Насоки

Насоки 07/2020 относно понятията „администратор“ и „обработващ лични данни“ в ОРЗД

Версия 2.0

Приети на 7 юли 2021 г.

История на версиите

Версия 2.0	7 юли 2021 г.	Приемане на насоките след обществена консултация
Версия 1.0	2 септември 2020 г.	Приемане на насоките за обществена консултация

РЕЗЮМЕ

Понятията „администратор“, „съвместен администратор“ и „обработващ лични данни“ имат ключова роля за прилагането на Общия регламент относно защитата на данните 2016/679 (ОРЗД), тъй като служат за определяне на това кой е отговорен за спазването на различните правила за защита на данните и как субектите на данни могат практически да упражняват своите права. Точното значение на тези понятия и критериите за тяхното правилно тълкуване трябва да бъдат достатъчно ясни и съгласувани в цялото Европейско икономическо пространство (ЕИП).

Понятията „администратор“, „съвместен администратор“ и „обработващ лични данни“ са *функционални,* тъй като се използват с цел разпределяне на отговорностите в съответствие с действителната роля на страните и са *автономни*, в смисъл че те следва да се тълкуват основно в съответствие с правото на ЕС в областта на защитата на данните.

Администратор

По принцип няма ограничение по отношение на вида правен субект, който може да поеме ролята на администратор, но на практика обикновено самата организация действа като администратор, а не физическо лице в нейните рамки (например- главен изпълнителен директор, служител или член на управителния съвет).

Администраторът е структурата, която *взема решения* по отношение на някои ключови елементи на обработването. Администрирането може да бъде определено със закон или въз основа на анализ на фактическите елементи или обстоятелства по случая. Някои дейности по обработване могат да бъдат разглеждани като естествено свързани с ролята на даден правен субект (работодател и служители, издател и абонати или сдружение и неговите членове). В много случаи условията на договора могат да помогнат за определяне на администратора, въпреки че не са решаващи във всички обстоятелства.

Администраторът определя целите и средствата за обработването, т.е. *защо* и *как* се извършва обработването. Той трябва да вземе решение както по отношение на целите, така и по отношение на средствата. Въпреки това някои по-практични аспекти на изпълнението („средства от второстепенна важност“) могат да бъдат оставени на обработващия лични данни. Не е необходимо администраторът да има действителен достъп до обработваните данни, за да бъде квалифициран като администратор.

Съвместни администратори

Квалифицирането като съвместни администратори може да възникне, когато в обработването участва повече от един администратор. С ОРЗД се въвеждат специфични правила за съвместните администратори и се установява рамка за уреждане на техните отношения. Общият критерий за наличието на съвместно администриране е съвместното участие на два или повече правни субекта в определянето на целите и средствата за дадена операция по обработване. Например, съвместното участие може да бъде под формата на *общо решение*, взето от два или повече правни субекта, или да произтича от *унифициране на решенията*, ако те са взаимнодопълващи се и необходими за извършването на обработването по такъв начин, че да имат осезаемо въздействие върху определянето на целите и средствата за обработването. Важен критерий е, че обработването не би било възможно без участието на двете страни, тоест че обработването от всяка една от страните съставлява неделимо цяло, т.е. е неразривно свързано. Съвместното участие трябва да включва определянето на целите, от една страна, и определянето на средствата, от друга страна.

Обработващ лични данни

Обработващият лични данни е физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора. Двете основни условия за квалифициране като обработващ лични данни са: да бъде отделен правен субект по отношение на администратора и да обработва лични данни от името на администратора.

Обработващият лични данни не трябва да обработва данните по никакъв друг начин, освен съгласно указанията на администратора. Тези указания все пак могат да предоставят известна свобода на преценка по отношение на това кой е най-добрият начин за обслужване на интересите на администратора, което позволява на обработващия лични данни да избере най-подходящите технически и организационни средства. Обработващият обаче нарушава ОРЗД, в случай че излезе извън рамките на указанията на администратора и започне да определя свои собствени цели и средства за обработването. В такъв случай обработващият лични данни ще се счита за администратор по отношение на това обработване и може да подлежи на санкции, ако излезе извън рамките на инструкциите на администратора.

Отношение между администратор и обработващ лични данни

Администраторът трябва да използва само обработващи лични данни, които предоставят достатъчни гаранции за прилагането на подходящи технически и организационни мерки по такъв начин, че обработването да протича в съответствие с изискванията на ОРЗД. Изискванията, които трябва да се вземат предвид, биха могли да бъдат експертните познания на обработващия лични данни (напр. технически експертен опит по отношение на мерките за сигурност и нарушенията на сигурността на данните); надеждността на обработващия; ресурсите на обработващия и придържането му към даден одобрен кодекс за поведение или механизъм за сертифициране.

Всяко обработване на лични данни от страна на обработващ лични данни трябва да се урежда с договор или с друг правен акт, който е в писмена форма, включително електронна, и е обвързващ. Администраторът и обработващият лични данни могат да изберат да сключат свой собствен договор, съдържащ всички задължителни елементи, или да разчитат изцяло или частично на стандартни договорни клаузи.

В ОРЗД са изброени елементите, които трябва да бъдат посочени в споразумението за обработване. В споразумението за обработване обаче не следва просто да бъдат повторени разпоредбите на ОРЗД; по-скоро то следва да включва по-конкретна специфична информация относно това как ще бъдат изпълнени изискванията и какво равнище на сигурност е необходимо за обработването на лични данни, което е предметът на споразумението.

Отношения между съвместните администратори

Съвместните администратори определят и съгласуват по прозрачен начин съответните си отговорности за изпълнение на задълженията по ОРЗД. Определянето на съответните им отговорности трябва по-специално да се отнася до упражняването на правата на субектите на данни и задълженията за предоставяне на информация. Освен това разпределението на отговорностите следва да обхваща и други задължения на администратора, например свързаните с общите принципи за защита на данните, правното основание, мерките за сигурност, задължението за уведомяване за нарушения на сигурността на данните, оценките на въздействието върху защитата на данните, използването на обработващи лични данни,

предаването на данни на трети държави и комуникирането със субектите на данни и надзорните органи.

Всеки съвместен администратор е длъжен да гарантира, че има правно основание за обработването и че данните не се обработват допълнително по начин, който е несъвместим с целите, за които данните първоначално са били събрани от администратора, който ги споделя.

Правната форма на договорността между съвместните администратори не е предвидена в ОРЗД. С оглед на правната сигурност и за да се осигури прозрачност и отчетност, Европейският комитет по защита на данните (ЕКЗД) препоръчва тази договореност да бъде под формата на обвързващ документ, например договор или друг правно обвързващ акт съгласно правото на ЕС или правото на държава членка, приложимо по отношение на администраторите.

Договорността надлежно отразява съответните роли и връзки на съвместните администратори със субектите на данни, като нейните съществени характеристики са достъпни за субекта на данни.

Независимо от условията на договорността, субектите на данни могат да упражняват своите права по отношение на всеки и срещу всеки от съвместните администратори. Надзорните органи не са длъжни да приемат условията на договорността, независимо дали става въпрос за квалифициране на страните като съвместни администратори или за посочената точка за контакт.

СЪДЪРЖАНИЕ

Европейският комитет по защита на данните

като взе предвид член 70, параграф 1, буква д) от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 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 (по-нататък „ОРЗД“ или „Регламентът“),

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

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

като има предвид, че работата по изготвянето на настоящите насоки включваше събирането на сведения от заинтересовани страни, както в писмен вид, така и по време на мероприятие с участието на заинтересовани страни с оглед определянето на най-неотложните предизвикателства,

ПРИЕ СЛЕДНИТЕ НАСОКИ:

ВЪВЕДЕНИЕ

1. Настоящият документ има за цел да предостави насоки относно понятията „администратор“ и „обработващ лични данни“ въз основа на правилата на ОРЗД, свързани с определенията в член 4 и разпоредбите относно задълженията в глава IV. Основната цел е да се изясни значението на понятията и различните роли, както и разпределението на отговорностите между тези участници.

2. Понятието „администратор“ и взаимодействието му с „обработващ лични данни“ имат решаваща роля за прилагането на ОРЗД, тъй като служат за определяне на това кой е отговорен за спазването на различните правила за защита на данните и как субектите на данни могат практически да упражняват правата си. ОРЗД изрично въвежда принципа на отчетност, т.е. администраторът носи отговорност и е в състояние да докаже спазването на принципите, свързани с обработването на лични данни, определени в член 5. Освен това ОРЗД въвежда и по-конкретни правила относно използването на обработващ(и) лични данни, а някои от разпоредбите относно обработването на лични данни са насочени не само към администраторите, но и към обработващите лични данни.

3. Поради това е особено важно точните значения на тези понятия, както и критериите за правилното им използване, да бъдат достатъчно ясни и общи за целия Европейски съюз и ЕИП.

4. Работната група по член 29 издаде насоки относно понятията „администратор/обработващ лични данни“ в своето Становище 1/2010 (РД 169)[2], за да предостави разяснения и конкретни

[1] Позоваванията на „държави членки“ в настоящия документ следва да се разбират като позовавания на „държавите — членки на ЕИП“.
[2] Становище 1/2010 на Работната група по член 29 относно понятията „администратор“ и „обработващ лични данни“, прието на 16 февруари 2010 г., 264/10/EN, РД 169.

примери. След влизането в сила на ОРЗД бяха повдигнати много въпроси относно това до каква степен са внесени промени в понятията „администратор“ и „обработващ лични данни“, както и в съответните им роли. Бяха повдигнати въпроси, по-специално, относно същността и значението на понятието „съвместно администриране“ (напр. както е определено в член 26 от ОРЗД) и относно специфичните задължения на обработващите лични данни, определени в глава IV (напр. както е посочено в член 28 от ОРЗД). Поради това и тъй като ЕКЗД признава, че за целите на специфичното прилагане на понятията е необходимо допълнителното им изясняване, е счетено за необходимо да се дадат по-подробни и конкретни насоки, за да се гарантира систематичен и хармонизиран поход в целия ЕС и ЕИП. Настоящите насоки заменят предходното становище на Работната група по член 29 относно тези понятия (РД 169).

5. В част I на настоящите насоки са разгледани определенията на различните понятия за „администратор“, „съвместни администратори“, „обработващ лични данни“ и „трета страна/получател“. В част II са предоставени допълнителни указания относно последствията, свързани с различните роли на администратора, съвместните администратори и обработващия лични данни.

ЧАСТ I — ПОНЯТИЯ

1 ОБЩИ НАБЛЮДЕНИЯ

6. В член 5, параграф 2 от ОРЗД изрично се въвежда принципът на отчетност, съгласно който:

   - администраторът *носи отговорност за спазването* на принципите, определени в член 5, параграф 1 от ОРЗД; и
   - администраторът е в състояние да *докаже спазването* на принципите, определени в член 5, параграф 1 от ОРЗД.

   Този принцип е описан в становище на Работната група по член 29[3] и няма да бъде подробно разгледан тук.

7. Целта на включването на принципа на отчетност в ОРЗД и превръщането му в основен принцип беше да се изтъкне, че администраторите на лични данни трябва да прилагат подходящи и ефективни мерки и да са в състояние да докажат съответствие. [4]

8. Понятието за принципа на отчетност е доразвито в член 24, в който се посочва, че администраторът въвежда подходящи технически и организационни мерки, за да гарантира и да е в състояние **да докаже**, че обработването се извършва в съответствие с ОРЗД. Тези мерки подлежат на преглед, като при необходимост биват актуализирани. Принципът на отчетност е отразен и в член 28, в който се определят задълженията на администратора при включване на обработващ лични данни.

9. Принципът на отчетност е пряко насочен към администратора. Някои от по-специфичните правила обаче са насочени както към администраторите, така и към обработващите лични данни, например правилата относно правомощията на надзорните органи в член 58. Както администраторите, така и обработващите лични данни, могат да бъдат глобени в случай на

[3] Становище 3/2010 на Работната група по член 29 относно принципа на отчетност, прието на 13 юли 2010 г., 00062/10/EN, РД 173.
[4] Съображение 74 от ОРЗД.

неизпълнение на задълженията по ОРЗД, които се приложими по отношение на тях, като както администраторите, така и обработващите, се отчитат пряко пред надзорните органи съгласно заложените задълженията да водят и предоставят необходимата документация при поискване, да си сътрудничат в случай на разследване и да спазват административните разпореждания. Същевременно следва да се припомни, че обработващите лични данни трябва винаги да спазват, както и да действат единствено съгласно, указанията на администратора.

10. Следователно, принципът на отчетност, заедно с останалите, по-специфични правила, свързани със спазването на ОРЗД и разпределението на отговорността, налага определянето на различните роли на няколко участници в дадена дейност по обработване на лични данни.

11. Общото наблюдение по отношение на понятията „администратор“ и „обработващ лични данни“ в ОРЗД е, че те не са променени в сравнение с Директива 95/46/ЕО и че като цяло критериите за определяне на различните роли остават същите.

12. Понятията „администратор“ и „обработващ лични данни“ са *функционални*: имат за цел да разпределят отговорностите в съответствие с действителната роля на страните[5].Това означава, че правният статут на даден участник в качеството му на „администратор“ или „обработващ лични данни“ по принцип трябва да се определя от действителните му дейности в конкретна ситуация, а не от формалното определяне на даден участник като „администратор“ или „обработващ лични данни“ (напр. в договор)[6]. Това означава, че разпределението на ролите обикновено се основава на анализ на фактическите елементи или обстоятелства по случая и поради това не подлежи на договаряне.

13. Определенията „администратор“ и „обработващ лични данни“ са също така и *автономни* понятия, което означава, че въпреки че външни правни източници могат да помогнат за определянето на това кой е администратор, това определение следва да се тълкува основно в съответствие с правото на ЕС в областта на защитата на данните. Понятието „администратор“ не следва да се засяга от други — понякога противоречиви или припокриващи се — термини в други области на правото, например „учредител“ или „носител на права“ в областта на правата върху интелектуалната собственост или в конкурентното право.

14. Тъй като основната цел на определянето на ролята на администратора е да се гарантира отчетността и ефективната, и всеобхватна защита на личните данни, понятието „администратор“ следва да се тълкува достатъчно широко, като се отдава предимство във възможно най-голяма степен на ефективната и цялостна защита на субектите на данни[7], така че да се гарантира пълното действие на правото на ЕС в областта на защитата на данните, да се избегнат пропуски и да се предотврати евентуално заобикаляне на правилата, като същевременно не се намалява ролята на обработващия лични данни.

---

[5] Становище 1/2010 на Работната група по член 29, РД 169, стр. 9.

[6] Вж. също Заключението на генералния адвокат Mengozzi по дело *„Свидетели на Йехова“ (Jehovah’s Witnesses*), C-25/17, ECLI:EU:C:2018:57, точка 68 (*„За целите на определянето на „администратора“ по смисъла на Директива 95/46 съм склонен да смятам [….] че прекомерният формализъм би позволил лесно да се заобиколят разпоредбите на Директива 95/46 и че следователно е необходимо да се основем на един по-скоро фактически, отколкото формален анализ […].*“)

[7] CEC, дело C-131/12, Google Spain SL и Google Inc. срещу Agencia Española de Protección de Datos (AEPD) и Mario Costeja González, решение от 13 май 2014 г., точка 34; CEC, дело C-210/16, Wirtschaftsakademie Schleswig-Holstein, решение от 5 юни 2018 г., точка 28; CEC, дело C-40/17, Fashion ID GmbH & Co.KG срещу Verbraucherzentrale NRW eV, решение от 29 юли 2019 г., точка 66.

2 ОПРЕДЕЛЕНИЕ ЗА „АДМИНИСТРАТОР“

2.1 Определение за „администратор“

15. Понятието „администратор“ е определено в член 4, параграф 7 от ОРЗД като:

> „***физическо или юридическо лице, публичен орган, агенция или друга структура,*** *която* ***сама или съвместно с други определя целите и средствата за обработването на лични данни****; 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****“*.

16. Определението за „администратор“ съдържа пет основни съставни елемента, които ще бъдат анализирани поотделно за целите на настоящите насоки. Те са следните:

- „физическо или юридическо лице, публичен орган, агенция или друга структура“
- „определя“
- „сама или съвместно с други“
- „целите и средствата“
- „за обработването на лични данни“.

2.1.1 „Физическо или юридическо лице, публичен орган, агенция или друга структура“

17. Първият съставен елемент е свързан с вида на правния субект, който може да бъде администратор. Съгласно ОРЗД, администраторът може да бъде *„физическо или юридическо лице, публичен орган, агенция или друга структура“*. Това означава, че по принцип няма ограничение по отношение на вида на правния субект, който може да поеме ролята на администратор. То може да бъде организация, но може да бъде и физическо лице или група физически лица[8]. На практика обаче обикновено самата организация, а не дадено физическо лице в рамките на организацията (като главен изпълнителен директор, служител или член на управителния съвет), действа като администратор по смисъла на ОРЗД. Що се отнася до обработването на данни в рамките на група от дружества, трябва да се обърне специално внимание на въпроса дали дадено предприятие може да действа като администратор или обработващ лични данни, например, когато се обработват данни от името на дружеството майка.

18. Понякога дружествата и публичните структури назначават конкретно лице, което отговаря за изпълнението на дейността по обработване. Дори ако конкретно физическо лице е назначено, за да се гарантира спазването на правилата за защита на данните, то няма да бъде администратор, а ще действа от името на юридическото лице (дружество или публичен орган), което в крайна сметка ще носи отговорност в случай на нарушение на правилата в качеството му

[8] Например, в своето решение по делото *„Свидетели на Йехова“* (*Jehovah’s witnesses*), C-25/17, ECLI:EU:C:2018:551, точка 75, СЕС е преценил, че религиозната общност „Свидетели на Йехова“ е действала като администратор съвместно със своите отделни членове. Решение по дело *„Свидетели на Йехова“ (Jehovah’s witnesses)*, C-25/17, ECLI:EU:C:2018:551, точка 75.

на администратор. По същия начин, дори ако определен отдел или звено на организация носи оперативна отговорност за гарантиране на съответствието по отношение на определена дейност по обработване, това не означава, че този отдел или звено (вместо организацията като цяло) става администратор.

Пример:

Маркетинговият отдел на дружеството ABC стартира рекламна кампания за популяризиране на продуктите на ABC. Маркетинговият отдел решава какво да бъде естеството на кампанията, средствата, които да се използват (електронна поща, социални медии...), към кои клиенти да бъде насочена и какви данни да се използват, за да може кампанията да бъде възможно най-успешна. Дори отделът да действа със значителна независимост, дружеството ABC ще се счита принципно за администратор, предвид факта, че рекламната кампания е стартирана от дружеството и се провежда в рамките на неговата стопанска дейност и за неговите цели.

19. По принцип може да се приеме, че всяко обработване на лични данни от служители, което се извършва в рамките на стопанската дейност на дадена организация, се извършва под контрола на тази организация[9]. При извънредни обстоятелства обаче може да се окаже, че служителят решава да използва лични данни за свои собствени цели, като по този начин незаконосъобразно превишава правомощията, които са му/ѝ предоставени. (напр. да учреди свое собствено дружество или нещо подобно). Поради това организацията е задължена, в качеството си на администратор, да гарантира наличието на подходящи технически и организационни мерки, включително, например, предоставяне на обучение и информация на служителите, за да се гарантира съответствие с ОРЗД[10].

2.1.2 „Определя“

20. Вторият съставен елемент на понятието „администратор“ се отнася до *влиянието* на администратора върху обработването чрез *упражняване на правомощия за вземане на решения*. Администраторът е структурата, която *взема решения* по отношение на някои ключови елементи във връзка с обработването. Това администриране може да бъде определено със закон или въз основа на анализ на фактическите елементи или обстоятелства по случая. Следва да се вземат предвид конкретните операции по обработване и да се установи кой ги определя, като първо бъдат разгледат следните въпроси: *„Защо се извършва това обработване?“ и „Кой е взел решение, че обработването следва да се извършва за конкретна цел?“.*

<u>Обстоятелства, на които се основава администрирането</u>

21. Понятието „администратор“ е функционално понятие, следователно то се основава **по-скоро на фактически, отколкото на формален анализ**. С цел улесняване на анализа могат да се използват някои презумпции, основаващи се на практиката, с цел насочване и опростяване на процеса. В повечето случаи „определящата структура“ може лесно и ясно да бъде идентифицирана чрез позоваване на определени правни и/или фактически обстоятелства, от които обикновено може да се направи извод за наличието на „влияние“, освен ако други елементи не сочат обратното. Могат да бъдат разграничени две категории ситуации: (1) администриране, основаващо се на *правни разпоредби*; и (2) администриране, основаващо се на *фактическо влияние*.

[9] Служителите, които имат достъп до лични данни в рамките на дадена организация, обикновено не се считат за „администратори“ или за „обработващи лични данни“, а по-скоро за „лица, действащи под ръководството на администратора или на обработващия лични данни“ по смисъла на член 29 от ОРЗД.
[10] член 24, параграф 1 от ОРЗД.

1) *Администриране, основаващо се на правни разпоредби*

22. Има случаи, в които администрирането може да се основава на изрични законови правомощия, например когато администраторът или специалните критерии за неговото назначаване се определят от националното право или правото на Съюза. Действително в член 4, параграф 7 се предвижда, 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*“. Докато член 4, параграф 7 се отнася само до „администратор“ в единствено число, ЕКЗД счита, че е възможно правото на Съюза или правото на държава членка да определя повече от един администратор, евентуално дори като съвместни администратори.

23. В случаите, в които администраторът е изрично определен от закона, това ще бъде от решаващо значение за установяване на това кой действа като администратор. Това предполага, че законодателят е определил като администратор правен субект, който действително е в състояние да извършва администрирането. В някои държави националното законодателство предвижда, че публичните органи носят отговорност за обработването на лични данни в рамките на своите задължения.

24. По-често обаче, вместо директно да назначава администратор или да определя критериите за неговото назначаване, законът възлага задача или налага задължение на някого да събира и обработва определени данни. В тези случаи целта на обработването често се определя от закона. Обикновено администратор е администраторът, определен от закона за осъществяването на тази цел — тази обществена задача. Такъв например би бил случаят, в който даден правен субект, на който са възложени определени обществени задачи (напр. социална сигурност), които не могат да бъдат изпълнявани без събиране на поне някои лични данни, създаде база данни или регистър за целите на изпълнението на тези обществени задачи. В този случай законът, макар и непряко, определя кой е администраторът. По-общо, законът може също така да наложи задължение на публичноправни или частноправни субекти да съхраняват или предоставят определени данни. В такъв случай тези правни субекти обикновено се считат за администратори по отношение на обработването, което е необходимо за изпълнението на това задължение.

Пример: Правни разпоредби

Националното законодателство на държава А предвижда задължение за общинските органи да предоставят социални обезщетения, например месечни плащания на гражданите в зависимост от финансовото им положение. За да извърши тези плащания, общинският орган трябва да събира и обработва данни относно финансовите обстоятелства на кандидатите. Въпреки че в закона не се посочва изрично, че общинските органи са администратори на това обработване, това следва имплицитно от правните разпоредби.

2) *Администриране, основаващо се на фактическо влияние*

25. В случай че администрирането не се основава на правни разпоредби, квалифицирането на дадена страна като администратор трябва да се основава на оценка на фактическите обстоятелства, свързани с обработването. Всички относими фактически обстоятелства трябва да се вземат предвид, за да се направи заключение дали определен правен субект упражнява решаващо влияние по отношение на въпросното обработване на лични данни.

26. Необходимостта от фактическа оценка означава също, че ролята на администратора не се основава на естеството на правния субект, който обработва данните, а на конкретните му дейности в конкретната ситуация. С други думи, същият правен субект може да действа едновременно като администратор за определени операции по обработването и като обработващ лични данни за други, а по отношение на квалифицирането като администратор или обработващ лични данни трябва да се извършва оценка за всяка специфична дейност по обработване на данни.

27. На практика някои дейности по обработване могат да се считат за естествено свързани с ролята или дейностите на даден правен субект, които по своето естество включват отговорности от гледна точка на защитата на данните. Това може да се дължи на по-общи правни разпоредби или на установена правна практика в различни области (гражданско право, търговско право, трудово право и т.н.). В този случай съществуващите обичайни роли и професионални експертни познания, които обикновено предполагат определена отговорност, ще помогнат за определянето на администратора, например: работодател във връзка с обработването на лични данни за своите служители, издател, който обработва лични данни за своите абонати, или сдружение, което обработва лични данни за своите членове или спонсори. Когато даден правен субект участва в обработването на лични данни като част от своите взаимодействия със свои служители, клиенти или членове, обикновено той определя целта и средствата, свързани с обработването и следователно действа като администратор по смисъла на ОРЗД.

Пример: Правни кантори

Дружеството ABC наема правна кантора, която да го представлява в спор. За да изпълни тази задача, правната кантора трябва да обработва лични данни, свързани със случая. Основанията за обработването на личните данни са правомощията на правната кантора да представлява клиента в съда. Целта на тези правомощия обаче не е конкретно обработването на лични данни. Правната кантора действа със значителна степен на независимост, например когато решава каква информация да използва и как да я използва, и не са налице указания от дружеството клиент относно обработването на лични данни. Следователно обработването, което правната кантора извършва, за да изпълни задачата в качеството си на законен представител на дружеството, е свързано с функционалната роля на правната кантора, поради което тя трябва да се счита за администратор на това обработване.

Пример: Телекомуникационни оператори[11]:

Предоставянето на електронна съобщителна услуга, например услуга за електронна поща, включва обработване на лични данни. Доставчикът на такива услуги обикновено се счита за администратор по отношение на обработването на лични данни, което е необходимо за извършването на самата услуга (напр. данни за трафика и за фактурирането). Ако единствената цел и роля на доставчика е да способства предаването на съобщения по електронна поща, доставчикът няма да се счита за администратор по отношение на личните данни, съдържащи се в самото съобщение. По отношение на всички лични данни, съдържащи се в съобщението, обикновено се счита, че администраторът е лицето, което предава съобщението, а не доставчикът на услуги, предлагащ услуги за предаване.

[11] ЕКЗД счита, че този пример, включен преди това в съображение 47 от Директива 95/46/ЕО, продължава да е уместен и съгласно ОРЗД.

28. В много случаи извършването на оценка на договорните условия между различните участващи страни може да улесни определянето на това коя страна (или страни) действа(т) като администратор. Дори ако в договора не се посочва кой е администраторът, той може да съдържа достатъчно елементи, въз основа на които да се направи извод чия е определящата роля при вземането на решения по отношение на целите и средствата за обработването. Възможно е също така в договора изрично да е заявена самоличността на администратора. Ако не са налице основания за съмнение, че това отразява точно действителното положение, няма причина да не бъдат спазени условията на договора. Условията на договора обаче не са определящи при всички обстоятелства, тъй като това просто би позволило на страните да разпределят отговорността по своя преценка. Не е възможно нито дадено лице да стане администратор, нито да избегне задълженията на администратор, просто чрез оформяне на договора по определен начин, когато фактическите обстоятелства показват друго.

29. Ако една от страните всъщност взема решенията защо и как да се обработват личните данни, тази страна е администратор, дори ако в договора се посочва, че тя е обработващ лични данни. Аналогично, самото използване в търговския договор на термина „подизпълнител“, не може да бъде причина правният субект да се счита за обработващ лични данни от гледна точка на правото в областта на защитата на данните[12].

30. В съответствие с фактологичния подход думата „определя“ означава, че правният субект, който действително упражнява решаващо влияние върху целите и средствата за обработването, е администраторът. Обикновено в споразумението за изпълнение се определя коя е определящата страна (администраторът) и страната, на която са дадени указания (обработващият лични данни). Дори ако обработващият лични данни предлага услуга, която е предварително определена по конкретен начин, на администратора трябва да бъде предоставено подробно описание на услугата и той трябва да вземе окончателното решение с цел фактическото одобрение на начина, по който се извършва обработването, и при необходимост — да поиска изменения. Освен това, обработващият лични данни не може на по-късен етап да променя съществените елементи на обработването без одобрението на администратора.

Пример: стандартизирана услуга съхранение „в облак“

Големите доставчици на услуги за съхранение на данни „в облак“ предлагат на своите клиенти възможността да съхраняват големи обеми лични данни. Услугата е напълно стандартизирана, като клиентите разполагат с малка или не разполагат с никаква възможност да я персонализират. Условията на договора се определят и изготвят едностранно от доставчика на услуги „в облак“ и се предоставят на клиента на принципа „предварително едностранно определени договорни условия“. Дружеството X решава да използва доставчика на услуги „в облак“, за да съхранява лични данни относно своите клиенти. Дружеството X ще продължи да се счита за администратор, предвид решението му да използва този конкретен доставчик на услуги „в облак“, за да обработва лични данни за своите цели. Доколкото доставчикът на услуги „в облак“ не обработва личните данни за свои собствени цели и съхранява данните единствено от името на своите клиенти и в съответствие с указанията, той се счита за обработващ лични данни.

[12] Вж. например Становище 10/2006 на Работната група по член 29 относно обработването на лични данни от Дружеството за световни междубанкови финансови телекомуникации (SWIFT), 22 ноември 2006 г., РД 128, стр. 11.

2.1.3 „Сам или съвместно с други“

31. В член 4, параграф 7 се посочва, че „целите и средствата“ за обработването могат да бъдат определени от повече от един участник. В него се определя, че администраторът е участникът, който „сам или съвместно с други“ определя целите и средствата за обработването. Това означава, че няколко различни правни субекта могат да действат като администратори за едно и също обработване, като след това всеки от тях подлежи на приложимите разпоредби за защита на данните. Съответно, дадена организация все пак може да бъде администратор, дори ако не взема всички решения по отношение на целите и средствата. Критериите за съвместно администриране и степента, в която двама или повече участници извършват заедно администриране могат да приемат различни форми, както е пояснено по-нататък[13].

2.1.4 „Цели и средствата“

32. Четвъртият съставен елемент на определението за администратор се отнася до предмета на влиянието на администратора, а именно „целите и средствата“ за обработването. Той представлява съществената част от понятието „администратор“: какво следва да определя дадена страна, за да бъде квалифицирана като администратор.

33. В речниците определението за „цел“ е „очакван резултат, който е зададен като цел или който служи за насочване на планираните от вас действия“, а за „средства“ — „начинът, по който се получава даден резултат или се постига крайна цел“.

34. В ОРЗД се посочва, че данните са събирани за конкретни, изрично указани и легитимни цели и не се обработват по-нататък по начин, несъвместим с тези цели. Поради това определянето на „целите“ на обработването и „средствата“ за постигането им е от особена важност.

35. Определянето на целите и средствата е равносилно на вземане на решение по отношение на въпросите „защо“ и „как“, касаещи обработването:[14] що се отнася до конкретна операция по обработване администраторът е участникът, който е определя *защо* се извършва обработването (т.е. „с каква цел“ или „по каква причина“) и *как* тази цел следва да бъде постигната (т.е. какви средства трябва да бъдат използвани за постигане на целта). Следователно, физическо или юридическо лице, което упражнява такова влияние по отношение на обработването на лични данни, участва в определянето на целите и средствата за това обработване, в съответствие с определението в член 4, параграф 7 от ОРЗД[15].

36. Администраторът трябва да вземе решение както относно целта, така и относно средствата за обработването, както е описано по-долу. В резултат на това администраторът не може да се ограничи единствено до определяне на целта. Той трябва също така да взема решения относно средствата за обработване. Обратно, страната, действаща като обработващ лични данни, никога не може да определи целта на обработването.

37. На практика, ако даден администратор включи обработващ лични данни, който да извършва обработването от негово име, това често означава, че обработващият може сам да взема определени решения относно начина на извършване на обработването. ЕКЗД признава, че може да съществува известна свобода на действие, за да може и обработващият да взема някои решения във връзка с обработването. От тази гледна точка е необходимо да се предоставят

[13] Вж. част I, точка 3 („Определение за съвместни администратори“).

[14] Вж. заключението на генералния адвокат Bot по дело *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2017:796, точка 46.

[15] Решение по дело *„Свидетели на Йехова“ (Jehovah’s witnesses*), C-25/17, ECLI:EU:C:2018:551, точка 68.

указания относно това каква **степен** квалифицирането на даден правен субект като администратор **оказва влияние** по отношение на въпросите „защо“ и „как“, и до каква степен обработващият лични данни може сам да взема решения.

38. В случаите, в които един правен субект ясно определя целите и средствата, като възлага на друг правен субект дейности по обработване, които по същество представляват изпълнение на неговите подробни указания, ситуацията е ясна и няма съмнение, че вторият правен субект следва да се разглежда като обработващ лични данни, а първият е администраторът.

Средства от първостепенна важност и средства от второстепенна важност

39. Въпросът е къде следва да се постави разграничителна линия между решенията, които са запазени за администратора, и тези, които могат да бъдат оставени на преценката на обработващия лични данни. Очевидно е, че решенията относно целта на обработването винаги се вземат от администратора.

40. Що се отнася до определянето на средствата, може да се направи разграничение между средства от първостепенна важност и тези от второстепенна важност. „Средствата от първостепенна важност“ обичайно и по своята същност са запазени за администратора. Докато средствата от второстепенна важност могат да бъдат определени също и от обработващия лични данни, средствата от първостепенна важност трябва да бъдат определени от администратора. „Средствата от първостепенна важност“ са средствата, които са тясно свързани с целта и обхвата на обработването, например вида лични данни, които се обработват (*„кои данни се обработват“*), продължителността на обработването (*„колко дълго ще бъдат обработвани“*), категориите получатели (*„кой ще има достъп до тях“*) и категориите субекти на данни (*„чии лични данни се обработват“*). Заедно с целта на обработването средствата от първостепенна важност са също така тясно свързани с въпроса дали обработването е законосъобразно, необходимо и пропорционално. „Средствата от второстепенна важност“ се отнасят до по-практически аспекти на изпълнението, например избора на конкретен вид хардуер или софтуер или подробните мерки за сигурност, по отношение на които решенията може да се вземат от обработващия лични данни.

Пример: Администриране на възнаграждения

Работодател А наема друго дружество, което да управлява изплащането на възнагражденията на неговите служители. Работодател А дава ясни указания относно това на кого се изплащат възнагражденията, какви суми, до коя дата, от коя банка, колко време следва да се съхраняват данните, какви данни следва да се разкриват на данъчния орган и т.н. В този случай обработването на данните се извършва за целите на дружество А във връзка с изплащането на възнаграждения на неговите служители, като лицето, администриращо възнагражденията, не може да използва данните за свои собствени цели. Начинът, по който лицето, администриращо възнагражденията, следва да извършва обработването, по същество е ясен и точно определен. Въпреки това лицето, администриращо възнагражденията, може да вземе решение във връзка с някои по-специфични елементи, свързани с обработването, например какъв софтуер да използва, как да разпредели правата на достъп в рамките на собствената си организация и т.н. Това не променя ролята му на обработващ лични данни, при условие че лицето, администриращо възнагражденията, не нарушава и не излиза извън рамките на указанията, дадени от дружество А.

Пример: Банкови плащания

Като част от указанията на работодател А лицето, администриращо възнагражденията, предава информация на банка В, за да може тя да извърши действителното плащане на служителите на работодател А. Тази дейност включва обработване на лични данни от банка В, което тя извършва за целите на банковата дейност. В рамките на тази дейност банката решава независимо от работодател А кои данни трябва да бъдат обработвани за предоставяне на услугата, колко дълго трябва да се съхраняват данните и т.н. Работодател А не може да оказва влияние върху целта и средствата за обработването на данни от банка В. Следователно банка В трябва да се разглежда като администратор на това обработване, а предаването на лични данни от лицето, администриращо възнагражденията, трябва да се разглежда като разкриване на информация между двама администратори — от работодател А на банка В.

Пример: Счетоводители

Работодател А също така наема счетоводна фирма С да извършва одити на счетоводството му и следователно предава данни за финансови операции (включително лични данни) на С. Счетоводна фирма С обработва тези данни без подробни указания от А. Счетоводна фирма С сама решава, в съответствие с правните разпоредби, уреждащи задачите, свързани с одиторските дейности, извършвани от С, събираните от нея данни да бъдат обработвани само за целите на одитирането на А и определя с какви данни трябва да разполага, кои категории лица трябва да бъдат регистрирани, колко дълго ще се съхраняват данните и какви технически средства трябва да се използват. При тези обстоятелства счетоводна фирма С трябва да се счита сама по себе си за администратор, когато извършва своите одиторски услуги за А. Това обаче може да бъде различно в зависимост от равнището на указания от А. В случай че законът не предвижда специфични задължения за счетоводната фирма и дружеството клиент предоставя много подробни указания относно обработването, счетоводната фирма действително би действала като обработващ лични данни. Възможно е разграничение между ситуация, в която обработването — в съответствие със законите, уреждащи тази професия — се извършва като част от основната дейност на счетоводната фирма и ситуация, в която обработването е по-ограничена, спомагателна задача, която се извършва като част от дейността на дружеството клиент.

Пример: Хостинг услуги

Работодател А наема хостинг услуга Н за съхранение на криптирани данни на сървърите на Н. Хостинг услугата не определя дали данните, които съхранява, са лични данни, нито обработва данните по друг начин, освен да ги съхранява на своите сървъри. Тъй като съхранението е пример за дейност по обработване на лични данни, хостинг услугата обработва лични данни от името на работодателя А и следователно е обработващ лични данни. Работодателят А трябва да предостави необходимите указания на Н и трябва да бъде сключено споразумение за обработване на данни съгласно член 28, съгласно което от Н се изисква да приложи технически и организационни мерки за сигурност. Н трябва да съдейства на А като гарантира, че са взети необходимите мерки за сигурност, и да уведоми А в случай на нарушение на сигурността на личните данни.

41. Въпреки че вземането на решения относно средствата от второстепенна важност може да бъде оставено на обработващия лични данни, администраторът все пак трябва да посочи, във връзка

с изискването за сигурност, някои елементи в споразумението за изпълнение, например указания за предприемане на всички мерки, изисквани съгласно член 32 от ОРЗД. Споразумението трябва също така да предвижда, че обработващият лични данни подпомага администратора при гарантирането на съответствие, например, с член 32. Във всички случаи администраторът продължава да носи отговорност за прилагането на подходящи технически и организационни мерки, за да гарантира и да бъде в състояние да докаже, че обработването се извършва в съответствие с регламента (член 24). За целта администраторът трябва да вземе предвид естеството, обхвата, същността и целите на обработването, както и рисковете за правата и свободите на физическите лица. Поради това администраторът трябва да бъде напълно осведомен относно използваните средства, за да може да вземе информирано решение по този аспект. За да може администраторът да докаже законосъобразността на обработването, е препоръчително да се документират като минимум необходимите технически и организационни мерки в договора или в друг правно обвързващ инструмент между администратора и обработващия лични данни.

Пример: Кол център

Дружество X решава да възложи на кол център част от своите услуги по обслужване на клиенти. Кол центърът получава данни за покупките на клиентите, които могат да бъдат идентифицирани, както и информация за контакт. За да управлява личните данни относно клиентите на дружество X, кол центърът използва свой собствен софтуер и ИТ инфраструктура. Дружество X подписва споразумение за изпълнение с доставчика на услугата „кол център“ в съответствие с член 28 от ОРЗД, след като установи, че техническите и организационните мерки за сигурност, предложени от кол центъра, са подходящи за съответните рискове и че кол центърът ще обработва личните данни само за целите на дружество X и в съответствие с неговите указания. Дружество X не предоставя никакви допълнителни указания на кол центъра по отношение на конкретния софтуер, който да бъде използван, нито подробни указания по отношение на специфичните мерки за сигурност, които да бъдат предприети. В този пример дружество X остава администратор въпреки факта, че кол центърът е определил някои средства за обработването, които са от второстепенна важност.

2.1.5 „Относно обработването на лични данни“

42. Целите и средствата, определени от администратора, трябва да са свързани с „обработването на лични данни“. В член 4, параграф 2 от ОРЗД се съдържа следното определение относно обработването на лични данни: *„означава всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни“*. В резултат на това понятието „администратор“ може да бъде свързано или с една операция по обработване или със съвкупност от операции. На практика, това може да означава, че администрирането, извършвано от конкретен правен субект, може да обхваща въпросното обработване в неговата цялост, но може да се ограничава и до определен етап на обработването.[16]

[16] Решение по дело *Fashion ID*, C-40/17, ECLI:EU:C:2019:629, точка 74: *„както посочва генералният адвокат [...-] физическо или юридическо лице може да отговаря като администратор по смисъла на член 2, буква г) от Директива 5/46, съвместно с други, само за операциите по обработване на лични данни, на които, съвместно с други, определя целите и средствата. От друга страна, [...] въпросното физическо или юридическо лице не може да отговаря като администратор по смисъла на тази разпоредба за предходните или последващите операции по веригата, на които не определя нито целите, нито средствата“*

43. На практика, обработването на лични данни, в което участват няколко участници, може да бъде разделено на няколко по-малки операции по обработване, за които всеки участник може да се счита, че определя самостоятелно целта и средствата. От друга страна, поредица или съвкупност от операции по обработване, в които участват няколко участници, може да се извършват и за една(и) и съща(и) цел(и), като в този случай е възможно в обработването да участват един или повече съвместни администратори. С други думи, възможно е на „микроравнище“ различните операции по обработване по веригата да изглеждат несвързани, тъй като всяка от тях може да има различна цел. Необходимо е обаче да се извърши повторна проверка дали на „микроравнище“ тези операции по обработване не следва да се считат за „съвкупност от операции“, които имат обща цел, като се използват съвместно определени средства.

44. Всеки, който реши да обработва данни, трябва да прецени дали това включва лични данни и ако е така, какви са задълженията съгласно ОРЗД. Даден участник ще се счита за „администратор“, дори ако неговата съзнателна цел не са самите лични данни или ако погрешно е преценил, че не обработва лични данни.

45. Не е необходимо администраторът действително да има достъп до обработваните данни[17]. Лице, което възлага на външни изпълнители дейност по обработване и по този начин оказва определящо влияние върху целта и средствата за обработването (от първостепенна важност) (напр. като адаптира параметрите на дадена услуга по такъв начин, че да оказва влияние върху това чии лични данни следва да се обработват), трябва да бъде считано за администратор, въпреки че никога няма да има действителен достъп до данните.

Пример: Пазарно проучване 1

Дружество ABC желае да разбере кои видове потребители е най-вероятно да се интересуват от неговите продукти и сключва договор с доставчик на услуги XYZ, за да получи съответната информация.

Дружество ABC дава указания на XYZ относно вида информация, от която се интересува, и предоставя списък с въпроси, които да бъдат зададени на участниците в пазарното проучване.

Дружество ABC получава само статистическа информация (напр. идентифициране на потребителските тенденции по региони) от XYZ и няма достъп до самите лични данни. Въпреки това решението обработването да се извърши е взето от дружество ABC, обработването се извършва за целите и дейността му и дружество ABC е предоставило на XYZ подробни указания относно това каква информация да събира. Следователно дружество ABC все пак трябва да се счита за администратор по отношение на обработването на лични данни, което се извършва с цел предоставяне на поисканата от него информация. XYZ може да обработва данните единствено за целите, определени от дружество ABC и съгласно неговите подробни указания, и следователно трябва да се счита за обработващ лични данни.

Пример: Пазарно проучване 2

Дружество ABC желае да разбере кои видове потребители е най-вероятно да се интересуват от неговите продукти. Доставчикът на услуги XYZ е агенция за проучване на пазара, която е събрала информация относно интересите на потребителите, използвайки различни въпросници, които се отнасят до широк набор от продукти и услуги. Доставчикът на услуги XYZ е събрал и

[17] Решение по дело *Wirtschaftsakademie*, C-201/16, ECLI:EU:C:2018:388, точка 38.

анализирал тези данни независимо, използвайки собствената си методика, без да е получил указания от дружество ABC. За да изпълни искането на дружество ABC, доставчикът на услуги XYZ ще генерира статистическа информация, но без да получава допълнителни указания относно това какви лични данни следва да се обработват или как да се обработват, за да се генерират тези статистически данни. В този пример доставчикът на услуги XYZ действа като единствен администратор, като обработва лични данни за целите на пазарното проучване, като определя средствата за това по автономен начин. Дружество ABC няма никаква конкретна роля или отговорност, произтичащи от правото в областта на защитата на данните, във връзка с тези дейности по обработване, тъй като дружество ABC получава анонимизирани статистически данни и не участва в определянето на целите и средствата за обработването.

3 ОПРЕДЕЛЕНИЕ ЗА „СЪВМЕСТНИ АДМИНИСТРАТОРИ“

3.1 Определение за „съвместни администратори“

46. Квалифицирането като съвместни администратори може да възникне, когато в обработването участва повече от един администратор.

47. Въпреки че понятието не е ново и вече съществува съгласно Директива 95/46/ЕО, в член 26 от ОРЗД се въвеждат специфични правила по отношение на съвместните администратори и се установява рамка за уреждане на техните отношения. Освен това Съдът на Европейския съюз (СЕС) в неотдавнашни решения внесе разяснения относно това определение и неговия обхват.[18]

48. Както е обяснено по-подробно в част II, точка 2, квалифицирането като „съвместни администратори“ ще има последствия главно по отношение на разпределението на задълженията за спазване на правилата за защита на данните, и по-специално — по отношение на правата на физическите лица.

49. С оглед на това, целта на следващата точка е да се предоставят насоки относно понятието „съвместни администратори“ в съответствие с ОРЗД и съдебната практика на Съда на ЕС, с цел да се помогне на правните субекти да установят случаите, в които може би действат като съвместни администратори и да прилагат определението на практика.

3.2 Наличие на съвместно администриране

3.2.1 Общи съображения

50. Определението за „администратор“ в член 4, параграф 7 от ОРЗД представлява отправната точка за определянето на „съвместното администриране“. Следователно съображенията в настоящата точка са пряко свързани със съображенията в точката относно понятието „администратор“ и ги

[18] Вж. по-специално *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein срещу Wirtschaftsakademie*, (C-210/16), *Tietosuojavaltuutettu срещу Jehovan todistajat — uskonnollinen yhdyskunta* (C-25/17), *Fashion ID GmbH & Co. KG срещу Verbraucherzentrale NRW eV* (C-40/17). Важно е да се отбележи, че макар тези решения да са постановени от Съда на ЕС във връзка с тълкуването на понятието „съвместни администратори“ съгласно Директива 95/46/ЕО, те запазват валидността си в контекста на ОРЗД, при условие че елементите за определяне на това понятие съгласно ОРЗД остават същите като в Директивата.

допълват. Оценката на съвместното администриране следва да отразява оценката на „отделното“ администриране, разгледана по-горе.

51. В член 26 от ОРЗД, който отразява определението в член 4, параграф 7 от ОРЗД, се предвижда, че *„[к]огато двама или повече администратори съвместно определят целите и средствата на обработването, те са съвместни администратори.“* В общи линии съвместно администриране по отношение на конкретна дейност по обработване е налице, когато различни страни определят *съвместно* целта и средствата за тази дейност по обработване. Поради това, за да се оцени дали е налице съвместно администриране, трябва да се провери дали решенията по отношение на определянето на целите и средствата, които характеризират администратора, се вземат от повече от една страна. „Съвместно“ трябва да се тълкува в значение на „заедно“ или „не самостоятелно“ в различни форми и комбинации, както е обяснено по-долу.

52. Оценката на съвместното администриране следва да се извършва въз основа на фактически, а не на формален анализ на действителното влияние върху целите и средствата за обработването. Всички съществуващи или предвидени договорености следва да бъдат проверявани спрямо фактическите обстоятелства, свързани с отношението между страните. Един чисто формален критерий не би бил достатъчен поради минимум две причини: в някои случаи формалното назначаване на съвместен администратор — предвидено например в закон или в договор — няма да бъде налице; в други случаи формалното назначаване може да не отразява действителността на договореностите, като ролята на администратор формално се възлага на правен субект, който всъщност не е в състояние да „определи“ целите и средствата за обработването.

53. Не всяко обработване, включващо няколко правни субекта, води до съвместно администриране. Общият критерий за наличието на съвместно администриране е **съвместното участие на два или повече правни субекта в определянето на целите и средствата за** обработването. По-конкретно, съвместното участие трябва да включва определянето на целите, от една страна, и определянето на средствата, от друга страна. Ако всеки от тези елементи се определя от всички участващи правни субекти, те следва да се считат за съвместни администратори на въпросното обработване.

3.2.2 Оценка на съвместното участие

54. Съвместното участие в определянето на целите и средствата предполага, че повече от един правен субект има решаващо влияние върху това дали и как се извършва обработването. На практика съвместното участие може да бъде под няколко различни форми. Например съвместното участие може да бъде под формата на **общо решение**, взето от два или повече правни субекта, или да произтича от **унифициране на решенията** на два или повече правни субекта по отношение на целите и средствата от първостепенна важност.

55. Съвместното участие чрез *общо решение* означава вземане на решения заедно и включва общо намерение в съответствие с най-общото разбиране на термина „съвместно“, посочен в член 26 от ОРЗД.

Положението, свързано със съвместно участие чрез *унифициране на решенията* произтича по-специално от съдебната практика на Съда на ЕС във връзка с понятието „съвместни администратори“. Може да се счита, че е налице уеднаквяване на решенията по отношение на целите и средствата, **ако те са взаимнодопълващи се и са необходими за извършването на обработването по такъв начин, че да имат осезаемо въздействие върху определянето на целите и средствата за обработването**. Следва да се изтъкне, че понятието „унифициране на

решенията“ трябва да се разглежда във връзка с целите и средствата за обработването, но не и с други аспекти на търговските отношения между страните[19]. Поради това важен критерий за установяването на възможността за взимане на унифицирани решенията е **дали обработването не би било възможно без участието на двете страни, в смисъл че обработването от всяка от страните е неделимо, т.е. неразривно свързано**. Случаят на съвместните администратори, действащи въз основа на унифициране на решенията, следва обаче да се разграничава от случая на обработващ лични данни, тъй като последният — докато участва в извършването на обработването — не обработва данните за свои собствени цели, а от името на администратора.

56. Фактът, че една от страните няма достъп до обработваните лични данни, не е достатъчен, за да се изключи съвместното администриране[20]. Например по делото *„Свидетели на Йехова“ (Jehovah’s Witnesses*), СЕС счита, че религиозната общност трябва да се счита за администратор, съвместно с нейните членове, участващи в проповедническа дейност, на обработването на лични данни, извършвано от тях в хода на проповедническата дейност „от врата на врата“[21]. СЕС счита, че не е било необходимо общността да има достъп до въпросните данни, или съдът да установи, че тази общност е дала на своите членове писмени насоки или указания относно обработването на данни[22]. Религиозната общност „Свидетели на Йехова“ е участвала в определянето на целите и средствата, като е организирала и координирала дейностите на своите членове, което е спомогнало за постигане на целта на общността[23]. Освен това религиозната общност „Свидетели на Йехова“ по принцип е наясно, че обработването на такива данни се извършва с цел разпространяване на вярата ѝ[24].

57. Важно е също така да се подчертае, както е пояснено от СЕС, че даден правен субект ще се счита за съвместен администратор с другия(ите) правен субект(и) само по отношение на онези операции, за които съвместно с други определя средствата и целите за едно и също обработване на данни, по-специално в случай на уеднаквяване на решенията. Ако един от тези правни субекти вземе самостоятелно решение по отношение на целите и средствата на операциите, които са предходни или последващи по веригата на обработване, този правен субект трябва да се счита за единствен администратор на тази предходна или последваща операция.[25]

58. Наличието на съвместна отговорност не се изразява непременно в равна отговорност на различните субекти за едно и също обработване на лични данни. Тъкмо обратното, СЕС пояснява, че тези правни субекти могат да участват на различни етапи от обработването и в различна степен, поради което конкретната отговорност на всеки от тях трябва да се преценява с оглед на всички релевантни обстоятелства по случая.

---

[19] Всъщност всички търговски договорености включват унифициране на решенията като част от процеса за постигане на споразумение.

[20] Решение по дело *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, точка 38.

[21] Решение по дело *„Свидетели на Йехова“ (Jehovah’s Witnesses*), C-25/17, ECLI:EU:C:2018:551, точка 75.

[22] Пак там.

[23] Пак там, точка 71.

[24] Пак там.

[25] Решение по дело *Fashion ID*, C-40/17, ECLI:EU:2018:1039, точка 74 *„От друга страна, и без да се засяга предвидената в това отношение от националното право гражданска отговорност, въпросното физическо или юридическо лице не може да отговаря като администратор по смисъла на тази разпоредба за предходните или последващите операции по веригата, на които не определя нито целите, нито средствата“.*

3.2.2.1 Съвместно определена(и) цел(и)

59. Съвместно администриране е налице, когато правните субекти, участващи в едно и също обработване, извършват обработването за съвместно определени цели. Такъв ще бъде случаят, ако участващите правни субекти обработват данните за едни и същи или общи цели.

60. Освен това, когато правните субекти нямат една и съща цел на обработването, с оглед на съдебната практика на СЕС, може също така да се установи съвместно администриране, когато участващите правни субекти преследват тясно свързани или допълващи се цели. Такъв може да бъде случаят например, когато е налице взаимна полза, произтичаща от една и съща операция по обработване, при условие че всеки от участващите правни субекти участва в определянето на целите и средствата за съответната операция по обработване. Понятието „взаимна полза“ обаче не е от решаващо значение и може единствено да бъде показателно. По дело *Fashion ID*, например, СЕС пояснява, че оператор на уебсайт участва в определянето на целите (и средствата) на обработването, като е интегрирал в своя уебсайт социална приставка, за да оптимизира рекламата на своите стоки, правейки ги по-видими в социалната мрежа. СЕС счита, че въпросните операции по обработване са извършени в икономическия интерес както на оператора на уебсайта, така и на доставчика на социалната приставка[26].

61. Също така, както отбелязва СЕС в решение по дело *Wirtschaftsakademie*, обработването на лични данни чрез водене на статистика на посетителите на фен страницата има за цел да позволи на Facebook да подобри системата си за реклама, която разпространява посредством своята мрежа, както и да позволи на администратора на фен страницата да получава статистически данни за целите на управлението на рекламата на собствената му дейност[27]. Всеки правен субект по това дело преследва свой собствен интерес, но и двете страни участват в определянето на целите (и средствата) за обработването на лични данни по отношение на посетителите на фен страницата[28].

62. В тази връзка е важно да се изтъкне, че самото наличие на взаимна изгода (например търговска), произтичаща от дейност по обработване, не води до съвместно администриране. Ако правният субект, участващ в обработването, не преследва своя(и) собствена(и) цел(и) във връзка с дейността по обработване, а само получава заплащане за предоставени услуги, той действа като обработващ лични данни, а не като съвместен администратор.

3.2.2.2 Съвместно определени средства

63. Съвместното администриране изисква също така два или повече правни субекта да са упражнили влияние по отношение на средствата за обработване. Това не означава, че за да бъде налице съвместно администриране, всеки участващ правен субект трябва във всички случаи да определи всички средства. Всъщност, както е пояснено от Съда на ЕС, различни правни субекти могат да участват на различни етапи от това обработване и в различна степен. Следователно, различните съвместни администратори могат да определят средствата за обработването в различна степен, в зависимост от действителните им възможности.

64. Възможно е също така някой от участващите правни субекти да осигури средствата за обработването и да ги предостави на разположението на други правни субекти за целите на дейностите по обработване на лични данни. Правният субект, който вземе решение да използва

[26] Решение по дело *Fashion ID,* C-40/17, ECLI:EU:2018:1039, точка 80.
[27] Решение по дело *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, точка 34.
[28] Решение по дело *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, точка 39.

тези средства, така че личните данни да могат да бъдат обработвани за конкретна цел, също участва в определянето на средствата за обработването.

65. Този сценарий може да възникне по-специално в случаите на платформи, стандартизирани инструменти или друга инфраструктура, които позволяват на страните да обработват едни и същи лични данни и които са настроени по определен начин от една от страните, за да бъдат използвани от други страни, които също могат да решат как да ги настройват[29]. Използването на вече съществуваща техническа система не изключва съвместно администриране, стига ползвателите на системата да могат да вземат решения относно обработването на лични данни, което трябва да се извърши.

66. Като пример за това в своето решение по дело *Wirtschaftsakademie* СЕС счита, че администраторът на фен страница, хоствана във Facebook, който определя параметрите въз основа на целевата си аудитория, както и целите за управлението и популяризирането на своите дейности, трябва да се счита за участващ в определянето на средствата за обработване на лични данни, свързани с посетителите на неговата фен страница.

67. Освен това изборът, направен от даден правен субект, да използва за свои собствени цели инструмент или друга система, разработени от друг правен субект и спомагащи обработването на лични данни, вероятно ще представлява съвместно решение относно средствата за това обработване от тези правни субекти. Това следва от решението по дело Fashion ID, по което СЕС заключава, че като интегрира в уебсайта си Facebook бутона „харесва ми“, предоставян на операторите на уебсайтове от Facebook, Fashion ID оказва решаващо влияние по отношение на операциите по събирането на лични данни на посетителите на този сайт и предаването им на Facebook и по този начин съвместно с Facebook е определило средствата за тази обработка[30].

68. Важно е да се подчертае, че **използването на обща система или инфраструктура за обработване на данни няма да доведе във всички случаи до квалифицирането на участващите страни като съвместни администратори,** по-специално, когато обработването, което извършват, е делимо и може да се извърши от едната страна без намесата на другата страна или в случаите, в които доставчикът е обработващ лични данни, при положение, че не е налице собствена цел (наличието на чисто търговска полза за участващите страни не е достатъчно основание за квалифициране като цел на обработването).

Пример: Туристическа агенция

Туристическа агенция изпраща лични данни на своите клиенти на авиокомпания и на хотелска верига, за да направи резервации за организирано туристическо пътуване с обща цена. Авиокомпанията и хотелът потвърждават наличието на местата и стаите, за които е направено запитването. Туристическата агенция издава документи за пътуване и ваучери за своите клиенти. Всеки от участниците обработва данните за извършване на своите собствени дейности, използвайки свои собствени средства. В този случай туристическата агенция, авиокомпанията и хотелът са трима различни администратори на данни, които обработват данните за свои собствени и отделни цели, и не е налице съвместно администриране.

[29] Доставчикът на системата може да бъде съвместен администратор, ако са изпълнени горепосочените критерии, т.е. ако доставчикът участва в определянето на целите и средствата. В противен случай доставчикът следва да се счита за обработващ лични данни.

[30] Решение по дело Fashion ID, C-40/17, ECLI:EU:2018:1039, точки 77—79.

След това туристическата агенция, хотелската верига и авиокомпанията решават да участват съвместно в създаването на обща интернет платформа за общата им цел — предоставяне на услуга, която включва организирани туристически пътувания с обща цена. Те се споразумяват относно средствата от първостепенна важност, които да бъдат използвани, например кои данни ще бъдат съхранявани, как ще бъдат разпределени и потвърдени резервациите и кой може да има достъп до съхраняваната информация. Освен това те решават да обменят данните на своите клиенти, за да осъществят съвместни маркетингови действия. В този случай туристическата агенция, авиокомпанията и хотелската верига съвместно определят защо и как се обработват личните данни на съответните им клиенти и следователно ще бъдат съвместни администратори по отношение на операциите по обработване, свързани с общата интернет платформа за резервации и със съвместните маркетингови действия. Всяка от тях обаче ще продължи да бъде единствен администратор по отношение на други дейности по обработване, извън рамките на общата интернет платформа.

Пример: Изследователски проект на институти

Няколко изследователски института решават да участват в конкретен съвместен изследователски проект и за тази цел да използват съществуващата платформа на един от участващите в проекта институти. За целите на съвместните изследвания всеки институт въвежда в платформата лични данни, с които вече разполага, като използва данните, предоставени от останалите чрез платформата, с цел извършване на изследванията. В този случай всички институти биват квалифицирани като съвместни администратори на обработването на лични данни, което се извършва чрез съхраняване и разкриване на информация от тази платформа, тъй като те заедно са взели решение относно целта на обработването и средствата, които да се използват (съществуващата платформа). Всеки от институтите обаче е отделен администратор за всяко друго обработване, което може да бъде извършено за техните съответни цели, извън платформата.

Пример: Маркетингова операция

Дружества A и B са пуснали на пазара продукт C, който се предлага в рамките на сътрудничеството на различни марки, и желаят да организират събитие за популяризирането му. За тази цел те решават да обменят данни от своите бази данни, съдържащи информация относно техни клиенти и потенциални клиенти, и въз основа на това да определят списъка с поканените на събитието. Те също така се споразумяват относно реда и условията за изпращане на поканите за събитието, начините за събиране на отзиви по време на мероприятието и последващите маркетингови действия. Дружества A и B могат да се считат за съвместни администратори за обработването на лични данни във връзка с организирането на събитието за популяризиране на продукт, тъй като, в този случай, те заедно вземат решение относно съвместно определената цел и средствата от първостепенна важност за обработването на данните.

Пример: Клинични изпитвания[31]

Доставчик на здравно обслужване (изследователят) и университет (спонсорът) вземат решение да започнат съвместно клинично изпитване с една и съща цел. Те си сътрудничат при изготвянето на протокола за проучването (т.е. цел, методика/план на проучването, данни, които трябва да бъдат събрани, критерии за изключване/включване на субекти на данни, повторно използване на бази данни (по целесъобразност) и т.н.). Те могат да се считат за съвместни администратори на това клинично изпитване, тъй като съвместно определят и съгласуват една и съща цел и средствата за обработването, които са от първостепенна важност. Събирането на лични данни от здравните досиета на пациентите за целите на научните изследвания трябва да се разграничава от съхраняването и използването на същите данни за целите на болничната помощ, по отношение на която доставчикът на здравни услуги остава администратор.

В случай че изследователят не участва в изготвянето на протокола (той просто приема вече изготвения от спонсора протокол) и протоколът се изготвя единствено от спонсора, изследователят следва да се счита за обработващ лични данни, а спонсорът — за администратор на това клинично изпитване.

Пример: Агенции за подбор на персонал

Дружество X помага на дружество Y да набира нови служители — с прочутата си услуга с добавена стойност „global matchz“. Дружество X търси подходящи кандидати както по автобиографиите, които дружество Y получава директно, така и сред кандидатите, които вече фигурират в собствената му база данни. Тази база данни е създадена и се управлява самостоятелно от дружество X. Това гарантира, че дружество X спомага за намирането на съответствия между предложенията за работа и лицата, които търсят работа, като по този начин увеличава приходите си. Въпреки че формално не са взели решение заедно, дружества X и Y участват съвместно в обработването, целящо намирането на подходящи кандидати, въз основа на унифициране на решенията: решението за създаване и управление на услугата „global matchz“ от страна на дружество X и решението на дружество Y да обогати базата данни с автобиографиите, които получава директно. Тези решения са взаимнодопълващи се, неделими и необходими за обработването за целите на намирането на подходящи кандидати. Поради това, в този конкретен случай, горепосочените дружества следва да се считат за съвместни администратори на това обработване. Дружество X обаче е единственият администратор на обработването, необходимо за управление на неговата база данни, а дружество Y е единственият администратор на обработването за целите на последващото наемане на работа, за своята собствена цел (организиране на интервюта, сключване на договори и управление на данни относно човешките ресурси).

Пример: Анализ на здравни данни

Дружество ABC, разработващо приложение за наблюдение на кръвното налягане, и дружество XYZ, което е доставчик на приложения за медицински специалисти, желаят да проучат как промените в кръвното налягане могат да помогнат за прогнозирането на някои заболявания.

[31] ЕКЗД планира да предостави допълнителни насоки във връзка с клиничните изпитвания в предстоящите си Насоки относно обработването на лични данни за медицински и научноизследователски цели.

Дружествата решават да създадат съвместен проект и да се свържат с болница DEF, която също да участва.

Личните данни, които ще бъдат обработвани в рамките на този проект, се състоят от лични данни, които дружество ABC, болница DEF и дружество XYZ обработват поотделно като отделни администратори. Решението за обработването на тези данни с цел оценка на промените в кръвното налягане се взема съвместно от тримата участници. Дружество ABC, болница DEF и дружество XYZ съвместно определят целите на обработването. Дружество XYZ поема инициативата да предложи средствата за обработването, които са от първостепенна важност. Както дружество ABC, така и болница DEF, одобряват тези средства от първостепенна важност, след като и те са участвали в разработването на някои от характеристиките на приложението, така че да могат да използват резултатите в достатъчна степен. По този начин трите организации се споразумяват да имат обща цел на обработването, а именно оценка на начина, по който промените в кръвното налягане могат да помогнат за прогнозирането на определени заболявания. След приключване на проучването дружество ABC, болница DEF и дружество XYZ могат да се възползват от оценката, като използват резултатите от нея в собствените си дейности. Поради всички тези причини те биват квалифицирани като съвместни администратори на това конкретно съвместно обработване.

Ако дружество XYZ просто е било помолено от другите две организации да извърши тази оценка, без да е имало каквато и да било цел и просто е обработвало данните от тяхно име, дружество XYZ би било квалифицирано като обработващ лични данни, дори и на него да е било поверено определянето на средствата от второстепенна важност.

3.2.3 Ситуации, при които не е налице съвместно администриране

69. Фактът, че има няколко участници в едно и също обработване, не означава, че те непременно действат като съвместни администратори на това обработване. Не всички видове партньорства, сътрудничество или съвместно използване предполагат квалифициране като съвместни администратори, тъй като за такова квалифициране се изисква анализ за всеки отделен случай на всяко обработване и на точната роля на всеки правен субект във всяко обработване. Случаите, посочени по-долу, предоставят неизчерпателни примери за ситуации, в които не е налице съвместно администриране.

70. Например, обменът на едни и същи данни или множество от данни между два правни субекта без съвместно определени цели или съвместно определени средства за обработването следва да се счита за предаване на данни между отделни администратори.

Пример: Предаване на данни на служители на данъчните органи

Дружество събира и обработва лични данни на своите служители с цел управление на заплатите, здравно осигуряване и т.н. Даден закон задължава дружеството да изпраща всички данни относно заплатите на данъчните органи, с цел засилване на данъчния контрол.

В този случай, въпреки че както дружеството, така и данъчните органи, обработват едни и същи данни относно заплатите, липсата на съвместно определени цели и средства по отношение на това обработване на данни ще доведе до квалифицирането на двата правни субекта като двама отделни администратори на данни.

71. Съвместното администриране може да бъде изключено и в ситуация, в която няколко правни субекта използват обща база данни или обща инфраструктура, ако всеки правен субект определя самостоятелно собствените си цели.

Пример: Маркетингови операции в група от дружества, използващи обща база данни:

Група дружества използват една и съща база данни за управлението на своите клиенти и потенциални клиенти. Тази база данни е обслужвана от сървърите на дружеството майка, което следователно е администратор на дружествата по отношение на съхранението на данните. Всеки правен субект в рамките на групата въвежда данните за собствените си клиенти и потенциални клиенти и обработва тези данни единствено за свои собствени цели. Освен това всеки правен субект решава самостоятелно относно достъпа, сроковете на съхраняване, коригирането или заличаването на данни за своите клиенти и потенциални клиенти. Те не могат да имат достъп до или да използват взаимно своите данни. Самият факт, че тези дружества използват обща база данни на групата, сам по себе си не предполага съвместно администриране. Следователно при тези обстоятелства всяко дружество е отделен администратор.

Пример: Независими администратори, когато използват споделена инфраструктура

Дружество XYZ обслужва база данни и я предоставя на разположението на други дружества, за да обработват и съхраняват лични данни на своите служители. Дружество XYZ е обработващ лични данни по отношение на обработването и съхранението на данни на служители на други дружества, тъй като тези операции се извършват от името и съгласно указанията на тези други фирми. Освен това тези други компании обработват данните без каквото и да е участие на дружество XYZ и за цели, които по никакъв начин не биват споделяни от дружество XYZ.

72. Също така може да има ситуации, в които различни участници обработват последователно едни и същи лични данни в рамките на поредица от операции, като всеки от тези участници има независима цел и средства, участвайки в тази поредица от операции. При липса на съвместно участие при определянето на целите и средствата за една и съща операция или верига от операции по обработване, съвместното администриране трябва да бъде изключено и различните участници трябва да се разглеждат като независими администратори, действащи по реда си.

Пример: Статистически анализ за целите на задача от обществен интерес

Публичният орган (орган А) има правната задача да извърши съответния анализ и да изготви статистика относно това какво е развитието на равнището на заетост в държавата. За тази цел много други публичноправни субекти са задължени по закон да разкриват конкретни данни пред орган А. Орган А решава да използва специална система за обработването на данните, включително за събирането им. Това означава също така, че другите правни субекти са задължени да използват системата, за да разкриват данни. В този случай, без да се засяга каквото и да било законово разпределение на ролите, Орган А ще бъде единственият администратор на обработването за целите на анализа и статистическите данни относно равнището на заетост, обработвани в рамките на системата, тъй като Орган А определя целта на обработването и е взел решение как ще бъде организирано то. Разбира се, останалите публични органи, в качеството им на администратори на техните собствени дейности по обработване, отговарят за гарантиране на точността на данните, които са обработили преди това и които след това разкриват на Орган А.

4 ОПРЕДЕЛЕНИЕ ЗА „ОБРАБОТВАЩ ЛИЧНИ ДАННИ“

73. Определението за „обработващ лични данни“ в член 4, параграф 8 е: физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора. Подобно на определението за администратор, определението за обработващ лични данни предвижда широк кръг от участници — те могат да бъдат *„физическо или юридическо лице, публичен орган, агенция или друга структура“*. Това означава, че по принцип няма ограничение по отношение на вида на участника, който може да поеме ролята на администратор. Този участник може да бъде организация, но може да бъде и физическо лице.

74. В ОРЗД се определят задължения, пряко приложими специално по отношение на обработващите лични данни, както е посочено по-подробно в част II, точка 1 от настоящите насоки. Обработващият лични данни може да бъде подведен под отговорност или да му бъде наложена глоба в случай на неизпълнение на такива задължения или ако действа извън правомерните инструкции на администратора или в противоречие с тях.

75. Обработването на лични данни може да включва множество обработващи лични данни. Например самият администратор може да избере да включи пряко множество обработващи лични данни, въвличайки различни обработващи на отделни етапи на обработването (множество обработващи лични данни). Администраторът може също така да реши да ангажира един обработващ лични данни, който на свой ред — с разрешението на администратора — наема един или повече други обработващи („обработващ(и) лични данни подизпълнител(и)“). Дейността по обработването, възложена на един обработващ лични данни, може да бъде ограничена до много специфична задача или цел, или може да бъде по-обща и всеобхватна.

76. Двете основни условия за квалифициране като обработващ лични данни са:

    а) да бъде *отделен правен субект* по отношение на администратора и

    б) да обработва лични данни *от името на администратора*.

77. *Отделен правен субект* означава, че администраторът решава да делегира всички или част от дейностите по обработване на външна организация. В рамките на група компании едно дружество може да бъде обработващ лични данни на друга фирма, действаща като администратор, тъй като и двете дружества са отделни правни субекти. От друга страна, даден отдел в рамките на едно юридическо лице не може да бъде обработващ лични данни на друг отдел в рамките на същия правен субект.

78. Ако администраторът реши сам да обработва данните, като използва собствените си ресурси в рамките на своята организация, например чрез собствен персонал, това не е ситуация, в която е налице обработващ лични данни. Служителите и другите лица, които действат под прякото ръководство на администратора, например временно наети служители, не трябва да се разглеждат като обработващи лични данни, тъй като те ще обработват лични данни като част от структурата на администратора. В съответствие с член 29 указанията на администратора са обвързващи и за тях.

79. Първо, за *обработването на лични данни от името на администратора* се изисква отделен правен субект да обработва лични данни в полза на администратора. В член 4, параграф 2 „обработването“ е определено като понятие, включващо широк набор от операции, вариращи от събиране, съхранение и консултиране до употреба, разпространяване или друг начин, по

който данните стават достъпни, както и унищожаване. Понятието „обработване“ е описано по-подробно в точка 2.1.5. по-горе.

80. Второ, обработването трябва да се извършва от името на администратор, но не под негово пряко ръководство или контрол. Извършването на действия „от името на“ означава да се обслужва интересът на друго лице и наподобява правното понятие „делегиране“. В случая с правото в областта на защитата на данните, обработващият лични данни трябва да изпълни указанията, дадени от администратора, най-малко по отношение на целта на обработването и съществените елементи от средствата. Законосъобразността на обработването съгласно член 6 и, ако е приложимо, член 9 от регламента ще произтича от дейността на администратора, като обработващият лични данни не трябва да обработва данните по друг начин, освен съгласно указанията на администратора. Указанията на администратора все пак могат да оставят известна свобода на преценката по отношение на това как най-добре да бъдат обслужвани интересите на администратора, което дава възможност на обработващия лични данни да избере най-подходящите технически и организационни средства[32].

81. Извършване на действия „от името на“ означава също, че обработващият лични данни не може да извършва обработване за своя(и) собствена(и) цел(и). Както е предвидено в член 28, параграф 10, обработващият обаче нарушава ОРЗД, в случай че излезе извън рамките на указанията на администратора и започне да определя собствените си цели и средства за обработването. Обработващият лични данни ще се счита за администратор по отношение на това обработване и може да подлежи на санкции, ако излезе извън инструкциите на администратора.

Пример: Доставчик на услуги, който се счита за обработващ лични данни, но действа като администратор

Доставчикът на услуги MarketinZ предоставя на различни дружества рекламни услуги и услуги, свързани с директен маркетинг. Дружество GoodProductZ сключва договор с MarketinZ, съгласно който MarketinZ предоставя търговска реклама на клиентите на GoodProductZ и се счита за обработващ лични данни. MarketinZ обаче решава да използва клиентската база данни на GoodProducts и за други цели, освен за реклама на GoodProducts, например за развиване на своята собствена дейност. Решението за добавяне на допълнителна цел към целта, за която са били предадени личните данни, превръща MarketinZ в администратор на данни за тази съвкупност от операции по обработване и тяхното обработване за тази цел би представлявало нарушение на ОРЗД.

82. ЕКЗД припомня, че не всеки доставчик на услуги, който обработва лични данни в хода на предоставяне на услуга, е „обработващ лични данни“ по смисъла на ОРЗД. Ролята на администратора не се основава на естеството на правния субект, който обработва данните, а на конкретните му дейности в определен случай. С други думи, един и същ правен субект може да действа едновременно като администратор за определени операции по обработването и като обработващ лични данни за други, а по отношение на квалифицирането като администратор или обработващ лични данни трябва да се извършва оценка за всяко конкретно обработване на данни. Естеството на услугата ще определи дали дейността по обработване представлява обработване на лични данни от името на администратора по смисъла на ОРЗД. На практика, когато предоставяната услуга не е специално насочена към обработването на лични данни или

[32] Вж. част I, под точка 2.1.4, в която е описана разликата между средствата от първостепенна важност и средствата от второстепенна важност.

когато това обработване не представлява ключов елемент от услугата, доставчикът на услуги може да бъде в състояние самостоятелно да определи целите и средствата на това обработване, което е необходимо за предоставянето на услугата. В тази ситуация доставчикът на услуги трябва да се разглежда като отделен администратор, а не като обработващ лични данни[33]. Извършването на анализ за всеки отделен случай обаче остава необходимо, за да се установи степента на влияние, която всеки правен субект действително оказва при определянето на целите и средствата за обработването.

Пример: Таксиметрова услуга

Доставчик на таксиметрови услуги предлага онлайн платформа, която дава възможност на дружествата да резервират такси за превоз на служители или гости до и от летището. Когато резервира такси, дружество АВС посочва името на служителя, който следва да бъде взет от летището, така че шофьорът да може да потвърди самоличността на служителя в момента на вземането му. В този случай доставчикът на таксиметрови услуги обработва личните данни на служителя като част от услугата, която предоставя на дружество АВС, но обработването само по себе си не е целта на услугата. Доставчикът на таксиметрови услуги е разработил платформата за онлайн резервации като част от развитието на собствената си стопанска дейност по предоставяне на транспортни услуги, без каквито и да било указания от дружество АВС. Освен това доставчикът на таксиметрови услуги самостоятелно определя категориите данни, които събира, и срока на тяхното съхраняване. Следователно доставчикът на таксиметрови услуги, от свое име, действа като администратор, независимо от факта, че обработването се извършва в резултат от искане за услуга, отправено от дружество АВС.

83. ЕКЗД отбелязва, че доставчик на услуги може все пак да действа като обработващ лични данни, дори ако обработването на лични данни не е главният или основният предмет на услугата, при условие че на практика клиентът на услугата определя целите и средствата за обработването. Когато преценяват дали да поверят обработването на лични данни на конкретен доставчик на услуги, администраторите следва внимателно да преценят дали въпросният доставчик на услуги им позволява да упражняват достатъчна степен на контрол, като вземат предвид естеството, обхвата, същността и целите на обработването, както и потенциалните рискове за субектите на данни.

Пример: Кол център

Дружество X възлага обслужването на своите клиенти на дружество Y, което предоставя кол център, за да оказва съдействие на клиентите на дружеството X по отношение на техните въпроси. За целите на услугата за обслужване на клиенти дружество Y трябва да има достъп до клиентските бази данни на дружество X. Дружество Y единствено може да осъществява достъп до данни, с цел да осигури обслужването, което дружество X трябва да предоставя на клиентите си, като не може да обработва данни за цели, различни от посочените от дружество X. Дружество Y следва да се счита за обработващ лични данни, като между дружеството X и дружеството Y трябва да бъде сключено споразумение за изпълнение.

[33] Вж. също съображение 81 от ОРЗД, в което изразът „когато на обработващия се възлагат дейности по обработването“ означава, че дейността по обработване по своята същност е важна част от решението на администратора да отправи искане към обработващия лични данни да обработва лични данни от негово име.

Пример: Обща ИТ поддръжка

Дружество Z наема доставчик на ИТ услуги, за да извършва обща поддръжка на информационните системи на дружеството, които съдържат огромно количество лични данни. Достъпът до лични данни не е основният предмет на услугата по поддръжка, но е неизбежно доставчикът на ИТ услуги систематично да има достъп до лични данни, когато извършва услугата. Поради това дружество Z заключава, че доставчикът на ИТ услуги, в качеството си на отделно дружество, от което неизбежно се изисква да обработва лични данни, въпреки че това не е основната цел на услугата, трябва да се счита за обработващ лични данни. Поради това с доставчика на ИТ услуги се сключва споразумение за изпълнение.

Пример: Консултант в областта на ИТ, отстраняващ софтуерен проблем

Дружество ABC наема ИТ специалист от друго дружество, за да отстрани проблем със софтуер, използван от дружеството. Консултантът в областта на ИТ не е нает да обработва лични данни, а дружество ABC определя, че всеки достъп до лични данни ще бъде от чисто инцидентен характер и следователно на практика ще бъде много ограничен. Поради това ABC заключава, че специалистът в областта на ИТ не е обработващ лични данни (нито администратор от свое име) и че дружество ABC ще предприеме подходящи мерки съгласно член 32 от ОРЗД, за да предотврати неразрешено обработване на лични данни от страна на консултанта в областта на ИТ.

84. Както е посочено по-горе, нищо не възпрепятства обработващия лични данни да предложи предварително определена услуга, но администраторът трябва да вземе окончателното решение по отношение на фактическото одобрение на начина, по който се извършва обработването, поне що се отнася до средствата за обработването, които са от първостепенна важност. Както е посочено по-горе, даден обработващ лични данни има свобода на действие по отношение на средствата от второстепенна важност, вж. по-горе в подточка 2.1.4.

Пример: Доставчик на услуги „в облак“

Дадена община е решила да използва доставчик на услуги „в облак“ за обработването на информация в областта на училищните и образователните услуги. Услугата „в облак“ предлага услуги за изпращане на съобщения, видеоконференции, съхранение на документи, управление на събития, текстообработка и т.н. и ще включва обработване на лични данни относно ученици и учители. Доставчикът на услуги „в облак“ е предложил стандартизирана услуга, която се предлага в световен мащаб. Общината обаче трябва да гарантира, че действащото споразумение е в съответствие с член 28, параграф 3 от ОРЗД — че личните данни, на които тя е администратор, се обработват единствено за целите на общината. Общината трябва също така да гарантира, че дадените от нея специфични указания относно сроковете на съхранение, заличаването на данни и т.н. се спазват от доставчика на услуги „в облак“, независимо от това какво обикновено се предлага като част от стандартизираната услуга.

5 ОПРЕДЕЛЕНИЕ ЗА „ТРЕТА СТРАНА/ПОЛУЧАТЕЛ“

85. Регламентът определя не само понятията „администратор“ и „обработващ лични данни“, но и понятията „получател“ и „трета страна“. За разлика от понятията „администратор“ и „обработващ лични данни“, регламентът не определя специфични задължения или отговорности за получателите и третите страни. Може да се каже, че това са относителни понятия

в смисъл, че описват отношение с администратор или с обработващ лични данни от определена гледна точка, например администратор или обработващ лични данни разкрива данни пред получател. Всеки получател на лични данни, както и всяка трета страна, може едновременно да бъдат считани за администратор или за обработващ лични данни, от други гледни точки. Например правните субекти, които трябва да се разглеждат като получатели или трети страни от една гледна точка, са администратори на обработването, по отношение на което те определят целта и средствата.

Трета страна

86. Член 4, параграф 10 определя *„трета страна“* като физическо или юридическо лице, публичен орган, агенция или друг орган, различен от:

- субекта на данни,
- администратора,
- обработващия лични данни и
- лицата, които под прякото ръководство на администратора или на обработващия лични данни имат право да обработват личните данни.

87. Като цяло определението съответства на предишното определение за *„трета страна“* в Директива 95/46/ЕО.

88. Въпреки че Регламентът съдържа определение за термините *„лични данни“*, *„субект на данни“*, *„администратор“* и *„обработващ лични данни“*, в него не се съдържа определение за понятието *„лица, които под прякото ръководство на администратора или на обработващия лични данни имат право да обработват личните данни“*. Това понятие обаче обикновено се разбира като отнасящо се до лица, които са част от юридическото лице на администратора или обработващия лични данни (служител или длъжност, сравнима до голяма степен с тази на служителите, напр. временно наети служители, осигурени от агенция за временна заетост), но само доколкото те са оправомощени да обработват лични данни. Служител и т.н., който получава достъп до данни, за които няма разрешение за достъп, и за цели, различни от тези на работодателя, не попада в тази категория. Вместо това този служител следва да се счита за трета страна по отношение на обработването, предприето от работодателя. Доколкото служителят обработва лични данни за свои собствени цели, различни от тези на своя работодател, той/тя ще се счита за администратор и ще поеме всички произтичащи от това последствия и отговорности по отношение на обработването на лични данни[34].

89. Следователно „трета страна“ се отнася за лице, което в конкретната ситуация не е субект на данни, администратор, обработващ лични данни или служител. Например, администраторът може да наеме обработващ лични данни и да му даде указания да предава лични данни на трета страна. В такъв случай тази трета страна ще се счита за администратор на обработването, което извършва за свои собствени цели. Следва да се отбележи, че в рамките на група дружества, дружество, което не е администратор или обработващ лични данни, е трета страна, въпреки че принадлежи към същата група като фирмата, която действа като администратор или обработващ лични данни.

[34] Въпреки това работодателят (като първоначален администратор) може да запази известна отговорност, в случай че новото обработване се извършва поради липса на подходящи мерки за сигурност.

Пример: Услуги по почистване

Дружество А сключва договор с доставчик на услуги по почистване, за да почиства офисите на дружеството. Не се очаква почистващият персонал да има достъп до лични данни или по друг начин да обработва лични данни. Въпреки че понякога е възможно тези служители да се натъкнат на такива данни, докато извършват дейността си в офиса, те могат да изпълняват задачите си без достъп до данни и им е забранено, по силата на договор, да осъществяват достъп или да обработват по друг начин лични данни, които дружество А съхранява като администратор. Почистващият персонал не са служители на дружество А, нито пък бива считан за намиращ се под прякото ръководство на това дружество. Не е налице намерение доставчикът на услуги по почистване или неговите служители да бъдат ангажирани да обработват лични данни от името на дружество А. Следователно доставчикът на услуги по почистване и неговите служители трябва да се считат за трета страна и администраторът трябва да гарантира, че са въведени подходящи мерки за сигурност, за да се предотврати достъпът им до данни и да се установи задължение за спазване на поверителност, в случай че почистващият персонал инцидентно се натъкне на лични данни.

Пример: Групи от дружества — компания майка и дъщерни фирми

Фирмите X и Y са част от група Z. Фирмите X и Y обработват данни за съответните си служители за целите на управлението на служителите. В един момент компанията майка ZZ решава да поиска данни за служителите от всички дъщерни фирми, за да изготви статистика за цялата група. При предаването на данни от дружества X и Y на компанията ZZ, тя следва да се счита за трета страна, независимо от факта, че всички дружества са част от една и съща група. Дружеството ZZ ще се счита за администратор на обработването на данните за статистически цели.

Получател

90. Определението за *„получател“* в член 4, параграф 9 е физическо или юридическо лице, публичен орган, агенция или друга структура, пред която се разкриват личните данни, независимо дали е трета страна или не. Когато получават лични данни в рамките на конкретно разследване, в съответствие с правото на Съюза или правото на държава членка, обаче публичните органи не трябва да се разглеждат като „получатели“ (напр. данъчни и митнически органи, звена за финансово разследване и т.н.)[35].

91. Като цяло определението съответства на предишното определение за *„получател“* в Директива 95/46/ЕО.

92. Определението обхваща всяко лице, което получава лични данни, независимо дали е трета страна или не. Например, когато администратор изпраща лични данни на друг правен субект, който е обработващ лични данни или трета страна, този правен субект е получател. Третата страна — получател се счита за администратор на всяко обработване, което извършва за своя(и) собствена(и) цел(и), след като получи данните.

[35] Вж. също съображение 31 от ОРЗД.

Пример: Разкриване на данни между дружества

Пътническата агенция ExploreMore организира пътувания по искане на отделни свои клиенти. В рамките на тази услуга те изпращат личните данни на клиентите на авиокомпании, хотели и организатори на екскурзии, за да могат те съответно да предоставят своите услуги. ExploreMore, хотелите, авиокомпаниите и организаторите на екскурзии трябва да се считат за администратори на обработването, което извършват в рамките на своите услуги. Не е налице никакво отношение между администратора и обработващия лични данни. Авиокомпаниите, хотелите и организаторите на екскурзии обаче трябва да се считат за получатели при получаване на личните данни от ExploreMore.

ЧАСТ II – ПОСЛЕДСТВИЯ ОТ ОПРЕДЕЛЯНЕТО НА РАЗЛИЧНИ РОЛИ

1 ОТНОШЕНИЕ МЕЖДУ АДМИНИСТРАТОР И ОБРАБОТВАЩ ЛИЧНИ ДАННИ

93. Отличителна нова характеристика на ОРЗД са разпоредбите, които пряко налагат задължения на обработващите лични данни. Например всеки обработващ лични данни трябва да гарантира, че лицата, оправомощени да обработват личните данни, са поели ангажимент за поверителност (член 28, параграф 3); всеки обработващ лични данни трябва да поддържа регистър на всички категории дейности по обработването (член 30, параграф 2) и трябва да прилага подходящи технически и организационни мерки (член 32). Обработващият лични данни трябва също така да определи длъжностно лице по защита на данните при определени условия (член 37) и е задължен да уведоми администратора без ненужно забавяне, след като узнае за нарушение на сигурността на личните данни (член 33, параграф 2). Освен това правилата относно предаването на данни на трети държави (глава V) се прилагат както по отношение на обработващите лични данни, така и по отношение на администраторите. В тази връзка ЕКЗД счита, че при регламентиране на конкретно съдържание на необходимия договор между администратора и обработващия лични данни, член 28, параграф 3 от ОРЗД налага преки задължения на обработващите лични данни, включително задължението да подпомагат администратора, за да се гарантира изпълнението на задълженията[36].

1.1 Избор на обработващ лични данни

94. Администраторът е **длъжен да „използва само обработващи лични данни, които предоставят достатъчни гаранции** за прилагането на подходящи технически и организационни мерки“, по такъв начин, че обработването да протича в съответствие с изискванията на ОРЗД, включително за сигурността на обработването, и да осигурява защита на правата на субектите на данни[37]. Поради това администраторът носи отговорност за това да прецени дали гаранциите,

[36] Например, при необходимост и при поискване, обработващият лични данни следва да подпомага администратора, за да се гарантира изпълнението на задълженията, свързани с извършването на оценки на въздействието върху защитата на личните данни (съображение 95 от ОРЗД). Това трябва да бъде отразено в договора между администратора и обработващия лични данни, съгласно член 28, параграф 3, буква е) от ОРЗД.

[37] Член 28, параграф 1 и съображение 81 от ОРЗД.

предоставени от обработващия лични данни, са достатъчни и следва да може да докаже, че е взел сериозно предвид всички елементи, предвидени в ОРЗД.

95. Гаранциите, „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. Често това налага обмен на съответната документация (напр. 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 сертификати по стандарт от серията ISO 27000).

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.

97. Администраторът следва да вземе предвид следните елементи[38], за да оцени дали гаранциите са достатъчни: **експертните познания** на обработващия лични данни (напр. технически експертен опит по отношение на мерките за сигурност и нарушенията на сигурността на данните); **надеждността** на обработващия лични данни; **ресурсите** на обработващия лични данни. Репутацията на обработващия лични данни на пазара също може да бъде важен фактор, който администраторите да вземат предвид.

98. Освен това придържането към одобрен кодекс за поведение или механизъм за сертифициране може да се използва като елемент за доказване на достатъчно гаранции[39]. Поради това на обработващите лични данни се препоръчва да уведомят администратора за това обстоятелство, както и за всяка промяна в придържането към тях.

99. Задължението да се използват само обработващи лични данни, „които предоставят достатъчни гаранции“, съдържащо се в член 28, параграф 1 от ОРЗД, е постоянно задължение. То не приключва в момента, в който администраторът и обработващият лични данни сключат договор или друг правен акт. По-скоро администраторът следва, на подходящи интервали от време, да проверява гаранциите на обработващия лични данни, включително чрез одити и проверки, когато това е целесъобразно[40].

1.2 Форма на договора или на друг правен акт

100. Всяко обработване на лични данни от обработващ лични данни трябва да се урежда с договор или друг правен акт съгласно правото на ЕС или правото на държава членка, между администратора и обработващия лични данни, във връзка с изискванията в член 28, параграф 3 от ОРЗД.

[38] Съображение 81 от ОРЗД.
[39] Член 28, параграф 5 и съображение 81 от ОРЗД.
[40] Вж. също член 28, параграф 3, буква з) от ОРЗД.

101. Този правен акт трябва да бъде **в писмена форма, включително в електронен формат**[41]. Поради това споразуменията, които не са в писмена форма (независимо колко изчерпателни или ефективни са те), не могат да се считат за достатъчни за изпълнението на изискванията, определени в член 28 от ОРЗД. За да се избегнат всякакви трудности при доказването на това, че договорът или другият правен акт действително е в сила, ЕКЗД препоръчва да се гарантира, че необходимите подписи фигурират в правния акт в съответствие с приложимото право (напр. договорно право).

102. Освен това договорът или другият правен акт съгласно правото на Съюза или правото на държава членка трябва да бъде **обвързващ за обработващия лични данни** по отношение на администратора, т.е. той трябва да установява задължения за обработващия лични данни, които са обвързващи съгласно правото на ЕС или правото на държава членка. Договорът трябва също така да определя задълженията на администратора. В повечето случаи се касае за договор, но регламентът се позовава и на „друг правен акт“, например национално право (първично или вторично) или друг законодателен акт. Ако правният акт не включва цялото минимално изисквано съдържание, той трябва да бъде допълнен с договор или друг правен акт, включващ липсващите елементи.

103. Тъй като регламентът установява ясно задължение за сключване на писмен договор, когато не е в сила друг съответен правен акт, липсата на такъв договор е нарушение на ОРЗД[42]. Както администраторът, така и обработващият лични данни, носят отговорност за това да се гарантира наличието на договор или друг правен акт, уреждащ обработването[43]. Съгласно разпоредбите на член 83 от ОРЗД компетентният надзорен орган може да наложи административно наказание „глоба“ както на администратора, така и на обработващия лични данни, като взема предвид обстоятелствата във всеки отделен случай. Договорите, сключени преди датата на прилагане на ОРЗД, е трябвало да бъдат актуализирани с оглед на член 28, параграф 3. Неактуализирането на такива съществуващи договори, с цел привеждането им в съответствие с изискванията на ОРЗД, представлява нарушение на член 28, параграф 3.

Писмен договор съгласно член 28, параграф 3 от ОРЗД може да бъде интегриран в договор с по-голям обхват, например споразумение за нивото на обслужване. За да се улесни доказването на съответствието с ОРЗД, ЕКЗД препоръчва елементите на договора, целящи привеждането в действие на член 28 от ОРЗД, да бъдат ясно определени като такива, на едно място (например в приложение).

[41] Член 28, параграф 9 от ОРЗД.

[42] Наличието (или липсата) на писмено споразумение обаче не е от решаващо значение за това дали съществува отношение между администратор и обработващ лични данни. Когато има основание да се счита, че договорът не съответства на действителността, що се касае до действителното извършване на администриране, основаващо се на фактически анализ на обстоятелствата във връзка с отношенията между страните и извършваното обработване на лични данни, споразумението може да бъде отменено. Обратно, при липса на писмено споразумение за обработване пак може да се счита, че съществува отношение между администратор и обработващ лични данни. Това обаче би означавало нарушение на член 28, параграф 3 от ОРЗД. Освен това при определени обстоятелства липсата на ясно определяне на отношенията между администратора и обработващия лични данни може да постави проблема за липсата на правно основание, на което следва да се основава всяко обработване, например по отношение на предаването на данни между администратора и предполагаемия обработващ лични данни.

[43] Член 28, параграф 3 е приложим не само по отношение на администраторите. В случаите, в които само обработващият лични данни попада в териториалния обхват на ОРЗД, задължението е пряко приложимо само по отношение на обработващия лични данни, вж. също Насоки № 3/2018 на ЕКЗД относно териториалния обхват на ОРЗД, стр. 12.

104. За да изпълнят задължението за сключване на договор, **администраторът и обработващият лични данни могат да изберат да сключат свой собствен договор**, включващ всички задължителни елементи, **или да се основават изцяло или отчасти на стандартни договорни клаузи във връзка със задълженията по член 28**[44].

105. Като алтернативна възможност Комисията или надзорният орган може да приеме редица стандартни договорни клаузи (СДК)[45] в съответствие с механизма за съгласуваност[46]. Тези клаузи могат да бъдат част от сертифициране, предоставено на администратора или обработващия лични данни съгласно членове 42 и 43.[47]

106. ЕКЗД би желал да поясни, че администраторите и обработващите лични данни не са задължени да сключат договор, основаващ се на СДК, нито непременно да предпочетат такъв договор пред това да договарят индивидуален договор. И двете възможности са приложими за целите на спазването на правото в областта на защитата на данните, в зависимост от конкретните обстоятелства, при условие че отговарят на изискванията на член 28, параграф 3.

107. Ако страните желаят да се възползват от стандартни договорни клаузи, клаузите за защита на данните в тяхното споразумение трябва да бъдат същите като СДК. В СДК често се оставят празни полета, които трябва да бъдат попълнени, или опции, които да бъдат избрани от страните. Също така, както е посочено и по-горе, СДК по принцип ще бъдат интегрирани в споразумение с по-голям обхват, в което се описват предметът на договора, финансовите му условия и други договорени клаузи: страните ще могат да добавят допълнителни клаузи (напр. приложимо право и юрисдикция), при условие че те не противоречат пряко или косвено на СДК[48] и не засягат защитата, предвидена в ОРЗД и в правото в областта на защитата на данните на Съюза или на държава членка.

---

[44] Член 28, параграф 6 от ОРЗД. ЕКЗД припомня, че стандартните договорни клаузи за целите на спазването на член 28 от ОРЗД не са същите като стандартните договорни клаузи, посочени в член 46, параграф 2. Докато в първия допълнително се определя и пояснява как ще бъдат изпълнени разпоредбите на член 28, параграфи 3 и 4, вторият предвижда подходящи гаранции в случай на предаване на лични данни на трета държава или международна организация, при липса на решение относно адекватното ниво на защита съгласно член 45, параграф 3.

[45] Член 28, параграф 7 от ОРЗД. Член 28, параграф 7 от ОРЗД. Член 28, параграф 7 от ОРЗД. Член 28, параграф 7 от ОРЗД. Вж. Съвместно становище 1/2021 на ЕКЗД и ЕНОЗД относно стандартните договорни клаузи между администратори на лични данни и обработващи лични данни: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-12021-standard_bg.

[46] Член 28, параграф 8 от ОРЗД. Регистърът на решенията, взети от надзорните органи и съдилищата по въпроси, разглеждани в рамките на механизма за съгласуваност, включително стандартни договорни клаузи за целите на спазването на член 28 от ОРЗД, е достъпен тук: https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-decisions_bg.

[47] Член 28, параграф 6 от ОРЗД.

[48] ЕКЗД припомня, че същата степен на гъвкавост се допуска, когато страните решат да използват СДК като подходяща гаранция за предаване на данни на трети държави съгласно член 46, параграф 2, буква в) или член 46, параграф 2, буква г) от ОРЗД. В съображение 109 от ОРЗД се пояснява, че *„[в]ъзможността администраторът или обработващият лични данни да използва стандартни клаузи за защита на данните, приети от Комисията или от надзорен орган, не следва да възпрепятства администраторите или обработващите лични данни да включат стандартни клаузи за защита на данните в договор с по-голям обхват, като договор между обработващия лични данни и друг обработващ лични данни, нито да добавят други клаузи или допълнителни гаранции, при условие че същите не противоречат пряко или косвено на стандартните договорни клаузи [...], нито засягат основните права или свободи на субектите на данни. Администраторите и обработващите лични данни следва да бъдат насърчавани да предоставят допълнителни гаранции чрез договорни ангажименти, които допълват стандартните клаузи за защита.“*

108. Договорите между администраторите и обработващите лични данни понякога могат да бъдат изготвяни едностранно — от една от страните. Това коя страна или страни изготвя(т) договора може да зависи от няколко фактора, включително: позицията на страните на пазара и договорното им правомощие, техния технически експертен опит, както и достъпа им до правни услуги. Например някои доставчици на услуги са склонни да определят стандартни условия, които включват споразумения за обработване на данни.

109. Споразумението между администратора и обработващия лични данни трябва да отговаря на изискванията на член 28 от ОРЗД, за да се гарантира, че обработващият 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 включени във всеки договор, уреждащ отношенията между администраторите и обработващите, той оставя възможност за преговори между страните по такива договори. В някои ситуации администраторът или обработващият лични данни може да е в по-слаба преговорна позиция, при изготвянето на персоналните клаузи в споразумението за защита на данните. Използването на стандартни договорни клаузи, приети съгласно член 28 (параграфи 7 и 8), може да допринесе за възстановяването на баланса в преговорните позиции и за това да се гарантира, че договорите са в съответствие с ОРЗД.

110. Фактът, че договорът и подробните търговски условия, които се предвиждат в него, се изготвят от доставчика на услуги, а не от администратора, сам по себе си не е проблематичен и не е достатъчно основание да се заключи, че доставчикът на услуги следва да се счита за администратор. Също така диспропорцията по отношение на договорните правомощия на един малък администратор на данни спрямо големите доставчици на услуги не следва да се счита за обосновка, въз основа, на която администраторът да приема клаузи и договорни условия, които не са в съответствие с правото в областта на защитата на данните, нито може да освободи администратора от неговите задължения за защита на данните. Администраторът трябва да прецени условията и ако свободно ги приема и се възползва от услугата, той също така поема пълна отговорност за спазването на ОРЗД. Всяко предложение от страна на обработващ лични данни за изменение на споразумения за обработване на данни, включени в стандартните условия, следва да бъде съобщено пряко на администратора и одобрено от него, като се има предвид степента на свобода на действие, с която разполага обработващият лични данни по отношение на елементи от второстепенна важност на средствата (вж. точките 40-41 по-горе). Публикуването на тези изменения на уебсайта на обработващия лични данни само по себе си не представлява спазване на член 28.

1.3 Съдържание на договора или на друг правен акт

111. Преди да се съсредоточим върху всяко едно от подробните изисквания, определени в ОРЗД по отношение на съдържанието на договора или на друг правен акт, са необходими някои общи бележки.

112. Въпреки че елементите, определени в член 28 от Регламента, съставляват основното съдържание на договора, договорът следва да бъде средство, чрез което администраторът и обработващият лични данни с подробни указания допълнително да изяснят как ще бъдат прилагани тези основни елементи. Въпреки това **в споразумението за обработване не следва просто да бъдат повторени разпоредбите на ОРЗД**: по-скоро то следва да включва по-конкретна специфична информация относно това как ще бъдат изпълнени изискванията и какво равнище на сигурност е необходимо за обработването на лични данни, което е предметът на споразумението за обработване. Преговорите и условията на договора далеч не са просто

формалност, а дават възможност да се уточнят подробностите относно обработването[49]. Всъщност „защитата на правата и свободите на субектите на данни, както и отговорността и задълженията на администраторите и обработващите лични данни, [...] изискват ясно определяне на отговорностите“ съгласно ОРЗД[50].

113. Същевременно, в договора следва да се **вземат предвид *„конкретните задачи и отговорности на обработващия лични данни в контекста на обработването, което следва да се извърши, както и рискът за правата и свободите на субекта на данни“***[51]. Най-общо казано, договорът между страните следва да бъде изготвен с оглед на конкретната дейност по обработване на данни. Например, не е необходимо да се прилагат особено строги защити и процедури по отношение на обработващ лични данни, на когото е възложена дейност по обработване, от която произтичат само незначителни рискове: въпреки че всеки обработващ трябва да отговаря на изискванията, определени в Регламента, мерките и процедурите следва да бъдат съобразени с конкретната ситуация. Във всички случаи всички елементи на член 28, параграф 3 трябва да бъдат включени в договора. Същевременно договорът следва да включва и някои елементи, които могат да помогнат на обработващия лични данни да разбере рисковете за правата и свободите на субектите на данни, произтичащи от обработването: тъй като дейността се извършва от името на администратора, често администраторът има по-задълбочено разбиране по отношение на рисковете, които включва обработването, тъй като той е наясно с обстоятелствата, които са свързани с обработването.

114. Що се касае до **изискваното съдържание** на договора или на друг правен акт, според начина, по който ЕКЗД тълкува член 28, параграф 3, съдържанието трябва да предвижда:

- **предмета** на обработването (например записи от видеонаблюдение на лица, влизащи в и напускащи съоръжение с високо равнище на сигурност). Въпреки че предметът на обработването е широко понятие, то трябва да бъде формулирано, като се използват достатъчно конкретни характеристики, така че да бъде ясно какъв е основният предмет на обработването;

- **продължителността**[52] на обработването: следва да бъде определен точният период от време или да бъдат посочени критериите, използвани за неговото определяне; например може да се упомене срокът на действие на споразумението за обработване;

- **естеството** на обработването: вида на операциите, извършвани като част от обработването (например: „заснемане“, „записване“, „архивиране на изображения“, ...) **и целта** на обработването (например: установяване на незаконно влизане). Това описание следва да бъде възможно най-изчерпателно, в зависимост от конкретната дейност по обработване, за да се даде възможност на външни страни (напр. надзорни органи) да разберат съдържанието и рисковете, свързани с обработването, възложено на обработващия лични данни.

- **вида лични данни**: следва да бъде уточнен възможно най-подробно (например: видеоизображения на физически лица при влизане и излизане от съоръжението). Не би

[49] Вж. също Становище 14/2019 на ЕКЗД относно проекта на стандартни договорни клаузи, внесен от датския надзорен орган (член 28, параграф 8 от ОРЗД), стр. 5.
[50] Съображение 79 от ОРЗД.
[51] Съображение 81 от ОРЗД.
[52] Продължителността на обработването не съвпада непременно със срока на действие на споразумението (може да има правни задължения за запазване на данните за по-дълъг или по-кратък срок).

било достатъчно единствено да се уточни, че това са „лични данни съгласно член 4, параграф 1 от ОРЗД“ или „специални категории лични данни съгласно член 9“. В случай на специални категории данни, в договора или в правния акт следва като минимум да се определи за кои видове данни става въпрос, например „информация относно здравните досиета“ или „информация дали субектът на данни е член на профсъюз“;

- **категориите субекти на данни**: те също следва да бъдат определени по доста конкретен начин (например: „посетители“, „служители“, куриерски услуги и др.);

- **задълженията и правата на администратора**: правата на администратора са разгледани допълнително в следващите точки (напр. по отношение на правото на администратора да извършва проверки и одити). Що се отнася до задълженията на администратора, примерите включват задължението на администратора да предоставя на обработващия данните, посочени в договора, да предоставя и документира всички указания, свързани с обработването на данни, извършвано от обработващия лични данни, да гарантира преди и по време на обработването изпълнението на задълженията, определени в ОРЗД, от страна на обработващия, да упражнява надзор върху обработването, включително чрез извършване на одити и проверки на обработващия .

115. Въпреки че в ОРЗД са изброени елементи, които винаги трябва да бъдат включени в споразумението, може да е необходимо да бъде включена друга релевантна информация, в зависимост от съдържанието и рисковете, свързани с обработването, както и всяко допълнително изискване, което е приложимо.

1.3.1 Обработващият лични данни трябва да обработва данни само по документирано нареждане на администратора (член 28, параграф 3, буква а) от ОРЗД)

116. Необходимостта от уточняване на това задължение произтича от факта, че обработващият лични данни обработва данни от името на администратора. Администраторите трябва да предоставят на своите обработващи указания, свързани с всяка дейност по обработването. Тези инструкции могат да включват допустимо и недопустимо обработване на лични данни, по-подробни процедури, начини за гарантиране на сигурността на данните и т.н. Обработващият лични данни не трябва да излиза извън указанията, дадени от администратора. Възможно е обаче обработващият да предложи елементи, които, ако бъдат приети от администратора, да станат част от дадените указания.

117. Когато обработващ лични данни обработва данни извън инструкциите на администратора посредством решение, с което се определят целите и средствата за обработването, обработващият ще бъде в нарушение на своите задължения и дори ще се счита за администратор по отношение на това обработване в съответствие с член 28, параграф 10 (вж. подточка 1.5 по-долу[53]).

118. Указанията, дадени от администратора, трябва да бъдат **документирани**. За тази цел се препоръчва, в приложение към договора или към друг правен акт, да бъдат включени процедура и образец за даване на допълнителни инструкции. Като алтернативна възможност указанията могат да бъдат предоставени във всякаква писмена форма (напр. електронна поща), както и във всякаква друга документална форма, стига да е възможно документирането на тези инструкции.

[53] Вж. част II, подточка 1.5 („Обработващ лични данни, определящ целите и средствата за обработването“).

Във всички случаи, за да се избегнат трудности при доказването на надлежното документиране на указанията на администратора, ЕКЗД препоръчва тези инструкции да се съхраняват заедно с договора или с другия правен акт.

119. Задължението на обработващия лични данни да се въздържа от всякаква дейност по обработване, която не се основава на указанията на администратора, се прилага и по отношение на **предаването** на лични данни на трета държава или международна организация. В договора следва да се определят изискванията по отношение на предаването на данни на трети държави или международни организации, като се вземат предвид разпоредбите на глава V от ОРЗД.

120. ЕКЗД препоръчва администраторът да обърне необходимото внимание на тази конкретна точка, особено когато обработващият лични данни ще делегира някои дейности по обработване на други обработващи и когато обработващият има подразделения или звена, намиращи се в трети държави. Ако указанията на администратора не дават възможност за предаване или разкриване на данни на трети държави, обработващият лични данни няма да има право да възлага обработването на данни на подизпълнител в трета държава, който да действа като обработващ лични данни, нито ще има право да възлага обработването на данните на някое от своите подразделения извън ЕС.

121. Обработващият лични данни може да обработва данни, различни от тези, определени в документираните указания на администратора, **когато обработващият лични данни е длъжен да обработва и/или предава лични данни по силата на правото на ЕС или правото на държава членка, което се прилага спрямо обработващия лични данни.** Освен това тази разпоредба разкрива важността на внимателното договаряне и изготвяне на споразумения за обработване на данни, тъй като, например, може да се наложи да се потърси правен съвет от една от страните във връзка със съществуването на такова правно изискване. Това трябва да се извърши своевременно, тъй като обработващият лични данни е задължен да информира администратора за това изискване, преди да започне обработването. Само когато същото право (на ЕС или на държава членка) забранява на обработващия лични данни да информира администратора на „важни основания от публичен интерес“, няма такова задължение за информиране. Във всички случаи, всяко предаване или разкриване на данни може да се извършва само, ако е разрешено от правото на Съюза, включително в съответствие с член 48 от ОРЗД.

1.3.2 Обработващият лични данни трябва да гарантира, че лицата, оправомощени да обработват личните данни, са поели ангажимент за поверителност или са задължени по закон да спазват поверителност (член 28, параграф 3, буква б) от ОРЗД)

122. В договора трябва да е заложено задължението за обработващия лични данни да гарантира, че всеки, оправомощен от него да обработва личните данни, е поел ангажимент за поверителност. Това е изпълнимо посредством конкретно договорно споразумение или по силата на законови задължения, които вече съществуват.

123. Широкото понятие „лицата, оправомощени да обработват личните данни“ включва служителите и временно наетите работници. Като цяло обработващият лични данни следва да предоставя личните данни единствено на служителите, на които те действително са необходими за изпълнението на задачите, за които обработващият лични данни е бил нает от администратора.

124. Ангажиментът или задължението за поверителност трябва да бъдат „подходящи“, т.е. трябва ефективно да забраняват на оправомощеното лице да разкрива каквато и да било поверителна информация без разрешение и трябва да бъдат достатъчно широкообхватни, така че да

обхващат всички лични данни, обработвани от името на администратора, както и условията, при които се обработват личните данни.

1.3.3 Обработващият лични данни трябва да предприема всички необходими мерки съгласно член 32 (член 28, параграф 3, буква в) от ОРЗД)

125. Член 32 изисква администраторът и обработващият лични данни да прилагат подходящи технически и организационни мерки за сигурност. Въпреки че това задължение вече е наложено пряко на обработващия лични данни, чиито операции по обработване попадат в обхвата на ОРЗД, задължението за предприемане на всички мерки, изисквани съгласно член 32, трябва да бъде отразено в договора по отношение на дейностите по обработване, възложени от администратора.

126. Както беше посочено по-горе, в договора за обработване не следва просто да се повтарят разпоредбите на ОРЗД. Договорът трябва да включва или да се позовава на информация относно мерките за сигурност, които трябва да бъдат приети — **задължение на обработващия лични данни да получи одобрението на администратора, преди да прави изменения** — както и да извършва редовен преглед на мерките за сигурност, за да гарантира, че са подходящи спрямо рисковете, които могат да претърпят развитие с течение на времето. Степента на детайлност на информацията относно мерките за сигурност, която трябва да бъде включена в договора, трябва да бъде такава, че да позволи на администратора да прецени целесъобразността на мерките съгласно член 32, параграф 1 от ОРЗД. Освен това описанието е необходимо също така, за да се предостави възможност на администратора да изпълни задължението си за отчетност по отношение на мерките за сигурност, съгласно член 5, параграф 2 и член 24 от ОРЗД, наложено на обработващия лични данни. От член 28, параграф 3, букви е) и з) от ОРЗД може да се изведе съответно задължение на обработващия лични данни да подпомага администратора и да предоставя цялата информация, необходима за доказване на изпълнението на задълженията.

127. Равнището на указанията, предоставяни от администратора на обработващия лични данни по отношение на мерките, които трябва да бъдат приложени, зависи от конкретните обстоятелства. В някои случаи администраторът може да предостави ясно и подробно описание на мерките за сигурност, които трябва да бъдат приложени. В други случаи администраторът може да опише минималните цели по отношение на сигурността, които трябва да бъдат постигнати, като същевременно изисква от обработващия лични данни да предложи специфични мерки за сигурност, които да бъдат приложени. Във всички случаи администраторът трябва да предостави на обработващия лични данни описание на дейностите по обработването и на целите по отношение на сигурността (въз основа на извършената от администратора оценка на риска), както и да одобри мерките, предложени от обработващия. Това може да бъде включено в приложение към договора. Администраторът упражнява правомощията си за вземане на решения по отношение на основните характеристики на мерките за сигурност посредством изрично изброяване или одобряване на мерките, предложени от обработващия лични данни.

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).

128. Споразумението трябва да определя, че обработващият лични данни не може да включва друг обработващ без предварителното писмено разрешение на администратора, както и дали това разрешение ще бъде конкретно или общо. В случай на общо разрешение обработващият трябва да информира администратора за всяка замяна на подизпълнители, които обработват лични

данни, по отношение на които е дадено писмено разрешение, предоставяйки възможност на администратора да възрази. Препоръчително е в договора да се определи процедурата за това. Следва да се отбележи, че 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[54]. Освен това, когато се изисква конкретно разрешение, в договора следва да се определи процедурата за неговото получаване.

129. Когато обработващият лични данни включва друг обработващ, между тях трябва да бъде сключен договор, с който се налагат същите задължения за защита на данните като задълженията, наложени на първоначалния обработващ лични данни, или те трябва да бъдат наложени чрез друг правен акт, съгласно правото на Съюза или правото на държава членка (вж. също точка 160 по-долу). Това включва задължението по член 28, параграф 3, буква з) да позволява и допринася за извършването на одити от страна на администратора или друг одитор, оправомощен от администратора[55]. Обработващият лични данни носи отговорност пред администратора за изпълнението на задълженията за защита на данните на другите обработващи лични данни (за повече подробности относно препоръчителното съдържание на споразумението вж. подточка 1.6 по-долу[56]).

1.3.5 Обработващият лични данни трябва да подпомага администратора при изпълнението на задължението му да отговори на искания за упражняване на правата на субектите на данни (член 28, параграф 3, буква д) от ОРЗД).

130. Освен че гарантира, че обработването на исканията на субектите на данни зависи от администратора, договорът трябва да предвижда задължението за обработващия лични данни да подпомага администратора „доколкото е възможно, чрез подходящи технически и организационни мерки“. Естеството на тази помощ може значително да варира „като взема предвид естеството на обработването“ и в зависимост от вида дейност, възложена на обработващия. Подробна информация относно помощта, която трябва да бъде предоставена от обработващия лични данни, следва да бъде включена в договора или в приложение към него.

131. Въпреки че помощта може да се състои просто в своевременно предаване на всяко получено искане и/или в даване на възможност на администратора пряко да извлече, и управлява съответните лични данни, при някои обстоятелства на обработващия лични данни ще бъдат възложени по-конкретни, технически задължения, по-специално, когато е в състояние да извлече, и управлява личните данни.

132. От изключителна важност е да се вземе предвид фактът, че въпреки че управлението на отделните искания на практика може да бъде възложено на обработващия лични данни, администраторът носи отговорността тези искания да бъдат изпълнявани. Поради това преценката дали исканията на субектите на данни са допустими и/или дали изискванията,

[54] В тази връзка, например, не е достатъчно обработващият лични данни просто да предостави на администратора общ достъп до списък с обработващите лични данни подизпълнители, който може периодично да бъде актуализиран, без да го информира относно всеки нов подизпълнител, който планира да включи. С други думи, обработващият лични данни трябва активно да информира администратора относно всяка промяна в списъка (т.е. по-специално за всеки нов подизпълнител, който планира да включи).

[55] Вж. също Становище 14/2019 на ЕКЗД относно проекта на стандартни договорни клаузи, внесен от датския надзорен орган (член 28, параграф 8 от ОРЗД), 9 юли 2019 г., точка 44.

[56] Вж. част II, подточка 1.6 („Подизпълнители, които обработват лични данни“).

определени в ОРЗД, са изпълнени, следва да се извършва от администратора за всеки отделен случай или чрез ясни указания, предоставени на обработващия в договора, преди началото на обработването. Също така, сроковете, предвидени в глава III, не могат да бъдат удължавани от администратора поради факта, че необходимата информация трябва да бъде предоставена от обработващия лични данни.

1.3.6 Обработващият лични данни трябва да подпомага администратора да гарантира изпълнението на задълженията съгласно членове 32—36 (член 28, параграф 3, буква е) от ОРЗД).

133. Това, което трябва да се предотврати в договора, е просто да бъдат повторно заявени тези задължения за оказване на помощ: **в споразумението следва да се съдържат подробности относно начина, по който от обработващия лични данни се изисква да подпомага администратора при изпълнение на изброените задължения**. Например в приложенията към споразумението могат да се добавят процедури и образец, посредством които обработващият лични данни да има възможността да предостави на администратора цялата необходима информация.

134. Видът и равнището на помощта, която трябва да бъде предоставена от обработващия лични данни, могат да варират значително, *„като се отчита естеството на обработване и информацията, до която е осигурен достъп на обработващия лични данни“*. Администраторът трябва да информира по подходящ начин обработващия относно риска, свързан с обработването, както и относно всяко друго обстоятелство, което може да помогне на обработващия лични данни да изпълни задължението си.

135. По отношение на специфичните задължения обработващият лични данни е длъжен първо да подпомага администратора при изпълнението на задължението да предприема подходящи технически и организационни мерки с оглед да гарантира сигурността на обработването[57]. Въпреки че това задължение може до известна степен да се припокрива с изискването самият обработващ лични данни да предприема подходящи мерки за сигурност, когато операциите по обработване на обработващия попадат в обхвата на ОРЗД, те продължават да бъдат две отделни задължения, тъй като едното се отнася за собствените мерки на обработващия лични данни, а другото се отнася за тези на администратора.

136. Второ, обработващият лични данни трябва да подпомага администратора да изпълнява задължението да уведомява надзорния орган и субектите на данни за нарушения на сигурността на личните данни. Обработващият лични данни трябва да уведоми администратора, когато открие нарушение на сигурността на личните данни, засягащо съоръженията/информационните системи на обработващия или на подизпълнител, и да подпомага администратора да получи информацията, която трябва да се съдържа в доклада до надзорния орган[58]. С ОРЗД се определя изискването администраторът, без ненужно забавяне, да уведомява за нарушение на сигурността на личните данни, за да се сведе до минимум причиняването на вреда на физическите лица и да се увеличи максимално възможността за подходящо справяне с нарушението. Поради това администраторът също следва да бъде уведомен от обработващия лични данни без ненужно забавяне[59]. В зависимост от специфичните характеристики на

[57] Член 32 от ОРЗД.

[58] Член 33, параграф 3 от ОРЗД.

[59] За повече информация вж. Насоките относно уведомленията за нарушения на сигурността на личните данни съгласно Регламент 2016/679, РД 250ред.01, 6 февруари 2018 г., стр. 13—14.

обработването, възложено на обработващия, може да бъде целесъобразно страните да включат в договора конкретен срок (напр. брой часове), в рамките на който обработващият лични данни следва да уведоми администратора и точката за контакт, която може да получава такива уведомления, както и условията и минималното съдържание, които администраторът очаква[60]. Договорността между администратора и обработващия лични данни може също така да включва разрешение и изискване обработващият лични данни пряко да уведомява за нарушение на сигурността на данните, в съответствие с членове 33 и 34, но правната отговорност за уведомяването остава на администратора[61]. В случай че обработващият лични данни пряко уведоми надзорния орган за нарушение на сигурността на данните и информира субектите на данни в съответствие с членове 33 и 34, обработващият трябва също така да уведоми администратора и да му предостави копия от уведомлението и информацията, предоставена на субектите на данни.

137. Освен това обработващият лични данни трябва също така да подпомага администратора при извършването на оценки на въздействието върху защитата на данните, когато е необходимо, както и при консултирането с надзорния орган, когато резултатът от оценката показва, че съществува висок риск, който не може да бъде намален.

138. Това, че обработващият лични данни е длъжен да подпомага администратора не представлява прехвърляне на отговорността, тъй като задълженията са наложени на администратора. Например, въпреки че оценката на въздействието върху защитата на данните може на практика да бъде извършена от обработващ лични данни, задължението за извършване на оценката остава отговорност на администратора[62], като от обработващия лични данни се изисква да подпомага администратора само „при необходимост и при поискване“[63]. В резултат на това администраторът е този, който трябва да поеме инициативата да извърши оценката на въздействието върху защитата на данните, а не обработващият лични данни.

1.3.7 По избор на администратора заличава или връща на администратора всички лични данни след приключване на дейностите по обработване и заличава съществуващите копия (член 28, параграф 3, буква ж) от ОРЗД).

139. Договорните условия имат за цел да гарантират, че след приключване на „услугите по обработване“ се осигурява подходяща защита на личните данни: следователно, що се отнася до личните данни — администраторът решава какво следва да направи обработващият лични данни.

140. Администраторът може да вземе решение в началото дали личните данни да бъдат заличени или върнати, като посочи решението си в договора, чрез писмено съобщение, което трябва да бъде изпратено своевременно на обработващия лични данни. Договорът или друг правен акт следва да отразява възможността администраторът на данни да промени взетото решение,

[60] Вж. също Становище 14/2019 на ЕКЗД относно проекта на стандартни договорни клаузи, внесен от датския надзорен орган (член 28, параграф 8 от ОРЗД), 9 юли 2019 г., точка 40.
[61] Насоки относно уведомленията за нарушения на сигурността на личните данни съгласно Регламент 2016/679, РД250ред.01, 6 февруари 2018 г., стр. 14.
[62] Работна група за защита на личните данни по член 29, Насоки относно оценката на въздействието върху защитата на данните (ОВЗД) и определяне на това дали е налице вероятност обработването „да породи висок риск“ за целите на Регламент 2016/679, РД 248 ред.01, стр. 14.
[63] Съображение 95 от ОРЗД.

преди приключване на услугите по обработване. Договорът следва да определя процедурата за предоставяне на тези указания.

141. Ако администраторът реши личните данни да бъдат заличени, обработващият лични данни следва да гарантира, че заличаването се извършва по сигурен начин, също и с цел спазване на член 32 от ОРЗД. Обработващият следва да потвърди пред администратора, че заличаването е извършено в рамките на договорен срок и по съгласуван начин.

142. Обработващият лични данни трябва да заличи всички съществуващи копия на данните, освен ако правото на ЕС или правото на държава членка не изисква по-нататъшното им съхранение. Ако обработващият или администраторът знае за такова правно изискване, той следва да уведоми другата страна във възможно най-кратък срок.

1.3.8 Обработващият лични данни осигурява достъп на администратора до цялата информация, необходима за доказване на изпълнението на задълженията, определени в член 28, и позволява и допринася за извършването на одити, включително проверки, от страна на администратора или друг одитор, оправомощен от администратора (член 28, параграф 3, буква з) от ОРЗД).

143. Договорът включва подробности относно това колко често и как следва да се осигурява потокът от информация между обработващия лични данни и администратора, така че администраторът да бъде напълно информиран относно подробностите за обработването, които са от значение за доказване на изпълнението на задълженията, посочени в член 28 от ОРЗД. 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 подизпълнители и т.н.

144. В договора се посочват и допълнителни подробности относно способността за извършване на, както и задължението за участие в проверки и одити от страна на администратора или от страна на друг одитор, оправомощен от администратора.

В ОРЗД се уточнява, че проверките и одитите се извършват от администратора или от трета страна, оправомощена от администратора. 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. Обработващият лични данни може да предложи да бъде избран конкретен одитор, но окончателното решение трябва да бъде взето от администратора, съгласно член 28, параграф 3, буква з) от ОРЗД.[64] Освен това, дори когато проверката се извършва от одитор, предложен от

[64] Вж. Съвместно становище 1/2021 на ЕКЗД и ЕНОЗД относно стандартните договорни клаузи между администратори на лични данни и обработващи лични данни, точка 43.

обработващия лични данни, администраторът си запазва правото да оспори обхвата, методиката на проверката и резултатите от нея[65].

Страните следва да си сътрудничат добросъвестно и да извършват оценка по отношение на това дали и кога е необходимо да се извършват одити в помещенията на обработващия лични данни, както и какъв вид одит или проверка (дистанционно/на място/друг начин за събиране на необходимата информация) би бил необходим и подходящ в конкретния случай, като се вземат предвид и опасенията във връзка със сигурността; окончателният избор в това отношение трябва да бъде направен от администратора. След резултатите от проверката администраторът следва да може да поиска от обработващия лични данни да предприеме последващи мерки, например за отстраняване на установените недостатъци и пропуски[66]. По същия начин трябва да бъдат установени специфични процедури във връзка с проверката на обработващите лични данни подизпълнители от страна на обработващия лични данни и администратора (вж. подточка 1.6 по-долу[67]).

145. Въпросът за разпределението на разходите между администратора и обработващия лични данни във връзка с одитите не попада в обхвата на ОРЗД и е предмет на търговски съображения. Член 28, параграф 3, буква з) обаче изисква договорът да включва задължение на обработващия лични данни да предоставя на администратора цялата необходима информация, както и задължение да позволява и допринася за извършването на одити, включително проверки, от страна на администратора или друг оправомощен одитор. На практика това означава, че страните не следва да включват в договора клаузи, предвиждащи плащането на разходи или такси, които биха били явно непропорционални или прекомерни, като по този начин имат възпиращ ефект върху една от страните. Такива клаузи действително биха означавали, че правата и задълженията, посочени в член 28, параграф 3, буква з), никога няма да бъдат упражнявани на практика и ще станат чисто теоретични, предвид че те съставляват неразделна част от гаранциите за защита на данните, предвидени в член 28 от ОРЗД.

1.4 Указания, нарушаващи правото в областта на защитата на данните

146. Съгласно член 28, параграф 3 обработващият лични данни трябва незабавно да уведомява администратора, ако според него дадено указание нарушава ОРЗД или други разпоредби на Съюза или на държава членка относно защитата на данни.

147. Всъщност обработващият лични данни е длъжен да спазва указанията на администратора, но също така има общо задължение да спазва правото. Всяка инструкция, нарушаваща правото в областта на защитата на данните, изглежда поражда конфликт между посочените по-горе две задължения.

148. След като бъде уведомен, че някое от неговите указания може да е в нарушение на правото в областта на защитата на данните, администраторът ще трябва да направи оценка на ситуацията и да реши дали указанието действително нарушава правото в областта на защитата на данните.

149. ЕКЗД препоръчва на страните да проведат преговори и да определят в договора последствията от уведомяването за изпратено от обработващия лични данни неправомерно указание, както и

[65] Вж. Становище 14/2019 относно проекта на стандартни договорни клаузи, внесен от датския надзорен орган (член 28, параграф 8 от ОРЗД), точка 43.
[66] Вж. Становище 14/2019 относно проекта на стандартни договорни клаузи, внесен от датския надзорен орган (член 28, параграф 8 от ОРЗД), точка 43.
[67] Вж. част II, подточка 1.6 („Подизпълнители, които обработват лични данни“).

в случай на бездействие от страна на администратора в тази връзка. Един пример би бил включването на клауза за прекратяване на договора, в случай че администраторът продължи да дава неправомерни инструкции. Друг пример би бил клауза относно възможността обработващият лични данни да преустанови изпълнението на съответното указание, докато администраторът не го потвърди, измени или оттегли[68].

1.5 Обработващ лични данни, определящ целите и средствата за обработването

150. Ако обработващият лични данни наруши регламента, определяйки целите и средствата за обработването, той се счита за администратор по отношение на това обработване (член 28, параграф 10 от ОРЗД).

1.6 Подизпълнители, които обработват лични данни

151. 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 подизпълнител следва да се извърши в съответствие с описанието по-горе относно понятието „обработващ лични данни“ (вж. точката по-горе 83).

152. Въпреки че веригата може да бъде твърде дълга, администраторът запазва основната си роля при определянето на целта и средствата за обработването. В член 28, параграф 2 от ОРЗД се предвижда, че обработващият лични данни не може да включва друг обработващ без предварителното конкретно или общо писмено разрешение на администратора (включително в електронен формат). В случай на общо писмено разрешение, обработващият лични данни винаги информира администратора за всякакви планирани промени за включване или замяна на други обработващи лични данни, като по този начин предоставя възможност на администратора да оспори тези промени. И в двата случая обработващият лични данни трябва да получи писмено разрешение от администратора, преди което и да е обработване на лични данни да бъде възложено на подизпълнител. За да извърши оценка и да вземе решение дали да разреши възлагането на подизпълнители, администраторът трябва да получи от обработващия лични данни списък с предвидените подизпълнители (включително за всеки от тях: местоположенията им, какво ще вършат и доказателство за това какви гаранции са били използвани)[69].

153. Предварителното писмено разрешение може да бъде конкретно, т.е. отнасящо се до конкретен подизпълнител за конкретна дейност по обработване и в определен момент, или общо. Това следва да бъде уточнено в договора или в друг правен акт, уреждащ обработването.

154. В случаите, в които администраторът реши да приеме определени подизпълнители към момента на подписване на договора, в договора или в приложение към него следва да бъде

[68] Вж. Съвместно становище 1/2021 на ЕКЗД и ЕНОЗД относно стандартните договорни клаузи между администратори на лични данни и обработващи лични данни, точка 39.

[69] Тази информация е необходима, за да може администраторът да спази принципа на отчетност, определен в член 24 и разпоредбите на член 28, параграф 1, член 32 и глава V от ОРЗД.

включен списък с одобрените подизпълнители. След това списъкът следва да се актуализира в съответствие с общото или конкретното разрешение, предоставено от администратора.

155. В случай че администраторът реши да предостави **конкретното разрешение**, той следва да посочи в писмен вид за кой подизпълнител, който ще обработва лични данни и за коя дейност се отнася разрешението. За всяка последваща промяна ще се изисква допълнително разрешение от администратора, преди тя да бъде въведена. Ако на искането на обработващия лични данни за конкретно разрешение не бъде отговорено в рамките на определения срок, то следва да се счита, че е отхвърлено. Администраторът следва да вземе решение да предостави или да откаже разрешение, взимайки предвид своето задължение да използва само обработващи лични данни, които предоставят „достатъчни гаранции“ (вж. подточка 1.1 по-горе[70]).

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), което следва да бъде допълнено с критерии, които да насочват избора на обработващ лични данни (напр. гаранции по отношение на техническите и организационните мерки, експертни познания, надеждност и ресурси)[71]. При този сценарий обработващият лични данни трябва своевременно да уведомява администратора за всякакво планирано включване или замяна на обработващ(и) лични данни подизпълнител(и), като по този начин предоставя възможност на администратора да ги оспори.

157. Следователно, основната разлика между сценария, включващ конкретно разрешение, и този, включващ общо разрешение, се състои в значението, което се отдава на мълчанието на администратора: в случая с общото разрешение липсата на оспорване от страна на администратора в рамките на определения срок може да се тълкува като разрешение.

158. И в двата случая договорът следва да включва подробна информация относно сроковете за предоставяне на одобрение или оспорване от страна на администратора и относно начина, по който страните възнамеряват да комуникират по тази тема (напр. образци). Този срок трябва да бъде разумен, с оглед на вида обработване, сложността на дейностите, възложени на обработващия лични данни (и на подизпълнителите), и отношенията между страните. Освен това договорът следва да включва подробности относно практическите стъпки след оспорването от страна на администратора (напр. като се определи срок, в рамките на който администраторът и обработващият лични данни следва да решат дали обработването да бъде прекратено).

159. Независимо от предложените от администратора критерии за избор на доставчици, обработващият лични данни остава изцяло отговорен пред администратора за изпълнението на задълженията от страна на подизпълнителите (член 28, параграф 4 от ОРЗД). Поради това обработващият лични данни следва да гарантира, че предлага обработващи лични данни подизпълнители, предоставящи достатъчни гаранции.

160. Освен това, когато обработващ лични данни възнамерява да наеме (оправомощен) подизпълнител, той трябва да сключи договор с него, който налага същите задължения като тези, наложени на първия обработващ лични данни от администратора, или задълженията трябва да бъдат наложени по силата на друг правен акт съгласно правото на ЕС или правото на държава членка. Цялата верига на дейностите по обработване се урежда посредством писмени

[70] Вж. част II — подточка 1.1 („Избор на обработващ лични данни“).

[71] Това задължение на администратора произтича от принципа на отчетност, определен в член 24 и от задължението за спазване на разпоредбите на член 28, параграф 1, член 32 и глава V от ОРЗД.

споразумения. 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. Това означава също така, че ако обработващият лични данни възложи на подизпълнител конкретна част от обработването, за която някои от задълженията не са приложими, тези задължения не следва да бъдат включени „по подразбиране“ в договора с подизпълнителя, тъй като това само би породило несигурност. Например, що се отнася до предоставянето на помощ по отношение на задълженията, свързани с нарушения на сигурността на данните, администраторът може пряко да бъде уведомяван от подизпълнителя, който обработва личните данни за нарушения на сигурността на данните, ако и трите страни са съгласни. В случай на такова пряко уведомяване обаче обработващият лични данни следва да бъде информиран и да получи копие от уведомлението.

2 ПОСЛЕДСТВИЯ ОТ СЪВМЕСТНОТО АДМИНИСТРИРАНЕ

2.1 Определяне по прозрачен начин на съответните отговорности на съвместните администратори за изпълнение на задълженията по ОРЗД

161. Съгласно член 26, параграф 1 от ОРЗД съвместните администратори определят и съгласуват по прозрачен начин съответните си отговорности за изпълнение на задълженията по ОРЗД.

162. Поради това съвместните администратори трябва да определят „кой какво ще извършва“ като решат помежду си кой какви задачи ще трябва да изпълнява, за да гарантират, че обработването е в съответствие с приложимите задължения по ОРЗД във връзка с въпросното съвместно обработване. С други думи, трябва да се направи разпределение на отговорностите за спазване на изискванията, произтичащо от използването на термина *„съответните“* в член 26, параграф 1. Това не изключва факта, че определени отговорности на всеки съвместен администратор вече може да са предвидени в правото на ЕС или правото на държава членка. В такива случаи в договореността между съвместните администратори следва също така да се определят всички допълнителни отговорности, необходими, за да се гарантира съответствие с ОРЗД, които не са включени в правните разпоредби[72].

163. Целта на тези правила е да се гарантира, че когато участват множество участници, особено в сложна среда за обработване на данни, отговорностите за спазването на правилата за защита на данните са ясно разпределени, за да се избегне намаляване на защитата на личните данни или неизпълнение на задълженията от която и да е от страните, участващи в обработването, поради пропуски в резултат на „отрицателен“ спор за компетентност. Тук следва да се поясни, че всички отговорности трябва да се разпределят в зависимост от фактическите обстоятелства, за да се постигне работещо споразумение. ЕКЗД отбелязва, че съществуват ситуации, в които влиянието на един съвместен администратор и неговото фактическо влияние усложняват постигането на

[72] „Във всички случаи договореността между съвместните администратори следва да обхваща изцяло всички отговорности на съвместните администратори, включително тези, които може вече да са предвидени в съответното право на ЕС или в правото на държава членка, като не се засяга задължението на съвместните администратори да осигуряват достъпността на съществените характеристики на договореността помежду им, в съответствие с член 26, параграф 2 от ОРЗД.“

споразумение. Тези обстоятелства обаче не засягат съвместното администриране и не могат да послужат за освобождаване на никоя от страните от нейните задължения съгласно ОРЗД.

164. По-конкретно в член 26, параграф 1 се посочва, че определянето на съответните им отговорности (т.е. задачите) за изпълнение на задълженията по ОРЗД се извършва от съвместни администратори *„по-специално“* по отношение на упражняването на правата на субекта на данни и задълженията за предоставяне на информацията, посочена в членове 13 и 14, освен ако и доколкото съответните отговорности на администраторите не са определени от правото на Съюза или правото на държава членка, което се прилага спрямо администраторите.

165. От тази разпоредба става ясно, че съвместните администратори трябва да определят съответно кой ще бъде задължен да отговаря на исканията, когато субектите на данни упражняват правата си, предоставени им по силата на ОРЗД, както и да им предоставя информация, съгласно изискванията, предвидени в членове 13 и 14 от ОРЗД. Това се отнася само за определянето, в рамките на вътрешните им отношения, на това коя от страните е задължена да отговаря на исканията на субектите на данни. Независимо от всяка такава договореност субектът на данните може да се свърже с който и да е от съвместните администратори в съответствие с член 26, параграф 3 от ОРЗД. Използването на термина *„по-специално“* обаче показва, че задълженията, които са предмет на разпределение на отговорностите по отношение на изпълнението от всяка участваща страна, както е посочено в настоящата разпоредба, са неизчерпателни. От това следва, че разпределението на отговорностите за изпълнение на задълженията сред съвместните администратори не се ограничава до темите, посочени в член 26, параграф 1, а обхваща и задълженията на други администратори съгласно ОРЗД. Всъщност съвместните администратори трябва да гарантират, че цялото съвместно обработване е в пълно съответствие с ОРЗД.

166. С оглед на това, мерките за изпълнение на задълженията и задълженията, които следва да се вземат предвид при определянето на отговорностите на съвместните администратори, заедно с изрично посочените в член 26, параграф 1, включват, наред с другото, без ограничения:

- Прилагане на общите принципи за защита на данните (член 5)
- Правно основание на обработването[73] (член 6)
- Мерки за сигурност (член 32)
- Уведомяване на надзорния орган и на субекта на данни за нарушение на сигурността на личните данни[74] (членове 33 и 34)
- Оценки на въздействието върху защитата на данните (членове 35 и 36)[75]

[73] Въпреки че ОРЗД допуска съвместните администратори да използват различно правно основание за различните извършвани от тях операции по обработване, се препоръчва да се използва, когато е възможно, едно и също правно основание за конкретна цел.

[74] Вж. също Насоки относно уведомленията за нарушения на сигурността на личните данни съгласно Регламент 2016/679, РД 250ред.01, които предвиждат, че съвместният администратор ще включва *„определяне на страната, която ще носи отговорност за изпълнение на задълженията съгласно членове 33 и 34. Работната група по член 29 препоръчва договореностите между съвместните администратори да включват разпоредби, които определят кой администратор ще поеме водеща роля или ще носи отговорност за изпълнението на задълженията за уведомяване за нарушения на сигурността на данните съгласно ОРЗД“ (стр. 13).*

[75] Вж. също Насоките на ЕКЗД относно оценките на въздействието върху защитата на данните (ОВЗД), РД 248.ред01, предвиждащи следното: *„Когато в операцията по обработване участват съвместни*

- Включването на обработващ лични данни (член 28)
- Предаване на лични данни на трети държави (глава V)
- Организиране на комуникацията със субектите на данни и надзорните органи

167. Други теми, които могат да бъдат разгледани в зависимост от въпросното обработване и намерението на страните, са например ограниченията по отношение на използването на лични данни от страна на един от съвместните администратори за друга цел. В тази връзка и двамата администратори винаги са задължени да гарантират, че имат правно основание за обработването. Понякога при съвместното администриране личните данни се споделят от един администратор на друг. Що се отнася до отчетността, всеки съвместен администратор е длъжен да гарантира, че данните не се обработват допълнително по начин, който е несъвместим с целите, за които първоначално са били събрани от администратора, споделящ данните[76].

168. Съвместните администратори могат да разполагат с известна степен на гъвкавост при разпространението и разпределението на задълженията помежду си, при условие че гарантират пълно съответствие на даденото обработване с ОРЗД. За целите на разпределението следва да се вземат предвид фактори като това кой е компетентен и е в състояние ефективно да гарантира правата на субекта на данни, както и да изпълнява съответните задължения по ОРЗД. ЕКЗД препоръчва да се документират съответните фактори и вътрешният анализ, извършен с цел разпределяне на различните задължения. Този анализ е част от документацията, която се изисква с оглед спазването на принципа на отчетност.

169. Не е необходимо задълженията да се разпределят поравно между съвместните администратори. В тази връзка СЕС наскоро постанови, че *„наличието на съвместна отговорност не се изразява непременно в равна отговорност на различните субекти за едно и също обработване на лични данни“*[77]. Възможно е обаче да има случаи, в които не всички задължения могат да бъдат разпределени и може да се наложи всички съвместни администратори да спазват едни и същи изисквания, произтичащи от ОРЗД, като се вземат предвид естеството и причината за съвместното обработване. Например съвместните администратори, използващи общи инструменти или системи за обработване на данни, трябва да гарантират спазването по-специално на принципа на „ограничение на целите“ и да предприемат подходящи мерки за осигуряване на сигурността на личните данни, обработвани в рамките на общите инструменти.

170. Друг пример е изискването всеки съвместен администратор да поддържа регистър на дейностите по обработване или да определи длъжностно лице по защита на данните (ДЛЗД),

---

администратори, те трябва точно да определят съответните си задължения. В техните ОВЗД следва да се посочва коя страна носи отговорност за различните мерки за справяне с рисковете и за защита на правата и свободите на субектите на данни. Всеки администратор следва да посочи своите потребности и да обменя полезна информация, без да разкрива тайни (например: защита на търговски тайни, интелектуална собственост, поверителна търговска информация) или да разкрива уязвимости“ (стр. 7).

[76] За всяко разкриване от страна на администратор се изисква правно основание и оценка на съвместимостта, независимо дали получателят е отделен администратор или съвместен администратор. С други думи, наличието на отношения между съвместни администратори не означава автоматично, че съвместният администратор, който получава данните, може законно да обработва данните и за допълнителни цели, които са извън обхвата на съвместното администриране.

[77] Решение по дело *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, точка 43.

ако са изпълнени условията на член 37, параграф 1. Тези изисквания не са свързани със съвместното обработване, но са приложими за тях в качеството им на администратори.

2.2 Разпределението на отговорностите трябва да се извършва посредством договореност

2.2.1 Форма на договорността

171. В член 26, параграф 1 от ОРЗД като ново задължение на съвместните администратори се предвижда те да определят съответните си отговорности *„посредством договореност помежду си“*. Правната форма на тази договореност не е определена в ОРЗД. Поради това съвместните администратори имат свободата да се споразумеят относно формата на договорността.

172. Освен това договорността относно разпределението на отговорностите е обвързваща за всеки от съвместните администратори. Всеки от тях се съгласява и се ангажира *спрямо* останалите да носи отговорност за изпълнението на съответните задължения, предвидени в договорността помежду им.

173. С оглед на правната сигурност, дори и ОРЗД да не предвижда правно изискване за договор или друг правен акт, ЕКЗД препоръчва тази договореност да бъде под формата на обвързващ документ, например договор или друг обвързващ правен акт съгласно правото на ЕС или правото на държава членка, приложимо по отношение на администраторите. Това би осигурило сигурност и би могло да се използва за доказване на прозрачността и отчетността. Всъщност в случай на неспазване на предвиденото договорено разпределение, обвързващия характер на договорността позволява на единия администратор да потърси отговорност от другия по отношение на предвидените задължения. Също така, в съответствие с принципа на отчетност, използването на договор или на друг правен акт ще позволи на съвместните администратори да докажат, че изпълняват задълженията, наложени им по силата на ОРЗД.

174. Начинът, по който отговорностите, т.е. задачите, са разпределени между всеки един от съвместните администратори, трябва да бъде заявен в договорността, като се използва ясен и прост език[78]. Това изискване е важно, тъй като чрез него се гарантира правна сигурност и се избягват възможни конфликти, не само в отношенията между съвместните администратори, но и спрямо субектите на данни и органите за защита на данните.

175. С цел по-добро определяне на разпределението на отговорностите между страните, ЕКЗД препоръчва в договорността да се предоставя и обща информация относно съвместното обработване, като се посочват по-специално предметът и целта на обработването, видът на личните данни и категориите субекти на данни.

2.2.2 Задължения към субектите на данни

176. ОРЗД предвижда няколко задължения на съвместните администратори към субектите на данни:

[78] Както е посочено в съображение 79 от ОРЗД *„(...) отговорността и задълженията на администраторите и обработващите лични данни, а също и по отношение на наблюдението и мерките от страна на надзорните органи, изискват ясно определяне на отговорностите съгласно настоящия регламент, включително когато администраторът определя целите и средствата на обработването съвместно с други администратори“*.

Договорeността надлежно отразява съответните роли и връзки на съвместните администратори *спрямо* субектите на данни.

177. В допълнение към обяснението по-горе в точка 2.1 от настоящите насоки е важно съвместните администратори да изяснят в договорeността съответната си роля, *„по-специално“* по отношение на упражняването на правата на субекта на данни и задълженията за предоставяне на информацията, посочена в членове 13 и 14. В член 26 от ОРЗД се изтъква важното значение на тези специфични задължения. Поради това съвместните администратори трябва да организират и да договорят как и от кого ще бъде предоставяна информацията, и как и от кого ще бъдат предоставяни отговорите на исканията на субекта на данните. Независимо от съдържанието на договорeността по този конкретен въпрос физическото лице може да се свърже с всеки от съвместните администратори, за да упражни правата си в съответствие с член 26, параграф 3, както е обяснено по-долу.

178. Начинът, по който тези задължения са организирани в договорeността, следва *„надлежно“*, т.е. точно, да отразява действителното съвместно обработване. Например, ако само един от съвместните администратори комуникира със субектите на данни за целите на съвместното обработване, той би могъл да бъде в по-добра позиция да информира субектите на данни и евентуално да отговоря на техните искания.

Съществените характеристики на договорeността са достъпни за субекта на данни.

179. Целта на тази разпоредба е да се гарантира, че субектът на данни е запознат със *„съществените характеристики на договорeността“*. Например субектът на данни трябва да е напълно наясно кой администратор на данни служи като точка за контакт за упражняването на правата му (независимо от факта, че той може да упражнява правата си по отношение на и срещу всеки съвместен администратор). Задължението за предоставяне на достъп на субектите на данни до съществените характеристики на договорeността е важно в случай на съвместно администриране, за да е наясно физическото лице кой от администраторите за какво носи отговорност.

180. В ОРЗД не се пояснява какво включва понятието *„съществени характеристики на договорeността“*. ЕКЗД препоръчва съществените характеристики да включват като минимум всички елементи на информацията, посочена в членове 13 и 14, която вече следва да е достъпна за субекта на данни, като по отношение на всеки от тези елементи следва да се посочи кой съвместен администратор носи отговорност да гарантира спазването им. В съществените характеристики на договорeността следва също така да се посочи точката за контакт, ако е определена такава.

181. Начинът, по който тази информация се предоставя на субекта на данни, не е уточнен. За разлика от други разпоредби на ОРЗД (например член 30, параграф 4 относно регистъра на дейностите по обработване или член 40, параграф 11 относно регистъра на одобрените кодекси за поведение), в член 26 не се посочва, че достъпността следва да бъде *„при поискване*“ или *„обществено достъпни чрез всички подходящи средства“*. Поради това съвместните администратори трябва да определят кой е най-ефективният начин да направят съществените характеристики на договорeността достъпни за физическите лица (напр. заедно с информацията по член 13 или 14, в политиката за поверителност или, при поискване, на разположение на длъжностното лице по защита на данните, ако има такова, или на точката за контакт, която евентуално е била посочена). Съвместните администратори следва да гарантират, че информацията се предоставя по съгласуван начин.

В договорността може да се посочи точка за контакт за субектите на данни

182. В член 26, параграф 1 се предвижда възможността съвместните администратори да посочат в договорността точка за контакт за субектите на данни. Посочването на такава точка не е задължително.

183. Предоставянето на физическите лица на единен начин за комуникиране с множество евентуални съвместни администратори дава възможност на субектите на данни да знаят към кого да се обърнат по всички въпроси, свързани с обработването на техните лични данни. Освен това позволява на множество съвместни администратори да координират по по-ефективен начин своите отношения и комуникацията с лицата.

184. По тези причини, за да се улесни упражняването на правата на субектите на данни съгласно ОРЗД, ЕКЗД препоръчва съвместните администратори да посочат такава точка за контакт.

185. Точката за контакт може да бъде длъжностното лице по защита на данните (ДЛЗД), ако има такова, представителят в Съюза (за съвместните администратори, които не са установени в Съюза) или всяка друга точка за контакт, където може да бъде получена информация.

Независимо от условията на договорността, субектите на данни могат да упражняват своите права по отношение на и срещу всеки от съвместните администратори.

186. Съгласно член 26, параграф 3 субектът на данни не е обвързан от условията на договорността и може да упражнява правата си съгласно ОРЗД по отношение на и срещу всеки от съвместните администратори на данни.

187. Например в случай на съвместни администратори, установени в различни държави членки, или ако само един от съвместните администратори е установен в Съюза, субектът на данни може да се свърже, по свой избор, с администратора, установен в държавата членка на обичайното му местопребиваване или месторабота, или с администратора, установен в друга държава в ЕС или в ЕИП.

188. Дори в договорността и в нейните съществени характеристики да се посочва точка за контакт, която да получава и разглежда всички искания на субектите на данни, все пак физическите лица могат да изберат друго.

189. Поради това е важно съвместните администратори предварително да уредят в своите договорености как ще управляват процеса по изготвяне на отговори на исканията, които биха могли да получат от субектите на данни. Във връзка с това се препоръчва съвместните администратори да уведомяват другите отговорни администратори или посочената точка за контакт относно получените искания, с оглед на тяхното ефективно разглеждане.. Да се изисква от субектите на данни да комуникират с посочената точка за контакт или с отговорния администратор би наложило прекомерна тежест върху тях, която би била в противоречие със стремежа за улесняване на упражняването на правата им съгласно ОРЗД.

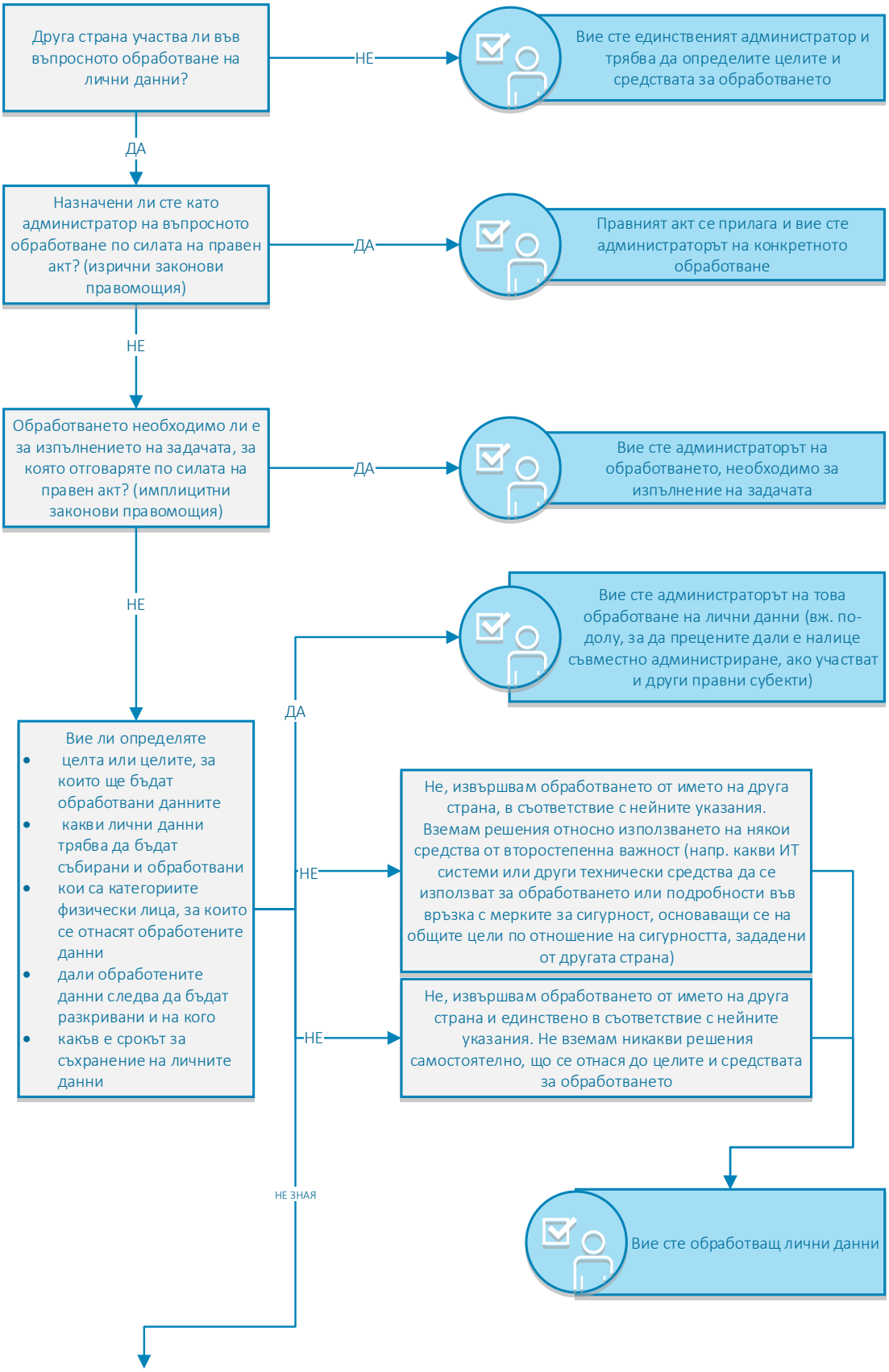
2.3 Задължения към органите за защита на данните

190. Съвместните администратори следва да уредят в договорността начина, по който ще комуникират с компетентните надзорни органи за защита на данните. Тази комуникация би могла да включва евентуална консултация съгласно член 36 от ОРЗД, уведомяване за нарушение на сигурността на личните данни, определяне на длъжностно лице по защита на данните.

191. Следва да се припомни, че органите за защита на данните не са обвързани от условията на договорността, независимо дали става въпрос за квалифицирането на страните като съвместни администратори или за посочената точка за контакт. Следователно, органите могат да се свържат с всеки от съвместните администратори, за да упражнят правомощията си съгласно член 58 по отношение на съвместното обработване.

Приложение I – Схема, показваща прилагането на понятията „администратор“, „обработващ лични данни“ и „съвместни администратори“ на практика

Забележка: за да се преценят правилно ролите на всяка от участващите страни, трябва първо да се определи въпросното конкретно обработване на лични данни и точната му цел. Ако участват множество правни субекти, е необходимо да се прецени дали целите и средствата се определят съвместно, което води до съвместно администриране.



НЕ ЗНАЯ

Не зная кой определя целите и средствата за обработването. :

Следните фактори може да спомогнат за правилното определяне на ролите:

Фактори, показващи, че вие сте администраторът

- Извличате полза от, или имате интереси свързани със, обработването (различни от самото плащане за услуги, което получавате от друг администратор)
- Вземате решения относно въпросните физически лица, като част от или в резултат на обработването (напр. субектите на данни са ваши служители)
- Дейностите по обработване могат да се считат за естествено свързани с ролята или дейностите на вашия правен субект (напр. поради обичайните роли или професионалните експертни познания), които включват отговорности от гледна точка на защитата на данните.
- Обработването е свързано с вашите отношения със субектите на данни, например служители, клиенти, членове и т.н.
- Разполагате с пълна автономност при определянето на начина, по който да бъдат обработвани личните данни
- Възложили сте обработването на личните данни на външна организация, която да ги обработва от ваше име

Фактори, показващи, че вие сте обработващият лични данни

- Обработвате личните данни за целите на друга организация и в съответствие с предоставените от нея документирани указания — нямате ваша собствена цел на обработването.
- Друга страна извършва наблюдение на дейностите ви по обработване, за да гарантира, че спазвате указанията и условията на договора.
- Не преследвате ваша собствена цел на обработването, различна от вашите собствени бизнес интереси, касаещи предоставянето на услуги.
- Наети сте да извършите конкретни дейности по обработването от някой, който от своя страна е нает да обработва данни от името на друга страна и съгласно документираните указания на тази страна (вие сте обработващ лични данни подизпълнител)

Съвместно администриране — ако вие сте администраторът, а другите страни участват в обработването на лични данни: