

Насоки



Насоки 01/2022 г. относно правата на субектите на данни — право на достъп

Версия 2.1

приета на 28 март 2023 г.

Хронология на версиите

Версия 1.0	18 януари 2022 г.	Приемане на насоките за обществена консултация
Версия 2.0	28 март 2023 г.	Приемане на насоките след обществена консултация
Версия 2.1	30 май 2024 г.	Незначителни поправки

РЕЗЮМЕ

Правото на достъп на субектите на данни е залегнало в член 8 от Хартата на основните права на Европейския съюз. То е част от европейската правна рамка за защита на данните от самото ѝ създаване и понастоящем е доразвито с по-точни и по-конкретни правила, включени в член 15 от Общия регламент относно защитата на данните (ОРЗД).

Цел и цялостна структура на правото на достъп

Общата цел на правото на достъп е предоставянето на лицата на достатъчна, прозрачна и леснодостъпна информация за обработването на личните им данни, така че да могат да бъдат запознати и да проверяват законосъобразността на обработването и точността на обработваните данни. Без да представлява условие, това ще улесни упражняването от страна на лицата на други права, като правото на изтриване или правото на коригиране.

Съгласно законодателството в областта на защитата на данните правото на достъп трябва да се разграничава от подобни права с други цели, например правото на достъп до публични документи, чиято цел е да се гарантират прозрачност при вземането на решения от публичните органи и добра административна практика.

Субектът на данните обаче не е задължен да посочва причини за искането за достъп и администраторът не може да анализира дали искането действително ще помогне на физическото лице да провери законосъобразността на съответното обработване или да упражни други права. Администраторът ще трябва да разгледа искането, освен ако не е ясно, че то е подадено съгласно правила, различни от тези за защита на данните.

Правото на достъп включва три различни компонента:

- потвърждение дали се обработват данни, свързани с лицето,
- достъп до тези лични данни и
- достъп до информация за обработването, като например цел, категории данни и получатели, продължителност на обработването, права на субектите на данни и подходящи гаранции в случай на предаване на трета държава.

Общи съображения относно оценката на искането на субекта на данните

При анализ на съдържанието на искането администраторът трябва да прецени дали искането се отнася до лични данни на лицето, което подава искането, дали попада в обхвата на член 15 и дали има други, по-конкретни разпоредби, с които се регламентира достъпът в даден сектор. Той трябва също да прецени дали искането се отнася до всички или само до част от обработваните данни за субекта на данните.

Няма конкретни изисквания относно формата на искането. Администраторът следва да предостави подходящи и удобни за ползване канали за комуникация, които могат да се използват лесно от субекта на данните. Физическото лице обаче не е задължено да използва тези конкретни канали, а вместо това може да изпрати искането до официалната точка за контакт на администратора. Администраторът не е задължен да предприема действия по искания, изпратени до напълно произволни или очевидно неточни адреси.

Когато администраторът не е в състояние да установи данните, които се отнасят до субекта на данните, той информира лицето за това и може да откаже да предостави достъп, освен ако

физическото лице не предостави допълнителна информация, която позволява установяването на такива данни. Освен това, ако администраторът има съмнения дали лицето е това, за което се представя, той може да поиска допълнителна информация с цел да потвърждение на самоличността. За да се избегне прекомерно събиране на данни искането за допълнителна информация трябва да бъде пропорционално на вида на обработваните данни, вредите, които могат да настъпят, и др.

Обхват на правото на достъп

Обхватът на правото на достъп се определя от обхвата на понятието за лични данни съгласно определението в член 4, точка 1 от ОРЗД. Освен основните лични данни, като име, адрес, телефонен номер и др., в обхвата на това определение може да попадне голямо разнообразие от данни, като например медицински заключения, история на покупките, показатели за кредитоспособност, регистрационни файлове за дейността, дейности по търсене и др. Лични данни, които са преминали през псевдонимизация, все още представляват лични данни, за разлика от анонимизираните. Правото на достъп се отнася до личните данни на лицето, което подава искането. То не следва да се тълкува твърде ограничително и може да обхваща данни, които биха могли да засягат и други лица, например хронология на комуникацията, включваща входящи и изходящи съобщения.

Освен достъпа до личните данни администраторът трябва да предостави допълнителна информация относно обработването и правата на субектите на данни. Тази информация може да се основава на вече наличните сведения в регистъра на дейностите по обработване на администратора (член 30 от ОРЗД) и в декларацията за поверителност (членове 13 и 14 от ОРЗД). Може обаче да се наложи тази обща информация да бъде актуализирана към момента на искането или да бъде адаптирана, така че да отразява операциите по обработване, които се извършват по отношение на конкретното лице, подало искането.

Как се предоставя достъп

Начините за предоставяне на достъп може да се различават в зависимост от количеството данни и от сложността на извършваното обработване. Освен ако изрично е посочено друго, искането следва да се разбира като отнасящо се до *всички* лични данни относно субекта на данните и администраторът може да поиска конкретизиране на искането, в случай че обработва голямо количество данни.

Администраторът ще трябва да търси лични данни във всички ИТ системи, както и в регистри с лични данни, които не са основани на ИТ, въз основа на критерии за търсене, съответстващи на начина, по който е структурирана информацията, например име и клиентски номер. Съобщаването на данни и друга информация за обработването трябва да се извършва в кратка, прозрачна, разбираема и леснодостъпна форма, като се използва ясен и разбираем език. Поспецифичните изисквания във връзка с това зависят от обстоятелствата относно обработването на данните, както и от способността на субекта на данните да възприема и разбира съобщението (например, като се взема предвид, че физическото лице е дете или лице със специални потребности). Ако данните се състоят от кодове или други „необработени данни“, може да се наложи да бъдат обяснени, за да имат смисъл за субекта на данните.

Основното условие за осигуряването на достъп е предоставянето на субекта на данните на копие от неговите данни, но е възможно да се предвидят и други условия (като устна информация и достъп на място), ако лицето поиска това. Данните може да бъдат изпратени по електронна поща, при условие че са приложени всички необходими гаранции, като например се вземе

предвид естеството на данните, или по други начини, например чрез инструмент за самообслужване.

В някои случаи, когато е налице голямо количество данни и за субекта на данните би било трудно да разбере информацията, ако му бъде предоставена наведнъж, особено при онлайн обработване, най-подходящата мярка би била използването на многослоен подход. Предоставянето на информация на различни слоеве може да улесни разбирането на данните от страна на физическото лице. Администраторът трябва да е в състояние да докаже, че многослойният подход осигурява добавена стойност за субекта на данните и всички слоеве следва да бъдат предоставени едновременно, в случай че лицето избере това.

Копието от данните и допълнителната информация следва да бъдат предоставени в траен формат, като например писмен текст, който може да бъде в широко използвана електронна форма, така че субектът на данните да може лесно да го изтегли. Данните може да бъдат предоставени под формата на препис или в обобщен вид, стига да е включена цялата информация и това да не изменя или променя съдържанието на информацията.

Искането трябва да бъде изпълнено възможно най-бързо и във всеки случай в рамките на един месец от неговото получаване. При необходимост този срок може да бъде удължен с още два месеца, като се вземат предвид сложността и броят на исканията. Впоследствие субектът на данните трябва да бъде уведомен за причината за забавянето. С цел възможно най-бързото разглеждане на исканията администраторът трябва да прилага необходимите мерки и да адаптира тези мерки към свързаните с обработването обстоятелства. Когато данните се съхраняват само за много кратък срок, трябва да са налице мерки, с които да се гарантира, че искане за достъп може да бъде изпълнено, без данните да бъдат изтрети, докато се обработва искането. Когато се обработва голямо количество данни, администраторът ще трябва да въведе рутинни практики и механизми, които да са адаптирани към сложността на обработването.

В оценката на искането следва да се отразява състоянието в момента на получаване на искането от администратора. Необходимо е да бъдат предоставени дори данни, които може да са неточни или незаконосъобразно обработени. Не е възможно предоставянето на вече заличени данни, например в съответствие с политиката на съхраняване на данните, които вече не са на разположение на администратора.

Рамки и ограничения

Съгласно ОРЗД са възможни някои ограничения на правото на достъп. Не са налице други изключения или дерогации. Правото на достъп не съдържа каквато и да било обща резерва относно пропорционалността по отношение на полаганите от страна на администратора усилия за изпълнение на искането на субекта на данните.

Съгласно член 15, параграф 4 правото на получаване на копие не трябва да влияе неблагоприятно върху правата и свободите на други лица. Европейският комитет по защита на данните (ЕКЗД) е на мнение, че тези права трябва да бъдат взети предвид не само при осигуряването на достъп чрез предоставяне на копие, но и ако достъпът до данните се предоставя с други средства (например достъп на място). Член 15, параграф 4 обаче не се прилага по отношение на допълнителната информация относно обработването, която е посочена в член 15, параграф 1, букви а—з). Администраторът трябва да е в състояние да докаже, че правата или свободите на други лица биха били повлияни неблагоприятно в конкретната ситуация. Прилагането на член 15, параграф 4 не следва да води до пълен отказ на искането на субекта на данните; то би довело само до пропускане или предаване в нечетлив вид

на онези части, които може да имат отрицателни последици за правата и свободите на други лица.

Съгласно член 12, параграф 5 от ОРЗД на администраторите се позволява да отхвърлят искания, които са явно неоснователни или прекомерни, или да налагат разумна такса за такива искания. Тези понятия трябва да се тълкуват в тесен смисъл. Тъй като са налице много малко необходими условия по отношение на исканията за достъп, възможността искане да бъде счетено за явно неоснователно е доста ограничена. Прекомерните искания зависят от специфичните характеристики на сектора, в който осъществява дейност администраторът. Колкото по-често настъпват промени в базата данни на администратора, толкова по-често на субекта на данните може да бъде разрешено да поиска достъп, без това да се счита за прекомерно. Вместо да откаже достъп, администраторът може да реши да наложи такса за субекта на данните. Това би било уместно само в случай на прекомерни искания с цел покриване на административните разходи, които такива искания може да породят. Администраторът трябва да може да докаже явно неоснователния или прекомерния характер на дадено искане.

Съгласно член 23 от ОРЗД и дерогациите в него ограничения на правото на достъп може да съществуват и в националното право на държавите членки. Администраторите, които възнамеряват да се позоват на такива ограничения, трябва внимателно да проверят изискванията на националните разпоредби и да вземат под внимание всички специфични условия, които може да се прилагат. Такива условия може да бъдат правото на достъп да бъде отложено само временно или ограничението да се прилага само за определени категории данни.

Съдържание

1	Въведение — общи наблюдения	9
2	Цел на правото на достъп, структура на член 15 от ОРЗД и общи принципи	12
2.1	Цел на правото на достъп	12
2.2	Структура на член 15 от ОРЗД.....	13
2.2.1	Определяне на съдържанието на правото на достъп	14
2.2.1.1	Потвърждение „дали“ личните данни се обработват	15
2.2.1.2	Достъп до личните данни, които се обработват	15
2.2.1.3	Информация относно обработването и правата на субекта на данните.....	15
2.2.2	Разпоредби относно способите	15
2.2.2.1	Предоставяне на копие	16
2.2.2.2	Предоставяне на допълнителни копия	17
2.2.2.3	Предоставяне на информацията в широко използвана електронна форма.....	18
2.2.3	Възможно ограничение на правото на достъп	18
2.3	Общи принципи на правото на достъп.....	18
2.3.1	Пълнота на информацията.....	19
2.3.2	Точност на информацията	21
2.3.3	Времеви обхват на оценката	21
2.3.4	Спазване на изискванията за сигурност на данните	23
3	Общи съображения относно оценката на исканията за достъп.....	23
3.1	Въведение	23
3.1.1	Анализ на съдържанието на искането	24
3.1.2	Формат на искането.....	26
3.2	Идентифициране и удостоверяване на самоличността.....	28
3.3	Оценка на пропорционалността относно удостоверяване на самоличността на лицето, отправило искането.....	31
3.4	Искания, подадени чрез трети страни/пълномощници	34
3.4.1	Упражняване на правото на достъп от името на деца	35
3.4.2	Упражняване на правото на достъп чрез портали/канални, предоставени от трета страна	36
4	Обхват на правото на достъп и личните данни и информация, за които се отнася	36
4.1	Определение за лични данни	37
4.2	Личните данни, за които се отнася правото на достъп	41
4.2.1	„лични данни, свързани с него“	41
4.2.2	Лични данни, които „се обработват“	43
4.2.3	Обхватът на ново искане за достъп.....	44

4.3	Информация относно обработването и правата на субекта на данните.....	44
5	Как администратор може да предостави достъп?	48
5.1	Как администраторът може да извлече поисканите данни?	48
5.2	Необходими мерки за предоставяне на достъп	49
5.2.1	Предприемане на „необходими мерки“	49
5.2.2	Различни средства за предоставяне на достъп	51
5.2.3	Предоставяне на достъп в „кратка, прозрачна, разбираема и леснодостъпна форма, на ясен и прост език“	53
5.2.4	Голямото количество информация налага специфични изисквания за начина на нейното предоставяне	54
5.2.5	Формат.....	56
5.3	Срок за предоставянето на достъп.....	59
6	Рамки и ограничения на правото на достъп	60
6.1	Общи бележки	60
6.2	Член 15, параграф 4 от ОРЗД	61
6.3	Член 12, параграф 5 от ОРЗД	65
6.3.1	Какво означава явно неоснователно?	65
6.3.2	Какво означава „прекомерно“?	66
6.3.3	Последици	69
6.4	Възможни ограничения в правото на Съюза или в правото на държавите членки въз основа на член 23 от ОРЗД и дерогации	70
	Приложение — схема.....	71

Европейският комитет по защита на данните,

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

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

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

като има предвид, че подготвителната работа по тези насоки включваше събиране на данни от заинтересованите страни, както в писмена форма, така и на специално организирано събитие за заинтересованите страни относно правата на субектите на данни, с цел установяване на предизвикателствата и проблемите при тълкуването, възникнали при прилагането на съответните разпоредби на ОРЗД,

ПРИЕ СЛЕДНИТЕ НАСОКИ

1 ВЪВЕДЕНИЕ — ОБЩИ НАБЛЮДЕНИЯ

1. В съвременното общество личните данни се обработват от публични и частни субекти, по време на редица дейности, за широк кръг от цели и по много различни начини. Лицата често могат да бъдат в неблагоприятно положение, когато става въпрос за разбирането за начина, по който се обработват техните лични данни, включително използваната в конкретния случай технология, независимо дали данните се обработват от частен или от публичен субект. С цел да се защитят личните данни на физическите лица в тези ситуации с ОРЗД е създадена съгласувана и надеждна правна рамка, която обикновено се прилага по отношение на различни видове обработване, като включва и специфични разпоредби относно правата на субекта на данните.
2. Правото на достъп до личните данни е едно от правата на субектите на данни, предвидено в глава III от ОРЗД наред с други права, като например правото на коригиране и изтриване, правото на ограничаване на обработването, правото на преносимост, правото на възражение или правото на субекта да не бъде обект на автоматизирано вземане на индивидуални решения, включително профилиране². Правото на достъп на субекта на данните е залегнало както в Хартата на основните права на ЕС (Хартата)³, така и в член 15 от ОРЗД, където е точно формулирано като правото на достъп до лични данни и друга свързана информация.
3. Съгласно ОРЗД правото на достъп се състои от три компонента, а именно потвърждение дали се обработват лични данни, достъп до данните и информация за самото обработване. Субектът на

¹ Позоваванията на „държави(те) членки“ в настоящия документ следва да се разбират като позовавания на „държави(те) — членки на ЕИП“.

² Членове 15—22 от ОРЗД.

³ Съгласно член 8, параграф 1 от Хартата на основните права на Европейския съюз всеки има право на защита на неговите лични данни. Съгласно член 8, параграф 2, второ изречение всеки има право на достъп до събраните данни, отнасящи се до него, както и правото да изиска поправянето им.

данните може да получи и копие от обработваните лични данни, като се има предвид, че тази възможност не е допълнително право, а представлява способ за предоставяне на достъп до данните. Следователно, правото на достъп може да се разбира както като възможност за физическото лице да поиска информация от администратора дали се обработват лични данни, свързани с него, така за достъп до тези данни и тяхната проверка. При искане от страна на субекта на данните администраторът му предоставя информацията, попадаща в обхвата на член 15, параграфи 1 и 2 от ОРЗД.

4. Упражняването на правото на достъп се осъществява както в рамките на законодателството в областта на защитата на данните, в съответствие с целите на въпросното законодателство, така и по-конкретно в рамките на *„основните права и свободи на физическите лица, и по-специално тяхното право на защита на личните данни“*, както е изтъкнато в член 1, параграф 2 от ОРЗД. Правото на достъп е важен елемент от цялата система за защита на данните.
5. Практическата цел на правото на достъп е да се даде възможност на физическите лица да имат контрол върху собствените си лични данни⁴. За да се реализира тази цел ефективно на практика, с ОРЗД се цели улесняване на упражняването чрез редица гаранции, позволяващи на субекта на данните да упражнява това право лесно, без ненужни ограничения, на разумни интервали и без прекомерно забавяне или разходи. Всичко това следва да доведе до по-ефективно прилагане на правото на достъп на субекта на данните в цифровата ера, част от което в по-широк смисъл е и правото на субекта на данните да подаде жалба до надзорния орган и правото на ефективна съдебна защита⁵.
6. По отношение на развитието на правото на достъп, като част от правната рамка за защита на данните, следва да се подчертае, че то е елемент от европейската система за защита на данните от самото ѝ създаване. В сравнение с Директива 95/46/ЕО посоченият в ОРЗД стандарт за правата на субектите на данни е едновременно прецизиран и укрепен; това важи и за правото на достъп. Тъй като условията и способите за упражняване на правото на достъп вече са по-точно определени в ОРЗД, това право е представено по по-съдържателен начин и от гледна точка на правната сигурност както за физическото лице, така и за администратора. Освен това конкретната формулировка на член 15 и точният срок за предоставянето на данните съгласно член 12, параграф 3 от ОРЗД задължават администратора да бъде подготвен за запитвания от субекти на данни чрез разработването на процедури за обработване на искания.
7. Правото на достъп не следва да се разглежда изолирано, тъй като то е тясно свързано с други разпоредби на ОРЗД, по-специално с принципите за защита на данните, включително добросъвестността и законосъобразността на обработването, задължението за прозрачност на администратора и с други права на субекта на данните, предвидени в глава III от ОРЗД.
8. В рамките на правата на лицата е важно да се подчертае и значението на член 12 от ОРЗД, в който се определят изискванията за необходимите мерки, приети от администратора при предоставяне на информацията, посочена в членове 13 и 14 от ОРЗД, и начините на комуникация, посочени в членове 15—22 и член 34 от ОРЗД; с тези изисквания обикновено се определят формата, начинът и срокът за отговорите до субекта на данните и по-специално за всяка информация, насочена към дете.
9. ЕКЗД счита за необходимо да се предоставят по-точни насоки относно начина на прилагане на правото на достъп в различни ситуации. Настоящите насоки са предназначени да анализират

⁴ Вж. съображения 7, 68, 75 и 85 от ОРЗД.

⁵ Вж. глава VIII, членове 77, 78 и 79 от ОРЗД.

различните аспекти от правото на достъп. По-конкретно, целта на раздела, следващ по-долу, е да се предоставят общ преглед и обяснение на съдържанието на член 15, докато в следващите раздели се предоставя по-задълбочен анализ на най-честите практически въпроси и проблеми, свързани с прилагането на правото на достъп.

2 ЦЕЛ НА ПРАВОТО НА ДОСТЪП, СТРУКТУРА НА ЧЛЕН 15 ОТ ОРЗД И ОБЩИ ПРИНЦИПИ

2.1 Цел на правото на достъп

10. В този смисъл предназначението на правото на достъп е да се даде възможност на физическите лица да имат контрол върху личните данни, свързани с тях, тъй като им се позволява „да бъдат осведомени за обработването и да проверяват законосъобразността му“⁶. По-конкретно, целта на правото на достъп е да се даде възможност на субектите на данни да разберат как се обработват техните лични данни, както и последиците от това обработване, и да проверят точността на обработваните данни, без да се налага да обосновават своето намерение. С други думи, целта на правото на достъп е предоставянето на лицата на достатъчна, прозрачна и леснодостъпна информация за обработването на данните, независимо от използваните технологии, и на възможност за проверка на различни аспекти на конкретна дейност по обработване съгласно ОРЗД (например законосъобразност, точност).
11. Предоставеното в настоящите насоки тълкуване на ОРЗД се основава на установената досега съдебна практика на Съда на Европейския съюз (Съда на ЕС). Като се има предвид значението на правото на достъп, може да се очаква свързаната с него съдебна практика да се развие значително в бъдеще.
12. В съответствие с решенията на Съда на ЕС⁷ правото на достъп има за цел да се гарантира защитата на правото на субектите на данни на неприкосновеност на личния живот и защитата на данните по отношение на обработването на свързани с тях данни⁸ и може да улесни упражняването на произтичащите от него права, например членове 16—19, 21—22 и член 82 от ОРЗД. Упражняването на правото на достъп обаче е индивидуално право и не зависи от упражняването на тези други права, както и на другите права не зависи от упражняването на правото на достъп.
13. Предвид широкообхватната цел на правото на достъп не е подходящо тя да бъде анализирана като предпоставка за упражняването на това право от администратора като част от оценката му на исканията за достъп. Следователно, администраторите не следва да оценяват „защо“ субектът на данните иска достъп, а само „какво“ иска субектът на данните (вж. раздел 3 относно анализа на искането) и дали притежават лични данни, свързани с това лице (вж. раздел 4). Поради това администраторът не следва например да отказва достъп на основание или заради подозрения, че исканите данни може да бъдат използвани от субекта на данните, за да се защити в съда в случай на уволнение или търговски спор с администратора⁹. Относно рамките и ограниченията на правото на достъп, моля, вж. раздел 6.

Пример 1: Работодател уволнява дадено лице. Една седмица по-късно лицето решава да събере доказателства, за да заведе срещу бившия си работодател дело за неправомерно уволнение. С оглед на това лицето пише на бившия си работодател, като иска достъп до всички лични данни,

⁶ Съображение 63 от ОРЗД.

⁷ Съд на ЕС, С-434/16, Nowak, и съединени дела С-141/12 и С-372/12, YS и др.

⁸ Съд на ЕС, С-434/16, Nowak, т. 56.

⁹ Свързаните с тази тема въпроси са предмет на дело, което понастоящем очаква решение пред Съда на ЕС (С-307/22).

свързани с него като субект на данни, които бившият работодател обработва в качеството си на администратор.

Администраторът не оценява намерението на субекта на данните, а от лицето не се изисква да посочва на администратора причината за искането си. Следователно, ако искането отговаря на всички други изисквания (вж. раздел 3), администраторът трябва да се съобрази с искането, освен ако искането се окаже явно неоснователно или прекомерно в съответствие с член 12, параграф 5 от ОРЗД (вж. раздел 6.3), което администраторът е задължен да докаже.

Разновидност: В хода на делото субектът на данните упражнява правото на достъп по отношение на личните данни, свързани с него. В националното право на държавата членка, с което се уреждат трудовите правоотношения между администратора и физическото лице, се съдържат обаче някои разпоредби, с които се ограничава обхватът на информацията, която трябва да се предоставя или обменя между страните по текущо или предстоящо съдебно производство, и които са приложими по отношение на заведеното от субекта на данни дело за неправомерно уволнение. В този случай и при условие че тези национални разпоредби отговарят на изискванията, произтичащи от член 23 от ОРЗД¹⁰, субектът на данните няма право да получава от администратора информация, която надвишава предвидената в разпоредбите на националното право на държавата членка, уреждащи обмена на информация между страните по правни спорове.

14. Въпреки че целта на правото на достъп е широкообхватна, Съдът на ЕС представя нагледно и границите на обхвата на законодателството в областта на защитата на данните и правото на достъп. Например, Съдът на ЕС установи, че целта на правото на достъп, гарантирано в законодателството на ЕС в областта на защитата на данните, трябва да се разграничава от тази на правото на достъп до публични документи, установено в законодателството на ЕС и националното законодателство, като последното цели да осигури „прозрачност на процеса на взимане на решения от публичните органи и да насърчава добрите административни практики“¹¹ — цел, която не е преследвана от законодателството в областта на защитата на данните. Съдът на ЕС стига до заключението, че правото на достъп до лични данни се прилага независимо от това дали се прилага различен вид право на достъп с различна цел, като например в рамките на процедурата по разглеждане.

2.2 Структура на член 15 от ОРЗД

15. С цел да се отговори на искане за достъп и да се гарантира, че нито един от неговите аспекти не може да бъде пренебрегнат, е необходимо първо да се разберат структурата на член 15 и съставните елементи на правото на достъп по този член.
16. Член 15 може да бъде разделен на осем различни елементи, които са изброени в таблицата по-долу:

1.	Потвърждение дали администраторът обработва лични данни, свързани с лицето, отправило искането	член 15, параграф 1, първа част на изречението
----	--	--

¹⁰ Насоки 10/2020 на Европейския комитет по защита на данните относно ограниченията по член 23 от ОРЗД, версия за обществена консултация, 18 декември 2020 г.

¹¹ Съд на ЕС, съединени дела C-141/12 и C-372/12, YS и др., т. 47.

2.	Достъп до личните данни, свързани с лицето, отпредило искането	Член 15, параграф 1, втора част на изречението (първа част)
3.	Достъп до следната информация относно обработването: а) целите на обработването; б) съответните категории лични данни; в) получателите или категориите получатели; г) предвидения срок, за който ще се обработват личните данни или критериите, използвани за определянето на продължителността; д) съществуването на права на коригиране, изтриване, ограничаване на обработването и възражение срещу обработването; е) правото на жалба до надзорен орган; ж) всяка налична информация относно източника на данни, ако те не са събрани от субекта на данните; з) съществуването на автоматизирано вземане на решения, включително профилиране и друга информация, свързана с това.	Член 15, параграф 1, втора част на изречението (втора част)
4.	Информация относно гаранциите по член 46, когато личните данни се предават на трета държава или на международна организация	Член 15, параграф 2
5.	Задължението на администратора да предоставя копие от личните данни, които са в процес на обработване	Член 15, параграф 3, първо изречение
6.	Налагане на разумна такса от администратора въз основа на административните разходи за допълнителни копия, поискани от субекта на данните	Член 15, параграф 3, второ изречение
7.	Предоставяне на информация в електронна форма	Член 15, параграф 3, трето изречение
8.	Вземането предвид на правата и свободите на други лица	Член 15, параграф 4

Макар че заедно всички елементи на член 15, параграфи 1 и 2 определят съдържанието на правото на достъп, в член 15, параграф 3 се разглеждат способите за достъп в допълнение към общите условия, определени в член 12 от ОРЗД. С член 15, параграф 4 се допълват предвидените в член 12, параграф 5 от ОРЗД рамки и ограничения за всички права на субекта на данните, с конкретен акцент върху правата и свободите на други лица при предоставяне на достъпа.

2.2.1 Определяне на съдържанието на правото на достъп

17. В член 15, параграфи 1 и 2 се съдържат следните три аспекта: първо, потвърдението дали личните данни на лицето, отпредило искането, се обработват, и ако това е така — второ, достъпа до тези данни, и трето, информация относно обработването. Те могат да се разглеждат като три различни компонента, които заедно изграждат правото на достъп.

2.2.1.1 Потвърждение „дали“ личните данни се обработват

18. Първото нещо, което субектите на данни трябва да знаят при подаване на искане за достъп до лични данни, е дали администраторът обработва данни, свързани с тях. Следователно тази информация съставлява първия компонент на правото на достъп по член 15, параграф 1. Когато администраторът не обработва лични данни, свързани с отправилния искането за достъп субект на данни, информацията, която трябва да бъде предоставена, ще бъде ограничена до потвърждение, че не се обработват лични данни, свързани с физическото лице. Когато администраторът обработва данни, свързани с лицето, отправило искането, той трябва да потвърди този факт пред въпросното лице. Това потвърждение може да бъде съобщено отделно или може да бъде включено като част от информацията относно обработваните лични данни (вж. по-долу).

2.2.1.2 Достъп до личните данни, които се обработват

19. Достъпът до лични данни е вторият компонент на правото на достъп по член 15, параграф 1 и представлява същността на това право. Той е свързан с понятието за лични данни, съгласно определението в член 4, точка 1 от ОРЗД. Освен основните лични данни, като име и адрес, в обхвата на това определение може да попаднат неограничено разнообразие от данни, при условие че попадат в материалния обхват на ОРЗД, особено по отношение на начина, по който се обработват (член 2 от ОРЗД). В настоящия случай достъп до лични данни означава достъп до самите лични данни, а не само общо описание на данните, нито просто позоваване на обработваните от администратора категории лични данни. Ако не се прилагат рамки или ограничения¹², субектите на данни имат право на достъп до всички обработени данни, свързани с тях, или до части от данните, в зависимост от обхвата на искането (вж. раздел 2.3.1). Задължението за предоставяне на достъп до данните не зависи от вида или източника на тези данни. То се прилага изцяло дори в случаите, когато лицето, отправило искането, е предоставило първоначално данните на администратора, тъй като с него се цели уведомяване на субекта на данните за действителното обработване на тези данни от администратора. Обхватът на личните данни съгласно член 15 е разяснен по-подробно в раздели 4.1 и 4.2.

2.2.1.3 Информация относно обработването и правата на субекта на данните

20. Третият компонент на правото на достъп е информацията относно обработването и правата на субектите на данни, която администраторът трябва да предостави съгласно член 15, параграф 1, букви а—з) и член 15, параграф 2. Тази информация може да се основава текст, взет например от декларацията за поверителност на администратора¹³ или от регистъра му на дейностите по обработване, посочен в член 30 от ОРЗД, но може да се наложи да бъде актуализирана или съобразена с искането на субекта на данните. Съдържанието и степента на конкретизация на информацията са разгледани по-подробно в раздел 4.3.

2.2.2 Разпоредби относно способите

21. С член 15, параграф 3 изискванията във връзка със способите за отговор на искания за достъп по член 12 от ОРЗД се допълват с някои специфики, свързани с исканията за достъп.

¹² Вж. раздел 6 от настоящите насоки.

¹³ Вж. за информация във връзка с това — Работна група по член 29, РД 260 ред.01, 11 април 2018 г., Насоки относно прозрачността съгласно Регламент 2016/679 — одобрени от ЕКЗД (наричани по-нататък „Насоки на РГ по член 29 относно прозрачността — одобрени от ЕКЗД“).

2.2.2.1 Предоставяне на копие

22. Съгласно член 15, параграф 3, първо изречение от ОРЗД администраторът предоставя безплатно копие от личните данни, с които е свързано обработването. Следователно, копието се отнася само до втория компонент на правото на достъп („достъп до обработваните лични данни“, вж. по-горе). Администраторът трябва да гарантира, че първото копие е безплатно, дори когато счита, че разходите за възпроизвеждане са високи (пример: разходите за предоставяне на копие от записа на телефонен разговор).
23. Задължението за предоставяне на копие не се разбира като допълнително право на субекта на данните, а като способ за предоставяне на достъп до данните. С него се укрепва правото на достъп до данните¹⁴ и се спомага за тълкуването на това право, тъй като се разяснява, че достъпът до данните съгласно член 15, параграф 1 включва пълна информация за всички данни и не може да се разбира като предоставяне единствено на обобщение на данните. В същото време задължението за предоставяне на копие не предвижда разширяване на обхвата на правото на достъп: то се отнася (само) до копие от личните данни, които са в процес на обработване, а не непременно до възпроизвеждането на първоначалните документи (вж. раздел 5, т. 152). Най-общо казано, няма допълнителна информация, която да трябва да бъде предоставена на субекта на данните при предоставяне на копие: обхватът на информацията, която трябва да се съдържа в копието, представлява обхватът на достъпа до данните съгласно член 15, параграф 1 (втори компонент на правото на достъп, както е посочено по-горе, вж. параграф 19), който включва цялата информация, необходима за субекта на данни, за да може да разбира и проверява законосъобразността на обработването¹⁵.
24. С оглед на горепосоченото, ако достъпът до данни по смисъла на член 15, параграф 1 се осигурява чрез предоставяне на копие, е спазено задължението за това съгласно член 15, параграф 3. Задължението за предоставяне на копие служи за упражняване на правото на достъп и цели да се позволи на субекта на данните да бъде запознат и да провери законосъобразността на обработването (съображение 63). За да бъдат постигнати тези цели, в повечето случаи субектът на данните ще трябва да разглежда информацията не само временно. Следователно субектът на данни ще трябва да получи достъп до информацията чрез получаване на копие от личните данни.
25. С оглед на горепосоченото, понятието копие трябва да се тълкува в широк смисъл и да включва различните видове достъп до лични данни, стига той да е пълнен (т.е. да включва всички поискани лични данни) и за субекта на данните да е възможно да го запази. Следователно, изискването за предоставяне на копие означава, че информацията за личните данни на лицето, което подава искането, му се предоставя по начин, който му позволява да запази цялата информация и да се върне към нея.
26. Въпреки това при някои обстоятелства може да бъдат подходящи други способности предвид широко разбиране за копие и използването му като основен способ за предоставяне на достъп. Допълнителни обяснения относно копията и други способности за предоставяне на достъп са дадени в раздел 5, по-специално в точки 5.2.2—5.2.5.

¹⁴ Задължението за предоставяне на копие не беше посочено в Директива 95/46/ЕО относно защитата на данните.

¹⁵ Свързаните с темата на този параграф въпроси са предмет на дело, което понастоящем очаква решение пред Съда на ЕС (C-487/21)

2.2.2.2 Предоставяне на допълнителни копия

27. Член 15, параграф 3, второ изречение се отнася до ситуации, в които субектът на данни иска от администратора повече от едно копие, например в случай, че е загубил или повредил първото копие или ако желае да предаде копие на друго лице или надзорен орган. С оглед на това, че допълнителни копия трябва да бъдат предоставени от администратора по искане на субекта на данните, в член 15, параграф 3 се постановява, че за всяко поискано допълнително копие, администраторът може да наложи разумна такса въз основа на административните разходи (член 15, параграф 3, второ изречение).
28. Ако физическото лице поиска допълнително копие след подаване на първото искане, може да възникнат въпроси дали това следва да се счита за ново искане или дали искането за допълнително копие от данните е направено по смисъла на член 15, параграф 3, второ изречение, в който случай може да бъде наложена такса. Отговорът на тези въпроси зависи единствено от съдържанието на искането: то следва да се разбира като искане за допълнително копие доколкото по време и обхват се отнася до същото обработване на лични данни като предишното. Ако обаче субектът на данните има за цел да получи информация за данните, обработвани в различен момент от време или отнасящи се до различен набор от данни от първоначално поискания, се прилага отново правото на получаване на безплатно копие съгласно член 15, параграф 3. Това е валидно и в случаите, когато субектът на данните е подал първото искане малко преди това. Физическото лице може да упражни правото си на достъп чрез последващо искане и да получи безплатно копие, освен ако искането се счита за прекомерно съгласно член 12, параграф 5, с възможност за налагане на разумна такса съгласно член 12, параграф 5, буква а) (относно прекомерния характер на повтарящи се искания, вж. раздел 6).

Пример 2: Потребител подава искане за достъп до търговско дружество. Една година след отговора на дружеството същият потребител подава искане за достъп съгласно член 15 до същото дружество. Независимо от това дали след предходното искане между страните е имало нови търговски сделки или други контакти, това второ искане трябва да се счита за ново искане. Дори и да не е настъпила промяна в обработваните от дружеството данни — което не е непременно очевидно за субекта на данните — лицето има право да получи безплатно копие от данните.

Разновидност 1: Дори клиентът в горепосочените случаи да подаде ново искане, например само една седмица след първото искане, това може да се счита за ново искане по член 15, параграфи 1 и 3, първо изречение, ако не трябва да се тълкува като просто напомняне за първото искане. Що се отнася до краткия интервал и зависимост от специфичните обстоятелства на новото искане, неговата прекомерност съгласно член 12, параграф 5 е спорна (вж. раздел 6).

Разновидност 2: Искането за „ново копие“ от информацията, която вече е била предоставена под формата на копие в отговор на предишно искане, например в случай, че клиентът е загубил полученото преди това копие, следва, разбира се, да се разглежда като искане за допълнително копие, тъй като се отнася до предишното искане по обхват и време на обработването.

29. Ако субектът на данните повтори първо искане за достъп на основание, че полученият отговор не е пълен или че не са посочени причини за отказа, това искане не трябва да се счита за ново искане, тъй като то е просто напомняне за първо неудовлетворено искане.
30. Относно разпределението на разходите в случаи на искания за допълнително копие, с член 15, параграф 3 се установява, че администраторът може да наложи разумна такса въз основа на административните разходи, породени от искането. Това означава, че административните разходи са решаващ критерий за определяне на размера на таксата. В същото време таксата

следва да бъде подходяща, като се взема предвид значението на правото на достъп като основно право на субекта на данните. Администраторът не следва да прехвърля режийни разходи или други общи разходи на субекта на данните, а трябва да се съсредоточи върху конкретните разходи, породени от предоставянето на допълнителното копие. При организирането на този процес администраторът следва да използва ефикасно своите човешки и материални ресурси с цел да поддържа ниски разходите за копиране, включително ако той използва външна подкрепа.

31. В случай че администраторът реши да наложи такса, той следва да посочи предварително, че такава ще бъде наложена, както и възможно най-точната сума на разходите, които планира да начисли на субекта на данните, с цел да се даде възможност на лицето да реши дали да запази или да оттегли искането.

2.2.2.3 Предоставяне на информацията в широко използвана електронна форма

32. В случай на подаване на искане с електронни средства, по възможност и освен ако субектът на данни не е поискал друго, информацията се предоставя с електронни средства (член 12, параграф 3 от ОРЗД). По отношение на исканията за достъп, това изискване се допълва с член 15, параграф 3, трето изречение, който гласи, че администраторът е задължен и да предостави отговора в широко използвана електронна форма, освен ако субектът на данни не е поискал друго. С член 15, параграф 3 се предполага, че администратори, които са в състояние да получават електронни искания, ще могат да предоставят отговора на искането в широко използвана електронна форма (за подробности, вж. раздел 5.2.5). Тази разпоредба се отнася до цялата информация, която трябва да бъде предоставена в съответствие с член 15, параграфи 1 и 2. Следователно, ако субектът на данни подаде искането за достъп с електронни средства, цялата информация трябва да бъде предоставена в широко използвана електронна форма. Въпросите за формата са доразвити в раздел 5. Администраторът следва, както винаги, да въведе подходящи мерки за сигурност, по-специално, когато работи със специална категория лични данни (вж. по-долу под т. 2.3.4).

2.2.3 Възможно ограничение на правото на достъп

33. Накрая, по отношение на правото на достъп, в член 15, параграф 4 е предвидено конкретно ограничение. То гласи, че трябва да бъдат взети предвид възможни неблагоприятни въздействия върху правата и свободите на други лица. В раздел 6 са разяснени въпроси, свързани с обхвата и последиците от това ограничение, както и с допълнителните рамки и ограничения, определени в член 12, параграф 5 от ОРЗД или съгласно член 23 от ОРЗД.

2.3 Общи принципи на правото на достъп

34. По принцип, когато субектите на данни подадат искане за достъп до своите данни, посочената в член 15 от ОРЗД информация винаги трябва да се предоставя изцяло. Съответно, когато администраторът обработва данни, свързани с физическите лица, той предоставя цялата информация, посочена в член 15, параграф 1 и, при целесъобразност, информацията, посочена в член 15, параграф 2. Администраторът трябва да предприеме подходящите мерки, за да гарантира, че информацията е пълна, точна и актуална, съответстваща във възможно най-голяма степен на състоянието на обработването на данните в момента на получаването на искането¹⁶. Когато двама или повече администратори съвместно обработват данни, договореността на

¹⁶ За Насоки относно подходящите мерки вж. раздел 5, т. 123—129

съвместните администратори относно съответните им отговорности по отношение на упражняването на правата на субекта на данните, особено относно отговорът на искания за достъп, не засяга правата на субектите на данни спрямо администратора, към когото отправят искането си¹⁷.

2.3.1 Пълнота на информацията

35. Субектите на данни имат право да получат, заедно с посочените по-долу изключения, пълно разкриване на всички данни, свързани с тях (за подробности относно обхвата вж. раздел 4.2). Освен ако е изрично поискано друго от физическото лице, искането за упражняване на правото на достъп се разбира в общ смисъл като обхващащо всички лични данни, свързани със субекта на данните¹⁸. Ограничаване на достъпа до част от информацията може да се обмисли в следните случаи:
- а) субектът на данните изрично е ограничил искането до подкатегория. С цел да се избегне предоставянето на непълна информация, администраторът може да разгледа това ограничение на искането само ако може да бъде сигурен, че това тълкуване съответства на желанието на лицето (за допълнителни подробности, вж. раздел 3.1.1, т. 51). По принцип, субектът на данните не трябва да повтаря искането за предаването на всички данни, които има право да получи.
 - б) В ситуации, в които администраторът обработва голямо количество данни относно субекта на данните, той може да има съмнения дали искането за достъп, което е формулирано много общо, действително има за цел получаването на информация за всички видове данни, които се обработват, или подробна информация за всички отрасли на дейност на администратора. Съмнения може да възникнат по-специално в ситуации, в които не е налице възможност за предоставяне на физическото лице на инструменти за уточняване на неговото искане от самото начало, или когато той не ги е използвал. Впоследствие администраторът е изправен пред проблеми във връзка с начина на предоставяне на пълен отговор, като същевременно избягва създаването на прекомерна по обем информация за субекта на данните, от която той не се интересува и която не може да обработва ефективно. В зависимост от обстоятелствата и техническите възможности може да са налице начини за решаване на този проблем, например чрез предоставяне на онлайн инструменти за самообслужване (вж. раздел 5 за многослойния подход). Ако такива решения не са приложими, администратор, който обработва голямо количество информация, свързана със субекта на данните, може да поиска от него да посочи точно информацията или обработването, за които се отнася искането, преди да бъде предадена информацията (вж. съображение 63 от ОРЗД). Примерите за това могат да включват дружество с няколко области на дейност или публичен орган с различни административни звена, ако администраторът установи, че в тези клонове се обработват множество данни, свързани със субекта на данните. В допълнение голямо количество данни може да бъде обработвано от администратори, които събират данни относно чести дейности на физическото лице за продължителен период от време.

Пример 3: Публичен орган обработва данни относно субекта на данните в редица различни отдели, отнасящи се до различни аспекти. Управлението и съхраняването на досиета се обработват частично с неавтоматични средства и повечето от данните се съхраняват само в досиета на хартиен носител. Предвид общата формулировка на искането, публичният орган

¹⁷ Насоки 07/2020 на ЕКЗД относно понятията „администратор“ и „обработващ лични данни“ в ОРЗД, т. 162, буква е). Обработващият лични данни трябва да подпомага администратора, пак там, т. 129

¹⁸ За повече подробности, моля, вж. раздел 5.2.3 по-долу относно темата за многослойния подход.

изразява съмнение дали субектът на данните е запознат с обхвата на искането, по-специално с разнообразието от операции по обработване, които то ще обхване, количеството информация и броя страници, които лицето ще получи.

Пример 4: Голямо застрахователно дружество получава искане за общ достъп с писмо от лице, което е клиент от много години. Въпреки пълното спазване на сроковете за заличаване, дружеството всъщност обработва огромно количество данни, отнасящи се до клиента, тъй като обработването все още е необходимо за изпълнение на договорни задължения, произтичащи от договорните отношения с клиента (включително например продължаващи задължения, комуникация по спорни въпроси с клиента и с трети страни, ...) или за спазване на законови задължения (архивирани данни, които трябва да се съхраняват за данъчни цели и др.). Застрахователното дружество може да има съмнения дали искането, което е формулирано много общо, действително има за цел да обхване всички видове от тези данни. Това може да бъде особено проблематично, ако застрахователното дружество разполага само с пощенски адрес на субекта на данните и следователно трябва да изпраща всяка информация на хартиен носител. Въпреки това същите съмнения могат да бъдат от значение и при предоставяне на информацията по друг начин.

Ако в такива случаи администраторът реши да поиска от субекта на данните да уточни искането, за да изпълни задължението си и да съдейства за упражняването на правото на достъп (член 12, параграф 2 от ОРЗД), едновременно с това той предоставя значима информация за своите операции по обработване, които биха могли да засягат лицето, като информира за съответните клонове на своите дейности, бази данни и др.

Пример 5: При трудово правоотношение, в случай на общо формулиране на искането за достъп, не е ясно само по себе си, че служителят иска да получи всички потребителски данни за влизане, данни за достъп до работното място, данни относно местата в столовата, данни относно плащането на заплати и др. Така например отправено от работодателя искане за доуточнение може да доведе до разяснението, че интересът на служителя се свежда до това да разбере или провери на кого е предадена оценката за неговата работа. Без искане за уточнение служителят ще получи голямо количество данни, без да се интересува от повечето от тях. В същото време работодателят ще трябва да предостави информация за различните видове контекст на обработването, които биха засегнали служителя, с цел да му предостави възможност да уточни в разумна степен искането.

Важно е да се подчертае, че искането за уточнение не цели ограничаване на отговора на искането за достъп и не се използва за скриване на каквато и да е информация относно данните или обработването, свързани със субекта на данните. Ако физическото лице, от което е поискано да уточни обхвата на своето искане, потвърди, че търси всички лични данни, свързани с него, администраторът, разбира се, трябва да ги предостави в пълен обем.

При всички случаи администраторът следва винаги да е в състояние да докаже, че начинът на обработване на искането цели най-широкото упражняване на правото на достъп и е в съответствие със задължението му да съдейства за упражняването на правата на субектите на данни (член 12, параграф 2 от ОРЗД). При спазване на тези принципи администраторът може да изчака отговора на лицето, преди да му предостави допълнителни данни според неговото желание, ако е предоставил на субекта на данните ясен преглед на всички операции по обработване, които биха могли да са свързани със субекта на данните, включващи по-специално тези, които той може да не е очаквал, ако също така е предоставил достъп до всички данни,

които са цел на лицето, и ако освен това тази информация е била комбинирана с ясно указание за начина на получаване на достъп до останалите части от обработваните данни.

- в) Прилагат се изключения или ограничения на правото на достъп (вж. по-долу в раздел 6). В такива случаи администраторът следва внимателно да провери за кои части от информацията се отнася изключението и да предостави цялата информация, която е допустима съгласно изключението. Например потвърждението за обработването на самите лични данни (компонент 1) не може да бъде засегнато от изключението. В резултат на това трябва да бъде предоставена информация за всички лични данни и цялата информация, посочена в член 15, параграфи 1 и 2, която не е засегната от изключението или ограничението.

2.3.2 Точност на информацията

36. Включената в копието от личните данни информация, която се предоставя на субекта на данните, трябва да съдържа действително притежаваната информация или лични данни за лицето. Това включва задължението за предоставяне на информация за данни, които са неточни, или за обработване на данни, което не е или вече не е законосъобразно. Субектът на данните може например да използва правото на достъп, за да установи източника на неточни данни, които се разпространяват между различни администратори. Ако администраторът коригира неточни данни, преди да информира субекта на данните за това, лицето ще бъде лишено от тази възможност. Същото важи и в случай на незаконосъобразно обработване. Възможността да се знае за незаконосъобразно обработване, свързано със субекта на данните, представлява една от основните цели на правото на достъп. Задължението за информиране за непромененото състояние на обработването не засяга задължението на администратора да прекрати незаконосъобразно обработване или да коригира неточни данни. По-долу са представени отговорите на въпросите относно реда, в който трябва да бъдат изпълнени тези задължения.

2.3.3 Времеви обхват на оценката

37. Оценката на обработваните данни отразява възможно най-близко ситуацията, в която администраторът получава искането, и отговорът следва да обхваща всички налични данни към този момент. Това означава, че администраторът трябва да се опита да установи без ненужно забавяне всички дейности по обработване на данни, свързани със субекта на данните. Следователно, администраторите не са задължени да предоставят лични данни, които са обработвали в миналото, но с които вече не разполагат¹⁹. Например администраторът може да е заличил лични данни в съответствие с политиката си за съхраняване на данните и/или законови разпоредби и следователно може повече да не е в състояние да предостави исканите лични данни. В този смисъл следва да се припомни, че периодът от време, за който се съхраняват данните, следва да се определи в съответствие с член 5, параграф 1, буква д) от ОРЗД, тъй като всяко съхраняване на данни трябва да бъде обективно оправдано.
38. В същото време администраторът предприема предварително необходимите мерки, за да съдейства за упражняването на правото на достъп и да се справи с такива искания възможно

¹⁹ За тази цел вж. допълнителните разяснения в раздел 4 от настоящите насоки, както и в решението на Съда на Европейския съюз от 7 май 2009 г. по дело C-553/07, *College van burgemeester en wethouders van Rotterdam/M. E. E. Rijkeboer*, относно правото на достъп до информация относно получателите или категориите получатели за минал момент.

най-скоро (вж. член 12, параграф 3) и преди данните да трябва да бъдат заличени. Следователно, в случай на кратки срокове на съхраняване, предприетите мерки в отговор на искането следва да се адаптират към подходящия срок на съхраняване с цел да се улесни упражняването на правото на достъп и да се избегне постоянната невъзможност за предоставяне на достъп до данните, обработвани в момента на искането²⁰. Въпреки това в някои случаи може да не е възможно да се отговори на искането преди момента, в който е планирано заличаването на данните. Например, ако при искане, на което трябва да се отговори възможно най-бързо, администратор извлича лични данни, които е планирано да бъдат заличени на следващия ден, той може да се нуждае от повече време, за да прецени дали преди да се предостави копие на лицето, отправилото искането, трябва да се направят редакции, за да защитят свободите на други лица. Ако данните са извлечени в рамките на планирания срок на съхраняване, администраторът може да продължи да обработва тези данни с цел да изпълни задължението си да отговори на искането. В тези случаи обработването може да се основава на член 6, параграф 1, буква в), заедно с член 15 от ОРЗД, и неговата продължителност трябва да е в съответствие с изискванията на член 12, параграф 3 от ОРЗД²¹. Прилагането на това правно основание е ограничено до обработването на данните, установени като необходими за отговор на конкретното искане и не трябва да се използва като обосновка за общо удължаване на сроковете на съхраняване.

39. Освен това администраторът не избягва умишлено задължението да предостави поисканите лични данни, като изтрива или променя личните данни в отговор на искане за достъп (вж. 2.3.2). Ако в хода на обработването на искане за достъп администраторът установи неточни данни или незаконосъобразно обработване, той трябва да оцени състоянието на обработването и съответно да уведоми субекта на данните преди да изпълни останалите си задължения. В свой собствен интерес, с цел да избегне необходимостта от по-нататъшна комуникация по този въпрос, както и за да е в съответствие с принципа на прозрачност, администраторът следва да добави информация за последващите корекции или заличавания.

Пример 6: При отговор на искане за достъп администратор разбира, че кандидатура, подадена от субекта на данните за свободно работно място в дружеството на администратора, е била съхранявана след изтичане на срока на съхраняване. В този случай администраторът не може първо да заличи данните и след това да отговори на субекта на данни, че не се обработват данни (относно кандидатурата). Необходимо е първо да предостави достъп и след това да заличи данните. За да се избегне последващо искане за изтриване, би било препоръчително да се добави информация във връзка с това, както и часа на заличаване.

С цел спазване на принципа на прозрачност, администраторите следва да уведомят субекта на данните за конкретния момент на обработването, за което се отнася отговорът на администратора. В някои случаи, например при чести контакти, може да се стигне до допълнително обработване или изменения на данните между този времеви обхват, в рамките на който е оценено обработването, и отговора на администратора. Ако администраторът е запознат с такива промени, се препоръчва да включи информация за тях, както и за допълнителното обработване, необходимо за да се отговори на искането.

²⁰ Например, използването на инструмент за самообслужване дава на субекта на данните възможност за лесен достъп до поисканите лични данни, а с цел да се улесни бързото действие може да се обмисли въвеждането на система за уведомяване, която да сигнализира на администратора за искане, свързано с лични данни с кратък срок на съхраняване.

²¹ Това не засяга последващото обработване на данни за доказателствени цели във връзка с обработването на искане за достъп за подходящ период от време.

2.3.4 Спазване на изискванията за сигурност на данните

40. Тъй като съобщаването и предоставянето на лични данни на субекта на данните представлява процес по обработване, администраторът винаги е задължен да прилага подходящи технически и организационни мерки, за да гарантира ниво на сигурност, което е подходящо спрямо риска от обработването (вж. член 5, параграф 1, буква е), член 24 и член 32 от ОРЗД). Това се прилага независимо от условието, при което се предоставя достъпа. В случай на предаване на данните на субекта на данните в неелектронен вид, администраторът може да обмисли използването на препоръчана поща или, алтернативно, да предложи, но не и да задължи субекта на данните, да вземе досието срещу подпис директно от някое от учрежденията на администратора, в зависимост от рисковете, породени от обработването. Ако в съответствие с член 12, параграфи 1 и 3, информацията се предоставя с електронни средства, администраторът избира тези от тях, които отговарят на изискванията за сигурност на данните. Също така в случай на предоставяне на копие от данните в широко използвана електронна форма (вж. член 15, параграф 3), при избиране на средствата за предаване на електронното досие на субекта на данните, администраторът взема предвид изискванията за сигурност на данните. Това може да включва прилагане на криптиране, защита с парола и др. За да се улесни достъпът до криптираните данни, администраторът трябва също така да гарантира, че е предоставена подходяща информация, така че субектът на данните да има достъп до декриптираната информация. В случаите, когато изискванията за сигурност на данните биха наложили криптиране от край до край на електронната поща, но администраторът би могъл да изпрати само стандартно писмо по електронната поща, той ще трябва да използва други средства, като например изпращане на USB устройство чрез (препоръчано) писмо по пощата до субекта на данните.

3 ОБЩИ СЪОБРАЖЕНИЯ ОТНОСНО ОЦЕНКАТА НА ИСКАНИЯТА ЗА ДОСТЪП

3.1 Въведение

41. При получаване на искания за достъп до лични данни, администраторът трябва да оцени всяко искане индивидуално. Той взема предвид, наред с другото, следните въпроси, които са доразвити в следващите параграфи: дали искането се отнася за лични данни, свързани с лицето, отправило искането, и кое е това лице. Този раздел има за цел да се изясни какви елементи от искането за достъп следва да бъдат взети предвид от администратора при неговата оценка, и да се обсъдят възможните сценарии за такава оценка, както и последствията от нея. При преценка на искане за достъп до лични данни администраторът взема предвид задължението съгласно член 12, параграф 2 от ОРЗД да съдейства за упражняването на правата на субекта на данните, като същевременно не забравя подходящата степен на сигурност на личните данни²².

²² Администраторът гарантира подходяща степен на сигурност на личните данни в съответствие с принципа на цялостност и поверителност (член 5, параграф 1, буква е) от ОРЗД), като прилага подходящите технически и организационни мерки, посочени в член 32 от ОРЗД и разгледани в член 24 от ОРЗД. Администраторът трябва да е в състояние да докаже, че осигурява адекватно ниво на защита на данните в съответствие с принципа на отчетност (вж. също: Становище 3/2010 на Работната група по член 29 относно принципа на отчетност, прието на 13 юли 2010 г., 00062/10/EN РД 173 и Насоки № 07/2020 на ЕКЗД относно понятията „администратор“ и „обработващ лични данни“ в ОРЗД).

42. Поради това администраторите трябва да имат проактивна готовност да обработват исканията за достъп до лични данни. Това означава, че администраторът следва да бъде подготвен да получи искането, да го прецени правилно (тази оценка е предмет на този раздел от насоките) и да предостави без ненужно забавяне подходящ отговор на лицето, отправило искането. Начинът, по който администраторите ще се подготвят за изпълнение на искания за достъп, следва да бъде адекватен и пропорционален и да зависи от естеството, обхвата, същността и целите на обработването, както и от рисковете за правата и свободите на физическите лица, съгласно член 24 от ОРЗД. В зависимост от конкретните обстоятелства от администраторите може да се изисква например да приложат подходяща процедура, чието изпълнение следва да гарантира сигурността на данните, без да се възпрепятства упражняването на правата на субекта на данните.

3.1.1 Анализ на съдържанието на искането

43. Този въпрос може да бъде оценен по-конкретно като се зададат следните въпроси.

а) Искането засяга ли лични данни?

44. Съгласно ОРЗД в обхвата на искането попадат само лични данни²³. Следователно всяко искане за информация по други въпроси, включително обща информация за администратора, неговите бизнес модели или дейностите му по обработване, които не са свързани с лични данни, не трябва да се счита за искане, подадено съгласно член 15 от ОРЗД. Освен това в обхвата на правото на достъп няма да попада искане за информация относно анонимни данни или данни, които не се отнасят до лицето, отправило искането, или до лицето, от чието име упълномощеното лице е отправило искането. Този въпрос ще бъде анализиран по-подробно в раздел 4.
45. За разлика от анонимните данни (които не са лични данни), псевдонимизираните данни, които могат да бъдат свързани с физическо лице чрез използването на допълнителна информация, са лични данни²⁴. Поради това следва да се счита, че в обхвата на искането попадат псевдонимизирани данни, които могат да бъдат свързани със субект на данни — например когато физическото предоставя съответния идентификатор, позволяващ тяхното идентифициране, или когато администраторът е в състояние да свърже данните с лицето, отправило искането, чрез свои собствени средства²⁵.

б) Искането отнася ли се до лицето, което го е отправило (или до лицето, от чието име упълномощеното лице отправя искането)?

46. Като общо правило искането може да се отнася само до данните на лицето, което отправя искането. Достъпът до данните на други лица може да бъде поискан само при наличието на съответно разрешение²⁶.

²³ Освен когато искането обхваща и нелични данни, неразривно свързани с личните данни на субекта на данните. За допълнителни разяснения вж. т. 100.

²⁴ Вж. съображение 26 от ОРЗД. Допълнителни разяснения относно понятията „анонимни данни“ и „псевдомизирани данни“ могат да бъдат намерени в Становище 4/2007 на Работната група по член 29 относно понятието „лични данни“, стр. 18—21.

²⁵ Работна група по член 29, РД 242, ред. 01, 5 април 2017 г., Насоки относно правото на преносимост на данните — одобрени от ЕКЗД (наричани по-нататък „Насоки на РГ по член 29 относно правото на преносимост на данните — одобрени от ЕКЗД“), стр. 9.

²⁶ Вж. раздел 3.4 („Искания, отправени чрез трети страни/пълномощници“).

Пример 7: Субектът на данни Х работи като ръководител на отдел за дружество, което предоставя на своите ръководители паркоместа на паркинг на дружеството. Въпреки че лицето Х разполага с постоянно паркомясто, при пристигането му в службата за втората му смяна това място често е вече заето от друг лек автомобил. Тъй като тази ситуация е повтаряща се, за да се установи кой е водачът, който неправомерно заема неговото място, субектът на данните иска от администратора на системата за видеонаблюдение, покриваща паркинга на службата, достъп до личните данни на този водач. В този случай искането на физическото лице Х няма да бъде искане за достъп до неговите лични данни, тъй като искането не се отнася до данните на лицето, отправило искането, а до данните на друго лице, и следователно не следва да се счита за искане съгласно член 15 от ОРЗД.

в) Прилагат ли се разпоредби, различни от ОРЗД, с които се урежда достъпът до някои категории данни?

47. Субектите на данни не са задължени да посочват в своето искане правното основание. Ако обаче субектите на данни разяснят, че искането им не се основава на ОРЗД, а на секторно или на национално законодателство, с което се урежда конкретният въпрос, свързан с достъпа до някои категории данни, такова искане се разглежда от администратора в съответствие с въпросното секторно или национално законодателство, когато е приложимо. Често пъти, в зависимост от съответното национално законодателство, администраторите може да бъдат задължени да предоставят отделни отговори, във всеки от които се разглеждат конкретните изисквания, определени в различните законодателни актове. Това не трябва да се бърка с националното законодателство или законодателството на ЕС, определящо ограничения върху правото на достъп, което трябва да се спазва при отговаряне на искания за достъп.
48. Ако администраторът има съмнения относно това кое право желае да упражни субектът на данните, се препоръчва да помоли отправящото искането лице да обясни предмета на искането. Тази кореспонденция със субекта на данните не засяга задължението на администратора да действа без ненужно забавяне²⁷. Въпреки това, в случай на съмнение, ако администраторът поиска от субекта на данните допълнително обяснение и не получи отговор, като се има предвид задължението му да съдейства за упражняването на правото на достъп на лицето, той следва да тълкува информацията, съдържаща се в първото искане, и да действа въз основа на нея. В съответствие с принципа на отчетност администраторът може да определи подходящ срок, в рамките на който субектът на данните може да предостави допълнително обяснение. При определянето на такъв срок администраторът следва да предвиди достатъчно време за изпълнение на искането след изтичането на срока и следователно да прецени колко време е обективно необходимо за събиране и предоставяне на исканите данни, след предоставянето (или не) на уточнението от субекта на данните.
49. Ако искането попада в обхвата на ОРЗД, съществуването на такова специално законодателство не отменя общото прилагане на правото на достъп, съгласно предвиденото в Регламента. Може да са налице ограничения, определени в правото на ЕС или в националното право, когато това е допустимо по член 23 от ОРЗД (вж. раздел 6.4).

г) Попада ли искането в обхвата на член 15?

50. Следва да се отбележи, че с ОРЗД не се въвеждат каквито и да е официални изисквания за лица, отправили искане за достъп до данни. За да се подаде искане за достъп е достатъчно лицето,

²⁷ Вж. допълнителни насоки относно срока в раздел 5.3.

отправило искането, да уточни, че желае да знае какви лични данни, свързани с него, се обработват от администратора. Следователно, администраторът не може да откаже предоставянето на данните, като се позове на непосочването на правното основание на искането, особено на липсата на конкретна препратка към правото на достъп или на ОРЗД.

Например, за да се подаде искане ще бъде достатъчно лицето, отправило искането, да посочи че:

- желае да получи достъп до личните данни, свързани с него;
- упражнява правото си на достъп; или
- желае да се запознае с обработваната от администратора информация, свързана с него.

Следва да се има предвид, че молителите може да не са запознати с особеностите на ОРЗД и се препоръчва да не се подхожда твърде строго към лица, упражняващи правото си на достъп, особено когато то се упражнява от ненавършили пълнолетие лица. Както е посочено по-горе, когато има някакви съмнения се препоръчва администраторът да поиска от субекта на данните да уточни предмета на искането.

д) Поискания от субектите на данни достъп дали се отнасят до цялата или до части от информацията, обработвана във връзка с тях?

51. Администраторът трябва да прецени и дали исканията, подадени от лицата, които са ги отправили, се отнасят до цялата или до части от обработваната във връзка с тях информация. Всяко ограничение на обхвата на подадено от субекта на данните искане за конкретно прилагане на член 15 от ОРЗД трябва да бъде ясно и недвусмислено. Например, ако субектите на данни поискат дословно „информация за данните, обработвани във връзка с тях“, администраторът следва да приеме, че субектите на данни възнамеряват да упражнят изцяло правото си съгласно член 15, параграфи 1—2 от ОРЗД. Такова искане не следва да се тълкува в смисъл, че физическите лица желаят да получават само категориите лични данни, които се обработват, и се отказват от правото си да получат информацията, посочена в член 15, параграф 1, букви а)—з). Случаят би бил различен, например, когато субектите на данни желаят да имат, по отношение на посочените от тях данни, достъп до източника или произхода на личните данни или до определения срок на съхраняване. Тогава администраторът може да ограничи отговора си до поисканата конкретна информация.

3.1.2 Формат на искането

52. Както беше отбелязано по-рано с ОРЗД на субектите на данни не се налагат каквито и да е изисквания относно формата на искането за достъп до личните данни. Следователно, съгласно Регламента по принцип няма изисквания, които физическите лица трябва да спазват при избора на канал за комуникация, чрез който да осъществяват контакт с администратора.
53. С цел да се позволи на субекта на данните да подаде ефективно искане, ЕКЗД насърчава администраторите да предоставят най-подходящите и удобни за ползване канали за комуникация в съответствие с член 12, параграф 2 и член 25 от ОРЗД. Въпреки това, ако лице

подаде искане, като използва предоставен от администратора канал за комуникация,²⁸ който е различен от посочения като предпочитан, такова искане по принцип се счита за ефективно и администраторът следва да го обработи по подходящия начин (вж. примерите по-долу). Администраторите следва да положат всички разумни усилия, за да се уверят, че упражняването на правата на субекта на данни е улеснено (например, когато физическо лице изпрати искане за достъп до служител, който е в отпуск, разумно усилие може да бъде автоматично съобщение, информиращо лицето за алтернативен канал за комуникация във връзка с това искане).

54. Следва да се отбележи, че администраторът не е задължен да действа по искане, изпратено до случаен или неточен адрес на електронна поща (или пощенски адрес), който не е предоставен пряко от администратора, или до друг комуникационен канал, който очевидно не е предназначен за получаване на искания относно правата на субекта на данните, ако администраторът е предоставил подходящ канал за комуникация, който може да бъде използван от субекта на данните.
55. Администраторът не е задължен да действа и по искане, изпратено до адрес на електронна поща на служител на администратора, който може да не участва в обработването на искания относно правата на субектите на данни (например шофьори, почистващ персонал и др.). Такива искания не се считат за ефективни, ако администраторът ясно е предоставил на субекта на данни подходящ канал за комуникация. Ако обаче физическото лице изпрати искане до служител на администратора, който е определен като лице за редовен контакт с него (като например личен управител, обслужващ сметките в банка (личен банкер) или постоянен консултант в мобилен оператор), такъв контакт не трябва да се счита за произволен и администраторът следва да положи всички разумни усилия, за да обработи такова искане, така че да може да бъде пренасочено към точката за контакт и да бъде отговорено в рамките на предвидените в ОРЗД срокове.
56. Независимо от това, ЕКЗД препоръчва като добра практика въвеждането от администраторите на подходящи механизми, за да съдействат за упражняването на правата на субектите на данни, включително системи за автоматичен отговор, с която да се информира за отсъствието на служители и подходящ алтернативен контакт и, когато е възможно, механизми за подобряване на вътрешната комуникация между служителите по искания, получени от лица, които може да не са компетентни да ги разглеждат.

Пример 8: Администратор С предоставя както на своя уебсайт, така и в декларацията за поверителност, два адреса на електронна поща — общият адрес на електронна поща на администратора: CONTACT@C.COM, и адреса на електронна поща на точката за контакт на администратора за защита на данните: QUERIES@C.COM. Освен това администратор С посочва на своя уебсайт, че за да се отправят запитвания или да се подава искане във връзка с обработването на лични данни, лицата следва да се свържат с точката за контакт за защита на данните чрез предоставения адрес на електронна поща. Субектът на данните обаче изпраща искане до общия адрес на електронна поща на администратора: CONTACT@C.COM.

²⁸ Това може да включва например данни за комуникация на администратора, предоставени в неговите съобщения, адресирани директно до субектите на данни, или данни за контакт, предоставени от администратора публично, като например в политиката за поверителност на администратора или други задължителни официални известия на администратора (например- информация за контакт със собственик или предприятие на уебсайт).

В този случай администраторът следва да положи всички разумни усилия, за да уведоми своите служби за искането, подадено чрез общата електронна поща, така че да може да бъде пренасочено към точката за контакт за защита на данните и да бъде отговорено в рамките на предвидените в ОРЗД срокове. Освен това администраторът няма право да удължи срока за отговор на искане, само защото субектът на данните е изпратил искане до общия адрес на електронна поща на администратора, а не до адреса на електронна поща на неговата точка за контакт за защита на данните.

Пример 9: Администратор Y ръководи мрежа от фитнес клубове. На своя уебсайт и в декларацията си за поверителност за клиенти на фитнес клуба администратор Y посочва, че за да се отправят запитвания или да се подават искания във връзка с обработването на лични данни, лицата следва да се свържат с администратора на адреса на електронна поща: QUERIES@Y.COM. Въпреки това, субектът на данните изпраща искане до адреса на електронна поща, намерен в съблекалнята, където е намерил съобщение, което гласи „Ако не сте доволни от чистотата на стаята, моля, свържете се с нас на адрес: CLEANERS@Y.COM“, което е адреса на електронната поща на почистващия персонал, нает от Y. Очевидно почистващия персонал не участва в разглеждането на въпроси, свързани с упражняването на правата на субектите на данни — клиенти на фитнес клуба. Макар че адресът на електронна поща е бил наличен в помещенията на фитнес клуба, физическото лице не би могло разумно да очаква, че това е подходящ адрес за контакт за такива искания, тъй като уебсайтът и съобщението за поверителност предоставят ясна информация за канала за комуникация, който трябва да се използва за упражняване на правата на субектите на данни.

57. По правило от датата на получаване на искането от администратора тече едномесечен срок, в който администраторът трябва да предостави информация за предприети действия по искане в съответствие с член 12, параграф 3 от ОРЗД (допълнителни насоки относно срока са предоставени в раздел 5.3). ЕКЗД счита за добра практика администраторите да потвърждават получаването на исканията в писмена форма, например чрез изпращане на електронни писма (или информация по пощата, ако е приложимо) до лицата, отправили искането, в които се потвърждава, че техните искания са получени и че едномесечният срок тече от ден X до ден Y.

3.2 Идентифициране и удостоверяване на самоличността

58. За да се гарантира сигурността на обработването и да се сведе до минимум рискът от неразрешено разкриване на лични данни, администраторът трябва да може да разбере кои данни се отнасят до субекта на данните (идентификация) и да потвърди самоличността на това лице (удостоверяване на самоличността).
59. Може да се припомни, че в ситуации, в които целта, за която се обработват личните данни, не изисква или вече не изисква идентифицирането на субект на данни, администраторът не трябва да поддържа идентификация с единствената цел да спазва правата на субектите на данни, също и с оглед на принципа за свеждане на данните до минимум. Тези ситуации се разглеждат в член 11, параграф 1 от ОРЗД.
60. Член 12, параграф 2 от ОРЗД гласи, че администраторът не отказва да предприеме действия по искане на субекта на данните за упражняване на правата му, освен ако обработва лични данни за цел, която не изисква идентифицирането на субекта на данните и докаже, че не е в състояние да идентифицира лицето. При тези обстоятелства обаче субектът на данните може да реши да

предостави допълнителна информация, позволяваща това идентифициране (член 11, параграф 2 от ОРЗД)²⁹.

61. Администраторът не е задължен да се сдобие с такава допълнителна информация, за да идентифицира субекта на данните с единствената цел да изпълни искането, както и с оглед на принципа на свеждане на данните до минимум. Той обаче не следва да отказва да приеме такава допълнителна информация, подадена от субекта на данни, за да подпомогне упражняването на неговите права (съображение 57 от ОРЗД).

Пример 10: С е администраторът на данните, обработвани във връзка с видеонаблюдение на сграда. В съответствие с член 11, параграф 1 от ОРЗД администраторът не е задължен да идентифицира всички лица, които са регистрирани от камера за сигурност като част от наблюдението (цел, която не изисква идентифициране). Администраторът получава искане за достъп до личните данни от лице, което твърди, че е записано от видеонаблюдението на администратора. Действията ще зависят от предоставената допълнителна информация. Ако лицето, отправило искането, посочи конкретен ден и час, когато камерите може да са записали въпросното събитие, има вероятност администраторът да може да предостави такива данни (член 11, параграф 2 от ОРЗД). Ако обаче администраторът не е в състояние да идентифицира субекта на данните (например ако не може да е сигурен, че отправилото искането лице е действително субектът на данните или ако искането се отнася например за дълъг период на записване и администраторът не може да обработи толкова голямо количество данни), той може да откаже да предприеме действия, ако се докаже, че не е в състояние да идентифицира физическото лице (член 12, параграф 2 от ОРЗД).

Пример 11: Администратор С обработва лични данни за целите на изпращане на поведенческа реклама към ползвателите на неговия уебсайт. Обикновено личните данни, събрани във връзка с поведенческа реклама, се събират с бисквитки и са свързани с псевдонимни произволни идентификатори. Субектът на данни г-н Х упражнява правото си на достъп до С чрез уебсайта на С. С е в състояние да идентифицира точно г-н Х, за да покаже поведенческата реклама на субекта на данните, като свърже крайното оборудване на г-н Х с неговия рекламен профил чрез бисквитките, пуснати в терминала. Впоследствие С също трябва да може да идентифицира точно г-н Х, за да му предостави достъп до личните му данни, тъй като може да се намери връзка между обработваните данни и субекта на данните. Следователно и като се вземат предвид принципите на ОРЗД, горепосоченият пример не попада в обхвата на член 11 от ОРЗД. По-точно, в горния пример, целите на С изискват идентифициране на субектите на данни, докато в член 11 от ОРЗД се разглежда ситуацията на обработване, при което не се изисква идентификация, когато администраторът не е длъжен да обработва допълнителни данни по смисъла на член 11, параграф 1 от ОРЗД с единствената цел да може да спазва Регламента. Следователно в някои случаи не следва да се изискват допълнителни данни, за да се упражнят правата на физическите лица.

Ако обаче г-н Х се опита да упражни правото си на достъп по електронна поща или по обикновена поща, тогава в този случай С няма да има друг избор, освен да поиска от г-н Х да предостави „допълнителна информация“ (член 12, параграф 6 от ОРЗД), за да може да

²⁹ Насоки на РГ по член 29 относно правото на преносимост на данните — одобрени от ЕКЗД, стр. 13.

идентифицира рекламния профил, свързан с г-н Х. Тогава допълнителната информация ще бъде идентификатор на бисквитки, съхранявани в крайното оборудване на г-н Х.

62. В случай на доказана невъзможност за идентифициране на субекта на данните (член 11 от ОРЗД), администраторът трябва да го информира по съответния начин, ако това е възможно, тъй като администраторът отговаря на искания на лицето без ненужно забавяне и посочва причините, когато не възнамерява да изпълни такива искания. Тази информация трябва да бъде предоставена само „ако е възможно“, тъй като администраторът може да не е в състояние да уведоми субектът на данните, ако е невъзможно да го идентифицира.
63. Както когато обработването не изисква идентифициране, така и когато го изисква, в случай че администраторът има основателни съмнения относно самоличността на физическото лице, отправил искането, той може да поиска предоставянето на допълнителна информация, необходима за потвърждаване на самоличността (член 12, параграф 6 от ОРЗД).
64. С ОРЗД не се налагат каквито и да е изисквания относно начина на удостоверяване на самоличността на субекта на данните. В членове 11 и 12 от ОРЗД се посочват обаче, условията за упражняването на всички права на физическото лице, включително правото на достъп до лични данни.
65. Следва да се припомни, че по правило администраторът не може да изисква повече лични данни, отколкото е необходимо, за да се позволи това удостоверяване, и че използването на такава информация трябва да бъде строго ограничено до изпълнение на искането на субектите на данни.
66. Често пъти между субектите на данни и администраторите вече съществуват процедури по удостоверяване на самоличността. Администраторите може да използват тези процедури, за да установят самоличността на субектите на данни, които са отправили искане за техните лични данни или упражняват правата, предоставени от ОРЗД³⁰. В противен случай администраторите следва да прилагат процедура по удостоверяване на самоличността, за да направят това³¹.
67. В случаите, когато администраторът изисква или получава от субекта на данните допълнителна информация, необходима за потвърждаване на неговата самоличност, администраторът преценява всеки път каква информация ще му позволи да потвърди самоличността на физическото лице и евентуално задава допълнителни въпроси на лицето, отправил искането, или иска представянето на някои допълнителни елементи за установяване на самоличността, ако това е пропорционално (вж. раздел 3.3).
68. За да се даде възможност на субекта на данните да предостави допълнителната информация, необходима за установяване на неговите данни, администраторът следва да уведоми лицето за естеството на допълнителната информация, необходима за установяването на самоличността. Тази допълнителна информация не следва да надвишава първоначално необходимата информация за удостоверяване на самоличността на субекта на данните. Като цяло, фактът, че администраторът може да поиска допълнителна информация за оценка на самоличността, не може да доведе до прекомерни изисквания и до събиране на лични данни, които не са

³⁰ Насоки на РГ по член 29 относно правото на преносимост на данните — одобрени от ЕКЗД, стр. 14.

³¹ Вж. допълнителни насоки относно удостоверяване на самоличността в раздел 3.3.

подходящи или необходими за затвърждаване на връзката между физическото лице и исканите лични данни³².

69. Вследствие на това, когато събраната онлайн информация е свързана с псевдоними или други уникални идентификатори, администраторът може да приложи подходящи процедури, позволяващи на лицето, отправило искането, да подаде искане за достъп до данни и да получи данните, свързани с него³³.

Пример 12: Субектът на данни г-жа Х иска достъп до данните си докато разговаря с консултант на телефонната линия на електрическа компания, с която е сключила договор. Консултантът, който се съмнява в самоличността на лицето, което е отправило искането, генерира в системата на компанията еднократен уникален код, който се изпраща на мобилния телефонен номер на ползвателя, предоставен при създаването на профила, като част от системата за двойна проверка, което действие следва да се счита за пропорционално в този случай.

3.3 Оценка на пропорционалността относно удостоверяване на самоличността на лицето, отправило искането

70. Както е посочено по-горе, ако администраторът има основателни причини да се съмнява в самоличността на лицето, отправило искането, той може да поиска допълнителна информация, за да потвърди самоличността. В същото време обаче администраторът трябва да гарантира, че не събира повече лични данни от необходимото, за да е възможно удостоверяването на самоличността на лицето, отправило искането. Следователно, администраторът извършва оценка на пропорционалността, при която трябва се да вземе предвид вида на личните данни, които се обработват (например- специални категории данни или не), естеството на искането, причината, поради която се подава искането, както и всички вреди, които биха могли да възникнат от неправилно разкриване. При оценката на пропорционалността следва да не се забравя да се избягва прекомерното събиране на данни, като същевременно се гарантира адекватно ниво на сигурност на обработването.
71. Администраторът следва да прилага процедура за удостоверяване на самоличността, за да е сигурен в самоличността на лицата, отправили искане за достъп до своите данни³⁴, и за да гарантира сигурността на обработването през целия процес на обработване на исканията за достъп в съответствие с член 32 от ОРЗД, включително например защитен канал за предоставяне на допълнителна информация. Методът, използван за удостоверяване на самоличността, следва да бъде целесъобразен, подходящ, пропорционален и да се спазва принципа за свеждане на данните до минимум. Ако администраторът налага мерки, целящи удостоверяване на автентичността на субекта на данните, които са обременяващи, той трябва адекватно да обоснове това и да гарантира спазването на всички основни принципи, включително свеждането до минимум на данните и задължението за оказване на съдействие за упражняването на правата на субектите на данни (член 12, параграф 2 от ОРЗД).

³² Пак там, стр. 14.

³³ Пак там, стр. 13—14.

³⁴ Насоки на РГ по член 29 относно правото на преносимост на данните — одобрени от ЕКЗД, стр. 14.

72. В онлайн среда механизмът за удостоверяване на самоличността може да включва използването от субекта на данни на една и съща информация за удостоверяване на идентичността при регистрация за онлайн услуга, предлагана от администратора на лични данни (съображение 57 от ОРЗД)³⁵.
73. На практика процедурите за удостоверяване на самоличността съществуват често и администраторите не трябва да въвеждат допълнителни гаранции за предотвратяване на непозволен достъп до услугите. За да се даде възможност на лицата да имат достъп до данните, съдържащи се в техните профили (като профил в електронна поща, профил в социални мрежи или онлайн магазини), администраторите най-вероятно ще поискат регистриране чрез данните за вход и парола на ползвателя, което в такива случаи трябва да е достатъчно за удостоверяване на автентичността на субект на данни³⁶. Освен това, често пъти администраторите вече са удостоверили самоличността на лицата преди да сключат договор или да получат тяхното съгласие за обработването и в резултат на това личните данни, използвани за регистриране на физическото лице, засегнато от обработването, могат също да бъдат използвани като доказателство за удостоверяване на автентичността на субекта на данните за целите на достъпа³⁷. Следователно, е непропорционално да се изисква копие на документ за самоличност в случай на вече извършено удостоверяване на самоличността на лицето, което е отправило искането.
74. Следва да се подчертае, че използването на копие от документ за самоличност като част от процеса на удостоверяване на самоличността създава риск за сигурността на личните данни и може да доведе до неразрешено или незаконосъобразно обработване, и като такова следва да се счита за неподходящо, освен ако е необходимо, подходящо и в съответствие с националното право. В тези случаи администраторите трябва да разполагат със системи, които осигуряват ниво на сигурност, подходящо за смекчаване на по-високите рискове за правата и свободите на субекта на данните да получава такива данни. Важно е да се отбележи и че удостоверяването на самоличността чрез лична карта не е непременно в помощ при онлайн комуникацията (например с използването на псевдоними), ако съответното лице не може да предостави някакви други доказателства, например допълнителни характеристики, съответстващи на потребителския профил.
75. Като се отчита фактът, че много организации (например хотели, банки, фирми за коли под наем) изискват копия от личната карта на своите клиенти, това обикновено не трябва да се счита за подходящ начин за удостоверяване на самоличността. Алтернативно, администраторът може да приложи бърза и ефективна мярка за сигурност с цел да идентифицира субект на данни въз основа на удостоверяването на самоличността, което е извършил преди това, например чрез електронна поща или текстово съобщение, съдържащо връзки за потвърждение, въпроси за сигурност или кодове за потвърждение³⁸.

³⁵ Вж. допълнителни насоки относно методите за удостоверяване на самоличността в Насоки 01/2021 на ЕКЗД относно примерни случаи, свързани с уведомяването за нарушение на сигурността на личните данни, приети на 14 януари 2021 г., стр. 30—31., и в Насоки 02/2021 на ЕКЗД относно виртуалните гласови асистенти, версия 2.0, приета на 7 юли 2021 г., раздел 3.7.

³⁶ Насоки на РГ по член 29 относно правото на преносимост на данните — одобрени от ЕКЗД, стр. 14.

³⁷ Насоки на РГ по член 29 относно правото на преносимост на данните — одобрени от ЕКЗД, стр. 14.

³⁸ Вж. също Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 г. относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО, с които се предлагат различни услуги, които позволяват сигурна идентификация от разстояние.

76. В зависимост от оценката на всеки отделен случай информация върху документа за самоличност, която не е необходима за потвърждение на самоличността на субекта на данните, като например достъп и сериен номер, гражданство, ръст, цвят на очите, снимка и машинночитаема зона, може да бъде редактирана или скрита от субекта на данните, преди подаването ѝ на администратора, освен когато съгласно националното законодателство се изисква пълно, нередактирано копие на личната карта (вж. точка 78 по-долу). По принцип, датата на издаване или на изтичане, издаващият орган и пълното име, съответстващо на онлайн профила, винаги са достатъчни за администратора да провери самоличността, при условие че са гарантирани автентичността на копие и връзката с молителя. Допълнителна информация като дата на раждане на субекта на данните може да се изисква само в случай, че е налице риск от погрешно установяване на самоличността, ако администраторът може да я сравни с информацията, която вече обработва.
77. За да следва принципа на свеждане на данните до минимум, администраторът следва да уведоми субекта на данните за информацията, която не е необходима, както и за възможността да редактира или скрие тези части от документа за самоличност. В този случай, ако физическото лице не знае как или не може да редактира такава информация, добра практика е тя да се поправи от администратора при получаване на документа, ако е възможно да го направи той, като се вземат предвид наличните средства при дадените обстоятелства.

Пример 13: Ползвателят г-жа У е създала защитено с парола потребителско име в онлайн магазин, като е предоставила своя адрес на електронна поща и/или потребителско име. Впоследствие, собственикът на профила иска от администратора информация дали обработва личните му данни и ако е така, иска достъп до тях в рамките на посочения в член 15 обхват. Администраторът иска документа за самоличност на лицето, отправил искането, за да потвърди неговата самоличност. Действието на администратора в този случай е непропорционално и води до ненужно събиране на данни.

За да се потвърди обаче самоличността на лицето, отправил искането, като същевременно се попречи на ненужното събиране на данни, администраторът може да изиска от лицето да удостовери самоличността си чрез влизане в профила или като му зададе (нелични) въпроси за сигурност, чийто отговор следва да е известен само на субекта на данните, или като използва многофакторно удостоверяване на самоличността, което е конфигурирано при регистрирането на профила на лицето, или като използва други съществуващи средства за комуникация, за които е известно, че принадлежат на субекта на данните, като адрес на електронна поща или телефонен номер, за да изпрати парола за достъп.

Пример 14: Клиент на банка г-н У планира да получи потребителски кредит. За тази цел г-н У отива до клон на банката, за да получи информация, включително личните му данни, необходими за оценката на неговата кредитоспособност. За да провери самоличността на субекта на данните, консултантът иска нотариално заверено удостоверение на данните за неговата самоличност, за да е в състояние да му предостави исканата информация.

Администраторът не следва да изисква нотариално заверено потвърждение на данните за самоличността, освен ако е необходимо, подходящо и в съответствие с националното право (например, когато дадено лице временно не притежава документ за самоличност и доказателството за самоличността на субекта на данни се изисква съгласно националното право за извършване на правно действие). Тази практика води до допълнителни разходи за лицето,

отправило искането, и налага прекомерна тежест върху субектите на данни, като възпрепятства упражняването на техните права на достъп.

78. Без да се засягат горепосочените общи принципи, при определени обстоятелства удостоверяването на автентичността въз основа на документ за самоличност може да бъде оправдана и пропорционална мярка, по-специално във връзка със субекти, обработващи специални категории лични данни или извършващи обработване на данни, което може да представлява риск за лицето (например медицинска или здравна информация). В същото време обаче следва да се има предвид, че в някои национални разпоредби се предвиждат ограничения на обработването на данни, съдържащи се в публични документи, включително документи, потвърждаващи самоличността на лице (също въз основа на член 87 от ОРЗД). Ограниченията върху обработването на данни от тези документи може да се отнасят по-специално до сканирането или фотокопирането на лични карти или обработването на официални лични идентификационни номера³⁹.
79. Като се има предвид горепосоченото, когато се иска документ за самоличност (и това е едновременно в съответствие с националното законодателство и обосновано и пропорционално съгласно ОРЗД), администраторът трябва да въведе гаранции за предотвратяване на незаконосъобразното обработване на документа за самоличност. Независимо от приложимите национални разпоредби относно удостоверяването на автентичността на документ за самоличност, това може да включва непредприемане на действия по изготвяне на копие или заличаване на копие на документ за самоличност веднага след успешното удостоверяване на самоличността на субекта на данните. Основанието за това е, че по-нататъшното съхраняване на копие от документ за самоличност вероятно ще представлява нарушение на принципите за ограничение на целите и ограничение на съхранението (член 5, параграф 1, букви б) и д) от ОРЗД), както и на националното законодателство относно обработването на националния идентификационен номер (член 87 от ОРЗД). С цел да се избегне ненужно копиране или съхраняване на копия от лични карти ЕКЗД препоръчва като добра практика изготвянето след проверката на личната карта от страна на администратора на бележка, например „Личната карта беше проверена“.

3.4 Искания, подадени чрез трети страни/пълномощници

80. Въпреки че правото на достъп обикновено се упражнява от субектите на данни, тъй като е присъщо на тях, е налице възможност за подаване на искане от трета страна от името на лицето. Това може да се отнася, наред с другото, за действие чрез пълномощник или законни настойници от името на ненавършили пълнолетие лица, както и за действие чрез други субекти чрез онлайн портали. При някои обстоятелства самоличността на лицето, упълномощено да упражнява правото на достъп, както и разрешението да действа от името на субекта на данните, може да изисква проверка, когато това е подходящо и пропорционално (вж. раздел 3.3 по-горе)⁴⁰. Следва да се припомни, че предоставянето на лични данни на лице, което няма право на достъп до тях, може да представлява нарушение на сигурността на личните данни⁴¹.

³⁹ Няколко държави членки въведоха в националните си разпоредби ограничения във връзка с това, като посочват например, че изготвянето на копия на лични карти е законосъобразно само ако произтича пряко от разпоредбите на правен акт.

⁴⁰ Относно сроковете за упражняване на правото на достъп, когато администраторът трябва да получи допълнителна информация, вж. т. 157.

⁴¹ Член 4, точка 12 от ОРЗД.

81. Във връзка с това следва да се вземат предвид националните законодателства, уреждащи законното представителство (например пълномощни), с които могат да се налагат специфични изисквания за доказване на упълномощаване за отправяне на искане от името на субекта на данните, тъй като този въпрос не е уреден в ОРЗД. В съответствие с принципа на отчетност, както и с другите принципи за защита на данните, администраторите трябва да са в състояние да докажат наличието на съответното разрешение за подаване на искане от името на субекта на данните и да получат исканата информация, освен при разлики в националното законодателство (например в националното законодателство се съдържат специфични правила относно благонадеждността на адвокатите), в резултат на което администраторът трябва да провери самоличността на пълномощника (например в случай на адвокати се проверява членството в адвокатската колегия). Поради това се препоръчва събирането на подходяща документация съгласно посочените по-горе общи правила, свързани с потвърждаване на самоличността на физическо лице, което подава искане, и ако администраторът има основателни съмнения относно самоличността на лице, действащо от името на субекта на данните, той изисква допълнителна информация, за да потвърди самоличността на това лице.
82. Като се има предвид, че упражняването на правото на достъп до личните данни на починали лица представлява друг пример за достъп от трета страна, различна от субекта на данните, в съображение 27 се уточнява, че ОРЗД не се прилага за личните данни на починали лица. Следователно, този въпрос се разглежда в националното право и държавите членки може да предвидят правила относно обработването на личните данни на починали лица. Следва да се има предвид обаче, че данните може освен това да се отнасят и до живи трети лица, например в случай на поискан достъп до кореспонденцията на починало лице. Поверителността на тези данни все още трябва да бъде защитена.

3.4.1 Упражняване на правото на достъп от името на деца

83. Децата заслужават специална защита на личните данни, тъй като те не познават достатъчно добре съответните рискове, последици и гаранции, както и своите права, свързани с обработването на лични данни⁴². Всяка информация и комуникация с дете, когато се обработват неговите лични данни, следва да се предоставя с ясни и недвусмислени формулировки, които да бъдат лесноразбираеми за детето⁴³.
84. Децата са субекти на данни сами по себе си и като такива правото на достъп им принадлежи. В зависимост от зрелостта и способността на детето то може да се нуждае от трета страна, която да действа от негово име, например носителят на родителската отговорност.
85. Висшите интереси на детето следва да са водещо съображение във всички решения, взети по отношение на упражняването на правото на достъп във връзка с децата, по-специално когато правото на достъп се упражнява от името на детето, например от носителят на родителските права.

⁴² Съображение 38 от ОРЗД. Както е предвидено в работната програма на ЕКЗД, намерението му е да предостави насоки относно данните на децата. Очаква се с такъв документ да се предоставят повече насоки относно условията, при които дете може да упражнява правото си на достъп и носителят на родителската отговорност може да упражнява правото на достъп от името на детето.

⁴³ Съображение 58 от ОРЗД. Насоки 05/2020 на ЕКЗД относно съгласието в съответствие с Регламент 2016/679, раздел 7.

86. Поради включената в ОРЗД специална защита на личните данни на децата администраторът предприема подходящи мерки, за да избегне разкриването на лични данни на ненавършило пълнолетие лице на неупълномощено лице (във връзка с това вж. също раздел 3.4 по-горе).
87. Накрая, правото на носителя на родителска отговорност да действа от името на детето не следва да се бърка със случаи извън законодателството в областта на защитата на данните, при които съгласно националното законодателство на носителя на родителска отговорност може да се предостави правото да иска и да получава информацията относно детето (например представянето на детето в училище).

3.4.2 Упражняване на правото на достъп чрез портали/канални, предоставени от трета страна

88. Съществуват дружества, които предоставят услуги, даващи възможност на субектите на данни да подават искания за достъп чрез портал. Субектът на данните влиза и получава достъп до портал, чрез който може да изпрати например искане за достъп, да поиска коригиране на данни или заличаване на данни от различни администратори. При използването на портали, предоставени от трета страна, възникват различни въпроси.
89. Първият въпрос, който трябва да решат администраторите, когато са изправени пред тези обстоятелства, е да гарантират, че третата страна действа законосъобразно от името на субекта на данните, тъй като е необходимо да се гарантира, че не се разкриват каквито и да е данни на неупълномощени страни.
90. Освен това администратор, който получава искане, подадено през такъв портал, трябва неизменно да обработи това искане своевременно⁴⁴. Администраторът обаче не е задължен да предоставя данните по член 15 от ОРЗД директно на портала, ако той например установи, че мерките за сигурност са недостатъчни или би било сметено за подходящо да се използва друг начин за разкриване на данни на субекта на данните. При тези обстоятелства, когато администраторът разполага с други процедури за обработване на искания за достъп по ефикасен и сигурен начин, той може да предостави исканата информация чрез тези процедури.

4 ОБХВАТ НА ПРАВОТО НА ДОСТЪП И ЛИЧНИТЕ ДАННИ И ИНФОРМАЦИЯ, ЗА КОИТО СЕ ОТНАСЯ

91. Целта на настоящия раздел е да се разясни определението за лични данни (параграф 4, точка 1) и да се изясни обхватът на информацията, засегната от правото на достъп като цяло (параграф 4, точки 2) и 3). Трябва да се отбележи, че обхватът на понятието за лични данни, а оттам и разграничението между лични данни и други данни, е неразделна част от оценката, извършвана от администратора с цел установяване на обхвата на данните, до които физическото лице има право да получи достъп⁴⁵.

⁴⁴ Относно сроковете за упражняване на правото на достъп, когато администраторът трябва да получи допълнителна информация, вж. т. 157.

⁴⁵ В съответствие с принципа на неприкосновеност на личния живот още при проектирането такъв анализ е част от оценката на подходящи мерки и гаранции за защита на принципите за защита на данните и правата на субектите на данни, която се извършва „*както към момента на определянето на средствата*“

92. Като предварително съображение следва да се припомни, че правото на достъп може да се упражнява само по отношение на обработването на лични данни, попадащи в материалния и териториален обхват на ОРЗД. Следователно, в обхвата на правото на достъп не попадат личните данни, които не се обработват с автоматични средства или които не са част или не са предназначени да съставляват част от регистъра с лични данни съгласно член 2, параграф 1 от ОРЗД или се обработват от физическо лице в хода на чисто лични или домакински занимания съгласно член 2, параграф 2 от ОРЗД.

4.1 Определение за лични данни

93. В член 15, параграфи 1 и 3 от ОРЗД се посочват „лични данни“ и съответно „лични данни, които са в процес на обработване“. Следователно обхватът на правото на достъп се определя първо и преди всичко от обхвата на понятието за лични данни, определено в член 4, точка 1 от ОРЗД⁴⁶. Понятието „лични данни“ вече беше предмет на няколко документа⁴⁷ на Работната група по член 29⁴⁸ и беше тълкувано от Съда на ЕС, включително по отношение на правото на достъп съгласно член 12 от Директива 95/46/ЕО.
94. РГ по член 29 счита, че определението за лични данни в Директива 95/46/ЕС „отразява намерението на европейския законодател за създаване на широко понятие „лични данни“⁴⁹. Съгласно ОРЗД определението все още се отнася до „всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано“. Освен основните лични данни, като име и адрес, телефонен номер и др., в обхвата на това определение може да попадне голямо разнообразие от данни, като например медицински заключения, история на покупките, показатели за кредитоспособност, съдържание на комуникациите и др. С оглед на широкия обхват на определението за лични данни, ограничителна оценка на това определение от страна на администратора би довела до погрешна класификация на личните данни⁵⁰ и в крайна сметка до нарушаване на правото на достъп.

за обработване, така и към момента на самото обработване“, например един от тези показатели може да бъде намаляването на времето за отговор при упражняване на правата от субектите на данни. За допълнителни разяснения вж. Насоки 4/2019 относно член 25 „Защита на данните на етапа на проектирането и по подразбиране“.

⁴⁶ Съгласно член 4, точка 1 от ОРЗД „лични данни“ означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице;“.

⁴⁷ Например РД 251 ред.01, „Насоки относно автоматизираното вземане на индивидуални решения и профилирането за целите на Регламент 2016/679“, т.е. стр. 19; Насоки на РГ по член 29 относно правото на преносимост на данните — одобрени от ЕКЗД, стр. 9.

⁴⁸ Работната група по член 29 (РГ по член 29) е независимата европейска работна група, която се занимаваше с въпроси, свързани със защитата на неприкосновеността на личния живот и личните данни, до 25 май 2018 г. (влизането в сила на ОРЗД) и е предшественик на ЕКЗД.

⁴⁹ Становище 4/2007 на РГ по член 29 относно понятието „лични данни“, стр. 4.

⁵⁰ Като информация, която не е свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано.

95. В съединени дела C-141/12 и C-372/12⁵¹ Съдът на ЕС постанови, че правото на достъп обхваща лични данни, съдържащи се в докладната записка, а именно „*име, дата на раждане, гражданство, пол, етническа и религиозна принадлежност и език на молителя*“ „и, „*евентуално тези, които се съдържат във включения в нея правен анализ*“, но не и самия правен анализ⁵². В този смисъл правният анализ не можеше сам по себе си да бъде предмет на проверката на неговата точност от страна на субекта на данните, нито на коригиране. Освен това предоставянето на достъп до правния анализ не отговаря на целта за гарантиране на неприкосновеността на личния живот, а на достъпа до административни документи.
96. В решението по делото Nowak⁵³ Съдът на ЕС извърши по-всеобхватен анализ и установи, че писмените отговори, дадени от кандидат на изпит за професионални умения, и всички коментари на проверителя по тези отговори, представляват лични данни, свързани с кандидата за изпита. По-точно тази субективна информация представлява лични данни „*под формата на становища или преценки, при условие че „засяга“ съответното лице*“⁵⁴, за разлика от изпитните въпроси, които не се считат за лични данни⁵⁵. По този начин контекстуалната оценка следва да разяснява последиците или резултата от определена информация върху дадено лице и следователно, и обхвата на правото на достъп.

Пример 15: Лице има интервю за работа в дружество. В тази връзка кандидатът за работа предава автобиография и писмо за кандидатстване. По време на интервюто служителят по човешки ресурси си води бележки на компютър, за да документира интервюто. След това кандидатът за работа, като субект на данни, иска достъп до личните данни, свързани с него, които дружеството в качеството си на администратор е събрало в хода на процедурата по набиране на персонал.

Администраторът е задължен да предостави на субекта на данните личните данни, съобщени по негова инициатива в неговата автобиография и писмото за кандидатстване. Освен това администраторът трябва да предостави на субекта на данните обобщение на интервюто, включително субективните коментари относно поведението на субекта на данните, написани от служителя по човешки ресурси по време на интервюто за работа, при спазване на всички изключения съгласно националното право и в съответствие с член 23 от ОРЗД.

97. По този начин, в зависимост от конкретните факти по случая, при оценяване на конкретно искане за достъп администраторите трябва да предоставят, наред с другото, следните видове данни, без да се засяга член 15, параграф 4 от ОРЗД:
- специални категории лични данни по член 9 от ОРЗД;
 - лични данни, свързани с присъди и нарушения по член 10 от ОРЗД;
 - данни, предоставени съзнателно и по желание на субекта на данните (например данни за сметка, подадени чрез формуляри, отговори на въпросник)⁵⁶;

⁵¹ Съд на ЕС, съединени дела C-141/12 и C-372/12, YS/Minister voor Immigratie, Integratie en Asiel и Minister voor Immigratie, Integratie en Asiel/M и S, 17 юли 2014 г.

⁵² Съд на ЕС, съединени дела C-141/12 и C-372/12, YS и др., т. 38 и 48.

⁵³ Съд на ЕС, C-434/16, Peter Nowak/Комисар по защита на данните, 20 декември 2017 г.

⁵⁴ Съд на ЕС, C-434/16, Nowak, т. 34—35.

⁵⁵ Съд на ЕС, C-434/16, Nowak, т. 58.

⁵⁶ Насоки на РГ по член 29 относно правото на преносимост на данните — одобрени от ЕКЗД, стр. 9.

- записани или необработени данни, предоставени от субекта на данните чрез използване на услугата или устройството (например данни, обработвани от свързани обекти, хронология на сделката, регистрационни файлове за дейността, като регистрационни файлове за достъп, история на използване на уебсайт, дейности за търсене, данни за местоположение, щраквания, специални аспекти на поведението на дадено лице, като почерк, натискане на клавиши, конкретен начин на ходене или говорене)⁵⁷;
- данни, получени по-скоро от други данни, отколкото предоставени пряко от субекта на данните (например кредитно съотношение, класификация въз основа на общи характеристики на субектите на данни, държава на пребиваване, установена от пощенския код)⁵⁸;
- данни, изведени по-скоро от други данни, отколкото предоставени пряко от субекта на данните (например за определяне на кредитен рейтинг или спазване на правилата за борба с изпирането на пари, алгоритмични резултати, резултати от здравна оценка или персонализиране или процес по изготвяне на препоръки)⁵⁹;
- Псевдомизирани данни вместо анонимизирани данни (вж. раздел 3 от настоящите насоки).

Пример 16: Елементи, които са използвани за вземане на решение относно например повишението на служител, увеличението на заплата или назначението на нова работа (например годишни прегледи на качеството на изпълнението, искания за обучение, записи, свързани с дисциплинарни процедури, класиране, потенциал за кариерно развитие) са лични данни, свързани с този служител. Следователно субектът на данните може да получи достъп до тези елементи при поискване и при зачитане на член 15, параграф 4 от ОРЗД в случай, че личните данни се отнасят например и за друго лице (например самоличността или елементите, разкриващи самоличността на друг служител, чиито показания относно професионалното представяне са включени в годишен преглед на качеството на изпълнението, могат да бъдат предмет на ограничения по член 15, параграф 4 от ОРЗД и следователно е възможно те да не могат да бъдат съобщени на субекта на данните, за да се защитят правата и свободите на посочения служител). Независимо от това е възможно да се прилагат разпоредбите на националното трудово законодателство, например по отношение на достъпа на служителите до досиетата на персонала или други национални разпоредби, като например тези, свързани с професионалната тайна. При всички обстоятелства при подобни ограничения на упражняването на правото на достъп на субекта на данните (или други права), предвидени в национално законодателство, трябва да се спазват условията на член 23 от ОРЗД (вж. раздел 6.4).

98. От горепосочения неизчерпателен списък на лични данни могат да бъдат изведени няколко съображения, които могат да бъдат предоставени на субекта на данните при подадено искане за достъп. Видно е, че при предоставянето на достъп до лични данни администраторът не може да прави разлика между данните, съдържащи се в досиета на хартиен носител, и тези, съхранявани в електронен формат, стига да попадат в обхвата на ОРЗД. С други думи лични

⁵⁷ Становище 4/2007 на РГ по член 29 относно понятието „лични данни“, стр. 8.

⁵⁸ Насоки на РГ по член 29 относно правото на преносимост на данните — одобрени от ЕКЗД, стр. 10—11.

⁵⁹ Насоки на РГ по член 29 относно правото на преносимост на данните — одобрени от ЕКЗД, стр. 10—11; РГ по член 29, РД 251 ред.01, 6 февруари 2018 г., „Насоки относно автоматизираното вземане на индивидуални решения и профилирането за целите на Регламент 2016/679“ — одобрени от ЕКЗД (наричани по-нататък „Насоки на РГ по член 29 относно автоматизираното вземане на индивидуални решения и профилирането — одобрени от ЕКЗД“), стр. 9—10.

данни, които се съдържат в досиета на хартиен носител като част от регистър с лични данни или които са предназначени да съставляват част от регистър с лични данни, попадат в обхвата на правото на достъп по същия начин, както лични данни, съхранявани в компютърна памет чрез например бинарен код или видеокасета.

99. Освен това, както повечето права на субекта на данни, правото на достъп включва както изведени, така и извлечени данни, включително лични данни, създадени от доставчик на услуги, докато правото на преносимост на данните включва само данни, предоставени от субекта на данните⁶⁰. Следователно, в случай на искане за достъп и за разлика от искане за преносимост на данни, на субекта на данните следва да бъдат предоставени не само лични данни, предоставени на администратора, за да се направи последващ анализ или оценка на тези данни, но и резултатът от всеки такъв последващ анализ или оценка.
100. Важно е да се припомни и че е налице информация, като например анонимизирани данни⁶¹, която представлява данни, които не са пряко или косвено свързани с лице, което може да бъде идентифицирано, и следователно не попадат в обхвата на ОРЗД. Например местоположението на сървъра, на който се обработват личните данни на субекта на данните, не представлява лични данни. Разграничението може да представлява предизвикателство и администраторите може да се чудят как да определят ясна граница между лични и нелични данни, особено в случай на набори от смесени данни. Тогава може да е полезно да се прави разлика между набори от смесени данни, в които личните и неличните данни са неразривно свързани, и тези, в които това не е така. Личните и неличните данни може да бъдат неразривно свързани в набори от смесени данни и да попадат изцяло в обхвата на правото на достъп на субекта на данните, за който се отнасят личните данни⁶². В други случаи личните и неличните данни в набори от смесени данни може да не са неразривно свързани, като на субектите на данни се предоставя достъп само до личните данни в набора. Например дадено дружество може да трябва да предостави на субект на данни отделните доклади за ИТ инциденти, които е предизвикало, но не и базата данни от знания на дружеството за ИТ проблеми. Въпреки това мерките за сигурност, които администраторът е въвел, обикновено не трябва да се разбират като лични данни, при условие че те не са неразривно свързани с личните данни и следователно не са обхванати от правото на достъп.
101. Преди да завърши раздела, ЕКЗД припомня, че защитата на физическите лица по отношение на обработването на лични данни обхваща всички видове лични данни, изброени по-горе, и че ограничителното тълкуване на определението противоречи на разпоредбите на ОРЗД и в крайна сметка нарушава член 8 от Хартата на основните права. Прилагането на различен режим при упражняването на право във връзка с някои видове лични данни, които не са предвидени в ОРЗД, може да бъде въведено изключително със закон в съответствие с член 23 от ОРЗД (както е допълнително обяснено в раздел 6.4). Следователно, администраторите не могат да

⁶⁰ Както беше посочено по-рано в Насоки на РГ по член 29 относно правото на преносимост на данните — одобрени от ЕКЗД, стр. 10, и потвърдено в „Насоки относно автоматизираното вземане на индивидуални решения и профилирането“ на РГ по член 29 — одобрени от ЕКЗД, стр. 17.

⁶¹ Допълнителни разяснения относно понятието анонимизиране могат да бъдат намерени в Становище 05/2014 на Работната група по член 29 относно техническите способности за анонимизиране, РД 216, 10 април 2014 г., стр. 5—19.

⁶² Съобщение на Комисията до Европейския парламент и Съвета, Насоки във връзка с Регламента относно рамка за свободното движение на нелични данни в Европейския съюз, 29.5.2019 г., COM/2019/250 final.

ограничават упражняването на правото на достъп чрез ненужно ограничаване на обхвата на личните данни.

4.2 Личните данни, за които се отнася правото на достъп

102. Съгласно член 15, параграф 1 от ОРЗД „*субектът на данните има право да получи от администратора потвърждение дали се обработват лични данни, свързани с него, и ако това е така, да получи достъп до данните и следната информация*“ (добавен е курсив).
103. От член 15, параграф 1 от ОРЗД произтичат няколко елемента. В параграфа изрично се посочва „*лични данни, свързани с него*“ (4.2.1), които „*се обработват*“ (4.2.2) от администратора:

4.2.1 „лични данни, свързани с него“

104. Правото на достъп може да се упражнява изключително по отношение на лични данни, свързани със субекта на данните, който иска достъп или, когато е приложимо, от упълномощено лице или пълномощник (вж. раздел 3.4). Съществуват и ситуации, в които данните не са свързани с лицето, упражняващо правото на достъп, а с друго лице. Субектът на данните обаче има право на достъп само до лични данни, свързани с него, с изключение на данни, които се отнасят изключително до някой друг⁶³.
105. Класифицирането на данните като лични данни относно субекта на данните обаче не зависи от факта, че тези лични данни също се отнасят до някой друг⁶⁴. Поради това е възможно личните данни да са свързани едновременно с повече от едно лице. Това не означава автоматично предоставянето на достъп до лични данни, които са свързани с някой друг, тъй като администраторът трябва да спазва член 15, параграф 4 от ОРЗД.
106. Текстът „*лични данни, свързани с него*“, не следва да се тълкува от администратора по „*прекомерно ограничителен*“ начин, както вече бе посочено от Работната група по член 29 по отношение на правото на преносимост на данните⁶⁵. При прилагането му към правото на достъп,

⁶³ Насоки на РГ по член 29 относно правото на преносимост на данните — одобрени от ЕКЗД, стр. 9: „*В обхвата на искане за преносимост на данните се включват само лични данни. Следователно всички данни, които са анонимни, или не се отнасят до субекта на данните, не биха попаднали в обхвата. В обхвата обаче се включват данни за псевдонимите, които ясно могат да бъдат свързани с даден субект на данни (например тъй като той е предоставил съответния идентификатор, вж. член 11, параграф 2).*“

⁶⁴ Съд на ЕС, решение по дело C-434/16 Peter Nowak/Комисар по защита на данните, 2017 г., т. 44.

⁶⁵ Насоки на РГ по член 29 относно правото на преносимост на данните — одобрени от ЕКЗД, стр. 9: *В много случаи администраторите обработват информация, която съдържа личните данни на различни субекти на данни. Когато случаят е такъв, администраторите на данни не следва да тълкуват изречението „лични данни, свързани със субекта на данните“ прекалено ограничително. Например записите в телефон, при обмен на съобщения между абонати или интернет телефония (VoIP) може да включват (в хронологията в акаунта на абоната) данни на трети страни, които участват във входящи или изходящи повиквания. Макар че в такъв случай записите ще съдържат лични данни, които засягат множество лица, абонатите следва да имат възможност тези записи да им се предоставят в отговор на искания за преносимост на данните, тъй като записите (също) засягат субекта на данните. Когато обаче тези записи след това се предават на нов администратор на данни, този нов*

ЕКЗД счита например, че записите на телефонни разговори (и тяхната транскрипция) между субектът на данните, който иска достъп, и администратора, може да попадат в обхвата на правото на достъп, при условие, че в последния случай става въпрос за лични данни⁶⁶. При условие, че се прилага ОРЗД и че обработването не е обхванато от изключение във връзка с домашни занимания съгласно член 2, параграф 2, буква в) от ОРЗД, ако субектът на данните използва получения запис, който включва лични данни на събеседника, за други цели, например като публикува записа, субектът на данните ще стане администратор по отношение на това обработване на лични данни, свързани с другото лице, чийто глас е записан. Въпреки че това няма да освободи администратора от неговите задължения във връзка със защитата на данните, когато надлежно анализира дали може да бъде предоставен достъп до пълния запис, той бива насърчаван да информира субекта на данните за това, че в този случай може да стане администратор. Това не засяга по-нататъшна оценка съгласно член 15, параграф 4 от ОРЗД, подробно описана в раздел 6. По същия начин съобщения, които субектите на данни са изпратили до други под формата на междуличностни съобщения и са се изтрили от устройството им, които все още са достъпни за доставчика на услуги, могат да попаднат в обхвата на правото на достъп.

107. Има обаче и ситуации, в които връзката между данните и няколко лица може да изглежда неясна за администратора, като например в случай на кражба на самоличност. В случай на кражба на самоличност дадено лице действа чрез измама от името на друго лице. В този смисъл е важно да се припомни, че на жертвата следва да бъде предоставена информация относно всички лични данни, които администраторът съхранява във връзка с нейната самоличност, включително тези, събрани въз основа на действията на измамника. С други думи, дори и след като администраторът е научил за кражбата на самоличност, личните данни, които са свързани или се отнасят до самоличността на жертвата, представляват лични данни на субекта на данни.

Пример 17: Лице използва чрез измама самоличността на някой друг, за да играе покер онлайн. Извършителят плаща на онлайн казиното с кредитната карта, която е откраднал от жертвата. Когато жертвата разбира за откраднатата самоличност, той иска от доставчика на онлайн казиното да му предостави достъп до личните му данни и по-специално до играните онлайн игри и информацията за използваната от извършителя кредитна карта.

Налице е връзка между събраните данни и жертвата, тъй като е използвана самоличността на жертвата. След откриването на измамата, посочените по-горе лични данни все още имат връзка поради тяхното съдържание (кредитната карта на жертвата е очевидно за жертвата), целта и ефекта (информацията за онлайн игрите, играни от извършителя, може например да се използва за издаване на фактури на жертвата). Поради това онлайн казиното предоставя на жертвата достъп до горепосочените лични данни.

108. Ако е целесъобразно, вътрешните регистрационни файлове за свързване се използват за съхраняване на запис относно достъпите до файл и за проследяване на това кои действия са били извършени във връзка с достъп до запис, като отпечатване, копиране или заличаване на лични данни. Тези регистрационни файлове може да включват времето на регистриране, причината за достъпа до файловете, както и информация за установяване на лицето, което е

администратор на данни не следва да ги обработва за никакви цели, които влияят неблагоприятно върху правата и свободите на трети страни (вж. по-долу: трето условие).“

⁶⁶ Вж. пример 34 в раздел 6.2.

имало достъп. Свързаните с тази тема въпроси са предмет на дело, което понастоящем очаква решение пред Съда на ЕС (С-579/21). Въвеждането, надзорът и преразглеждането на регистрационните файлове за свързване попадат в обхвата на отговорността на администратора и подлежат на проверка от надзорните органи. Поради това администраторът следва да се увери, че действащите под неговото ръководство лица, които имат достъп до личните данни, обработват лични данни само по указание на администратора съгласно член 29 от ОРЗД. Ако въпреки това лицето обработва личните данни за други цели, различни от изпълнението на указанията на администратора, то може да стане администратор във връзка с това обработване и да подлежи на дисциплинарно или наказателно производство или административни санкции, издадени от надзорни органи. ЕКЗД отбелязва, че част от отговорността на работодателя съгласно член 24 от ОРЗД е да използва подходящи мерки — от образователни до дисциплинарни процедури — с цел да се гарантира, че обработването се извършва в съответствие с ОРЗД и няма да има нарушение.

4.2.2 Лични данни, които „се обработват“

109. Член 15, параграф 1 от ОРЗД се отнася и до лични данни, които „се обработват“. Времевият обхват за определяне на обхвата на личните данни, попадащи в рамките на искането за достъп, вече е доразвит в раздел 2.3.3. Формулировката обаче предполага и че при правото на достъп не се прави разлика между целите на операциите по обработване.

Пример 18: Дружество е обработвало личните данни, свързани със субект на данни, с цел да обработи поръчката му за покупка и да организира изпращането ѝ до домашния адрес на физическото лице. След като тези първоначални цели, за които са били събрани личните данни, престанат да съществуват, администраторът съхранява част от личните данни единствено, за да спазва законовите си задължения, свързани с воденето на записи.

Субектът на данните иска достъп до личните данни, свързани с него. За да изпълни задължението си по член 15, параграф 1 от ОРЗД, администраторът трябва да предостави на лицето исканите лични данни, които се съхраняват, за да спазва своите законови задължения.

110. Архивираните лични данни трябва да се различават от резервните копия на данни, които са лични данни, съхранявани единствено за целите на възстановяване на данните в случай на тяхната загуба. Следва да се отбележи, че по отношение на принципите на защита на данните на етапа на проектирането и свеждането на данните до минимум, резервните копия на данни са подобни по принцип на данните в системата, действаща в реално време. Когато са налице малки разлики между личните данни в системата за резервни копия и системата, действаща в реално време, те обикновено са свързани със събирането на допълнителни данни след последното архивиране. Намалването на данните в системата, действаща в реално време (например изтриване след края на срока на съхраняване на някои данни или след искане за изтриване) в някои случаи ще бъде записано само в резервното копие на данните към момента на последващото архивиране. Когато искане за достъп е подадено в момент, в който в резервното копие на данни има повече лични данни, свързани със субекта на данните, отколкото в системата, действаща в реално време или личните данни са различни (забелязващи се например чрез регистър на заличаванията в системата, действаща в реално време, въведен в пълно съответствие с принципа за свеждане на данните до минимум), администраторът трябва да действа прозрачно относно тази ситуация и, когато е технически осъществимо, да предостави достъп, както е поискано от субекта на данните, включително до личните данни, съхранявани в резервното копие на данни. Например, с цел да бъде прозрачен за физическите лица, които упражняват правото си, регистърът на изтриванията в системата, действаща в реално време,

може да позволи на администратора да установи, че в резервното копие на данни има такива, които вече не са в системата, тъй като са били изтрети наскоро и все още не са презаписани в резервното копие на данни.

4.2.3 Обхватът на ново искане за достъп

111. Това, което остава да се каже, е, че субектите на данни имат право на достъп до всички обработвани данни, свързани с тях, или до части от данните, в зависимост от обхвата на искането (вж. също 2.3.1 относно пълнотата на информацията и 3.1.1 за анализ на съдържанието на искането). В резултат на това, когато администратор вече е изпълнил искане за достъп в миналото и при условие че искането не е прекомерно, той не може да стесни обхвата на това ново искане. Това означава, че във връзка с всяко последващо искане за достъп на същия субект на данни, администраторът следва да го информира не само за самите промени в обработваните лични данни или за самото обработване след последното искане, освен при наличието на изрично съгласие от страна на субекта на данните. В противен случай субектите на данни ще бъдат задължени да съберат предоставените им лични данни, за да получат пълния набор от лични данни, свързани с обработването на тяхната информация и упражняването на техните права.

4.3 Информация относно обработването и правата на субекта на данните

112. Съгласно член 15, параграф 1, букви а) — з) и член 15, параграф 2 от ОРЗД, освен достъпът до самите лични данни, администраторът трябва да предостави информация относно обработването и правата на субекта на данните. По-голямата част от информацията по тези конкретни точки вече е събрана, поне в общ вид, в регистъра на администратора на дейностите по обработване, посочени в член 30 от ОРЗД и/или в неговата декларация за поверителност, разработена в съответствие с членове 12—14 от ОРЗД. Следователно като първа стъпка би било полезно да се направи справка в „Насоки относно прозрачността съгласно Регламент 2016/679“⁶⁷ на Работната група по член 29, по отношение на съдържанието на информацията, която трябва да се предостави съгласно членове 13 и 14 от ОРЗД.
113. За да спазват член 15, параграф 1, букви а) — з) и член 15, параграф 2, администраторите могат внимателно да използват текстовите модули на декларацията си за поверителност, доколкото са сигурни, че те са актуални и точни по отношение на искането на субекта на данните. Често пъти преди или в началото на обработването на данните, определена информация, например установяването на конкретни получатели или конкретна продължителност на обработването на данни, може все още да не е предоставена. Част от информацията, като например правото на подаване на жалба до надзорен орган (вж. член 15, параграф 1, буква е), не се променя в зависимост от лицето, което подава искането за достъп. Следователно тя може да бъде съобщена най-общо, тъй като се прави в декларацията за поверителност. Други видове информация, като например информация за получатели, категории и източник на данни, може да се различават в зависимост от това кой подава искането и какъв е неговият обхват. Следователно, при подаване на искане за достъп по член 15, всяка информация относно обработването, която е на разположение на администратора, може да се наложи да бъде актуализирана и съобразена с операциите по обработване, които действително се извършват по

⁶⁷ Работна група по член 29, РД 260 ред.01, 11 април 2018 г., Насоки относно прозрачността съгласно Регламент 2016/679 — одобрени от ЕКЗД (наричани по-нататък „Насоки на РГ по член 29 относно прозрачността — одобрени от ЕКЗД“).

отношение на субекта на данните, който подава искането. Поради това позоваването на формулировката в политиката за поверителност няма да бъде достатъчно за администратора, за да предостави изискваната информация съгласно член 15, параграф 1, букви а)–з) и параграф 2, освен когато «съобразената и актуализирана» информация е същата като информацията, предоставена в началото на обработването. При обяснението коя информация се отнася до лицето, отправило искането, администраторът може, когато е целесъобразно, да се позове на определени дейности (като „ако сте използвали тази услуга...“, „ако сте платили по фактура“), стига да е очевидно за субектите на данни, ако те са засегнати. По-долу се обяснява необходимата степен на спецификация във връзка с отделните видове информация.

114. Информацията относно целите съгласно член 15, параграф 1, буква а) трябва бъде конкретна по отношение на точната(точните) цел(и) в действителния случай на отправилия искането субект на данни. Няма да бъде достатъчно да се изброят общите цели на администратора, без да се изясни коя(и) цел(и) преследва той в настоящия случай на отправилия искането субект на данни. Ако обработването се извършва във връзка с няколко цели, администраторът трябва да разясни кои данни или кои категории данни се обработват и за коя(кои) цел(и). За разлика от член 13, параграф 1, буква в) и член 14, параграф 1, буква в) от ОРЗД, посочената в член 15, параграф 1, буква а) информация относно обработването не съдържа информация относно правното основание за обработването. Тъй като обаче някои права на субектите на данни зависят от приложимото правно основание, тази информация е важна за субектите на данни, за да се провери законосъобразността на обработването на данните и за да се определи кои права на субекта на данните са приложими в конкретната ситуация. Следователно, за да се улесни упражняването на правата на субектите на данни в съответствие с член 12, параграф 2 от ОРЗД, на администратора се препоръчва също така да информира субекта на данните за приложимото правно основание за всяка операция по обработване или да посочи къде може да намери тази информация. Във всеки случай принципът на прозрачно обработване изисква информацията относно правните основания на обработването да бъде предоставена на субекта на данните по достъпен начин (например в декларацията за поверителност).
115. Информацията за категориите данни (член 15, параграф 1, буква б) също може да се наложи да бъде съобразена със ситуацията на субекта на данните, така че категориите, които са се оказали неуместни за лицето, отправило искането, следва да бъдат премахнати.

Пример 19: Във връзка с информацията, посочена в членове 13 и 14 от ОРЗД, хотел заявява, че обработва редица категории данни на клиенти (идентификационни данни, данни за контакт, банкови данни и номер на кредитна карта и др.). Ако бъде подадено искане за достъп въз основа на член 15, субектът на данните, който подава искането, трябва да бъде информиран освен за достъпа до действителните данни, които се обработват (компонент 2), в съответствие с член 15, параграф 1, буква б), и за конкретните категории данни, които се обработват в конкретния случай (например без да включва банкови данни или данни за кредитна карта, в случай че плащането е извършено в брой).

116. В информацията относно „получателите или категориите получатели“ (член 15, параграф 1, буква в) трябва първо да се вземе предвид определението за получатели, дадено в член 4, точка 9 от ОРЗД. Определението за получатели се основава на разкриването на лични данни на

физическо или юридическо лице, публичен орган, агенция или друга структура⁶⁸. От член 4, точка 9 от ОРЗД следва, че публичните органи, действащи в рамките на конкретно запитване, предмет на специфични национални разпоредби, не трябва да се считат за получатели.

117. Що се отнася до въпроса дали администраторът е свободен да избира между информацията относно получатели или относно категории получатели, трябва да се отбележи, че “за разлика от членове 13 и 14 от ОРЗД, които предвиждат задължение за администратора (...), член 15 от ОРЗД предвижда истинско право на достъп в полза на субекта на данните, така че последният трябва да има избор да получи или информацията за конкретните получатели, пред които данните са или ще бъдат разкрити, когато това е възможно, или информацията за категориите получатели.”⁶⁹ Също така трябва да се припомни, че както е посочено в гореспоменатите насоки относно прозрачността⁷⁰, информацията относно получателите или категориите получатели вече по членове 13 и 14 от ОРЗД следва да бъде възможно най-конкретна съгласно принципите на прозрачност и добросъвестност. Съгласно член 15, ако субектът на данните не е поискал друго, администраторът е задължен да посочи името на действителните получатели, освен ако е невъзможно те да се идентифицират или администраторът докаже, че исканията за достъп на физическото лице са явно неоснователни или прекомерни по смисъла на член 12, параграф 5 от ОРЗД⁷¹ ⁷². ЕКЗД припомня във връзка с това, че съхраняването на информацията, свързана с действителните получатели, е необходимо, наред с другото, за може да се изпълни задължението на администратора съгласно член 5, параграф 2 и член 19 от ОРЗД.

Пример 20: В декларацията си за поверителност работодател дава информация за това кои категории данни са предадени на „пътнически агенции“ или „хотели“ в случай на работни пътувания в съответствие с член 13, параграф 1, буква д) и член 14, параграф 1, буква д) от ОРЗД. Ако служител подаде искане за достъп до личните данни след осъществени работни пътувания, тогава работодателят следва да посочи в отговора си, като получатели на личните данни съгласно член 15, параграф 1, буква в), туристическата(ите) агенция(и) и хотелът(ите), които са получили данните. Въпреки че в декларацията си за поверителност работодателят законно се позовава на категории получатели съгласно членове 13 и 14, тъй като на този етап все още не е възможно да се посочат получателите, информацията за конкретните получатели (име на туристически агенции, хотели и др.) следва да се предостави, когато служителът подава искане за достъп, освен ако той не е избрал друго.

Когато при зачитане на горепосочените условия администраторът може да предостави само категориите получатели, информацията трябва да бъде възможно най-конкретна, като се посочват видът на получателя (т.е. чрез позоваване на дейностите, които извършва), индустрията, секторът и подсекторът и местоположението на получателите⁷³.

⁶⁸ Освен това следва да се отбележи, че съгласно определението в член 4, точка 7 от ОРЗД, в едно и също дружество може да съществуват различни администратори. При тази конфигурация е възможно разкриването на данни от един получател на друг в рамките на едно дружество.

⁶⁹ Съд на ЕС, C-154/21 (Österreichische Post AG), т. 36.

⁷⁰ Работна група по член 29, РД 260 ред.01, 11 април 2018 г., Насоки относно прозрачността съгласно Регламент 2016/679 — одобрени от ЕКЗД (наричани по-нататък „Насоки на РГ по член 29 относно прозрачността — одобрени от ЕКЗД“), стр. 37, (Приложение)

⁷¹ Съд на ЕС, C-154/21 (Österreichische Post AG)

⁷² Самият факт, че данни са били разкрити на голям брой получатели не прави сам по себе си искането прекомерно, вж. раздел 6, т. 188.

⁷³ Насоки на РГ по член 29 относно прозрачността — одобрени от ЕКЗД, стр. 37 (Приложение)

118. Съгласно член 15, параграф 1, буква г) трябва да се предостави информация за предвидения срок, за който ще се съхраняват личните данни, когато това е възможно. В противен случай трябва да се предостави критерият, използван за определяне на този срок. Представената от администратора информация трябва да бъде достатъчно точна, за да може субектът на данните да знае колко дълго ще продължат да се съхраняват свързаните с него данни. Ако не е възможно да се посочи срокът за заличаване, се посочват продължителността на сроковете на съхраняване и началото на този период или събитието, което е предизвикало заличаването (например прекратяване на договор, изтичане на гаранционен срок и др.). Самото позоваване например на „заличаване след изтичане на законоустановените срокове за съхраняване“ не е достатъчно. Указанията относно сроковете за съхраняване на данните ще трябва да бъдат насочени към конкретни данни, свързани със субекта на данните. Ако личните данни на физическите лица подлежат на различни периоди на заличаване (например тъй като не всички данни подлежат на законоустановени задължения за съхранение), периодите се посочват във връзка със съответните операции по обработване и съответните категории данни.
119. Докато информацията относно правото на подаване на жалба до надзорен орган (член 15, параграф 1, буква е) не зависи от конкретните обстоятелства, правата на субектите на данни, посочени в член 15, параграф 1, буква д), се различават в зависимост от правното основание, което е в основата на обработването. По отношение на задължението да се оказва съдействие за упражняването на правата на субектите на данни съгласно член 12, параграф 2 от ОРЗД отговорът от страна на администратора относно тези права е индивидуално съобразен със случая на субекта на данните и се отнася до съответните операции по обработване. Следва да се избягва информация за права, които не са приложими за физическото лице в конкретната ситуация.
120. Съгласно член 15, параграф 1, буква ж), когато личните данни не се събират от субекта на данните, трябва да се предостави „всяка налична информация“ относно източника на данните. Степента на наличната информация може да се променя с времето.

Пример 21: Политиката за поверителност на голямо дружество гласи:

„Кредитните проверки ни помагат да предотвратим проблеми при платежните операции. Те гарантират защитата на нашето дружество срещу финансови рискове, които може да засегнат и продажните цени в средносрочен до дългосрочен план. Извършването на кредитна проверка е задължително, когато ни предстои изпращане на стоки, без същевременно да получаваме покупната цена, например в случай на покупка по сметка. Без извършване на кредитна проверка е възможно само предплащане (незабавен банков превод, доставчик на онлайн плащания, кредитна карта).

За целите на кредитната проверка ще изпратим Вашето име, адрес и дата на раждане до следните доставчици на услуги, например: 1) Агенция за финансова информация X 2) Доставчик на търговска информация Y, 3) Агенция за търговски кредити Z.

Данните се предават на горепосочените кредитни институции само в рамките на позволеното от закона и само за целите на анализа на разплащателните ви практики в миналото, както и за оценка на риска от неизпълнение въз основа на математически и статистически способности, при които се използват лични данни, както и за проверка на вашия адрес (проверка за доставката). В зависимост от резултата от кредитната проверка е възможно повече да не сме в състояние да ви предлагаме индивидуални методи на плащане, като например закупуване по фактури.“

По този начин декларацията за поверителност съдържа обща информация относно възможността за получаване на информация от изброените бюра за икономическа информация в съответствие с членове 13 и 14 от ОРЗД. Ако не е ясно предварително кое от дружествата ще участва в обработването, е достатъчно в политиката за поверителност да се посочат имената на отговарящите на условията дружества. Следователно при искане на основание член 15 в допълнение към информацията, че е получена информация за кредитоспособността, ще е необходимо (впоследствие) да се посочи кое точно от посочените дружества е участвало. В член 15, параграф 1, буква ж) е ясно изразено, че когато личните данни не се събират от субекта на данните, информацията относно обработването на данните съдържа „всяка налична информация за техния източник“.

121. В член 15, параграф 1, буква з) се предвижда, че всеки субект на данни следва да има право да получи, наред с другото, съществена информация за съществуването и основната логика на автоматизирано вземане на решения, включително профилирането, свързано с него, както и за значението и предвидените последици от това обработване⁷⁴. Ако е възможно, информацията съгласно член 15, параграф 1, буква з) трябва да бъде по-конкретна по отношение на мотивите, които водят до конкретни решения относно субекта на данни, който е поискал достъп.
122. Информация за предвиденото предаване на лични данни на трета държава или международна организация, включително съществуването на адекватно решение на Комисията или подходящи гаранции, трябва да бъде предоставена съгласно член 13, параграф 1, буква е) и член 14, параграф 1, буква е) от ОРЗД. Във връзка с искане за достъп по член 15, член 15, параграф 2, информацията относно подходящите гаранции съгласно член 46 от ОРЗД се изисква само в случаите, когато действително се извършва предаване на трета държава или международна организация.

5 КАК АДМИНИСТРАТОР МОЖЕ ДА ПРЕДОСТАВИ ДОСТЪП?

123. ОРЗД няма прекалено задължаващ характер по отношение на начина на предоставяне на достъп от администратора. Правото на достъп може да бъде лесно и директно приложимо в някои ситуации, например когато малка организация притежава ограничена информация за субекта на данните. В други ситуации правото на достъп е по-сложно, тъй като обработването на данните е по-сложно; по отношение на броя на субектите на данни, категориите обработени данни, както и потока на данни в рамките на и между различни организации. Предвид разликите в обработването на личните данни, е възможно да се различават и подходящите начини за предоставяне на достъп.
124. Този раздел има за цел да се предоставят някои насоки и практически примери за различните начини на изпълнение от администраторите на искане за достъп, както и за смисъла на член 12, параграф 1 от ОРЗД във връзка с правото на достъп. В него също така ще се предоставят някои насоки за това какво се счита за широко използвана електронна форма, както и сроковете за предоставяне на достъп съгласно член 12, параграф 3 от ОРЗД.

5.1 Как администраторът може да извлече поисканите данни?

⁷⁴ Вж. във връзка с това Насоки относно прозрачността съгласно Регламент 2016/679 (РД 260), т. 41, с препратка към „Насоки относно автоматизираното вземане на индивидуални решения и профилирането за целите на Регламент 2016/679“ (РД 251).

125. Субектите на данни следва да имат достъп до цялата информация, която администраторът обработва във връзка с тях. Това означава например, че администраторът е задължен да търси лични данни във всички ИТ системи, както и в регистри с лични данни, които не са основани на ИТ. При извършването на такова търсене, администраторът следва да използва наличната информация в организацията относно субекта на данните, което вероятно може да доведе съвпадения в системите, в зависимост от начина на структуриране на информацията⁷⁵. Например, ако информацията е сортирана във файлове в зависимост от име или референтен номер, търсенето може да бъде ограничено до тези фактори. Ако обаче структурата на тези данни зависи от други фактори, например семейни отношения или професионални квалификации, или всякакъв вид преки или непреки идентификатори (например клиентски номер, потребителско име или IP-адреси), търсенето трябва да бъде разширено, за да ги включи, при условие че администраторът притежава и тази информация, свързана със субекта на данните, или тя му е предоставена от лицето. Същото важи, когато има вероятност регистрите относно трети лица да съдържат лични данни относно субекта на данните. Администраторът може обаче да не изисква от физическото лице да предоставя повече информация от необходимата за неговото идентифициране. Ако администраторът използва обработващ лични данни за своите дейности по обработване на данни, търсенето естествено трябва да бъде разширено, за да включва и лични данни, обработвани от обработващия лични данни.
126. В съответствие с член 25 от ОРЗД относно защитата на данните на етапа на проектирането и по подразбиране, администраторът (и всички обработващи лични данни, които използва) също трябва вече да имат въведени функции, позволяващи спазването на правата на субектите на данни. В този смисъл това означава, че следва да съществуват подходящи начини за намиране и извличане на информация относно субекта на данните, когато се обработва искане. Трябва да се отбележи обаче, че прекомерното изпълнение може да доведе до функции за намиране и извличане на информация, които сами по себе си представляват риск за поверителността на субектите на данни. Ето защо е важно да се има предвид, че процесът за извличане на данни също трябва да бъде проектиран по удобен за защитата на данните начин, така че да не компрометира поверителността на другите, например служителите на администратора.

5.2 Необходими мерки за предоставяне на достъп

5.2.1 Предприемане на „необходими мерки“

127. В член 12 от ОРЗД се определят изисквания за предоставяне на достъп, т.е за предоставяне на потвърждението, личните данни и допълнителната информация съгласно член 15 и се уточняват формата, начина и срока във връзка с правото на достъп. В „Насоки относно прозрачността съгласно Регламент 2016/679“ на Работната група по член 29⁷⁶ се предоставят по-нататъшни указания относно член 12, главно във връзка с членове 13 и 14 от ОРЗД, но и във връзка с член 15 и прозрачността като цяло. Следователно, определеното в настоящите насоки често може да се прилага равностойно по отношение на предоставянето на достъп съгласно член 15.

⁷⁵ Такова търсене следва естествено да включва и информация, която се държи от обработващия лични данни, вж. член 28, параграф 3, буква д) от ОРЗД.

⁷⁶ Работна група по член 29, РД 260 ред.01, 11 април 2018 г., Насоки относно прозрачността съгласно Регламент 2016/679 — одобрени от ЕКЗД (наричани по-нататък „Насоки на РГ по член 29 относно прозрачността — одобрени от ЕКЗД“).

128. Член 12, параграф 1 от ОРЗД гласи, че администраторът предприема необходимите мерки за предоставяне на субекта на данните на всякаква информация по член 15, която се отнася до обработването, в кратка, прозрачна, разбираема и леснодостъпна форма, на ясен и прост език. В член 12, параграф 2 се предвижда, че администраторът съдейства на физическото лице за упражняването на правото на достъп. По-точните изисквания в това отношение ще трябва да бъдат оценени за всеки отделен случай. Когато решават кои мерки са подходящи, администраторите трябва да вземат предвид всички специфични обстоятелства, включително, но не само, количеството обработвани данни, сложността на тяхното обработване и информацията, които имат за техните субекти на данни, например, ако по-голямата част от лицата са деца, възрастни хора или хора с увреждания. Освен това, в ситуации, в които администраторът е уведомен за някакви конкретни потребности на субекта на данните, който подава искането, например чрез допълнителна информация в подаденото искане, администраторът трябва да вземе предвид тези обстоятелства. В резултат на това необходимите мерки, които следва да бъдат предприети ще са различни.
129. При оценката е важно да се има предвид, че понятието „необходими“ не следва никога да се разбира като начин на ограничаване на обхвата на данните, попадащи в обхвата на правото на достъп. Понятието „необходими“ не означава, че усилията за предоставяне на информация може да бъдат претеглени например спрямо всички интереси, които може да има субекта на данните при получаването на личните данни. Вместо това оценката следва да цели избирането на най-подходящия метод за предоставяне на цялата информация, обхваната от това право, в зависимост от конкретните обстоятелства във всеки отделен случай. Вследствие на това, администратор, който обработва голямо количество данни в голям мащаб, трябва да приеме, че ще се наложи да положи големи усилия, за да гарантира правото на достъп на субектите на данни в кратка, прозрачна, разбираема и леснодостъпна форма, на ясен и прост език.
130. В отговор на искане за достъп до данни той трябва да избягва да насочва субекта на данните към различни източници. Както беше посочено по-рано в Насоките относно прозрачността на РГ по член 29 (по отношение на понятието „предоставяне“ в членове 13 и 14 от ОРЗД), понятието „предоставяне“ предполага, че *„субектът на данните не трябва активно да търси информацията в обхвата на тези членове сред друга информация, като например реда и условията за използване на уебсайт или приложение“*⁷⁷. Следователно и с оглед на принципа на прозрачност субектите на данни трябва да получат от администратора информацията и личните данни, изисквани по член 15, параграфи 1, 2 и 3 по начин, който позволява пълен достъп до исканата информация. При специални обстоятелства би било неподходящо или дори незаконосъобразно да се споделя информацията в рамките на администратора, например поради чувствителния характер на информацията (като информация, свързана със сигнализиране на нередности). В тези случаи би било уместно информацията да бъде разделена на няколко отговора при предоставянето на отговор на искането за достъп на субектите на данни. С избрания от администратора метод трябва действително на субекта на данните да се предоставят исканите данни и информация, следователно не би било подходящо лицето да се насочва само към проверка на исканите данни, съхранени на собственото му устройство, включително, например, за проверка на хронологията на проследяване на пътя на потребителя в сайтовете и страниците в интернет („clickstream“) и IP адресите на мобилния му телефон.

⁷⁷ Насоки на РГ по член 29 относно прозрачността — одобрени от ЕКЗД, т. 33.

131. В съответствие с принципа на отчетност, администратор трябва да документира своя подход, за да бъде в състояние да докаже как начина, по който е избрал да предостави необходимата информация съгласно член 15, е подходящ при съответните обстоятелства.

5.2.2 Различни средства за предоставяне на достъп

132. Както вече беше обяснено в раздел 2.2.2 по-горе, когато се подава искане за достъп, субектите на данни имат право да получат копие от своите данни, които се обработват съгласно член 15, параграф 3, заедно с допълнителната информация, което се счита за основно условие за предоставяне на достъп до личните данни.
133. При някои обстоятелства обаче за администратора може да е уместно да предостави достъп по други начин, различни от предоставянето на копие. Такива непостоянни условия за достъп до данните могат да бъдат например: устна информация, проверка на файлове, достъп на място или от разстояние без възможност за изтегляне. Тези условия могат да бъдат подходящи начини за предоставяне на достъп например в случаите, когато това е в интерес на субекта на данните или лицето поиска това. Достъпът на място също може да бъде подходящ като първоначална мярка, когато администратор обработва голямо количество нецифровизирани данни, за да се позволи на субекта на данните да бъде информиран какви лични данни се обработват и да е в състояние да вземе информирано решение относно това какви лични данни желае да му бъдат предоставени чрез копие. В определени ситуации непостоянните начини за достъп могат да бъдат достатъчни и адекватни; например може да задоволят нуждата на субектите на данни да проверят дали обработвани от администратора данни са точни, като се даде възможност да се разгледат оригиналните данни. Администраторът не е задължен да предоставя информацията по други начини, различни от предоставянето на копие, но следва да предприеме разумен подход при разглеждането на такова искане. Предоставянето на достъп по други начини, различни от предоставянето на копие, не изключва правото на субектите на данни също да имат копие, освен ако решат да не искат такова.
134. В зависимост от ситуацията администраторът може да избере да предостави копие от данните, които се обработват, заедно с допълнителната информация, по различни начини, например по електронна поща, физическа поща или чрез използването на инструмент за самообслужване. Ако субектът на данни подава искане с електронни средства, по възможност, информацията се предоставя в широко използвана електронна форма, освен ако лицето не е поискало друго, както е посочено в член 15, параграф 3. Във всеки случай, когато предоставя информация чрез електронна поща или онлайн инструменти за самообслужване, администраторът трябва да обмисли подходящи технически и организационни мерки, включително подходящо криптиране.
135. В ситуация, в която администраторът обработва лични данни по отношение на лицето, което подава искането, само в малък мащаб, копието на личните данни и допълнителната информация могат и трябва да бъдат предоставени чрез проста процедура.

Пример 22: Местна книжарница поддържа регистър с имена и адреси на своите клиенти, които са правили поръчки от вкъщи. Клиент посещава книжарницата и подава искане за достъп. В тази ситуация би било достатъчно личните данни, свързани с клиента, да се разпечатат директно от търговската системата, като същевременно се предостави и допълнителната информация по член 15, параграфи 1 и 2.

Пример 23: Дарител, който прави месечни дарения за благотворителна организация, подава искане за достъп по електронна поща. Благотворителната организация съхранява информация

за дарения, направени през последните дванадесет месеца, както и имена и адреси на електронна поща на дарителите. Администраторът може да предостави копие от личните данни и допълнителната информация, като отговори на писмото по електронната поща, при условие че са приложени всички необходими гаранции, като се вземе предвид например естеството на данните.

136. Дори администратори, които обработват голямо количество данни, могат да изберат да използват ръчни рутинни практики при обработването на искания за достъп. Ако администраторът обработва данни в няколко различни отдела, той трябва да събере личните данни от всеки отдел, за да може да отговори на искането на субекта на данните.

Пример 24: Управител се назначава от администратор, за да се справи с практически въпроси относно исканията за достъп. При получаване на искане администраторът изпраща запитване по електронната поща до различните отдели на организацията с молба да съберат лични данни, свързани със субекта на данните. Представителите на всеки отдел предоставят на управителя обработваните от техния отдел лични данни. Впоследствие управителят изпраща на субекта на данните всички лични данни заедно с необходимата допълнителна информация, например и при целесъобразност, по електронната поща.

137. Въпреки че ръчните процеси по обработване на искания за достъп могат да се считат за подходящи, някои администратори могат да се възползват от използването на автоматизирани процеси по обработване на искания от субекти на данни. Такъв например може да бъде случаят с администратори, които получава голям брой искания. Един от начините за предоставяне на информация по член 15 е чрез предоставяне на субекта на данните на инструменти за самообслужване. Това може да улесни ефикасното и своевременно обработване на исканията за достъп на субектите на данни и също така ще позволи на администратора да включи механизма за проверка в инструмента за самообслужване.

Пример 25: Услуга на социални медии разполага с автоматизиран процес за обработване на искания за достъп, който дава право на субекта на данните на достъп до неговите лични данни от потребителския му профил. За да извлекат личните данни, ползвателите на социални медии могат да изберат опцията „Изтегляне на вашите лични данни“, когато влязат в своя потребителски профил. Опцията за самообслужване дава възможност на потребителите да изтеглят файл, съдържащ техните лични данни, директно от потребителския профил на личния им компютър.

138. Използването на инструменти за самообслужване не следва никога да ограничава обхвата на получените лични данни. При невъзможност да се предостави цялата информация по член 15 чрез инструмента за самообслужване, останалата информация трябва да бъде предоставена по различен начин. Администраторът може действително да насърчи субекта на данните да използва инструмент за самообслужване, който е въведен за обработване на искания за достъп. Следва да се отбележи обаче, че администраторът трябва да обработи и искания за достъп, които не са изпратени чрез установения канал за комуникация⁷⁸.

⁷⁸ Вж. раздел 3.1.2.

5.2.3 Предоставяне на достъп в „кратка, прозрачна, разбираема и леснодостъпна форма, на ясен и прост език“

139. Съгласно член 12, параграф 1 от ОРЗД администраторът предприема необходимите мерки за предоставяне на достъп по член 15 в кратка, прозрачна, разбираема и леснодостъпна форма, на ясен и прост език.
140. Изискването, че предоставянето на достъп на субекта на данните трябва да се извършва в кратка и прозрачна форма означава, че администраторите следва да представят информация по ефикасен и ясен начин, за да бъде лесноразбираема за субекта на данните, особено ако става въпрос за дете. При избора на средства за предоставяне на достъп съгласно член 15, администраторът трябва да вземе предвид количеството и сложността на данните.

Пример 26: Доставчик на социални медии обработва голямо количество информация за субект на данни. Голяма част от тези лични данни представляват информация, съдържаща се в стотици страници регистрационни файлове, където са регистрирани дейностите на лицето на уебсайта. Ако лицето поиска достъп до своите лични данни, личните данни в тези регистрационни файлове действително попадат в обхвата на правото на достъп. Следователно, правото на достъп може да бъде официално упражнено, ако тези стотици страници с регистрационни файлове бъдат предоставени на физическото лице. Без да се предприемат мерки за улесняване на разбирането на информацията в регистрационните файлове обаче, правото на достъп на субекта на данните не може да бъде зачетено на практика, тъй като изличаването на каквато и да е информация от регистрационните файлове е затруднено, поради което не е изпълнено изискването на член 12, параграф 1 от ОРЗД. Следователно, администраторът трябва да бъде внимателен и да извърши задълбочена оценка, когато избира начина на представяне на информацията и личните данни на субекта на данните.

141. При обстоятелствата в горепосочения пример, използването на многослоен подход, подобен на този, препоръчан в Насоките относно прозрачността по отношение на декларациите за поверителност⁷⁹, може да бъде подходяща мярка за изпълнение на изискванията както по член 15, така и по член 12, параграф 1 от ОРЗД. Това ще бъде доразвито в раздел 5.2.4 по-долу. Изискването информацията да бъде „разбираема“ означава, че тя следва да се разбира от предназначенията аудитория⁸⁰, като същевременно се отчитат всички конкретни потребности, които може да има субектът на данните и които са известни на администратора⁸¹. Тъй като с правото на достъп често се дава възможност за упражняване на други права на субект на данни, от решаващо значение е предоставената информация да е разбираема и ясна. Основанието за това е, че субектите на данни ще могат да преценят дали да се позоват на собственото си право, например на коригиране съгласно член 16 от ОРЗД, едва след като знаят какви лични данни се обработват, за какви цели и др. В резултат на това може да се наложи администраторът да предостави на лицето допълнителна информация, с която се обясняват предоставените данни. Следва да се подчертае, че сложността на обработването на данни задължава администратора

⁷⁹ Насоки на РГ по член 29 относно прозрачността — одобрени от ЕКЗД, т. 35.

⁸⁰ Разбираемостта е тясно свързана с изискването за използване на прост и ясен език (Насоки на РГ по член 29 относно прозрачността — одобрени от ЕКЗД, т. 9). Предвиденото във връзка с простия и ясен език в параграфи 12—16 по отношение на посочената в членове 13 и 14 от ОРЗД информация се прилага в същата степен във връзка със съобщаването по член 15.

⁸¹ Вж. т. 128.

да осигури средства, за да бъдат данните разбираеми, и това не може да се използва като довод за ограничаване на достъпа до всички данни. По същия начин задължението на администратора да предоставя данни по кратък начин не може да се използва като довод за ограничаване на достъпа до всички данни.

Пример 27: Уебсайт за електронна търговия събира за маркетингови цели данни за артикули, разгледани или закупени на техния уебсайт. Част от тези данни ще се състоят от данни в необработен формат⁸², които не са анализирани и може да нямат пряко значение за читателя (кодове, хронология на активността и др.). Такива данни, свързани с дейностите на субектите на данни, също попадат в обхвата на правото на достъп и вследствие на това следва да бъдат предоставени на лицето в отговор на искане за достъп. При предоставянето на данни в необработен формат е важно администраторът да предприеме необходимите мерки, за да гарантира, че субектът на данните разбира данните, например чрез предоставяне на обяснителен документ, в който необработените данни са предадени в удобен за ползване формат. Също така, в такъв документ може да се обясни, че съкращенията и други акроними, например „А“, означават, че покупката е била прекъсната, а „Б“ означава, че покупката е извършена успешно.

142. Елементът „леснодостъпна“ означава, че информацията по член 15 следва да бъде предоставена по начин, който я прави лесна за достъп от субекта на данните. Това се отнася например за оформлението, подходящите заглавия и определянето на параграфи. Информацията следва да се предоставя винаги по ясен и разбираем начин. Администратор, който предлага услуга в дадена държава, следва също да предлага отговори на езика, който се разбира от субектите на данни в тази държава. Използването на стандартизирани икони също се насърчава, когато то улеснява разбираемостта и достъпността на информацията. Когато искането за информация се отнася до физически лица с увредено зрение или други лица, които може да имат затруднения при достъпа или разбирането на информация, от администратора се очаква да предприеме мерки, с които се улеснява разбирането на предоставената информация, включително устна информация, когато това е подходящо⁸³. Администраторът следва да полага специални грижи, за да гарантира, че възрастни хора, деца, лица с увредено зрение или лица с когнитивни или други увреждания могат да упражняват правата си, например чрез проактивно предоставяне на леснодостъпни елементи с цел улесняване на упражняването на тези права.

5.2.4 Голямото количество информация налага специфични изисквания за начина на нейното предоставяне

143. Независимо от средствата, използвани за предоставянето на достъп, е възможно да възникне напрежение между количеството информация, което администраторът трябва да предостави на субектите на данни, и изискването, че тя трябва да бъде кратка. Един от начините за постигане и на двете е пример за подходяща мярка за някои администратори, когато трябва да се предостави голямо количество данни, е използването на многослоен подход. С този подход може да се улесни разбирането на данните от субектите на данни. Следва да се подчертае обаче, че този подход може да се използва само при определени обстоятелства и трябва да се прилага

⁸² Данните в необработен формат в примера трябва да се разбират като неанализирани данни, които са в основата на обработването, а не като най-ниското ниво на необработени данни, които могат да бъдат само в машинночитаем формат (като например „битове“).

⁸³ Вж. Насоки на РГ по член 29 относно прозрачността — одобрени от ЕКЗД, т. 21.

по начин, който не ограничава правото на достъп, както е обяснено по-долу. Освен това използването на многослоен подход не следва да поражда допълнителна тежест за субекта на данните. Следователно този подход би бил най-подходящ, когато достъпът се предоставя онлайн. Многослойният подход представлява просто способ за представяне на информацията по член 15 по начин, който е съобразен и с изискванията на член 12, параграф 1 от ОРЗД, и не бива да се бърка с възможността администраторите да поискат от субекта на данните да посочи информацията или дейностите по обработване, за които се отнася искането, както е посочено в съображение 63 от ОРЗД⁸⁴.

144. Многослойният подход във връзка с правото на достъп означава, че при определени обстоятелства администраторът може да предостави изискваните съгласно член 15 лични данни и допълнителна информация в различни слоеве. Първият слой трябва да включва информация за обработването и правата на субекта на данните съгласно член 15, параграф 1, букви а)–з) и член 15, параграф 2, както и първа част от обработваните лични данни. Повечето лични данни следва да бъдат предоставени във втория слой.
145. Когато се решава каква информация следва да бъде представена в различните слоеве, администраторът трябва да вземе предвид вида на информацията, която субектът на данни би счел като цяло за най-подходяща. В съответствие с принципа на добросъвестност, първият слой следва да съдържа и информация за обработването, която има най-голямо въздействие върху субекта на данните⁸⁵. Администраторите трябва да могат да докажат отчетност по отношение на мотивите за горепосоченото предоставяне на информация.

Пример 28: Администратор анализира големи масиви от данни, за да постави клиентите в различни сегменти в зависимост от тяхното онлайн поведение. В тази ситуация може да се предположи, че информацията, която е най-важна за получаване от субектите на данни, е информация за това в кой сегмент са били поставени. В резултат на това тази информация следва да бъде включена в първия слой. Данните в необработен формат⁸⁶, които все още не са били анализирани или допълнително обработени, като например дейността на потребителите на уебсайта, също представляват лични данни, попадащи в обхвата на правото на достъп, но в някои случаи може да е достатъчно тази информация да се предостави в друг слой.

146. С цел използването на многослоен подход да се счита за подходяща мярка, е необходимо субектът на данните да бъде уведомен в началото, че информацията по член 15 е структурирана в различни слоеве и е предоставено описание на видовете лични данни и информация, които ще се съдържат в различните слоеве. По този начин за физическото лице ще бъде по-лесно да реши до какви слоеве иска да има достъп. Описанието следва да отразява обективно всички категории лични данни, които действително се обработват от администратора. Също така трябва да е ясно как субектът на данните може да получи достъп до различните слоеве. Достъпът до различните слоеве не изисква каквито и да е непропорционални усилия от страна на лицето и не зависи от формулирането на ново искане от него. Това означава, че субектите на данни трябва да имат възможност да избират дали да имат едновременно достъп до всички слоеве или да имат достъп до един или два от слоевете, ако това ги удовлетворява.

Пример 29: Субект на данни отправя искане за достъп до услуги, свързани с излъчване на видеосъдържание. Искането е подадено чрез функция, която е достъпна, когато лицето е

⁸⁴ Вж. също раздел 2.3.1.

⁸⁵ Вж. Насоки на РГ по член 29 относно прозрачността — одобрени от ЕКЗД, т. 36.

⁸⁶ Вж. бележка под линия 82.

влезнало в своя профил. На субекта на данни се предоставят два варианта, които се появяват като бутони на уеб страницата. Вариант едно е да се изтегли част 1 от личните данни и допълнителната информация. Това съдържа например скорошна хронология на стрийминг, информация за профила и за плащане. Вариант две е да се изтегли част 2 от личните данни, която съдържа технически регистрационни файлове за дейностите на субекта на данни и хронологична информация за профила. В този случай администраторът е дал възможност на субекта на данни да упражнява правото си по начин, който не създава допълнителна тежест за него.

Разновидност 1: В случаите, когато субекта на данните избере само бутона за изтегляне на част 1 от личните данни, администраторът е длъжен да предостави само част 1 от данните.

Разновидност 2: В случаите, когато субекта на данните избере бутоните както за част 1, така и за част 2 от данните, администраторът не може да съобщи само част 1 от данните и да поиска ново потвърждение преди съобщаване на част 2 от данните. Вместо това на физическото лице трябва да бъдат предоставени и двете части на данните, както следва от подаденото искане.

147. Използването на многослоен подход няма да се счита за подходящо за всички администратори или във всички ситуации. Той следва да се използва само когато за субекта на данните би било трудно да разбере информацията, ако е предоставена наведнъж. С други думи, администраторът трябва да е в състояние да докаже, че използването на многослоен подход осигурява добавена стойност за физическото лице, като му помага да разбере предоставената информация. Следователно, многослойният подход би се считал за подходящ само когато администратор обработва голямо количество лични данни за субекта на данните, който подава искането, и когато той би изпитвал очевидни затруднения да възприеме или разбере информацията, в случай че трябва да бъде предоставена наведнъж. Обстоятелството, че предоставянето на информация по член 15 би изисквало от администратора големи усилия и ресурси не е само по себе си довод за използването на многослоен подход.

5.2.5 Формат

148. Съгласно член 12, параграф 1 от ОРЗД, информацията по член 15 ще бъде предоставена в писмен вид или с други средства, включително, при целесъобразност, с електронни такива. По отношение на достъпа до личните данни, които са в процес на обработване, член 15, параграф 3 гласи, че когато субектът на данни подава искане с електронни средства, по възможност информацията се предоставя в широко използвана електронна форма, освен ако той не е поискал друго. В ОРЗД не се уточнява какво представлява широко използвана електронна форма. Поради това има няколко възможни формата, които може да се използват. Представата за това какво се счита за широко използвана електронна форма също се променя с времето.
149. Това, което може да се счита за широко използвана електронна форма следва да се основава на обективна оценка, а не на това какъв формат използва администраторът при ежедневните си операции. За да определи какъв формат трябва да се счита за широко използван в настоящата ситуация, администраторът ще трябва да прецени дали има специфични формати, които се използват по правило в областта на действие на администратора или в дадения случай. Когато няма формати, които се използват по правило, за широко използвани електронни такива следва като цяло да се считат отворени формати, определени в даден международен стандарт, като например ISO. ЕКЗД не изключва обаче възможността други формати да могат да се считат за широко използвани по смисъла на член 15, параграф 3. Когато преценява дали даден формат е широко използван електронен формат, ЕКЗД счита за важно да се определи колко лесно лицето може да получи достъп до информацията, предоставена в текущата форма. В тази връзка следва

да се отбележи каква информация е предоставена на субекта на данните от администратора за начина на получаване на достъп до досие, което е предоставено в конкретен формат, като например какви програми или софтуер може да се използват, за да се направи формата достъпен за субектът на данните. Физическото лице не следва обаче да е задължено да купува софтуер с цел да получи достъп до информацията.

150. Когато взема решение относно формата, в който следва да бъдат предоставени копието от личните данни и информацията съгласно член 15, администраторът трябва да има предвид, че формата трябва да позволява представянето на информацията по начин, който е едновременно разбираем и леснодостъпен. Важно е информацията да се предоставя на субекта на данни в присъща, постоянна форма (текстова, електронна). По принцип предоставянето на информация в писмен вид, включително с електронни средства, е за предпочитане пред други форми, тъй като тя следва да се запази във времето. Копието от личните данни може да се съхранява, при целесъобразност, върху устройство за електронно съхранение, като например компактдиск или USB.
151. Следва да се отбележи, че за да може администраторът да счита, че на субектите на данни е предоставено копие от лични данни, не е достатъчно да им е предоставен достъп до техните лични данни. За да бъде изпълнено изискването за предоставяне на копие от лични данни и в случай че данните се предоставят по електронен път/цифрово, физическите лица трябва да са в състояние да изтеглят своите данни в широко използвана електронна форма.
152. Администраторът носи отговорност за вземането на решение за подходящата форма, в която ще бъдат предоставени личните данни. Въпреки че не е непременно задължен, администраторът може да предостави в първоначалната им форма документите, които съдържат лични данни за отправилите искане субекти на данни. Администраторът може например да предостави за всеки отделен случай достъп до копие на носителя като такъв, предвид необходимостта от прозрачност (например, за да се провери точността на данните, съхранявани от администратора, в случай на искане за достъп до медицинското досие или аудиозапис, чиято транскрипция е оспорена). При тълкуването си обаче на правото на достъп съгласно Директива 95/46/ЕО Съдът на ЕС заявява, че „за да бъде удовлетворено [правото на достъп], достатъчно е лицето да получи пълна справка за тези данни в разбираема форма, тоест във форма, която му позволява да се запознае с данните и да провери дали са точни и дали се обработват в съответствие с Директивата, за да може евентуално да упражни правата, които му предоставя“⁸⁷. За разлика от директивата, в ОРЗД изрично се съдържа задължение за предоставяне на субекта на данните на копие от личните данни, които са в процес на обработване. Това обаче не означава, че физическото лице винаги има право да получи копие от документите, съдържащи личните данни, а че има право на непроменено копие от обработваните лични данни в тези документи.⁸⁸ Такова копие от личните данни може да бъде предоставено чрез документ съдържащ всички лични данни, обхванати от правото на достъп, стига чрез него да е възможно субектът на данни да бъде информиран и да провери законосъобразността на обработването. Следователно по този въпрос няма противоречие между формулировката в ОРЗД и решението на Съда на ЕС. Думите „пълна справка“ в решението не следва да се тълкуват погрешно в смисъл, че сборът няма да включва всички данни, обхванати от правото на достъп, а е просто начин да се представят всички тези данни, без да се дава достъп до основните документи, които съдържат

⁸⁷ Съд на ЕС, съединени дела C-141/12 и 372/12, YS и др., т. 60.

⁸⁸ Свързаните с тази тема въпроси са предмет на дела, които понастоящем очакват решение пред Съда на ЕС (C-487/21 и C-307/21).

личните данни. Тъй като документът трябва да съдържа копие от личните данни, следва да се подчертае, че той не може да се изготвя по начин, с който се изменя или променя съдържанието на информацията.

Пример 30: Субект на данни е застрахован в застрахователно дружество от много години. Настъпили са няколко инцидента, свързани със застрахователно събитие. При всеки случай между субекта на данните и застрахователното дружество е водена писмена кореспонденция чрез електронна поща. Тъй като лицето е трябвало да предостави информация относно конкретните обстоятелства за всеки инцидент, кореспонденцията включва много лична информация за субекта на данните (хобита, съквартиранти, ежедневни навици и др.). В някои случаи възникна несъгласие относно задължението на застрахователното дружество да обезщети субекта на данните, което води до голяма по обем комуникация в двете посоки. Цялата кореспонденция е съхранявана от застрахователното дружество. Лицето подава искане за достъп. В тази ситуация администраторът не е задължен да предоставя електронните писма в оригиналната им форма, като ги препраща на субекта на данните. Вместо това той може да избере да обедини кореспонденцията по електронната поща, съдържаща личните данни на субекта на данните, във файл, който се предостави на лицето.

153. Независимо от формата, в която администраторът предоставя личните данни, например чрез предоставяне на действителните документи, съдържащи личните данни или сбор от лични данни, информацията отговаря на изискванията за прозрачност, определени в член 12 от ОРЗД. В някои случаи създаването на някакъв вид сбор и/или извличане на данните по начин, който прави информацията лесна за разбиране, може да представлява начин за спазване на тези изисквания. В други случаи информацията се разбира по-добре чрез предоставяне на копие от действителния документ, съдържащ личните данни. Следователно коя е най-подходящата форма трябва да се реши за всеки отделен случай.
154. В този смисъл е важно да се помни, че съществува разграничение между правото на достъп по член 15 от ОРЗД и правото на получаване на копие от административни документи, регламентирани в националното право, като последното е право на получаване на копие от действителния документ. Това не означава, че правото на достъп по член 15 от ОРЗД изключва възможността за получаване на копие от документа/носителя, в който се намират личните данни.
155. В някои случаи изискванията за формата, в които следва да се предоставят личните данни, се посочват в самите лични данни. Например, когато личните данни представляват саморъчно написана информация от субекта на данните, може да се наложи на субекта на данните да бъде предоставено фотокопие от тази саморъчно написана информация, тъй като самият ръкопис представлява лични данни. Такъв по-специално може да е случаят, когато почеркът е нещо, което е от значение за обработването, например анализ на написаното. Същото важи като цяло за аудиозаписите, тъй като самият глас на субекта на данни представлява лични данни. В някои случаи обаче достъп може да бъде предоставен чрез предоставяне на транскрипция на разговора, например ако е договорено между субекта на данните и администратора.
156. Следва да се отбележи, че разпоредбите относно изискванията за формата се различават в зависимост от правото на достъп и правото на преносимост на данните. Докато съгласно правото на преносимост на данните по член 20 от ОРЗС се изисква информацията да бъде предоставена в машинночитаем формат, това не се изисква съгласно правото на информация по член 15. Следователно формати, които се считат за неподходящи при изпълнение на искане за

преносимост на данни, например pdf файлове, все още могат да бъдат подходящи при изпълнение на искане за достъп.

5.3 Срок за предоставянето на достъп

157. Съгласно член 12, параграф 3 от ОРЗД от администратора се изисква да предоставя на субекта на данни информацията относно действията, предприети във връзка с искане по член 15, без ненужно забавяне и във всички случаи в срок от един месец от получаване на искането. Този срок може да бъде удължен с най-много два месеца, като се взема предвид сложността и броя на исканията, при условие че физическото лице е информирано за причините за такова забавяне в срок от един месец от получаването на искането. Това задължение за информиране на субекта на данните относно удължаването и причините за него не бива да се бърка с информацията, която трябва да бъде предоставена незабавно и най-късно в срок от един месец, когато администраторът не предприема действия по искането, както е подробно описано в член 12, параграф 4 от ОРЗД.
158. Администраторът реагира и по правило предоставя информацията по член 15 без ненужно забавяне, което означава, че информацията следва да бъде предоставена възможно най-скоро. Това означава, че ако е възможно поисканата информация да бъде предоставена в срок по-кратък от един месец, администраторът следва да го направи. ЕКЗД счита също така, че в някои ситуации срокът за отговор на искането трябва да бъде адаптиран спрямо срока на съхраняване, за да е възможно да се предостави достъп⁸⁹.
159. Срокът започва да тече, когато администраторът получи искане по член 15, което означава, че искането достига до администратора по един от неговите официални канали⁹⁰. Не е необходимо администраторът да е действително запознат с искането. Когато обаче администраторът трябва да комуникира със субекта на данните поради несигурност по отношение на самоличността на лицето, което подава искането, срокът може да бъде спрял, докато администраторът получи необходимата информация от лицето, при условие че е поискал допълнителна информация без ненужно забавяне. Същото важи и когато администратор е поискал от субект на данни да уточни операциите по обработване, с които е свързано искането, когато са изпълнени условията, определени в съображение 63⁹¹.

Пример 31: След получаване на искането, администратор реагира незабавно и иска необходимата информация, за да потвърди самоличността на лицето, което подава искането. Въпросното лице отговаря само няколко дни по-късно и изпратената от субекта на данните информация за проверка на самоличността не изглежда достатъчна, което налага искане на разяснения от страна на администратора. В тази ситуация ще е налице спиране на срока до получаването от администратора на достатъчно информация, за да извърши проверката на самоличността на субекта на данните.

160. Срокът за отговор на искане за достъп трябва да се изчислява в съответствие с Регламент № 1182/71⁹².

⁸⁹ Вж. раздел 2.3.3

⁹⁰ В някои държави членки има национално законодателство, в което се определя кога съобщение трябва да се счита за получено, като се вземат предвид почивните дни и националните празници.

⁹¹ Вж. допълнително раздел 2.3.1.

⁹² Регламент (ЕИО, Евратом) № 1182/71 на Съвета от 3 юни 1971 г. за определяне на правилата, приложими за срокове, дати и крайни срокове.

Пример 32: Организация получава искане на 5 март. Срокът започва да тече от същия ден. Така организацията трябва да изпълни искането най-късно до 5 април включително.

Пример 33: Ако организацията получи искане на 31 август и поради по-кратката продължителност на следващия месец няма съответстваща дата, най-късната дата за отговор е последния ден на следващия месец, следователно 30 септември.

161. Ако последният ден от този срок се пада през почивните дни или на официален празник, администраторът има време да отговори до следващия работен ден.
162. При определени обстоятелства администраторът може да удължи, при необходимост, срока за отговор на искане за достъп с още два месеца, като се вземат предвид сложността и броят на исканията. Следва да се подчертае, че тази възможност е изключение от общото правило и не следва да се използва твърде често. Ако администраторите често се оказват принудени да удължават срока, това може да сочи за необходимост от по-нататъшно развитие на техните общи процедури за обработване на искания.
163. Това, което представлява сложно искане, варира в зависимост от конкретните обстоятелства на всеки случай. Някои от факторите, които може да се считат за значими, са например:
- количеството данни, обработвани от администратора,
 - начинът, по който се съхранява информацията, особено когато е трудно нейното извличане, например когато данните се обработват от различни звена на организацията,
 - необходимостта от редактиране на информацията, когато се прилагат изключения, например информация относно други субекти на данни или която представлява търговски тайни, и
 - когато информацията изисква допълнителна работа, за да бъде разбираема.
164. Самият факт, че изпълнението на искането ще изисква големи усилия, не прави искането сложно. По същия начин, фактът, че голямо дружество получава голям брой искания, не би довело автоматично до удължаване на срока. Когато обаче администратор получава временно голям брой искания, например поради изключителна публичност във връзка с неговите дейности, това може да се счита за основателна причина за удължаване на срока за отговор. Независимо от това, администратор, особено такъв, който обработва голямо количество данни, следва да разполага с процедури и механизми, за да е в състояние да обработва искания в рамките на определения срок при нормални обстоятелства.

6 РАМКИ И ОГРАНИЧЕНИЯ НА ПРАВОТО НА ДОСТЪП

6.1 Общи бележки

165. Правото на достъп е предмет на граници, произтичащи от член 15, параграф 4 от ОРЗД (права и свободи на други лица) и член 12, параграф 5 от ОРЗД (явно неоснователни или прекомерни искания). Освен това правото на достъп може да бъде ограничено с правото на Съюза или правото на държава членка в съответствие с член 23 от ОРЗД. Дерогации относно обработването на лични данни за научни или исторически изследвания, за статистически цели или за целите на архивирането в обществен интерес може да се основават на член 89, параграф 2 и съответно на

член 89, параграф 3 от ОРЗД, а дерогации за обработването, извършвано за журналистически цели или за целите на академичното, художественото или литературното изразяване може да се основават на член 85, параграф 2 от ОРЗД.

166. Важно е да се отбележи, че освен горепосочените граници, дерогации и възможни ограничения, в ОРЗД не се допускат допълнителни изключения или дерогации от правото на достъп. Това означава, наред с другото, че правото на достъп не съдържа каквато и да било обща резерва относно пропорционалността по отношение на полаганите от страна на администратора усилия за изпълнение на искането на субекта на данните по член 15 от ОРЗД⁹³. Освен това не е позволено да се ограничава правото на достъп в договор между администратора и субекта на данните.
167. Съгласно съображение 63 правото на достъп се предоставя на субектите на данни, за да бъдат осведомени за обработването и да проверят законосъобразността му. Правото на достъп позволява на субекта на данни да получи наред с другото, в зависимост от обстоятелствата, коригиране, изтриване или блокиране на личните данни⁹⁴. Физическите лица обаче не са задължени да посочват причини или да обосновават искането си. Доколкото са изпълнени изискванията на член 15 от ОРЗД, целите в основава на искането следва да се считат за неуместни⁹⁵.

6.2 Член 15, параграф 4 от ОРЗД

168. Съгласно член 15, параграф 4 от ОРЗД правото на получаване на копие не влияе неблагоприятно върху правата и свободите на други лица. Разясненията за това ограничение са дадени в съображение 63, пето и шесто изречение. Това право не следва да влияе неблагоприятно върху правата или свободите на други лица, включително върху търговската тайна или интелектуалната собственост, и по-специално върху авторското право за защита на софтуера.

Тези съображения обаче не следва да представляват отказ за предоставяне на цялата информация на съответния субект на данни. Когато се тълкува член 15, параграф 4 от ОРЗД трябва да се обърне специално внимание, за да не се разшири неоснователно обхвата на ограниченията, определени в член 23 от ОРЗД, които са допустими само при строги условия.

169. Член 15, параграф 4 от ОРЗД се прилага по отношение на правото на получаване на копие от данните, което е основното условие за предоставяне на достъп до обработваните данни (втори компонент на правото на достъп). То се прилага, като се вземат предвид правата и свободите на други лица, и ако достъпа до личните данни се предоставя по изключение с други средства, различни от копие. Например няма разлика, с която да се обосновава дали търговските тайни са засегнати чрез предоставяне на копие или чрез предоставяне на достъп на място на субекта на

⁹³ Когато администраторът обработва голямо количество информация относно субекта на данните, както е посочено в съображение 63 от ОРЗД, администраторът може да поиска от субекта на данните да посочи точно информацията или дейностите по обработването, за които се отнася искането. Вж. също раздел 2.3.1.

⁹⁴ Съд на ЕС, съединени дела C-141/12 и C-372/12, YS и др.

⁹⁵ Това не засяга никое приложимо национално право, което отговаря на изискванията на член 23 от ОРЗД, вж. глава 6.4.

данните. Член 15, параграф 4 от ОРЗД не се прилага по отношение на допълнителна информация относно обработването, както е посочено в член 15, параграф 1, букви а) — з) от ОРЗД.

170. Съгласно съображение 63, противоположни права или свободи включват търговски тайни или интелектуална собственост, и по-специално авторското право за защита на софтуера. Тези изрично посочени права и свободи следва да се разглеждат само като примери, тъй като по принцип всяко право или свобода, основано на правото на Съюза или на правото на държава членка, може да се счита, че се позовава на ограничението в член 15, параграф 4 от ОРЗД⁹⁶. Следователно, правото на защита на личните данни (член 8 от Харта на основните права на Европейския съюз) може също да се счита за засегнато право от гледна точка на член 15, параграф 4 от ОРЗД. Що се отнася до правото на получаване на копие, правото на защита на данните на други лица е типичен случай, при който ограничението трябва да бъде оценено. Освен това трябва да се вземе предвид и правото на поверителност на кореспонденцията, например по отношение на личната кореспонденция по електронна поща в сферата на заетостта⁹⁷. Важно е да се отбележи, че не всеки интерес се отнася до „правата и свободите“ съгласно член 15, параграф 4 от ОРЗД. Например, икономическите интереси на едно дружество да не разкрива лични данни не достигат прага за прибягване до изключението в член 15, параграф 4, стига да не са засегнати търговски тайни, интелектуална собственост или други защитени права.
171. „Други лица“ означава всяко друго лице или субект, освен субекта на данните, което упражнява своите права на достъп. Следователно трябва да се зачитат правата и свободите на администратора или обработващия лични данни (например пазене на поверителния характер на търговски тайни и интелектуална собственост). Ако законодателния орган на ЕС искаше да изключи правата и свободите на администраторите или обработващите лични данни, той щеше да използва понятието „трета страна“, което е определено в член 4, точка 10 от ОРЗД.
172. Общата загриженост, че правата и свободите на други лица могат да бъдат засегнати от изпълнението на искането за достъп, не е достатъчна за позоваване на член 15, параграф 4 от ОРЗД. Администраторът трябва да е в състояние да докаже, че в конкретната ситуация, правата или свободите на други лица няма да бъдат действително засегнати.

Пример 34: В миналото лице, което вече е възрастен човек, е било под грижите на Службата за младежта в продължение на няколко години. Съответните досиета може да съдържат чувствителна информация за такива лица (родители, социални работници, други ненавършили пълнолетие лица). Това обаче не е причина искане за информация от субекта на данните да бъде отхвърлено като цяло с позоваване на член 15, параграф 4 от ОРЗД. По-скоро трябва да се разгледат подробно правата и свободите на други лица и да се представят доказателства за това от Службата за младежта, в качеството ѝ на администратор. В зависимост от въпросните интереси и тяхната относителна тежест искането за предоставяне на такава специфична информация може да бъде отхвърлено (например с редактиране на имената).

⁹⁶ Тежестта или приоритетът на противоположните права и свободи не е въпрос, включен в определението на понятията „права и свободи“. Претеглянето на тези интереси обаче е част от втория етап на оценката на това дали член 15, параграф 4 е приложим. Вж. точка 173 по-долу.

⁹⁷ ЕКПЧ, *Vărbulescu*/Румъния, № 61496/08, т. 80, 5 септември 2017 г.

173. По отношение на съображение 4 от ОРЗД и обосновката на член 52, параграф 1 от Харта на основните права на Европейския съюз, правото на защита на личните данни не е абсолютно право⁹⁸. Следователно упражняването на правото на достъп трябва да бъде претеглено спрямо други основни права в съответствие с принципа на пропорционалност. Когато при оценката съгласно член 15, параграф 4 от ОРЗД се докаже, че изпълнението на искане влияе неблагоприятно (отрицателно) върху правата и свободите на други участници (етап 1), интересите на всички участници трябва да бъдат претеглени, като се вземат предвид специфичните обстоятелства на случая и по-специално вероятността, и сериозността на съществуващите рискове при съобщаването на данните. Администраторът следва да се опита да съгласува противоположни права (етап 2), например чрез прилагането на подходящи мерки, които смекчават риска за правата и свободите на други лица. Както е подчертано в съображение 63, защитата на правата и свободите на други лица по силата на член 15, параграф 4 от ОРЗД не следва да води до отказ за предоставяне на цялата информация на субекта на данните. Това означава например случаите, в които се прилага ограничението, съгласно което информацията относно други лица трябва да бъде направена нечетлива, доколкото е възможно, вместо да се отказва предоставянето на копие от личните данни. Ако обаче е невъзможно да се намери решение за съгласуване на съответните права, на следващия етап администраторът трябва да реши кои от противоположните права и свободи са с предимство (етап 3).

Пример 35: Търговец на дребно предлага на своите клиенти възможността да поръчват продукти чрез гореща линия, поддържана от неговия отдел за обслужване на клиенти. За целите на доказване на търговските сделки, търговецът съхранява запис на разговора, в съответствие със строгите изисквания на действащото законодателство. Клиент иска да получи копие от разговора, който е провел с представител на отдела за обслужване на клиенти. На първия етап, търговецът на дребно анализира искането и установява, че записът съдържа лични данни, които са свързани и с някой друг, а именно представителя на отдела за обслужване на клиенти. На втория етап, за да прецени дали предоставянето на копие би засегнало правата и свободите на други лица, търговецът трябва да претегли противоположните интереси, особено като се вземе предвид вероятността и тежестта на възможните рискове за правата и свободите на представителя на отдела за обслужване на клиенти, които се срещат при съобщаването на записа на клиента. Търговецът стига до заключението, че в записа са налице много ограничени лични данни, свързани с представителя на отдела, а именно неговия глас. Търговецът на дребно/администраторът счита, че представителят не може да бъде лесно разпознат. Освен това съдържанието на дискусиата е от професионален характер и субектът на данните е събеседник. Въз основа на горепосочените обстоятелства администраторът обективно заключава, че правото на достъп не влияе неблагоприятно върху правата и свободите на представителя на отдела за обслужване на клиенти и следователно може да предостави на субекта на данните пълния запис, включително частите от гласовият запис, които се отнасят до представителя на отдела.

Пример 36: Клиент на магазин за медицински материали желае да получи достъп до резултатите от измерване, които се отнасят до нейните крака, въз основа на член 15 от ОРЗД. Магазинът за медицински материали разполага с мерките на краката на субекта на данните с

⁹⁸ Вж. например и Съд на ЕС, съединени дела C-92/09 и C-93/09, Volker und Markus Schecke GbR и Hartmut Eifert/Провинция Hessen [GC], 9 ноември 2010 г., т. 48.

цел изработването на индивидуални медицински компресивни чорапогащи. Очевидно в магазина за медицински материали имат голям опит и са създали специална техника за точно измерване. След измерването в магазина, клиентът иска да използва резултатите от измерването, за да закупи по-евтини чорапи от друго място (като ги поръча в онлайн магазин). От магазина за медицински материали отказват частично достъп до данните на основание член 15, параграф 4 от ОРЗД, като твърдят, че поради техните специални, точни техники за измерване, резултатите са защитени като търговска тайна. Ако и доколкото администраторът е в състояние да докаже, че:

- предоставянето на субекта на данните на информация за резултатите от измерването не е възможно без да се разкрие как са направени измерванията и
- информацията за това как са направени измерванията, включително, ако е приложимо, точното определяне на точките на измерване, са търговска тайна

той може да прилага член 15, параграф 4 от ОРЗД.

Администраторът все пак ще трябва да предостави възможно най-много информация за резултатите от измерването, която няма да разкрие неговата търговска тайна, дори ако това ще предполага усилия за преразглеждане и редактиране на резултатите.

Пример 37: ИГРАЧ Х е регистриран като потребител в платформа за игри на ПЛАТФОРМА Y. Един ден ИГРАЧ Х бива уведомен, че неговият онлайн профил е бил ограничен. Тъй като ИГРАЧ Х вече не е в състояние да влезе в платформата, той иска от администратора достъп до всички лични данни, свързани с него. Освен това ИГРАЧ Х иска достъп до причините за ограничаването на профила. ПЛАТФОРМА Y, т.е. администраторът на платформата за онлайн игри, към която е подадено искането, информира ползвателите в своите общи условия, достъпни на неговия уебсайт, че всеки вид измама (главно чрез използване на софтуер на трета страна) ще доведе до временна или постоянна забрана от платформата. Освен това в своята политика за поверителност ПЛАТФОРМА Y информира потребителите за обработването на личните данни за целите на откриване на измами в игри в съответствие с изискванията, определени в член 13 от ОРЗД.

При получаването на искането за достъп на ИГРАЧ Х, от ПЛАТФОРМА Y следва му предоставят копие от личните данни, обработвани във връзка с него. По отношение на причината за ограничаването на профила, от ПЛАТФОРМА Y следва да потвърдят за ИГРАЧ Х, че са решили да ограничат неговия достъп до онлайн игри поради използването на една или повтарящи се измами в игри, което е в нарушение на общите правила за използване. В допълнение към информацията, предоставена за обработването с цел откриване на измама в игрите, от ПЛАТФОРМА Y трябва да предоставят на ИГРАЧ Х достъп до информацията, съхранявана във връзка с измамите на ИГРАЧ Х в игрите, което е довело до ограничението. По-специално от ПЛАТФОРМА Y следва да предоставят на ИГРАЧ Х информацията, която е довела до ограничаването на профила (*например* преглед на регистрационния файл, дата и час на измамата, откриване на софтуер на трета страна,...), с цел субектът на данните (*т.е.* ИГРАЧ Х) да провери дали обработваните данни са точни.

Въпреки това съгласно член 15, параграф 4 и съображение 63 от ОРЗД от ПЛАТФОРМА Y не са задължени да разкриват каквато и да е част от техническите операции на софтуера за борба с измамите, дори когато тази информация е свързана с ИГРАЧ Х, доколкото това може да се

счита за търговска тайна. Необходимото претегляне на интересите съгласно член 15, параграф 4 от ОРЗД ще доведе до това търговските тайни на ПЛАТФОРМА Y да изключват разкриването на тези лични данни, тъй като познаването на техническите операции на софтуера за борба с измамите може също така да позволи на ползвателя да избегне бъдещо разкриване на измама или злоупотреба⁹⁹.

174. Ако администратори откажат изцяло или частично да изпълнят искане за право на достъп по член 15, параграф 4 от ОРЗД, те трябва незабавно и най-късно в срок до един месец да информират субекта на данните за причините (член 12, параграф 4 от ОРЗД). Мотивите трябва да се отнасят до конкретните обстоятелства, за да могат субектите на данни да преценят дали искат да предприемат действия срещу отказа. Те трябва да включват информация за възможността да се подаде жалба до надзорен орган (член 77 от ОРЗД) и да се потърсят съдебни средства за правна защита (член 79 от ОРЗД).

6.3 Член 12, параграф 5 от ОРЗД

175. С член 12, параграф 5 от ОРЗД на администраторите се дава възможност да отхвърлят искания за правото на достъп, които са явно неоснователни или прекомерни. Тези понятия трябва да се тълкуват в тесен смисъл, тъй като принципите на прозрачност и безплатните права на субектите на данни не трябва да бъдат накърнявани.
176. Администраторите трябва да са в състояние да докажат на лицето защо смятат, че искането е явно неоснователно или прекомерно, и ако това бъде поискано, да обяснят причините на компетентния надзорен орган. Всяко искане следва да се разглежда за всеки отделен случай в контекста, в който е подадено, за да се реши дали е явно неоснователно или прекомерно.

6.3.1 Какво означава явно неоснователно?

177. Искане за правото на достъп е явно неоснователно, ако при прилагането на обективен подход е налице ясно и очевидно неспазване на изисквания на член 15 от ОРЗД. Както е специално обяснено в раздел 3 по-горе обаче, има много малко необходими условия по отношение на исканията за правото на достъп. Поради това ЕКЗД подчертава, че съществува само много ограничена възможност за позоваване на алтернативата по член 12, параграф 5 от ОРЗД за „явно неоснователно“ искане по отношение на исканията за право на достъп.
178. Освен това е важно да се припомни, че преди да се позоват на ограничението, администраторите трябва внимателно да анализират съдържанието и обхвата на искането. Например искане не следва да се разглежда като явно неоснователно, ако то е свързано с обработването на лични данни, които не са предмет на ОРЗД (в този случай искането изобщо не следва да се разглежда като искане по член 15).

⁹⁹ Степента на информацията, предоставена на лицата, ще бъде силно зависима от контекста, като се вземат предвид естеството на администратора и на нарушението на условията за предлагане на услуга. В някои случаи е възможно администраторът да може да предостави само основна информация в отговор на искане за достъп, за което се прилага член 15, параграф 4.

179. Други случаи, в които приложимостта на член 12, параграф 5 от ОРЗД се поставя под въпрос, са искания, свързани с информация или дейности по обработване, които ясно и очевидно не са предмет на дейностите по обработване на администратора.

Пример 38: Субект на данни отправя искане до общински орган относно данни, които се обработват от държавен орган. Вместо да се твърди, че искането е явно неоснователно, би било по-подходящо, както и по-лесно за органа, до който е отправно искането, да се потвърди, че тези данни не се обработват от органа (първи компонент на член 15 от ОРЗД: „дали“ се обработват лични данни)¹⁰⁰.

180. Администратор не следва да предполага, че дадено искане е явно неоснователно, когато субектът на данните е подал преди това искания, които са били явно неоснователни или прекомерни, или ако включва необективен или неподходящ език.

6.3.2 Какво означава „прекомерно“?

181. В ОРЗД няма определение за понятието „прекомерно“. От една страна, формулировката в член 12, параграф 5 от ОРЗД „по-специално поради своята повторяемост“ дава възможност да се стигне до заключението, че основният сценарий за прилагането на този член във връзка с член 15 от ОРЗД е свързан с броя на исканията на субект на данни за право на достъп. От друга страна, горепосочената фраза показва, че не са *a priori* изключени други причини, които могат да причинят прекомерност.
182. Разбира се, съгласно член 15, параграф 3 от ОРЗД относно правото на получаване на копие субект на данни може да подаде повече от едно искане до администратор¹⁰¹. В случай на искания, които потенциално биха могли да се считат за прекомерни, оценката за „прекомерност“ зависи от анализа, извършен от администратора, и специфичните характеристики на сектора, в който той осъществява дейност.
183. В случай на последващи искания трябва да се оцени дали прагът за разумни интервали (вж. съображение 63) е надхвърлен или не. Администраторите трябва внимателно да вземат предвид конкретните обстоятелства на всеки случай.
184. Например в случай на социални мрежи ще се очаква промяната в набора от данни да се извършва на по-кратки интервали, отколкото в случай на поземлени регистри или централни регистри на дружества. В случай на търговски асоциации следва да се вземе предвид честотата на контактите с потребителя. Съответно „разумните интервали“, в рамките на които субектите на данни могат отново да упражняват правото си на достъп, също се различават. Колкото по-често настъпват промени в базата данни на администратора, толкова по-често на субектите на данните може да бъде разрешено да поискат достъп до личните си данни, без това да се счита за прекомерно. От друга страна, второ искане от същото лице може да се счита при определени обстоятелства за наличие на повторяемост.
185. Когато решават дали е изтекъл разумен интервал, администраторите следва да вземат предвид следното с оглед на разумните очаквания на субекта на данните:

¹⁰⁰ Друг е въпросът дали органът, към който е отправено искането за достъп, има право да препрати искането към компетентния държавен орган.

¹⁰¹ Съгласно член 15, параграф 3, второ изречение администраторът може да наложи разумна такса за допълнително поискани копия.

- колко често се променят данните — малко ли е вероятно да са настъпили промени между исканията? Ако набор от данни очевидно не подлежи на обработване, различно от съхранение, и субектът на данните е наясно с това, например поради предишно искане за право на достъп, това може да е показател за прекомерно искане;
- естеството на данните — това може да включва дали са особено чувствителни;
- целите на обработването — това може да включва дали е вероятно обработването да причини влошаване (вреда) за лицето, оправило искането, ако бъде разкрито;
- дали последващите искания се отнасят до същия или до различен тип информация или дейности по обработване¹⁰².

Пример 39 (дърводелец): Субект на данни подава искания за данни на **всеки два месеца** до дърводелеца, който му е изработил маса. Дърводелецът отговаря изцяло на първото искане. Когато се решава дали е изтекъл разумен интервал, следва да се вземе предвид, че дърводелецът обработва и събира лични данни само понякога (първа подточка по-горе) и не като част от основната си дейност, като съществува още по-малка вероятност да предоставя често услуги на един и същи субект на данни. Действително в случая дърводелецът не е предоставил повече от една услуга на субекта на данните, което прави малко вероятно да са настъпили промени в набора от данни относно субекта на данните. Главно предвид естеството и количеството на обработваните лични данни рисковете, свързани с обработването, може да се считат за ниски (втора подточка по-горе), като няма вероятност целта на обработването (целите за фактуриране и спазване на задължението за водене на регистри) да навреди на субекта на данните (трета подточка по-горе). Освен това искането се отнася до същата информация като последното искане (четвърта подточка по-горе). Вследствие на това такива искания могат да се считат за прекомерни поради тяхната повтораемост.

Пример 40 (платформа на социални медии): Платформа на социални медии, чиято основна стопанска дейност е събирането и/или обработването на лични данни на субекти на данни, извършва мащабни, сложни и непрекъснати дейности по обработване. Субект на данни, който използва услугите на платформата, подава искания за достъп на **всеки три месеца**. В този случай честите промени в личните данни, свързани с лицето, са много вероятни (първа подточка по-горе), широкият набор от събрани данни включва предполагаеми чувствителни лични данни (втора подточка по-горе), обработвани с цел показване на субекта на данните на подходящо съдържание и членове на мрежата (трета подточка). При тези обстоятелства исканията за достъп, подавани на всеки три месеца, няма да се считат по принцип за прекомерни поради повтораемост.

Пример 41 (агенции за кредитиране): Както при социалните мрежи, не може да се изключи възможността измененията на съответните данни, съхранявани от агенции за кредитиране, да се извършват на много по-кратки интервали, отколкото в други области (първата подточка по-горе). Това се дължи на редица фактори, с които обикновено субектът на данни в качеството му на външно лице не е запознат поради сложността на модела на стопанска дейност.

¹⁰² Ако последващото искане се отнася до същия тип информация като обхват и време, не става въпрос за прекомерност, а за искане за допълнително копие, вж. раздел 2.2.2.2.

Следователно, отговорът на въпроса кои видове данни са били събрани от администратора за изчисляване на количествена оценка за определяне на стойността и кои са включени в момента в изчислението може да бъде предоставен само от самата агенция за кредитиране. Освен това обработването на данни чрез агенции за кредитиране и произтичащата от това количествена оценка за определяне на стойността може да имат широкообхватни последици за субекта на данните по отношение на предвидени правни сделки, като например сключване на договори за покупка, наем или лизинг (трета подточка по-горе).

Не е възможно като цяло да се определи някакъв конкретен интервал, в рамките на който подаването на допълнително искане за достъп може да се счита за прекомерно съгласно член 12, параграф 5, второ изречение от ОРЗД. По-скоро се изисква цялостно разглеждане на обстоятелствата за всеки отделен случай. Като се има обаче предвид значението на обработването на данните за действителното ежедневие на субектите на данни, може да се приеме, че **едногодишен интервал** между случаите на безплатно предоставяне на информацията ще бъде във всеки случай твърде голям, за да се счита искането за прекомерно. Ако искане се подава в рамките на много кратък интервал, решаващият фактор следва да бъде дали субектът на данните има основание да предполага, че след последното искане е налице промяна в информацията или обработването. Например, ако субектът на данните е извършил операция с финансови средства, като вземане на заем, той трябва да има право да поиска достъп до кредитната информация, въпреки че такова искане е било подадено и на него е отговорено скоро преди това.

186. Когато информацията може да се предостави лесно по електронен път или чрез достъп до защитена система от разстояние, което означава, че изпълнението на такива искания всъщност не натоварва администратора, малко вероятно е последващите искания да се считат за прекомерни.
187. Ако дадено искане се припокрива с предишно искане, припокриващото се искане обикновено може да се счита за прекомерно, ако и доколкото обхваща точно същата информация или дейности по обработване и предишното искане все още не е изпълнено от администратора, без да се достига до състоянието на „ненужно забавяне“ (вж. член 12, параграф 3 от ОРЗД). На практика, като следствие двете искания могат да бъдат комбинирани.
188. Фактът, че администраторът ще отдели много време и усилия да предостави информацията или копие на субекта на данните, не може сам по себе си да направи искането прекомерно¹⁰³. Големият брой дейности по обработване обикновено изискват по-големи усилия при изпълнение на искания за достъп. Както е посочено по-горе обаче, при определени обстоятелства исканията може да се разглеждат като прекомерни поради други причини, различни от тяхната повтаряемост. Според ЕКЗД това включва предимно случаи на неоснователно позоваване на член 15 от ОРЗД, което означава случаи, в които субектите на данни използват прекомерно правото на достъп единствено с намерението да причинят щета или вреда на администратора.
189. Във връзка с гореизложеното дадено искане не следва да се разглежда като прекомерно въз основа на това, че:

¹⁰³ Не се извършва тест за пропорционалност, вж. по-горе т. 166.

- субектът на данните не посочва причини за искането или администраторът счита искането за безсмислено;
- субектът на данните е използвал неподходящ или неучтив език;
- субектът на данните възнамерява да използва данните, за да предяви последващи иски срещу администратора¹⁰⁴.

190. От друга страна, дадено искане може да бъде сметено за прекомерно, например ако:

- лице подаде искане, но в същото време предлага да го оттегли в замяна на някаква форма на облага от страна на администратора, или
- искането е злонамерено и се използва за тормоз на администратора или неговите служители единствено с цел да предизвика смущения, например въз основа на факта, че:
 - лицето изрично е заявило, в самото искане или в други съобщения, че възнамерява да причини единствено смущения; или
 - лицето систематично изпраща на администратора, например веднъж седмично, различни искания като част от кампания с намерението и целта да причини смущения¹⁰⁵.

6.3.3 Последици

191. В случай на явно неоснователно и прекомерно искане за право на достъп администраторите могат съгласно член 12, параграф 5 от ОРЗД или да наложат разумна такса (като вземат предвид административните разходи за предоставяне на информация или съобщение или за предприемането на поисканите действия), или да откажат да изпълнят искането.
192. ЕКЗД посочва, че от една страна, администраторите не са като цяло задължени да налагат разумна такса, преди да откажат да предприемат действия по искане. От друга страна, те не са и напълно свободни да избират между тези две алтернативи. Всъщност администраторите трябва да вземат адекватно решение в зависимост от конкретните обстоятелства по случая. Като се има предвид, че е трудно да си представим, че налагането на разумна такса е подходяща мярка в случай на явно неоснователни искания, за прекомерни искания — в съответствие с принципа на прозрачност — често налагането на такса ще бъде по-подходящо като компенсация за административните разходи, породени от повтарящите се искания.
193. Администраторите трябва да са в състояние да докажат явно неоснователния или прекомерния характер на дадено искане (член 12, параграф 5, трето изречение от ОРЗД). Поради това се препоръчва да се осигури подходящо документиране на основните факти. В съответствие с член 12, параграф 4 от ОРЗД, ако администратори откажат изцяло или частично да предприемат действия по искане за достъп, те трябва незабавно и най-късно в срок до един месец от получаването на искането да информират субекта на данните за

¹⁰⁴ Това не засяга никое приложимо национално законодателство, което отговаря на изискванията на член 23 от ОРЗД, вж. глава 6.4.

¹⁰⁵ „Систематично изпращане като част от кампания“ означава, че искания, които лесно могат да бъдат обединени в едно, са изкуствено разделени от субекта на данните не само на няколко, а на много отделни части с очевидното намерение да причинят смущения.

- основанията,
- правото на жалба до надзорен орган;
- възможността да се потърсят съдебни средства за правна защита.

194. Преди да наложат разумна такса въз основа на член 12, параграф 5 от ОРЗД, администраторите следва да информират субектите на данни за своя план да направят това. Физическите лица трябва да могат да решат дали да оттеглят искането си, за да избегнат налагането на таксата.
195. Неоснователното отхвърляне на искания за право на достъп може да се разглежда като нарушение на правата на субектите на данни съгласно членове 12—22 от ОРЗД и следователно може да бъде обект на упражняване на корективни правомощия от страна на компетентните надзорни органи, включително административно наказание „глоба“ или „имуществена санкция“ на основание член 83, параграф 5, буква б) от ОРЗД. Ако лицата считат, че правата им са нарушени, те имат право да подадат жалба на основание член 77 от ОРЗД.

6.4 Възможни ограничения в правото на Съюза или в правото на държавите членки въз основа на член 23 от ОРЗД и дерогации

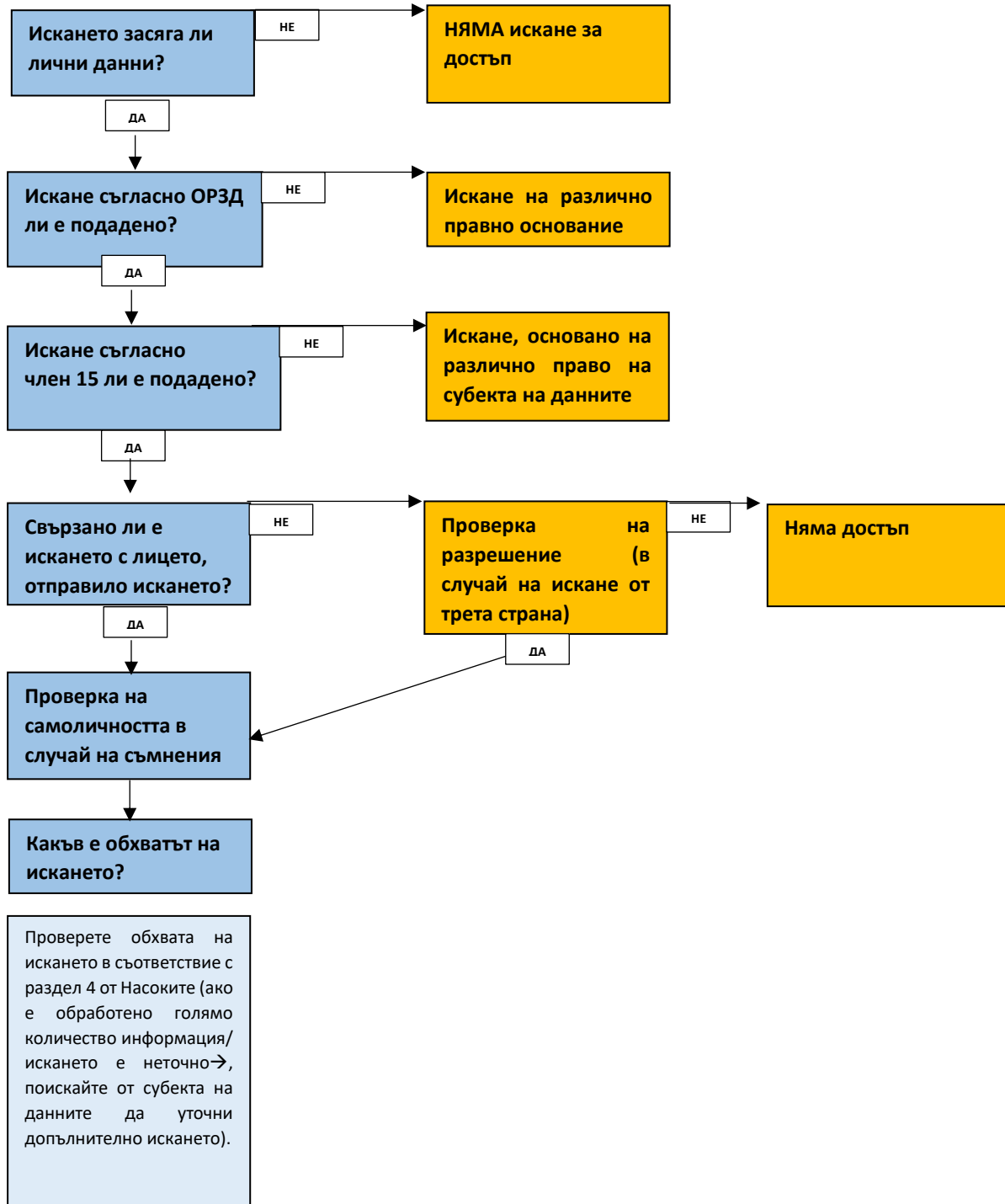
196. Обхватът на задълженията и правата, предвидени в член 15 от ОРЗД, може да бъде ограничен чрез законодателни мерки в правото на Съюза или правото на държавите членки¹⁰⁶.
197. Администраторите, които възнамеряват да разчитат на ограничение, основано на националното право, трябва внимателно да проверят изискванията на разпоредбата на съответното национално законодателство. Освен това е важно да се отбележи, че ограниченията на правото на достъп в правото на държавите членки (или на Съюза), които се основават на член 23 от ОРЗД, трябва стриктно да отговаря на условията, посочени в тази разпоредба. Европейският комитет по защита на данните издаде Насоки 10/2020 относно ограниченията по член 23 от ОРЗД с допълнителни разяснения по този въпрос. От гледна точка на правото на достъп ЕКЗД припомня, че администраторите следва да отменят ограниченията, щом престанат да са приложими обстоятелствата, които ги обосновават¹⁰⁷.
198. В законодателни мерки, които се отнасят до ограниченията по член 23 от ОРЗД, може също да се предвиди, че упражняването на дадено право е забавено във времето, че право се упражнява частично или че то е ограничено до определени категории данни или да може да се упражнява непряко чрез независим надзорен орган¹⁰⁸.

¹⁰⁶ Вж. например раздели 32—37 от Германския федерален закон за защита на данните (BDSG), раздели 16 и 17 от Норвежкия закон за защита на данните и глава 5 от Шведския закон за защита на данните.

¹⁰⁷ Точка 76 на Насоки 10/2020 относно ограниченията по член 23 от ОРЗД, версия 2.0, приета на 13 октомври 2021 г.

¹⁰⁸ Точка 12 от Насоки 10/2020 относно ограниченията по член 23 от ОРЗД, версия 2.0, приета на 13 октомври 2021 г. Член 34, параграф 3 от Германския федерален закон за защита на данните например гласи, че ако публичен орган не предостави информация на субект на данни, за да отговори на искане за право на достъп, поради определени ограничения, такава информация се предоставя на федералния надзорен орган по искане на субекта на данните, освен ако отговорният върховен федерален орган (спрямо органа, който е бил обект на искането) определи в отделния случай, че това би застрашило сигурността на Федерацията или на дадена провинция. Италианският кодекс за защита на данните предвижда непряк достъп (чрез органа), в случай че достъпът може да повлияе неблагоприятно върху редица интереси (например интерес, свързан с борбата с изпирането на пари), вж. член 2 от Италианския кодекс за защита на данните.

Етап 1: Как да се тълкува и да се оценява искането?



Етап 2: Как да отговорим на искането (1)?

3 основни компонента на правото на достъп (структура на член 15)		
Потвърждение дали личните данни се обработват	Достъп до личните данни	Допълнителна информация относно цели, получатели и др. (член 15, параграф 1, букви а)—з)

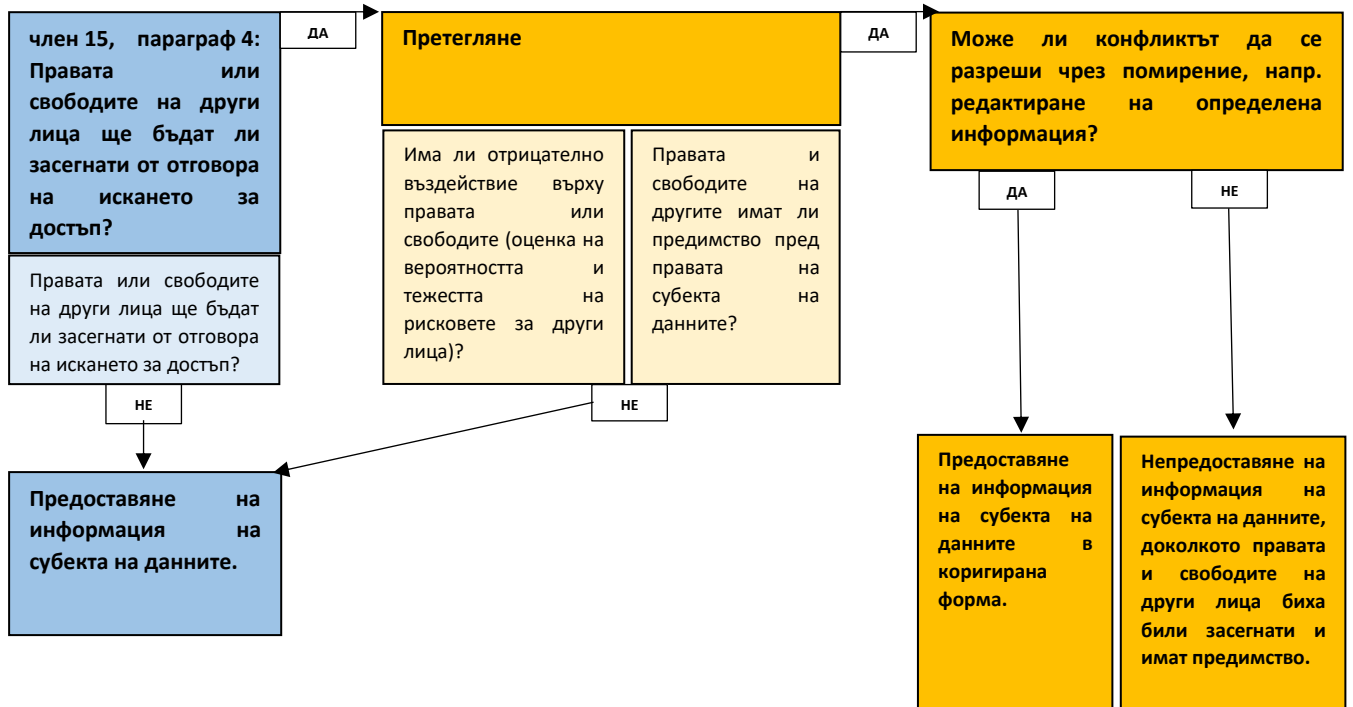
Етап 2: Как да отговорим на искането (2)?

Предприемане на необходими мерки			
член 12, параграф 1: кратка, прозрачна, разбираема и леснодостъпна форма		член 12, параграф 2: съдействие за упражняването на правото на достъп	
Избор между различни средства	Предоставяне на копие, ако не е договорено друго (член 15, параграф 3)	Използване на многослоен подход, ако е целесъобразно (най-подходящ в онлайн контекст)	Срок — без ненужно забавяне, при всички случаи в срок до един месец (удължаване с още два месеца в изключителни случаи) (член 12, параграф 3)

Етап 2: Как да отговорим на искането (3)?

Как може администраторът да извлече всички данни за субекта на данните?			
Определяне на критерии за търсене — въз основа на това, което субектът на данните е предоставил, друга информация, която администраторът притежава за лицето, и факторите, върху които са структурирани данните (например клиентски номер, IP-адреси, професионална квалификация, семейни отношения и т.н.)	Установяване на всички технически функции, които може да са налични за извличане на данни.	Търсене във всички ИТ системи, както и в регистри с лични данни, които не са основани на ИТ.	Обединяване, извличане или събиране по друг начин на данни, които са свързани със субекта на данните по начин, който отразява изцяло обработването, т.е. който включва всички лични данни относно лицето и му позволява да се запознае с обработването и да провери законосъобразността му. Извличането на информация може да се извърши за всеки отделен случай или, при целесъобразност, чрез използване на инструмент за поверителност на етапа на проектирането, който вече е въведен от администратора.

Етап 3: Проверка на рамки и ограничения (1)



Етап 3: Проверка на рамките и ограниченията (2)

