поражда въпроси, той следва да поиска допълнителна информация, да я провери/допълни/коригира, ако е необходимо.

89. Администраторът следва да получи тази информация[83], преди да бъде включен допълнителен обработващ лични данни. Следва също така да се припомни, че администраторът подлежи на специални изисквания за прозрачност по отношение на предаването на данни към трети държави съгласно член 13, параграф 1, буква е), член 14, параграф 1, буква е), член 15, параграф 1, буква в) и член 15, параграф 2 от ОРЗД, както и на изискването за поддържане на регистри на дейностите по обработване съгласно член 30, параграф 1, букви г) и д) от ОРЗД. За да изпълни тези изисквания, администраторът следва да знае къде се намират обработващите лични данни подизпълнители и къде се извършва предаването на данни, включително дистанционният достъп[84].

Използваното основание за предаване и когато е приложимо — „оценката на въздействието на предаването“ и допълнителните мерки:

90. Администраторът следва да оцени и да може да покаже документация, свързана с основанието за предаване[85], въз основа на което износителят разчита, в съответствие с инструкциите на администратора[86]. Това означава, че администраторът трябва да получи тази информация от обработващите лични данни (подизпълнители)/износителите преди извършване на предаването. В този смисъл ЕКЗД припомня, че администраторът подлежи на специални изисквания за прозрачност по отношение на „наличието или отсъствието на решение относно адекватното ниво на защита“ съгласно член 45 от ОРЗД или на „подходящи гаранции“, осигурени в съответствие с член 46 от ОРЗД (член 13, параграф 1, буква е), член 14, параграф 1, буква е) и член 15, параграф 2 от ОРЗД[87]).

91. Що се отнася до обхвата на задължението на администратора да оценява тази документация, той зависи от вида на основанието, използвано за първоначалното или последващото предаване от обработващите лични данни (подизпълнители) (като износител на данни)[88]:

92. Предаването на данни може да се извършва въз основа на **решение относно адекватното ниво на защита**, ако съгласно член 45 от ОРЗД Комисията е решила, че трета държава, територия, или един или повече конкретни сектори в тази трета държава или че дадена международна организация гарантира адекватно ниво на защита. За да оцени дали нивото на защита е адекватно, Комисията взема предвид — наред с други критерии — правилата за последващо предаване на лични данни на друга трета държава или международна организация, които се спазват в тази държава или международна организация, съдебната практика, както и

[82] Например, ако в описанието не се посочва местоположението на обработващите лични данни подизпълнители, или ако предаванията под формата на достъп от разстояние не са посочени в описанието, докато се извършват.

[83] Както е обяснено по-горе в точки 54—56.

[84] Такова описание е необходимо и когато страните попълват съответните приложения към стандартните договорни клаузи при международно предаване на лични данни на Европейската комисия и стандартните договорни клаузи между администратор и обработващ лични данни на Европейската комисия (вж. бележка под линия 80 по-горе).

[85] Препоръки на ЕКЗД 1/2020, раздел 2.2. „Стъпка 2: Определяне на инструментите за предаване, на които разчитате“.

[86] Член 28, параграф 3, буква а) от ОРЗД.

[87] Насоки на ЕКЗД 1/2022 (право на достъп), точка 122.

[88] В съответствие с писмените инструкции на администратора по отношение на предаването на лични данни по веригата на обработване.

ефективните и приложими права на субектите на данни и ефективната административна и съдебна защита за субектите на данни, чиито лични данни се предават[89].

93. В този смисъл, когато предаването се извършва от обработващ лични данни (подизпълнител) (от името на администратора) въз основа на решение относно адекватното ниво на защита съгласно член 45 от ОРЗД, степента на проверка, изисквана от администратора съгласно член 28, параграф 1 от ОРЗД, че неговият обработващ лични данни (подизпълнител) предоставя достатъчни гаранции по отношение на спазването на глава V от ОРЗД, следва да обхваща следните елементи:

- дали решението относно адекватното ниво на защита е в сила[90],

- и дали предаването, извършено от името на администратора, попада в обхвата на такова решение (напр. попадащи в обхвата категории лични данни или сектори)[91].

94. Когато личните данни, предавани от обработващ лични данни (подизпълнител) (от името на администратора) въз основа на решение относно адекватното ниво на защита, са предмет на **последващо предаване** от тази трета държава, нивото на защита на физическите лица, гарантирано от ОРЗД за такова последващо предаване, също не следва да бъде изложено на риск[92]. В тази връзка, съгласно член 45, параграф 2, буква а) от ОРЗД всяко решение относно адекватното ниво на защита, издадено от Европейската комисия, обхваща, наред с другото, правилата на трети държави, уреждащи последващите предавания на лични данни. Поради това съгласно член 44 от ОРЗД администраторът не трябва да проверява самостоятелно тези изисквания.

95. Що се отнася до задължението на администратора съгласно член 28, параграф 1 от ОРЗД, това означава, че администраторът следва да гарантира, че обработващият лични данни (подизпълнител) предоставя „достатъчни гаранции“ и по отношение на последващите предавания на лични данни, извършвани от обработващ лични данни (подизпълнител) от подходяща държава.

---

[89] Виж член 45 от ОРЗД и Референтен документ за адекватност на работната група по член 29, приет на 28 ноември 2017 г., РД 254, одобрен от ЕКЗД на 25 май 2018 г., стр. 7: „*По-нататъшно предаване на лични данни от първоначалния получател на първоначалното предаване на данни следва да бъде разрешено само когато последващият получател (т.е. получателят на последващото предаване) също е обект на правила (включително договорни правила), осигуряващи адекватно ниво на защита, и следва приложимите инструкции при обработването на данни от името на администратора на данни. Последващото предаване на данни не трябва да излага на риск нивото на защита на физическите лица, чиито данни биват предавани. Първоначалният получател на данните, предадени от ЕС, е длъжен да гарантира, че са осигурени подходящи гаранции за последващо предаване на данни при липса на решение относно адекватното ниво на защита. Такова последващо предаване на данни следва да се извършва само за ограничени и определени цели и при условие че е налице правно основание за това обработване*“.

[90] Препоръки на ЕКЗД 1/2020, точка 19: „*Ако вие [износителят на данни] 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*. *Въпреки това трябва да следите дали решенията относно адекватното ниво на защита, които са от значение за вашето предаване, са отменени или обявени за недействителни*“.

[91] Препоръки на ЕКЗД 1/2020, точка 19.

[92] Вж. член 44 от ОРЗД: „ *(...) спазват условията по настоящата глава, включително във връзка с последващи предавания на лични данни от третата държава или от международната организация на друга трета държава или на друга международна организация*“.

96. При липса на решение относно адекватното ниво на защита предаванията на лични данни може да бъдат обвързани с предоставянето на „**подходящи гаранции**“ в съответствие с **член 46 от ОРЗД**. В този случай администраторът следва да оцени подходящите защитни мерки, които са въведени, и да обърне внимание на всяко проблематично законодателство, което би могло да попречи на обработващия лични данни подизпълнител да изпълни задълженията, установени в договора му с първоначалния обработващ лични данни[93]. По-конкретно, администраторът следва да гарантира, че такава „оценка на въздействието на предаването“[94] е извършена в съответствие със съдебната практика[95] и както е обяснено в Препоръки на ЕКЗД 1/2020. Документацията, свързана с въведените подходящи гаранции, „оценката на въздействието на предаването“ и възможните допълнителни мерки, следва да бъде изготвена от обработващия лични данни/износителя[96] (когато е целесъобразно в сътрудничество с обработващия лични данни/вносителя[97]). Администраторът може да разчита на оценката, изготвена от обработващия лични данни (подизпълнител), и ако е необходимо, да я допълва. Например, когато оценката, получена от администратора, изглежда непълна, неточна или повдига въпроси, администраторът следва да поиска допълнителна информация, да я провери и да я допълни/коригира, ако е необходимо, като има предвид, че оценката следва да бъде в съответствие с Препоръки на ЕКЗД 1/2020 и стъпките, посочени в тях[98]. Това включва определяне на законите и практиките, които са от значение с оглед на всички обстоятелства на предаването[99], и определяне на подходящи допълнителни мерки, ако е необходимо[100]. В тази връзка администраторът следва да обърне особено внимание на това дали износителят на данни, т.е. обработващият лични данни или подизпълнителят, е оценил дали има някои аспекти

[93] В това отношение виж решение на Съда на ЕС по делото Schrems II, точки 132 и 133, където Съдът на ЕС набляга на договорния характер на стандартните договорни клаузи при международно предаване на лични данни на Европейската комисия.

[94] Тази оценка е обяснена по-подробно в Препоръки на ЕКЗД 1/2020, стъпка 3, озаглавена „Преценете дали инструментът за предаване по член 46 от ОРЗД, на който се базирате, е ефективен с оглед на всички обстоятелства на предаването“.

[95] Решение на Съда на ЕС по дело Schrems II, точка 134.

[96] Препоръки на ЕКЗД 1/2022 относно заявлението за одобрение и относно елементите и принципите, които се съдържат в задължителните фирмени правила на администратора (член 47 от ОРЗД), приети на 20 юни 2023 г., версия 2.1, точка 10: „(...) *отговорност на всеки износител на данни например е да прецени за всяко предаване поотделно в зависимост от всеки случай дали е необходимо да се приложат допълнителни мерки, за да се осигури ниво на защита, което по същество е равностойно на осигуреното от ОРЗД*.“

[97] В решението си по дело Schrems II, точка 134 Съдът на ЕС отбеляза, че такава проверка може да се извърши в сътрудничество с вносителя, когато е целесъобразно. Вж. също Препоръки на ЕКЗД 1/2020 на ЕНОП, раздел 4.

[98] Вижте по-специално „Стъпка 3: Преценете дали инструментът за предаване на данни по член 46 от ОРЗД е ефективен с оглед на всички обстоятелства в процеса на предаването“, „Стъпка 4: Да се приемат допълнителни мерки“ и „Стъпка 6: Извършвайте повторна оценка през подходящи интервали от време“, както е обяснено в Препоръки на ЕКЗД 1/2020.

[99] Решение на Съда на ЕС по дело Schrems II, точка 126. Вж. също Препоръки на ЕКЗД 1/2020, раздел 2.3. „Стъпка 3: Преценете дали инструментът за предаване на данни по член 46 от ОРЗД, та който се базирате, е ефективен с оглед на всички обстоятелства в процеса на предаването“, и по-специално точка 33. В решението си по дело Schrems II, точка 134 Съдът на ЕС отбеляза, че такава проверка може да се извърши в сътрудничество с вносителя при необходимост (вж. също Препоръки на ЕКЗД 1/2020, точка 30).

Въз основа на съдебната практика администраторът или обработващият лични данни трябва преди всичко да провери поотделно и евентуално в сътрудничество с получателя на предаването дали правото на третата държава на местоназначение осигурява подходяща от гледна точка на правото на Съюза защита на личните данни, предадени въз основа на стандартни клаузи за защита на данните, като при необходимост предостави допълнителни спрямо предоставените от тези клаузи гаранции[100]. Вж. също Препоръки на ЕКЗД 1/2020, раздел 2.4., „Стъпка 4: Приемане на допълнителни мерки“.

в законодателството и/или практиките в третата държава, които може да засегнат ефективността на подходящите гаранции на основанието за предаване, на което износителят се базира[101], особено поради законодателството и практиките, уреждащи достъпа до предадените лични данни от страна на публичните органи на третата държава[102].

97. Освен това, подобно на предаването на данни въз основа на решение относно адекватното ниво на защита (член 45 от ОРЗД, вж. по-горе в точки 94 и 95), когато личните данни се предават от обработващ лични данни (подизпълнител) въз основа на подходящи гаранции съгласно член 46 от ОРЗД, задължението на администратора съгласно член 28, параграф 1 от ОРЗД обхваща също така да се увери, че обработващият лични данни (подизпълнител) представя достатъчни гаранции по отношение на **последващите предавания**. Подходящите гаранции по член 46 от ОРЗД обикновено включват разпоредби, определящи правила, които ще регулират всяко последващо предаване[103]. Това означава, че администраторите не трябва да проверяват дали тези правила като такива са в съответствие с изискванията на глава V от ОРЗД. Въпреки това администраторите следва да са в състояние да покажат документация, свързана с такова последващо предаване. Това означава, че администраторът следва да получи такава информация от обработващите лични данни (подизпълнители)/износителите, която показва, че вносителите действително спазват изискванията за последващо предаване, както е предвидено в приложимия инструмент за подходящи гаранции.

2.3 Относно тълкуването на член 28, параграф 3, буква а) от ОРЗД (въпрос 2)

98. За да се осигури прозрачно разпределение на отговорностите и задълженията както вътрешно (между администраторите и обработващите лични данни), така и външно, по отношение на субектите на данни и регулаторите, съгласно член 28, параграф 3 от ОРЗД всяко обработване на лични данни от обработващ лични данни трябва да се урежда от договор или друг правен акт съгласно правото на ЕС или на държава членка[104] между администратора и обработващия лични данни. В съответствие с 28, параграф 3, буква а) от ОРЗД, в договора се уточнява по специално, че обработващият лични данни „*обработва личните данни само по документирано нареждане на администратора, включително що се отнася до предаването на лични данни на трета държава или международна организация, освен когато е длъжен да направи това по силата на правото на Съюза или правото на държава членка, което се прилага спрямо обработващия лични данни*“. В тази разпоредба се предвижда също, че „*в този случай обработващият лични данни информира администратора за това правно изискване преди обработването, освен ако това право забранява такова информиране на важни основания от публичен интерес*“.

99. Искането се отнася до съществуването на договори, които включват ангажимент за обработване на лични данни само по указание на администратора, „*освен ако това не се изисква по силата на закон или от задължителна заповед на правителствен орган*“ (без позоваване на правото на Съюза или правото на държава членка). Във връзка с това към ЕКЗД бяха отправени няколко въпроса, които са разгледани заедно в раздела по-долу:

[101] Вж. Препоръки на ЕКЗД 1/2020, раздел 2.3 („Стъпка 3“).

[102] Вж. Препоръки на ЕКЗД 1/2020, точка 41 и следващите.

[103] Вж. напр. клауза 8.7 (модул 1), съответно 8.8 (модули 2 и 3) от стандартните договорни клаузи при международно предаване на лични данни на Европейската комисия (Решение за изпълнение 2021/914 на Комисията) от 4 юни 2021 г.

[104] По-долу терминът „**договор**“ ще се използва за обозначаване на „договор или друг правен акт съгласно правото на ЕС или правото на държава членка“.

2 Трябва ли договор или друг правен акт, съгласно правото на Съюза или правото на държава членка съгласно член 28, параграф 3 от ОРЗД да съдържа изключението, предвидено в член 28, параграф 3, буква а) „*освен когато е длъжен да направи това по силата на правото на Съюза или правото на държава членка, което се прилага спрямо обработващия лични данни*“ (дословно или чрез много подобни изрази), за да е в съответствие с ОРЗД?

2а Ако отговорът на въпрос 2 е отрицателен, когато договор или друг правен акт съгласно правото на Съюза или на държава членка разширява изключението по член 28, параграф 3, буква а) от ОРЗД така, че да обхваща и правото на трета държава (например „освен ако това не се изисква по силата на закон или от задължителна заповед на правителствен орган“), това само по себе си представлява ли нарушение на член 28, параграф 3, буква а) от ОРЗД?

100. В Насоки на ЕКЗД 7/2020 се припомня „*важността на внимателното договаряне и изготвяне на споразумения за обработване на данни*“ по отношение на всяко правно изискване на ЕС или на държава членка, което се прилага спрямо обработващия лични данни[105]. Що се отнася до съдържанието, в Насоки на ЕКЗД 7/2020 се отбелязва, че „*споразумението между администратора и обработващия лични данни трябва да отговаря на изискванията на член 28 от ОРЗД, за да се гарантира, че обработващият лични данни обработва личните данни в съответствие с ОРЗД. Във всяко такова споразумение следва да бъдат взети предвид специфичните отговорности на администраторите и обработващите лични данни. Въпреки че член 28 съдържа списък с точки, които трябва да бъдат взети предвид във всеки договор, уреждащ отношенията между администраторите и обработващите лични данни, той оставя възможност за преговори между страните по такива договори*“[106]. Възможността за преговори е ограничена от изискванията, определени в член 28, параграф 3 от ОРЗД.

[105] Насоки на ЕКЗД 7/2020, точка 121.
[106] Насоки на ЕКЗД 7/2020, точка 109.

101. На първо място, ангажиментът на обработващия лични данни да обработва лични данни само по документирано нареждане от администратора е основен елемент на договора.

102. Въпреки това, както се отбелязва в член 28, параграф 3, буква а) от ОРЗД, обработващите лични данни могат да обработват законно лични данни — по друг начин, освен по документирано нареждане на администратора — с цел спазване на правни задължения съгласно законите на ЕС или държавите членки (наричани по-долу **правно изискване на ЕС/ДЧ**"). Същата разпоредба изисква и ангажимент от страна на обработващия лични данни да информира администратора — предварително — когато се прилага правно изискване на ЕС/ДЧ за обработване/предаване на лични данни на трета държава или международна организация, освен ако това законодателство забранява такава информация на важни основания от публичен интерес. Този ангажимент е изрично включен с формулировка, много сходна с тази на член 28, параграф 3, буква а) от ОРЗД, в стандартните договорни клаузи между администратор и обработващ лични данни на Европейската комисия[107] и в няколко стандартни договорни клаузи, по-специално в стандартните договорни клаузи, приети от НО на Дания[108], Словения[109] и Литва[110] за целите на спазването на член 28 от ОРЗД.

[107] Вж. по-специално клауза 7.1, буква а) и клауза 7.8, буква а):
клауза 7.1, буква а): „*Обработващият лични данни обработва лични данни единствено следвайки писмените инструкции на администратора, освен когато е длъжен да направи това по силата на правото на Съюза или правото на държава членка, което се прилага спрямо обработващия лични данни. В този случай обработващият лични данни информира администратора за това правно изискване преди обработването, освен ако това право забранява такова информиране на важни основания от публичен интерес. По време на целия период на обработване на личните данни администраторът може да дава и последващи указания. Тези инструкции винаги се документират*." (подчертаването е добавено). В съвместното си становище относно проекта на стандартни договорни клаузи на Европейската комисия, ЕКЗД и ЕНОЗД препоръчаха да се включи пълната формулировка на член 28, параграф 3, буква а) (като по този начин се добави позоваване на задължението на обработващия лични данни да информира администратора за правното изискване), за да се подобри съгласуваността. Съвместно становище 1/2021 на ЕКЗД и ЕНОЗД във връзка с Решението за изпълнение на Европейската комисия относно стандартни договорни клаузи между администратори и обработващи лични данни по въпросите, посочени в член 28, параграф 7 от Регламент (ЕС) 2016/679 и член 29, параграф 7 от Регламент (ЕС) 2018/1725, точка 38. Формулировката „*освен когато е длъжен да направи това по силата на правото на Съюза или правото на държава членка, което се прилага спрямо обработващия лични данни*" вече присъстваше в проекта на стандартните договорни клаузи.
— клауза 7.8, буква а): „*Всяко предаване на данни на трета държава или на международна организация от страна на обработващия лични данни се извършва само въз основа на документирано нареждане от администратора или за да се изпълни конкретно изискване съгласно правото на Съюза или правото на държава членка, което се прилага спрямо обработващия лични данни, и се извършва в съответствие с глава V от Регламент (ЕС) 2016/679 или Регламент (ЕС) 2018/1725*." По отношение на клауза 7.8, буква а) ЕКЗД и ЕНОЗД препоръчаха да се включи позоваване на възможността обработващият лични данни да извършва предаване на данни въз основа на конкретно изискване съгласно правото на Съюза или правото на държава членка, което се прилага спрямо обработващия лични данни, което първоначално не е посочено в проекта на стандартни договорни клаузи. Приложение 2 към Съвместно становище 1/2021 на ЕКЗД и ЕНОЗД, Бележки към клауза 7.7, буква а).
[108] Стандартни договорни клаузи на НО на Дания за целите на спазването на член 28 от ОРЗД, по-специално клаузи 4.1 и 8.2. В Становище на ЕКЗД 14/2019 относно проекта на стандартни договорни клаузи, представен от НО на Дания (член 28, параграф 8 от ОРЗД), ЕКЗД препоръча да се включи формулировката на член 28, параграф 3, буква а), за да се гарантира правна сигурност.
[109] Стандартни договорни клаузи на НО на Словения за целите на спазването на член 28 от ОРЗД, по-специално клаузи 3.1 и 7.2.
[110] Стандартни договорни клаузи на НО на Литва за целите на спазването на член 28 от ОРЗД, по-специално клаузи 4.1, 22 и 23.

103. Така, освен задължението за обработване само въз основа на документирано нареждане на администратора, член 28, параграф 3, буква а) от ОРЗД съдържа три основни елемента: а) правило, уреждащо случаите, в които дадено правно изискване задължава обработващия лични данни да извършва обработване на лични данни, което не се основава на нареждането на администратора, следователно не е от името на администратора; б) необходимостта обработващият лични данни да информира администратора[111] и в) позоваването на такова правно изискване, произтичащо от правото на ЕС или правото на държава членка.

104. В този смисъл ЕКЗД припомня, че като общ принцип договорите не могат да имат предимство над закона. Това означава, че независимо дали клаузата, предвидена в член 28, параграф 3, буква а) от ОРЗД *(„освен когато е длъжен да направи това по силата на правото на Съюза или правото на държава членка, което се прилага спрямо обработващия лични данни“*), е включена в договор, тя не може да попречи на прилагането на правни изисквания в допълнение към договорните изисквания или в някои случаи — в противоречие с тях. Освен това, в съответствие с общия принцип, че договорът не създава задължения към трети страни, договорът не може да обвързва например публичните органи на държава членка или на трета страна[112].

105. Всички договори между администратор и обработващ лични данни трябва да обхващат ситуациите, при които обработващият лични данни може да бъде задължен по силата на законодателството да обработва лични данни по друг начин, освен по документирано нареждане на администратора. Освен това задължението на обработващия лични данни да информира администратора преди извършване на обработването, което не се основава на неговото нареждане, също е основен елемент на договора и също трябва да бъде включен в него [113].

106. За личните данни, обработвани извън ЕИП, позоваването на правото на ЕС или на държавата членка може да няма особено значение, тъй като обработващият лични данни извън ЕИП само по изключение ще подлежи на правните изисквания на ЕС или на държавата членка. В това отношение ЕКЗД отбелязва, че стандартните договорни клаузи при международно предаване на лични данни на Европейската комисия, които са предвидени да удовлетворяват, освен изискванията на член 46, параграф 1 и член 46, параграф 2, буква г) от ОРЗД, и изискванията на

[111] В член 28, параграф 3, буква а) от ОРЗД се предвижда, че когато правото на Съюза или на държава членка изисква обработващият лични данни да обработва лични данни, *„обработващият лични данни информира администратора за това правно изискване преди обработването, освен ако това право забранява такова информиране на важни основания от публичен интерес“*.

[112] Поради това в стандартните договорни клаузи при международно предаване на лични данни на Европейската комисия са включени редица предпазни мерки, които изискват от износителя и вносителя да оценят задължителните изисквания на законодателството на трета държава преди предаването на данните, за да се гарантира, че те не надхвърлят необходимото в едно демократично общество (клауза 14, букви а)—г)), изискващи от вносителя да уведоми износителя в случай на промени, а от последният — да предприеме необходимите действия (клауза 14, букви д) и е)), и налагащи на вносителя задължения в случай на достъп от страна на публични органи (клауза 15). Вж. решение на Съда на ЕС по делото Schrems II, точки 125 и 141.

[113] В Становище на ЕКЗД 18/2021 относно проекта на стандартни договорни клаузи, представен от НО на Литва (член 28, параграф 8 от ОРЗД), ЕКЗД препоръча да се включи последният елемент от член 28, параграф 8 от ОРЗД. 28, параграф 3, буква а) в стандартните договорни клаузи (т.е. задължението на обработващия лични данни да информира администратора за приложимото правно изискване), Становище на ЕКЗД 18/2021, точка 19.

член 28, параграфи 3 и 4 от ОРЗД[114], не съдържат формулировка, подобна на клаузата „освен ако“ в член 28, параграф 3, буква а) от ОРЗД. Въпреки това изискването за обработване на лични данни само по документирано нареждане от администратора, освен ако това не се изисква от правото на ЕС или на държава членка, вече е разгледано косвено в клауза 8.1 от стандартните договорни клаузи при международно предаване на лични данни на Европейската комисия[115]. Освен това, това не означава, че задължението за предоставяне на информация по член 28, параграф 3, буква а) от ОРЗД не е отчетено, като се има предвид, че в стандартните договорни клаузи при международно предаване на лични данни на Европейската комисия изрично е включена необходимостта вносителят на данни да информира износителя на данни, ако не е в състояние да следва нареждането на администратора[116]. В резултат на това ангажиментът на обработващия лични данни да информира администратора, когато се прилага правно изискване за обработване (независимо дали произтича от правото на ЕС или правото на държава членка или от правото на трета държава), произтича от стандартните договорни клаузи при международно предаване на лични данни на Европейската комисия, без да се използва точната фраза „*освен когато е длъжен да направи това по силата на правото на Съюза или правото*

[114] Вж. съображение 9 от стандартните договорни клаузи при международно предаване на лични данни на Европейската комисия „*Когато обработването включва предавания на данни от администратори, попадащи в обхвата на Регламент (ЕС) 2016/679, на обработващи лични данни извън неговия териториален обхват или от обработващи лични данни, попадащи в обхвата на Регламент (ЕС) 2016/679, на обработващи лични данни подизпълнители извън неговия териториален обхват, стандартните договорни клаузи, заложени в приложението към настоящото решение, също следва да позволяват изпълнението на изискванията по член 28, параграфи 3 и 4 от Регламент (ЕС) 2016/679*“.

[115] Клауза 8 относно гаранциите за защита на данните (модул 2: Предаването на данни от администратора към обработващия лични данни) гласи в раздел 8.1 — указанието:

а) Вносителят на данни обработва личните данни само по документирано нареждане на износителя на данни. Износителят на данни може да дава такива указания през целия срок на договора.

б) Вносителят на данни незабавно уведомява износителя на данни, ако не е в състояние да изпълни тези указания.“

По подобен начин в модул 3 (Предаване на данни от обработващ лични данни на обработващ лични данни) клауза 8 относно гаранциите за защита на данните гласи в раздел 8.1 — указания:

„*а) Износителят на данни е уведомил вносителя на данни, че действа като лице, обработващо данните, съгласно указанията на своя(ите) администратор(и) на данни, като предоставя тези указания на вносителя на данни преди обработването.*

б) Вносителят на данни обработва личните данни само по документирано нареждане на администратора на данни, съобщено от износителя на данни на вносителя на данни, и по всички допълнителни документирано нареждане на износителя на данни. Такова допълнително нареждане не трябва да противоречи на нареждането на администратора на данни. Администраторът или износителят на данни може да дава допълнителни документирани нареждания относно обработването на данните през целия срок на договора.

в) Вносителят на данни незабавно уведомява износителя на данни, ако не е в състояние да изпълни тези указания. Когато вносителят на данни не е в състояние да изпълни указанията на администратора на данни, износителят на данни незабавно уведомява администратора.“

[116] В допълнение към клауза 8.1 (вж. предишната бележка под линия), клауза 14 гласи в раздел 14.д, че: „*Вносителят на данни се съгласява да уведоми износителя на данни своевременно, ако, след като е приел настоящите клаузи и по време на срока на договора, има основания да смята, че е длъжен, или ако стане длъжен да спазва закони или практики, които не са в съответствие с изискванията по буква а), включително след промяна на законите на третата държава или на мярка (като например искане за разкриване), сочеща за прилагане на тези закони на практика, което не е в съответствие с изискванията по буква а). [За модул 3: [За модул 3: Износителят на данни изпраща уведомлението на администратора на лични данни.]*“

на държава членка, което се прилага спрямо обработващия лични данни на член 28, параграф 3, буква а) от ОРЗД (елемент в), посочен по-горе).

107. Това е в съответствие с целта на член 28, параграф 3, буква а) от ОРЗД да се гарантира, че администраторът е информиран, когато по закон от обработващия лични данни се изисква да обработва лични данни по начин, различен от този по нареждане на администратора.

108. С оглед на горния анализ ЕКЗД счита, че включването в договор между администратора и обработващия лични данни на изключението[117], предвидено в член 28, параграф 3, буква а) от ОРЗД „*освен когато е длъжен да направи това по силата на правото на Съюза или правото на държава членка, което се прилага спрямо обработващия лични данни*“ (дословно или чрез много подобни изрази), е силно препоръчително, но не е строго задължително, за да бъде в съответствие с член 28, параграф 3, буква а) от ОРЗД. Тази позиция не засяга необходимостта от договорно задължение за информиране на администратора, когато обработващият лични данни е задължен по закон да обработва лични данни по друг начин, освен по указания на администратора, както е предвидено в член 28, параграф 3, буква а) от ОРЗД. Когато е ясно, че правните изисквания на ЕС или на държавата членка са от значение за обработването, използването на формулировката на член 28, параграф 3, буква а) от ОРЗД би помогнало да се докаже съответствие.

109. Сега ЕКЗД се насочва към въпроса дали договор, включващ по-широко изключение, обхващащо и правото на трета държава, например изключение от задължението личните данни да се обработват само въз основа на документирано нареждане от администратора, „*освен ако това не се изисква от закона или от задължителен акт на правителствен орган*“, сам по себе си представлява нарушение на член 28, параграф 3, буква а) от ОРЗД.

110. Тази формулировка, ако не е придружена от допълнителни уточнения, може да обхваща две отделни ситуации, които следва да бъдат анализирани поотделно с оглед на правния контекст:

- предвиденото правно изискване или задължителен акт произтича от правото на Съюза или на държава членка (ЕИП).
- предвиденото правно изискване или задължителен акт произтича от закони, различни от правото на Съюза или на държава членка (ЕИП).

[117] По-специално, когато администраторът и обработващият лични данни разчитат на собствения си договор за обработване, а не на стандартните договорни клаузи между администратор и обработващ лични данни на Европейската комисия, на стандартните договорни клаузи, приети от НО за целите на спазването на член 28 от ОРЗД, или стандартните договорни клаузи при международно предаване на лични данни на Европейската комисия. Вж. също съображение 109 и член 28, параграф 6 от Регламент (ЕС) 2016/679.

111. Първата ситуация попада в обхвата на изричните разпоредби на член 28, параграф 3, буква а) от ОРЗД, в които се определя договорно задължение за обработващия лични данни да обработва само по документирано нареждане на администратора, „*освен когато е длъжен да направи това по силата на правото на Съюза или правото на държава членка, което се прилага спрямо обработващия лични данни*“. Това е така, независимо дали обработването на лични данни се извършва в рамките на ЕИП или извън него.

112. Правото на ЕС, включително ОРЗД и правните изисквания на държавите членки, са част от същата конституционна традиция като ОРЗД, който включва защитата на физическите лица във връзка с обработването на лични данни като основно право, съгласно член 16, параграф 1 от Договора за функционирането на Европейския съюз („**ДФЕС**“) и член 8, параграф 1 от Хартата на основните права на Европейския съюз („**Хартата**“)[118].

113. Когато въз основа на други елементи от своя(ите) договор(и) страните могат да докажат, че само тази първа ситуация е обхванатa от думите „*освен ако това не се изисква от закона или от задължителен акт на правителствен орган*“, тази формулировка не оказва въздействие върху гаранциите, предвидени в член 28, параграф 3, буква а) от ОРЗД.

114. Ще има случаи, в които договорът(ите) на страните надхвърля тази първа ситуация, което означава, че позоваването на „*закон или от задължителен акт на правителствен орган*“ обхваща правни изисквания/задължителни актове, произтичащи от закони, различни от правото на Съюза или правото на държава членка (ЕИП) (втора ситуация).

115. ЕКЗД отбелязва, че изискванията за обработване на данни въз основа на закони, различни от правото на Съюза или на държава членка (ЕИП), сами по себе си не споделят конституционната традиция и не могат автоматично да се разглеждат по същия начин като тези в рамките на правния ред на ЕС (в светлината на член 44 от ОРЗД). Във връзка с това ЕКЗД припомня, че съгласно член 6 от ОРЗД термините „законово задължение“, „обществен интерес“ и „официални правомощия“ се отнасят до правото на Съюза или правото на държава членка[119]. Също така ЕКЗД отбелязва, че в член 29 от ОРЗД относно обработването под ръководството на администратора или обработващия лични данни се предвижда, че „*обработващият лични данни и всяко лице, действащо под ръководството на администратора или на обработващия лични данни, което има достъп до личните данни, обработва тези данни само по указание на*

[118] В Съображение 1 от ОРЗД се съдържа препратка към член 16, параграф 1 от Договора за функционирането на Европейския съюз („ДФЕС“) и член 8, параграф 1 от Хартата на основните права на Европейския съюз („Хартата“). В член 52, параграф 1 от Хартата се уточнява, че „*всяко ограничаване на упражняването на правата и свободите, признати от настоящата Харта, трябва да бъде предвидено в закон и да зачита основното съдържание на същите права и свободи. При спазване на принципа на пропорционалност ограничения могат да бъдат налагани, само ако са необходими и ако действително отговарят на признати от Съюза цели от общ интерес или на необходимостта да се защитят правата и свободите на други хора*.“

[119] В член 6, параграф 3 от ОРЗД се предвижда, че когато правното основание за обработването е „законово задължение“ (член 6, параграф 1, буква в) от ОРЗД) или „ задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора“ (член 6, параграф 1, буква д) от ОРЗД), това се отнася до разпоредбите, предвидени в правото на Съюза или в правото на държавата членка, което се прилага спрямо администратора. Във връзка с член 6 от ОРЗД, в съображение 40 от ОРЗД се пояснява, че когато правното основание за обработването е установено по законодателен път, това означава „*в настоящия регламент или в друг правен акт на Съюза или на държава членка, както е посочено в настоящия регламент*“. В член 49, параграф 4 от ОРЗД се предвижда, че само обществени интереси, признати в правото на Съюза или в правото на държавата членка, което се прилага спрямо администратора, могат да доведат до прилагането на тази дерогация.

администратора, <u>освен ако обработването не се изисква от правото на Съюза или правото на държава членка</u>“. (подчертаването е добавено)

116. В рамките на предаването може да се предвиди, че правни изисквания могат да произтичат и от законодателство, различно от правото на ЕС или правото на държава членка. ЕКЗД припомня, че когато се извършва предаване, глава V от ОРЗД се прилага в допълнение към член 28 от ОРЗД. ЕКЗД е на мнение, че по отношение на личните данни, обработвани извън ЕИП, член 28, параграф 3, буква а) от ОРЗД по принцип не възпрепятства включването в договора на разпоредби, които се уреждат изискванията на правото на трета държава за обработване на предадените лични данни. По специално, такива разпоредби могат да бъдат включени с цел да се гарантира спазването на глава V от ОРЗД, но е малко вероятно само включването на думите „*освен ако това не се изисква от закона или от задължителен акт на правителствен орган*“ да бъде достатъчно.

117. В този смисъл ЕКЗД отбелязва, че в клауза 14 от стандартните договорни клаузи при международно предаване на лични данни на Европейската комисия се разглеждат конкретно „Местните закони и практики, които засягат спазването на клаузите“, а в клауза 15 — „Задълженията на вносителя на данни в случай на достъп от страна на публични органи“. Преди подписването на стандартните договорни клаузи страните трябва да преценят дали има местни закони и практики, които засягат спазването на клаузите (клауза 14 от стандартните договорни клаузи при международно предаване на лични данни на Европейската комисия). Клауза 14 изисква от страните да гарантират, че не са им известни закони и практики в третата държава, в която е установен вносителят, които биха му попречили да изпълни задълженията си съгласно стандартните договорни клаузи при международно предаване на лични данни на Европейската комисия, след оценка от страна на вносителя на такива закони и практики, и изисква от вносителя да уведоми незабавно износителя за всяка промяна, като в този случай или износителят определя подходящи мерки за справяне със ситуацията, или клауза 14 му позволява да спре предаването и дори да прекрати договора. Клауза 15 налага определени задължения на вносителя на данни в случай на достъп от страна на публични органи на трета държава. В нея се определят редица стъпки, които вносителят на данни трябва да предприеме, когато се налага достъп на правителство на трета държава (по искане или директно), като целта е да се гарантира (в крайна сметка), че администраторът е информиран. Освен задължението да уведоми износителя на данни, вносителят има, *inter alia*, задължението да провери законосъобразността на искането за достъп и да документира тази правна оценка, както и задължението да оспори искането в определени случаи. В такъв случай износителят на данни — след консултация с администратора, когато износителят на данни не е администраторът — ще бъде в състояние да предприеме необходимите мерки, включително евентуално спиране на предаването или прекратяване на стандартните договорни клаузи при международно предаване на лични данни на Европейската комисия. Дали всяко (последващо) предаване на правителството на третата държава е в съответствие с ОРЗД, ще зависи от анализа на всеки отделен случай (наред с другото, от правното основание, контрола и спазването на глава V от ОРЗД). Съгласно модул 3 на стандартните договорни клаузи при международно предаване на лични данни на Европейската комисия (обработващ лични данни към обработващ лични данни) вносителят/обработващият лични данни има задължението да предостави правната оценка на износителя. В това отношение ЕКЗД се позовава и на точки 88—89 и 106 по-горе.

118. Освен това съгласно стандартните договорни клаузи при международно предаване на лични данни на Европейската комисия както износителят, така и вносителят са задължени да се уверят, че законодателството на третата държава на местоназначение позволява на вносителя да се

съобрази със стандартните договорни клаузи при международно предаване на лични данни на Европейската комисия, преди да предаде лични данни на тази трета държава[120]. Когато обработващият лични данни изнася лични данни от името на администратора, това задължение също попада върху администратора (вж. също точка 79 и следващите по-горе).

119. По подобен начин в препоръките относно задължителните фирмени правила за администраторите и позоваванията на задължителните фирмени правила за обработващите лични данни също така се определя набор от задължения, в случай че член на задължителните фирмени правила е обект на конфликт между местното си законодателство и задължителните фирмени правила[121], и/или получи искане за разкриване от правоприлагащ орган или държавен орган по сигурността[122]. По-конкретно, в препоръките на ЕКЗД 1/2022[123] се посочва, че в задължителните фирмени правила за администраторите (ЗФП-А) следва да се съдържат клаузи, които разглеждат местните закони и практики, които засягат спазването на ЗФП-А (раздел 5.4.1), както и задълженията на вносителя на данни в случай на правителствени искания за достъп (раздел 5.4.2). ЗФП-А може да служат като механизъм за предаване към обработващи лични данни в рамките на групата.

120. В случаите, когато предаването е регламентирано с решения относно адекватното ниво на защита, законодателството относно „*достъпа на публичните органи до лични данни, а също и прилагането на такова законодателство*“ е един от елементите, които Европейската комисия трябва да вземе предвид при оценката на адекватността на нивото на защита съгласно член 45, параграф 2, буква а) от ОРЗД[124].

[120] Решение на Съда на ЕС по дело *Schrems II*, т. 141. Вж. също стандартните договорни клаузи при международно предаване на лични данни на Европейската комисия, клауза 14, букви а) — г).

[121] Раздел 5.4.1 „Местни закони и практики, които засягат спазването на ЗФП-А“, Препоръки на ЕКЗД 1/2022 относно заявлението за одобрение и относно елементите и принципите, които трябва да се съдържат в задължителните фирмени правила за администраторите (член 47 от ОРЗД). Раздел 6.3 „Необходимост от прозрачност, когато националното законодателство възпрепятства групата да спазва ЗФП“ от работния документ на Работната група по член 29 за създаване на таблица с елементите и принципите, които трябва да се съдържат в задължителните фирмени правила за обработващите лични данни, РД 257 ред.01, одобрен от ЕКЗД на 25 май 2018 г.

[122] Раздел 5.4.2 „Задължения на вносителя на данни в случай на правителствени искания за достъп“, Препоръки на ЕКЗД 1/2022 относно заявлението за одобрение и относно елементите и принципите, които трябва да се съдържат в задължителните фирмени правила за администраторите (член 47 от ОРЗД); вж. също раздел 6.3 „Необходимост от прозрачност, когато националното законодателство възпрепятства групата да спазва ЗФП“, Работен документ за създаване на таблица с елементите и принципите, които трябва да се съдържат в задължителните фирмени правила за обработващите лични данни, РД 257 ред.01.

[123] Препоръки на ЕКЗД 1/2022 относно заявлението за одобрение и относно елементите и принципите, които трябва да се съдържат в задължителните фирмени правила на администраторите (член 47 от ОРЗД).

[124] Съдът на ЕС разгледа този елемент в решенията си по делата Schrems I и Schrems II. Решение на Съда на ЕС от 6 октомври 2015 г., *Maximillian Schrems срещу Data Protection Commissioner*, (наричано по-нататък „Решение на Съда на ЕС Schrems I“), дело C-362/14, ECLI:EU:C:2015:650, точка 91 и следващите. Решение на Съда на ЕС по дело Schrems II, точки 141, 174—177, 187—189.

121. Общото между решенията относно адекватното ниво на защита [125], стандартните договорни клаузи при международно предаване на лични данни на Европейската комисия [126] и препоръките и позоваванията във връзка със ЗФП [127] е разбирането, че законите и практиките на трета държава, които зачитат същността на основните права и свободи, залегнали в ДФЕС, Хартата и ОРЗД, и не надхвърлят необходимото и пропорционалното в едно демократично общество, за да се гарантира една от целите, изброени в член 23, параграф 1 от ОРЗД, няма да изложат на риск равнището на защита, гарантирано от ОРЗД [128]. По тази причина в стандартните договорни клаузи при международно предаване на лични данни на Европейската комисия[129] и в препоръките и позоваванията във връзка със ЗФП[130] са включени разпоредби, които обвързват законите и практиките с различни последици в зависимост от това дали те излагат на риск нивото на защита, гарантирано от ОРЗД. В специалните договори, основани на член 46, параграф 3, буква а) от ОРЗД, също следва да се съдържат подобни разпоредби[131].

122. От гореизложеното става ясно, че когато законите на третата държава изискват от обработващия лични данни да обработва лични данни по друг начин, освен по указания на администратора, нивото на защита, заложено в ОРЗД, ще бъде спазено само ако тези закони отговарят на горепосочените условия. Във всички случаи обработващият лични данни следва да прилага допълнителни мерки, в случай че посочените условия не са изпълнени, а договорът следва да гарантира, че тези условия са изпълнени.

123. Когато обработващият лични данни обработва лични данни в рамките на ЕИП, при определени обстоятелства той все пак може да бъде засегнат от законодателството на трета държава. ЕКЗД

---

[125] Вж. член 45, параграф 2, буква а) от ОРЗД, в който се предвижда, че Европейската комисия взема предвид *„ върховенството на закона, спазването на правата на човека и основните свободи, съответното законодателство — както общо, така и секторно, включително в областта на обществената сигурност, отбраната, националната сигурност и наказателното право и достъпа на публичните органи до лични данни, а също и прилагането на такова законодателство, правилата за защита на данните, професионалните правила и мерките за сигурност, включително правилата за последващо предаване на лични данни на друга трета държава или международна организация, които се спазват в тази държава или международна организация, съдебната практика, както и действителните и приложими права на субектите на данни и ефективната административна и съдебна защита за субектите на данни, чиито лични данни се предават“*. Вж. също Референтен документ на Работната група по член 29 относно адекватното ниво на защита, РД 254 ред.01, приет на 6 февруари 2018 г., одобрен от ЕКЗД на 25 май 2018 г. Понятието „адекватно ниво на защита“ е допълнително развито от Съда на ЕС в решението му по делото Schrems I (точки 73 и 74) и по делото Schrems II (точка 94).

[126] Клауза 14.а от стандартните договорни клаузи при международно предаване на лични данни на Европейската комисия.

[127] Това изрично е посочено в Препоръки на ЕКЗД 1/2022 (препоръки относно ЗФП-А), версия 2.1, в точки 5.4.1 и 5.4.2. Същото разбиране косвено е в основата на раздел 6.3 „Необходимост от прозрачност, когато националното законодателство възпрепятства групата да спазва ЗФП“ от работния документ на Работната група по член 29, в който се създава таблица с елементите и принципите, които трябва да се съдържат в задължителните фирмени правила на обработващия лични данни, РД 257 ред.01, одобрен от ЕКЗД на 25 май 2018 г.

[128] Препоръки на ЕКЗД 1/2020 относно мерките, които допълват инструментите за предаване, за да се гарантира спазването на нивото на ЕС за защита на личните данни, версия 2.0, точка 38, и Препоръки на ЕКЗД 2/2020 относно европейските основни гаранции за мерките за наблюдение, точки 22 и 24.

[129] Клауза 14 от стандартните договорни клаузи при международно предаване на лични данни на Европейската комисия.

[130] Вж. бележка под линия 127.

[131] Препоръки на ЕКЗД 1/2020 относно мерките, които допълват инструментите за предаване, за да се гарантира спазването на нивото на ЕС за защита на личните данни, версия 2.0, точка 66.

изтъква, че добавянето в договора на препратка към правото на трета държава не освобождава обработващия лични данни от задълженията му съгласно ОРЗД.

124. В светлината на горния анализ ЕКЗД счита, че включването на фраза, подобна на „*освен ако това не се изисква от закона или от задължителен акт на правителствен орган*“, е прерогатив на свободата на договаряне на страните и само по себе си не нарушава член 28, параграф 3, буква а) от ОРЗД. С това не се засяга задължението за спазване на ОРЗД винаги, когато се обработват лични данни. Освен това такава клауза не освобождава администратора и обработващия лични данни от изпълнение на задълженията им съгласно ОРЗД, по-специално, по отношение на информацията, която трябва да се предоставя на администратора, и когато е приложимо, условията за международно предаване на лични данни, обработвани от името на администратора[132].

125. Накрая, в искането се задава последващ въпрос:

> Ако отговорът на въпрос 2а е отрицателен, следва ли такова разширено изключение вместо това да се тълкува като документирано указание от администратора по смисъла на член 28, параграф 3, буква а) от ОРЗД?

126. Предвид отговора, даден по-горе, ЕКЗД разбира, че оставащият въпрос е дали страните могат да твърдят, че фразата „*освен ако това не се изисква от закона или от задължителен акт на правителствен орган*“ (дословно или чрез много подобни изрази) в техния договор трябва да се тълкува като документирано нареждане от администратора по смисъла на член 28, параграф 3, буква а) от ОРЗД.

127. ЕКЗД първо разглежда дали този аргумент е приемлив, когато правното изискване или задължителният акт произтича от правото на Съюза или на държава членка (ЕИП).

128. ЕКЗД отбелязва, че понятието „нареждане“, използвано в член 28, параграф 3, буква а) от ОРЗД, се отнася конкретно до администратора, който определя какво обработване на данни се очаква да извърши обработващият лични данни от негово име и по какъв начин[133]. Всяка разпоредба, която администраторът включва в договора със своя доставчик на услуги/обработващ лични данни и която не се състои от искане за извършване на обработване на лични данни от името на администратора, също не се счита за нареждане по смисъла на член 28, параграф 3, буква а) от ОРЗД. В допълнение, нареждането на администратора ще трябва да бъде достатъчно точно, за да обхваща конкретно обработване на лични данни, което не е така с въпросната фраза. Освен това администраторът винаги (ще трябва) да бъде в състояние — и ще бъде правно задължен, в случай че дадено нареждане за обработване на лични данни от името на администратора е в нарушение на ОРЗД — да оттегли такова нареждане. След това обработващият лични данни следва да се съобрази с направеното от администратора оттегляне на нареждането и да прекрати обработването.

129. Като дава нареждане на обработващия лични данни, администраторът прилага на практика своето определение на целите и средствата за обработване на данните, по-специално, като упражнява влияние върху основните елементи на обработването[134]. По принцип влиянието на

---

[132] По-специално задължението на администратора да гарантира, че по отношение на обработването извън ЕИП обработване може да се извършва от обработващия лични данни само съгласно законодателството на трета държава, което гарантира по същество равностойно ниво на защита. Вж. също точки 116—122 по-горе.

[133] Насоки на ЕКЗД 7/2020, точка 116.

[134] Насоки на ЕКЗД 7/2020, точка 20.

администратора върху обработването на лични данни се прекратява, когато в законодателството на ЕС или на държава членка се предвиждат изисквания обработващият лични данни да извършва обработване на лични данни, които администраторът не е в състояние да направлява или спира[135]. Въпреки че администраторът може да напомни на обработващия лични данни да спазва правото на ЕС или на държавата членка, това не може да се разбира като нареждане по смисъла на член 28, параграф 3, буква а) от ОРЗД[136]. В смият ОРЗД се отчита това положение, именно като посочва, че обработващият лични данни трябва да обработва само по документирано указание на администратора, освен когато е длъжен да направи това по силата на правото на Съюза или правото на държава членка, което се прилага спрямо обработващия лични данни (член 28, параграф 3, буква а) от ОРЗД), и трябва незабавно да информира администратора, ако дадено нареждане нарушава ОРЗД (член 28, параграф 3, последна алинея от ОРЗД).

130. ЕКЗД счита, че съображенията по-горе се прилагат и когато правното изискване или задължителният акт произтичат от правото на третата държава. В този случай въпросното право ограничава влиянието, което администраторът може да упражнява върху обработването на данните.

131. В допълнение към гореизложеното, дадена клауза, съгласно която обработващият лични данни се задължава да обработва лични данни само по документирано нареждане на администратора *„освен ако това не се изисква от закона или от задължителен акт на правителствен орган“*, сама по себе си означава, че обработването по нареждане на администратора е правилото, а изключението съществува именно за обработването не по нареждане на администратора (както е видно от думата „освен ако“). Освен това обработващият лични данни все още сам решава дали да спази правното искане или задължителния акт, който се прилага спрямо него, или да понесе правните последици от неспазването му.

132. Въз основа на това ЕКЗД заключава, че *„освен ако това не се изисква от закона или от задължителен акт на правителствен орган“* (дословно или чрез много подобни изрази) не може да се тълкува като документирано нареждане от страна на администратора. Администраторът продължава да носи отговорност, когато не е гарантирал, че обработващият лични данни (подизпълнител) обработва лични данни само въз основа на негово документирано нареждане. Това обаче не се прилага, когато обработването се изисква съгласно правото на ЕС или правото на държава членка или за обработване извън ЕИП се изисква съгласно правото на трета държава, което се прилага спрямо обработващия лични данни (подизпълнител), и това право гарантира по същество равностойно ниво на защита.

За Европейския комитет по защита на данните

Председател

[135] В това отношение ситуацията би могла да бъде тази, предвидена в член 4, параграф 7 от ОРЗД, който гласи, че когато целите и средствата за това обработване се определят от правото на Съюза или правото на държава членка, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на Съюза или в правото на държава членка. Вж. Решение на Съда на ЕС от 11 януари 2024 г., *État belge (Données traitées par un journal officiel),* дело C-231/22, ECLI:EU:C:2024:7, точки 28—30, 35 и 39; Насоки на ЕКЗД 7/2020, точки 22—24.

[136] По-скоро такова напомняне ще се разглежда като въвеждане на договорни гаранции от страна на администратора, за да се гарантира, че обработването от негово име ще отговаря на всички изисквания на ОРЗД и ще гарантира защитата на правата на субекта на данните.

(Anu Talus)