16/BG
WP 242 rev.01

Насоки относно правото на преносимост на данните

Приети на 13 декември 2016 г.
Последно преразгледани и приети на 5 април 2017 г.

Тази работна група е създадена в съответствие с член 29 от Директива 95/46/ЕО. Тя е независим европейски консултативен орган за защита на личните данни и неприкосновеността на личния живот. Нейните задачи са описани в член 30 от Директива 95/46/ЕО и член 15 от Директива 2002/58/ЕО.

Секретариатът се осигурява от Дирекция C (Основни права и върховенство на закона) на Генерална дирекция „Правосъдие и потребители“ на Европейската комисия, B-1049 Brussels, Belgium, Office No MO59 05/35.

Уебсайт: http://ec.europa.eu/justice/data-protection/index_en.htm

СЪДЪРЖАНИЕ

Обобщение

С член 20 от Общия регламент относно защитата на данните се въвежда ново право на преносимост на данните, което е тясно свързано с правото на достъп, но в много аспекти се различава от него. С това право субектите на данните могат да получават личните данни, които са предоставили на администратор, в структуриран, широко използван и пригоден за машинно четене формат и да прехвърлят тези данни на друг администратор. С това ново право се цели на субекта на данните да бъдат предоставени правомощия и по-висока степен на контрол над личните данни, които се отнасят до него.

Тъй като с правото на преносимост на данните се разрешава прякото предаване на лични данни от един администратор на данни на друг, то е също така важен инструмент, с който ще се подкрепя свободното движение на лични данни в ЕС и ще се насърчава конкуренцията между администраторите. Това право ще улесни преминаването от един доставчик на услуги към друг и следователно ще способства за развитието на нови услуги в контекста на стратегията за цифров единен пазар.

С настоящото становище се предоставят насоки относно начина на тълкуване и прилагане на правото на преносимост на данните, въведено с ОРЗД. То е насочено към обсъждане на правото на преносимост на данните и на неговия обхват. С него се изясняват условията, при които се прилага новото право, като се вземат предвид правното основание за обработване на данните (съгласието на субекта на данните или необходимостта от изпълнение на договор), както и фактът, че това право е ограничено до личните данни, предоставени от субекта на данните. В становището са дадени също така конкретни примери и критерии за пояснявӑне на обстоятелствата, при които правото е приложимо. В това отношение Работната група по член 29 счита, че правото на преносимост на данните обхваща данните, които са предоставени съзнателно и активно от субекта на данните, както и личните данни, генерирани от неговата дейност. Това ново право не може да бъде изпразвано от съдържание и да бъде ограничавано до личната информация, предоставена пряко от субекта на данните, например в онлайн формуляр.

Като добра практика администраторите на данни следва да започнат да разработват средствата, които ще допринесат за удовлетворяването на исканията за преносимост на данните, като инструменти за сваляне и приложно-програмни интерфейси. Те следва да гарантират, че личните данни се предават в структуриран, широко използван и пригоден за машинно четене формат, и следва да бъдат насърчавани да гарантират оперативната съвместимост на формата на данните, които се предоставят в изпълнение на искането за преносимост на данните.

Със становището се помага също така за ясното разбиране на съответните задължения на администраторите на данни и се препоръчват най-добри практики и инструменти, които подпомагат спазването на правото на преносимост на данните. Накрая, в становището се препоръчва заинтересованите страни от отрасъла и професионалните организации да разработят съвместно общ набор от оперативно съвместими стандарти и формати с цел изпълняване на изискванията, свързани с правото на преносимост на данните.

I. Въведение

С член 20 от Общия регламент относно защитата на данните (ОРЗД) се въвежда ново право на преносимост на данните. С това право субектите на данни могат да получават личните данни, които са предоставили на администратор на данни, в структуриран, широко използван и пригоден за машинно четене формат и да прехвърлят тези данни на друг администратор на данни без възпрепятстване. Това право, което е приложимо, при условие че са изпълнени определени условия, подкрепя избора на потребителя, контрола от негова страна и оправомощаването му.

Физическите лица, които желаеха да се възползват от своето право на достъп съгласно Директивата за защита на данните (Директива 95/46/ЕО), бяха ограничени от формата, избран от администратора на данни за предоставяне на поисканата информация. **С новото право на преносимост на данните се цели да бъдат предоставени правомощия на субектите на данни по отношение на техните собствени лични данни, тъй като то улеснява възможността им да преместват, копират или предават лични данни без затруднения от една ИТ среда към друга** (независимо дали към техните собствени системи, системите на доверени трети страни или на нови администратори на данни).

Като утвърждава личните права на физическите лица и техния контрол над личните данни, които ги засягат, преносимостта на данните представлява също така възможност за „възстановяване на равнопоставеността“ в отношението между субектите на данни и администраторите на данни[1].

Макар че правото на преносимост на личните данни може да подобри така също конкуренцията между услугите (като се улеснява смяната на доставчика), с ОРЗД се уреждат личните данни, а не аспектите на конкуренцията. По-специално с член 20 преносимите данни не са ограничени до такива, които са необходими или полезни за смяната на доставчика[2].

Въпреки че преносимостта на данните е ново право, вече съществуват и други типове преносимост или се обсъждат в други области на законодателството (например в контекста на прекратяването на договори, роуминга при съобщителните услуги и трансграничния достъп до услуги[3]). Възможно е да бъдат реализирани някои полезни взаимодействия между различните типове преносимост и дори ползи за физическите лица, ако се предоставят комбинирано, макар че към случаи, основани на аналогия, следва да се подхожда внимателно.

---

[1] С преносимостта на данните се цели основно да се засили контролът на физическите лица върху техните лични данни и да се гарантира, че те играят активна роля в екосистемата на данните.

[2] Например това право може да позволи на банките да предоставят допълнителни услуги под контрола на потребителя, като използват лични данни, които първоначално са събрани като част от услугата за доставка на електроенергия.

[3] Вж. Дневен ред на Европейската комисия за цифров единен пазар: https://ec.europa.eu/digital-agenda/en/digital-single-market, по-специално първият стълб на политиката „По-добър онлайн достъп до цифрови стоки и услуги“.

В настоящото становище са дадени насоки за администраторите на данни, за да могат да актуализират техните практики, процеси и политики, и се изяснява значението на понятието „преносимост на данните“, за да се даде възможност на субектите на данни ефективно да използват новото си право.

II. Кои са основните елементи на преносимостта на данните?

В член 20, параграф 1 от ОРЗД правото на преносимост на данните е определено, както следва:

> *Субектът на данните има право да получи личните данни, които го засягат и които той е предоставил на администратор, в структуриран, широко използван и пригоден за машинно четене формат и има правото да прехвърли тези данни на друг администратор без възпрепятстване от администратора, на когото личните данни са предоставени […].*

- **Право на получаване на лични данни**

Първо, преносимост на данните представлява **правото на субекта на данните да получи поднабор от личните данни,** които го засягат и които са обработени от администратора на данни, и да съхранява тези данни за по-нататъшна лична употреба. Това съхранение може да се осъществи на частно устройство или в частна облачна среда, без да е задължително данните да се предават на друг администратор на данни.

В това отношение правото на преносимост на данните допълва правото на достъп. Една от специфичните особености на преносимостта на данните се дължи на факта, че тя предлага лесен начин, по който субектите на данните самостоятелно да управляват и повторно да използват личните данни. Тези данни следва да бъдат получени *„в структуриран, широко използван и пригоден за машинно четене формат“*. Например субектът на данните може да се интересува от извличане на своята текуща плейлиста (или хронология на слушаните песни) от услуга за стрийминг на музика, за да разбере колко пъти е слушал определени песни или за да провери каква музика желае да закупи или да слуша на друга платформа. По същия начин той може да пожелае да извлече и списъка със своите контакти от приложението към уеб-базираната си поща, за да състави например сватбен списък, да получи информация за покупките с различни карти за лоялност или да определи своя въглероден отпечатък[4].

- **Право на предаване на лични данни от един администратор на данни към друг администратор на данни**

Второ, с член 20, параграф 1 на субектите на данните се предоставя **правото да предават лични данни от един администратор на данни към друг администратор**

[4] В тези случаи обработването на данните от страна на субекта на данни може или да попадне в обхвата на дейностите в рамките на домакинството, когато цялото обработване се извършва единствено под контрола на субекта на данните, или може да бъде осъществено от дадена друга страна от името на субекта на данните. В последния случай другата страна следва да се счита за администратор на данни, дори да е единствено с цел съхраняване на личните данни, като трябва да се спазват принципите и задълженията, определени в ОРЗД.

на данни „без възпрепятстване“. Данните може да се предават направо от един администратор на данни към друг по искане на субекта на данните и когато това е технически осъществимо (член 20, параграф 2). В тази връзка в съображение 68 администраторите на данни се насърчават да разработват оперативно съвместими формати, които дават възможност за преносимост на данните,[5] но без да се поражда задължение за администраторите да приемат или поддържат технически съвместими системи за обработване[6]. Съгласно ОРЗД обаче се забранява на администраторите да създават пречки пред предаването.

По същество този елемент на преносимостта на данните дава възможност на субектите на данни не само да получат и да използват повторно данните, които са предоставили, но също така да ги предават на друг доставчик на услуги (независимо дали в същия или в различен сектор на стопанска дейност). С правото на преносимост на данните, освен че на потребителя се предоставят правомощия чрез предотвратяване на поставянето му в зависимост („lock-in“), се очаква да се насърчават възможностите за иновации и да се споделят лични данни между администраторите на данни по безопасен и сигурен начин и под контрола на субекта на данните[7]. С преносимостта на данните може чрез потребителите да се поощрява контролираното и ограничено споделяне на лични данни между организации, а оттам и да се обогатява опита с услугите и потребителите[8]. Преносимостта на данните, които засягат потребителите, може да улесни предаването и повторното използване на лични данни между различните услуги, от които те се интересуват.

- **Администриране**

Преносимостта на данните гарантира правото да се получават и да се обработват лични данни според желанията на субекта на данните[9].

Администраторите на данни, когато отговарят на искания за преносимост, съгласно определените в член 20 условия, не носят отговорност за обработване, осъществено от субекта на данните или от друго дружество, получило личните данни. Те действат от името на субекта на данните, включително когато личните данни се предават направо на друг администратор на данни. В това отношение администраторът на данни не носи отговорност за съответствието на получаващия администратор на данни с правото в областта на защитата на данните, като се има предвид, че получателят не се избира от изпращащия администратор на данни. В същото време администраторът следва да предвиди гаранции с цел потвърждаване, че действително ще действа от името на субекта на данните. Например може да се въведат процедури, за да се гарантира, че

[5] Вж. също раздел V.

[6] В резултат на това следва да се обърне специално внимание на формата на предаваните данни, за да се гарантира, че с малко усилия данните може да се използват повторно от субекта на данните или от друг администратор на данни. Вж. също раздел V.

[7] Вж. няколко експериментални приложения в Европа, например MiData в Обединеното кралство, MesInfos / SelfData от FING във Франция.

[8] Областите, наречени „самоизмерване на жизнени показатели“ и „интернет на нещата“, са показали ползата (и рисковете) от свързването на личните данни от различни аспекти на живота на дадено физическо лице като фитнес, активност и прием на калории, за да се даде по-пълно описание за живота на физическото лице в рамките на един файл.

[9] Правото на преносимост на данните не е ограничено до лични данни, които са полезни и са от значение за аналогични услуги, предоставяни от конкурентите на администратора на данни.

предаваните лични данни наистина са от вида, който субектът на данните желае да предаде. Това може да се постигне, като се получи потвърждение от субекта на данните или преди предаването, или по-рано, когато е дадено първоначалното съгласие за обработване или е финализиран договорът.

Когато администраторите на данни отговарят на искане за преносимост на данните, те нямат специално задължение преди да предадат данните да проверяват и удостоверяват качеството им. Разбира се тези данни вече следва да са точни и актуални в съответствие с принципите, посочени в член 5, параграф 1 от ОРЗД. Освен това с преносимостта на данните не се налага задължение на администратора на данни да запазва лични данни за по-дълъг период от необходимото или след даден определен период на запазване[10]. Важно е да се отбележи, че няма допълнително изискване за запазване на данни след иначе приложимите периоди на запазване, само за да се отговори на евентуално бъдещо искане за преносимост на данните.

Когато поисканите лични данни се обработват от даден обработващ лични данни, сключеният в съответствие с член 28 от ОРЗД договор трябва да включва задължението да се подпомага „администратора, (…), чрез подходящи технически и организационни мерки (…) да отговори на искания за упражняване на предвидените (…) права на субектите на данни“. Следователно администраторът на данни следва да въведе специални процедури в сътрудничество с обработващите лични данни, с които работи, за да отговори на исканията за преносимост на данните. В случай на съвместно администриране, следва ясно да бъдат разпределени в договор отговорностите между всеки администратор на данни, що се отнася до обработването на искания за преносимост на данните.

Освен това получаващият администратор на данни[11] отговаря за осигуряването на гаранция, че предоставените преносими данни са релевантни и не са прекомерни във връзка с новото обработване на данните. Например ако към услуга за уеб-базирана поща е отправено искане за преносимост на данните, когато искането се използва от субекта на данните за получаването на електронни съобщения и за изпращането им към сигурна платформа за архивиране, не е необходимо новият администратор на данни да обработва данните за контакт на кореспондентите на субекта на данните. Ако тази информация не е от значение предвид целта на новото обработване, тя не следва да се пази и обработва. Във всички случаи получаващите администратори на данни не са задължени да приемат и обработват лични данни, които са предадени вследствие на искане за преносимост на данните. Аналогично, когато субект на данните поиска предаване на данни за неговите банкови операции към услуга, която подпомага управлението на бюджета му, получаващият администратор на данни не е нужно да приема всички данни или да запазва подробна информация за операциите, след като те са отбелязани за целите на новата услуга. С други думи, следва да се приемат и запазват само онези данни, които са необходими и релевантни за услугата, предоставяна от получаващия администратор на данни.

[10] В горния пример, ако администраторът на данни не запазва записи на пусканите песни от потребителя, тогава тези лични данни не могат да бъдат включвани в искането за преносимост на данните.

[11] т.е. който получава личните данни, след като субектът на данните е отправил искане за преносимост на данните към друг администратор на данни.

„Получаващата“ организация става новият администратор на данни по отношение на тези лични данни и трябва да спазва принципите, посочени в член 5 от ОРЗД. Следователно „новият“ получаващ администратор на данни трябва ясно и непосредствено да посочи целта на новото обработване при всяко искане за предаване на преносими данни в съответствие с изискванията за прозрачност, посочени в член 14[12]. Що се отнася до всяко друго обработване на данни, което се извършва на негова отговорност, администраторът на данни следва да прилага определените в член 5 принципи като законосъобразност, добросъвестност и прозрачност, ограничение на целите, свеждане на данните до минимум, точност, цялостност и поверителност, ограничение на съхранението и отчетност[13].

Администраторите на данни, които съхраняват лични данни, следва да са подготвени да способстват за упражняването на правото на преносимост на данните, предоставено на техните субекти на данните. Администраторите на данни могат да изберат така също да приемат данни от даден субект на данни, но не са задължени да го направят.

- **Преносимост на данните спрямо другите права на субектите на данните**

Когато физическото лице упражнява своето право на преносимост на данните, това се извършва без да се засяга никое друго право (какъвто е случаят с всички други права според ОРЗД). Субектът на данните може да продължи да използва и да се ползва от услугата на администратора на данни дори след операцията по преносимост на данните. Преносимостта на данните не води автоматично до изтриването на данните[14] от системите на администратора на данни и не засяга първоначалния период на запазване, който се отнася за предадените данни. Субектът на данните може да упражнява своите права, докато администраторът на данни продължава да обработва данните.

Също така, ако субектът на данните желае да упражни своето право на изтриване (правото „да бъдеш забравен“ съгласно член 17), администраторът на данни не може да използва преносимостта на данните като причина да отложи или откаже въпросното изтриване.

Ако субект на данните установи, че личните данни, поискани според правото на преносимост на данните, не отговарят напълно на неговото искане, всяко следващо искане на лични данни според правото на достъп следва да бъде изпълнено в пълна степен при спазване на член 15 от ОРЗД.

Освен това, ако специално европейско право или право на държава членка в друга област също предвижда някаква форма на преносимост на въпросните данни,

[12] Освен това новият администратор на данни не следва да обработва лични данни, които не са релевантни, а обработването трябва да бъде ограничено до необходимото за новите цели дори ако личните данни са част от по-голям набор от данни, който е предаден чрез процеса на преносимост. Личните данни, които не са необходими за постигането на целта на новото обработване, следва да бъдат изтрити възможно най-скоро.

[13] След като администраторът на данни получи личните данни, изпратени при упражняването на правото на преносимост на данните, те може да се считат за „предоставени от“ субекта на данните и да бъдат препредадени в съответствие с правото на преносимост на данните, доколкото са изпълнени останалите условия, които са приложими по отношение на това право (т.е. правното основание на обработването, …).

[14] както е посочено в член 17 от ОРЗД.

определените условия по тези специални закони също трябва да бъдат взети предвид, когато се удовлетворява искането за преносимост на данните съгласно ОРЗД. Първо, ако от направеното от субекта на данните искане е видно, че намерението му не е да упражнява права съгласно ОРЗД, а по-скоро да упражнява права само съгласно отрасловото законодателство, тогава разпоредбите за преносимост на данните според ОРЗД няма да се прилагат по отношение на това искане[15]. От друга страна, ако искането касае преносимостта съгласно ОРЗД, наличието на такова специално законодателство не отменя общоприложимостта на принципа на преносимост на данните по отношение на всеки администратор на данни, както е предвидено в ОРЗД. Вместо това на база конкретен случай трябва да се преценява как въпросното специално законодателство може да засегне правото на преносимост на данните, ако изобщо това е възможно.

III. Кога се прилага преносимост на данните?

- **Кои операции по обработване са обхванати от правото на преносимост на данните?**

С оглед на спазването на ОРЗД от администраторите на данни се изисква да разполагат с ясно правно основание за обработването на лични данни.

В съответствие с член 20, параграф 1, буква а) от ОРЗД, **за да попаднат в обхвата на преносимостта на данните**, операциите по обработване трябва да са основани:

- или на съгласието на субекта на данните (съгласно член 6, параграф 1, буква а), или съгласно член 9, параграф 2, буква а), когато става дума за специални категории лични данни);

- или на договор, по който субектът на данните е страна съгласно член 6, параграф 1, буква б).

Например заглавията на книгите, закупени от дадено физическо лице от онлайн книжарница, или песните, които са слушани чрез услуга за музикален стрийминг, представляват примери за лични данни, които обикновено попадат в обхвата на преносимостта на данните, защото се обработват въз основа на изпълнението на договор, по който субектът на данните е страна.

С ОРЗД не се установява общо право на преносимост на данните за случаите, когато обработването на лични данни не е основано на съгласие или на договор[16]. Например

[15] Например ако искането на субекта на данните се отнася изрично до предоставянето на достъп до информация за неговата банкова сметка към доставчик на услуги, свързани с информация за сметки, за целите на Втората директива за платежните услуги (ДПУ2), този достъп следва да бъде предоставен в съответствие с разпоредбите на тази директива.

[16] Вж. съображение 68 и член 20, параграф 3 от ОРЗД. В член 20, параграф 3 и съображение 68 се посочва, че преносимостта на данните не се прилага, когато обработването на данните е необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора на данни, както и когато администраторът на данни изпълнява обществените си задължения или спазва дадено правно задължение. По тази причина администраторите на данни не са задължени да осигуряват преносимост в тези случаи. Добра практика е обаче да се

финансовите институции не са задължени да отговарят на искане за преносимост на данните, което се отнася до лични данни, обработвани в рамките на техните задължения да предотвратяват и откриват изпиране на пари и други финансови престъпления; преносимостта на данните не обхваща също така данните за контакт в професионалната сфера, обработвани в отношението между дружества, когато обработването не се основава нито на съгласието на субекта на данните, нито на договор, по който той е страна.

Когато се касае за данни на служители, правото на преносимост на данните се прилага само ако обработването е основано на договор, по който субектът на данните е страна. В много случаи съгласието няма да се счита за свободно дадено в този контекст поради неравнопоставеността между работодателя и служителя по отношение на правомощията[17]. Вместо това някои случаи на обработване, касаещи човешките ресурси, се базират на правното основание за законен интерес или са необходими за спазването на конкретни правни задължения в областта на трудовата заетост. На практика правото на преносимост на данните в контекста на човешките ресурси несъмнено ще е свързано с определени операции по обработване (като услуги по заплащане и обезщетяване, вътрешно наемане на персонал), но в много други ситуации ще е необходим подход, основан на конкретен случай, за да се удостовери дали са изпълнени всички условия, които са приложими за правото на преносимост на данните.

Накрая, правото на преносимост на данните се прилага само ако обработването на данните „става по автоматичен начин“ и следователно не обхваща повечето досиета на хартиен носител.

- **Какви лични данни трябва да се включват?**

В съответствие с член 20, параграф 1, за да попадат в обхвата на правото на преносимост, данните трябва да бъдат:

- лични данни, които засягат субекта на данните; както и
- които субектът на данните е *предоставил* на администратор на данни.

В член 20, параграф 4 се казва също така, че спазването на това право не следва да влияе неблагоприятно върху правата и свободите на други лица.

Първо условие: лични данни, които засягат субекта на данните

В обхвата на искане за преносимост на данните се включват само лични данни. Следователно всички данни, които са анонимни[18], или не се отнасят до субекта на данните, не биха попаднали в обхвата. В обхвата обаче се включват данни за

разработват процеси за автоматично отговаряне на искания за преносимост чрез спазване на принципите, уреждащи правото на преносимост на данните. Пример за това би била дадена държавна служба, осигуряваща лесно сваляне на подадените документи за личните данъци върху доходите за минали периоди. Като добра практика за преносимост на данните в случай на обработване, основано на правно основание по необходимост, за законен интерес и за съществуващи доброволни схеми вж. стр. 47 и 48 от Становище 6/2014 относно законните интереси на Работната група по член 29 (WP217).

[17] Както беше посочено от Работната група по член 29 в нейното Становище 8/2001 от 13 септември 2001 г. (WP48).

[18] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

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).

В много случаи администраторите на данни 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 гласова връзка чрез интернет (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 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).

Второ условие: данните са предоставени от субекта на данните

Второто условие стеснява обхвата до данните, „предоставени от“ субекта на данните.

Има много примери за лични данни, които са „предоставени от“ субекта на данните съзнателно и активно, като данни за акаунт (например адрес за кореспонденция, потребителско име, възраст), които са предоставени чрез онлайн формуляр. Все пак данни, „предоставени от“ субекта на данните, също се генерират в резултат от наблюдението на неговата дейност. Съответно Работната група по член 29 счита, че, за да се осигурят всички ползи от това право, в „предоставени от“ трябва да се включват също така личните данни, които са генерирани при наблюдението на дейностите на потребителите, като първични данни, обработени от интелигентно измервателно устройство или други видове свързани предмети[19], дневници на дейността, хронология на използването на уебсайтове или търсения.

Тази последна категория данни не включва данните, създадени от администратора на данни (с използване на наблюдаваните данни или на пряко предоставените входни данни), като потребителски профил, създаден чрез анализ на първичните данни, събрани от интелигентно измервателно устройство.

Разграничават се различни категории данни в зависимост от техния произход, за да се определи дали са обхванати от правото на преносимост на данните. Следните категории данни може да бъдат определени като „предоставени от субекта на данните“:

- **данни, които активно и съзнателно са предоставени от субекта на данните** (например адрес за кореспонденция, потребителско име, възраст и т.н.);
- **наблюдавани данни, предоставени от субекта на данните посредством използването на дадена услуга или дадено устройство**. Те може да включват например хронология на търсенията на лицето, данни за трафика и данни за

[19] Благодарение на възможността да се извличат данни от наблюдението на неговата дейност, субектът на данните ще може също така да получи по-добра представа за изборите, свързани с прилагането и направени от администратора на данни във връзка с обхвата на наблюдаваните данни, и ще бъде в състояние по-добре да избере какви данни желае да предостави, за да получи аналогична услуга, както и да е наясно в каква степен се зачита правото му на неприкосновеност на личния живот.

местоположението. Може да включват също така други първични данни като например пулса, отчетен от носимо устройство.

Обратно, логически изведените данни и производните данни са създадени от администратора на данни въз основа на данните, „предоставени от субекта на данните“. Например резултатът от оценка на здравето на потребител или профилът, създаден в контекста на управлението на риска и финансовите разпоредби (например за определяне на кредитоспособността или за спазване на правилата за борба с изпирането на пари), не може сами по себе си да се считат за „предоставени от“ субекта на данните. Въпреки че тези данни може да са включени в профил, който се съхранява от администратор на данните, и да са логически изведени или производни от анализа на данните, предоставени от субекта на данните (например чрез действията му), тези данни обикновено не се считат за „предоставени от субекта на данните“ и съответно не попадат в обхвата на това ново право[20].

Обикновено, като се имат предвид целите на политиката във връзка с правото на преносимост на данните, терминът „предоставени от субекта на данните“ трябва да се тълкува разширително, като не се допускат „логически изведените данни“ и „производните данни“, които включват лични данни, създадени от доставчик на услуги (например алгоритмични резултати). Администраторът на данни може да изключи тези логически изведени данни, но следва да включи всички други лични данни, предоставени от субекта на данните чрез технически средства, които са осигурени от администратора[21].

Следователно терминът „предоставени от“ включва лични данни, които се отнасят до дейността на субекта на данните или са резултат от наблюдаването на поведението на даденото физическо лице, но не включва данните, генерирани от последващия анализ на това поведение. Обратно, всички лични данни, които са създадени от администратора на данни в рамките на обработването на данните, например чрез процес на персонализация или препоръчване, чрез категоризиране или профилиране на потребители, представляват производни или логически изведени данни от личните данни, предоставени от субекта на данните, и не са обхванати от правото на преносимост на данните.

<u>Трето условие: правото на преносимост на данните не следва да влияе неблагоприятно върху правата и свободите на други лица</u>

[20] Въпреки това субектът на данните все пак може да се възползва от своето „право да получи от администратора потвърждение дали се обработват лични данни, свързани с него, и ако това е така, да получи достъп до данните“, както и информация относно „съществуването на автоматизирано вземане на решения, включително профилирането, посочено в член 22, параграфи 1 и 4, и поне в тези случаи съществена информация относно използваната логика, както и значението и предвидените последствия от това обработване за субекта на данните“ в съответствие с член 15 от ОРЗД (който се отнася до правото на достъп).

[21] Тук се включват всички наблюдавани данни за субекта на данните по време на дейностите, за целите на които се събират данните, като хронология на операциите или дневник на достъпа. Данните, които се събират чрез проследяване и записване на субекта на данните (като приложение, което записва пулса, или технология, използвана за проследяване на разглежданията), също следва да се считат за „предоставени от“ него, дори когато данните не са предадени активно или съзнателно.

По отношение на личните данни, засягащи други субекти на данни:

С третото условие се цели да се избегне извличането и предаването на данни, съдържащи лични данни на други субекти на данни (които не са дали съгласие), към нов администратор на данни в случаи, когато има вероятност тези данни да бъдат обработвани по начин, който би повлиял неблагоприятно върху правата и свободите на други субекти на данни (член 20, параграф 4 от ОРЗД)[22].

Например подобно неблагоприятно влияние би настъпило, ако предаването на данни от един администратор на данни към друг, би попречило на трети страни да упражняват техните права като субекти на данни съгласно ОРЗД (като правата на информация, достъп и т.н.).

Субектът на данни, който инициира предаването на данните си към друг администратор на данни, или дава съгласие новият администратор да ги обработва, или сключва договор с този администратор. Когато лични данни на трети страни са включени в набора от данни, трябва да се определи друго правно основание за обработването. Например администраторът на данни може да преследва законен интерес съгласно член 6, параграф 1, буква е), по-специално когато целта на администратора на данни е да предостави услуга на субекта на данните, която позволява на последния да обработва лични данни за чисто лични или домакински дейности. Субектът на данните продължава да носи отговорност за операциите по обработването, инициирани от него в контекста на лична дейност, която засяга или евентуално влияе върху трети страни, доколкото решението за такова обработване по никакъв начин не е взето от администратора на данни.

Например услуга за уеб-базирана поща може да позволи създаването на директория с контактите, приятелите, родините, семейството и по-широкото обкръжение на субекта на данните. Тъй като тези данни са свързани с (и са създадени от) физическо лице, което може да бъде идентифицирано и което желае да упражни неговото право на преносимост на данните, администраторите на данни следва да предадат цялата директория с входящи и изходящи електронни съобщения на въпросния субект на данните.

Аналогично банковата сметна на субекта на данни може да съдържа лични данни относно операциите не само на титуляря на сметката, но също така на други физически лица (например ако са превели пари на титуляря на сметката). Съществува малка вероятност правата и свободите на тези трети страни да бъдат повлияни неблагоприятно от предаването на информация за банковата сметка на титуляря на сметката в изпълнение на отправено искане за преносимост, при условие че и в двата примера данните се използват за една и съща цел (например адрес за контакт, който се използва само от субекта на данните или хронология на операциите с банковата сметка на субекта на данните).

Обратно, правата и свободите на трети страни няма да бъдат зачетени, ако новият администратор на данни използва личните данни за други цели, например ако получаващият администратор на данни използва личните данни на други физически

[22] В съображение 68 се казва, че „[к]огато в определен пакет от лични данни е засегнат повече от един субект на данни, правото личните данни да бъдат получавани следва да не засяга правата и свободите на други субекти на данни в съответствие с настоящия регламент“.

лица, съдържащи се в директорията с контактите на субекта на данните, за целите на маркетинга.

Следователно, за да се избегнат неблагоприятни последици за свързаната трета страна, обработването на такива лични данни от друг администратор е разрешено само доколкото данните се съхраняват под пълния контрол на потребителя, отправил искането, и се управляват единствено за лични или домакински нужди. Получаващият „нов“ администратор на данни (на когото данните може да бъдат предадени по искане на потребителя) не може да използва предадените данни на трета страна за свои собствени цели, например за да предлага продукти и услуги на въпросните субекти на данни — трети страни. Например тази информация не следва да се използва за обогатяване на профила на субекта на данни трета страна, и за пресъздаването на неговата социална среда без неговото знание и съгласие[23]. Не може да се използва така също за извличането на информация за такива трети страни и за създаването на специфични профили дори когато техните лични данни вече се съхраняват от администратора на данни. В противен случай това обработване може да се окаже незаконосъобразно и недобросъвестно, и по-специално ако съответните трети страни не са уведомени и не могат да упражнят своите права като субекти на данни.

Освен това една от водещите практики за всички администратори на данни (както „изпращащите“, така и „получаващите“ страни) се състои във внедряването на инструменти, чрез които субектите на данните могат да избират съответните данни, които желаят да получат и предадат, и да изключват, когато е целесъобразно, данните на други физически лица. Това допълнително ще спомогне да се намалят рисковете за третите страни, чиито лични данни може да бъдат пренесени.

Освен това администраторите на данни следва да внедрят механизми за предоставяне на съгласие от другите свързани субекти на данни, за да се улесни предаването на данните в случаите, когато такива страни желаят да дадат съгласие, например ако те също желаят да прехвърлят техните данни към някой друг администратор на данни. Такава ситуация може да възникне например при социалните мрежи, но администраторите на данни следва да решат коя водеща практика да използват.

Относно данните, които са обект на интелектуална собственост и търговска тайна:
Правата и свободите на други лица се споменават в член 20, параграф 4. Въпреки че не са пряко свързани с преносимостта, това може да се разбира като включително „търговската тайна или интелектуалната собственост, и по-специално върху авторското право за защита на софтуера“. Макар че тези права трябва да бъдат взети предвид преди да се отговори на дадено искане за преносимост на данните, все пак „[т]ези съображения [обаче] не следва да представляват отказ за предоставяне на цялата информация на съответния субект на данни“. Освен това администраторът на данни не следва да отхвърля искане за преносимост на данните въз основа на нарушаване на друго договорно право (например неуреден дълг или търговски конфликт със субекта на данните).

[23] Услуга за социални мрежи не следва да обогатява профила на своите членове, като използва лични данни, предадени от даден субект на данни при упражняване на неговото право на преносимост на данните, без да се зачита принципът на прозрачност и също така като се гарантира, че те са базирани на подходящо правно основание, що се отнася до това конкретно обработване.

Правото на преносимост на данните не представлява право физическото лице да злоупотребява с информацията по начин, който би могло да се определи като нелоялна практика или който би бил нарушение на права на интелектуална собственост.

Потенциалният стопански риск обаче сам по себе си не може да служи като основание за отказ да се отговори на искане за преносимост и администраторите на данни могат да предават личните данни, предоставени от субекти на данни, по такъв начин, че да не се издава информация, която е обект на търговска тайна или права на интелектуална собственост.

IV. Как общите правила, уреждащи упражняването на правата на субектите на данни, се прилагат по отношение на преносимостта на данните?

- Каква предварителна информация трябва да бъде предоставена на субекта на данните?

В изпълнение на новото право на преносимост на данните, администраторите на данни трябва да уведомяват субектите на данни за наличието на новото право на преносимост. Когато съответните лични данни се събират направо от субекта на данните, това трябва да стане „в момента на получаване на личните данни“. Ако личните данни не са били получени от субекта на данните, администраторът на данни трябва да предостави информацията, предвидена по член 13, параграф 2, буква б) и член 14, параграф 2, буква в).

„Когато личните данни не са получени от субекта на данните“, според член 14, параграф 3 се изисква информацията да бъде предоставена в рамките на разумен срок, който да не превишава един месец след получаването на данните, при осъществяване на първия контакт със субекта на данните или когато данните се разкриват пред трети страни[24].

Когато предоставят изискваната информация, администраторите на данни трябва да гарантират, че те правят разликата между правото на преносимост на данните и останалите права. По тази причина Работната група по член 29 препоръчва по-специално администраторите на данни ясно да обясняват разликата между видовете данни, които субектът на данните може да получава въз основа на правата на субекта на достъп до данни и преносимост на данните.

Освен това Работната група препоръчва администраторите на данни винаги да включват информация относно правото на преносимост на данните, преди субектите на данни да закрият даден акаунт, който може да имат. Това позволява на потребителите да проверят техните лични данни и лесно да изпратят данните към свое собствено устройство или към друг доставчик, преди съответният договор да бъде прекратен.

В заключение трябва да се отбележи, че Работната група по член 29 препоръчва на „получаващите“ администратори на данни като водеща практика да се предоставя на субектите на данни пълна информация за естеството на личните данни, които са релевантни за изпълнението на техните услуги. Освен че по този начин се подкрепя

[24] Според член 12 се изисква администраторите на данни да предоставят „всякаква комуникация [...] в кратка, прозрачна, разбираема и лесно достъпна форма, на ясен и прост език, особено що се отнася до всяка информация, конкретно насочена към деца“.

добросъвестното обработване, по този начин се позволява на потребителите да ограничат рисковете за третите страни и също така всяко друго ненужно дублиране на личните данни дори когато не са обвързани други субекти на данни.

- **Как администраторът на данни може да идентифицира субекта на данните, преди да отговори на неговото искане?**

В ОРЗД не са предписани изисквания за това как да се установява автентичността на субекта на данните. В член 12, параграф 2 от ОРЗД все пак се казва, че администраторът на данни, не следва да отказва да предприеме действия по искане на субекта на данните за упражняване на правата му (в това число правото на преносимост на данните), освен ако обработва лични данни за цели, за които не се изисква идентифициране на субекта на данните и може да докаже, че не е в състояние да идентифицира субекта на данните. Съгласно член 11, параграф 2 обаче при такива обстоятелства субектът на данните може да предостави допълнителна информация, позволяваща неговото идентифициране. Освен това в член 12, параграф 6 се казва, че когато администраторът на данни има основателни опасения във връзка със самоличността на субекта на данните, той може да поиска допълнителна информация за потвърждаване на самоличността на субекта на данните. Когато субект на данните предоставя допълнителна информация, позволяваща неговото идентифициране, администраторът на данни не следва да отказва предприемане на действия по искането. Когато информацията и данните, събирани онлайн, са свързани с псевдоними или еднозначни идентификатори, администраторите на данни могат да прилагат подходящи процедури, позволяващи физическото лице да отправи искане за преносимост на данните и да получи данните, които се отнасят до него. Във всеки случай администраторите на данни трябва да приложат процедура за установяване на автентичността, за да могат категорично да се убедят в идентичността на субекта на данните, който иска своите лични данни или в по-общ план упражнява правата си, предоставени от ОРЗД.

Такива процедури вече съществуват в много случаи. Автентичността на субектите на данните често е установена от администратора на данни, преди още да се сключи договор или да се получи съгласието му относно обработването. В резултат на това личните данни, използвани за регистриране на физическото лице, което е засегнато от обработването, може да се използват също така като доказателство при установяване на автентичността на субекта на данните за целите на преносимостта[25].

Макар че в тези случаи предварителното идентифициране на субектите на данни може да налага изискването на доказателство за тяхната правосубектност, подобно удостоверяване може да не е релевантно за оценяването на връзката между данните и съответното физическо лице, тъй като тази връзка не е свързана с официалната или правната идентичност. По същество правото на администратора на данни да изисква допълнителна информация за удостоверяване на идентичността на дадено лице, не може да води до прекомерни изисквания и до събирането на лични данни, които не са релевантни или необходими за утвърждаване на връзката между физическото лице и поисканите лични данни.

[25] Когато например обработването на данните е свързано с потребителски акаунт, предоставянето на съответното потребителско име и парола може да е достатъчно, за да бъде идентифициран субектът на данните.

В много случаи вече са въведени подобни процедури за установяване на автентичността. Например потребителските имена и паролите често се използват, за да получат физическите лица достъп до своите данни в акаунтите си за електронна поща, акаунтите в социалните мрежи и акаунтите, използвани за различни други услуги, някои от които физическите лица избират да използват, без да разкриват тяхното пълно име и идентичност.

Ако предаването по интернет е проблемно с оглед на обема на поисканите данни от страна на субекта на данните, вместо евентуално да се възползва от удължения срок от най-много три месеца за изпълнение на искането[26], може да се наложи също така администраторът на данни да разгледа алтернативни средства за предоставяне на данните като използване на стрийминг или съхраняване на CD, DVD или други физически носители, както и създаване на възможност за предаване на личните данни директно към друг администратор на данни (съгласно член 20, параграф 2 от ОРЗД, когато това е технически осъществимо).

- **Какъв е определеният срок за отговор на искане за преносимост?**

Според член 12, параграф 3 се изисква администраторът на данни да предоставя на субекта на данните „информация относно действията, предприети [...], без ненужно забавяне“ и във всички случаи „в срок от един месец от получаване на искането“. Този едномесечен срок може да бъде удължен най-много до три месеца при сложни случаи, при условие че субектът на данните е бил уведомен относно причините за въпросното забавяне в рамките на един месец от първоначалното искане.

Администраторите на данни, които изпълняват услуги на информационното общество, вероятно са по-добре оборудвани, за да могат да изпълняват искания в много кратък срок. Добра практика, за да се отговори на очакванията на потребителите, е да се определи срокът, в рамките на който обичайно може да се отговори на дадено искане за преносимост на данните и субектите на данните да бъдат уведомени за този срок.

Съгласно член 12, параграф 4 администраторът на данни, който отказва да отговори на искане за преносимост на данните, следва да уведоми субекта на данните за „причините да не предприеме действия и за възможността за подаване на жалба до надзорен орган и търсене на защита по съдебен ред“ в рамките на един месец след получаване на искането.

Администраторите на данни трябва да спазват задължението за отговор в рамките на дадения срок, дори когато се касае за отказ. С други думи, администраторът на данни не може да запази мълчание, когато бъде помолен да отговори на искане за преносимост на данните.

- **В какви случаи искането за преносимост на данните може да бъде отхвърлено или да се наложи такса за него?**

С член 12 се забранява на администраторите на данни да налагат такса за предоставянето на лични данни, освен ако администраторът на данни може да докаже,

[26] Член 12, параграф 3: „Администраторът предоставя на субекта на данни информация относно действията, предприети във връзка с искане“.

че исканията са явно неоснователни или прекомерни, „по-специално поради своята повторяемост“. За услуги на информационното общество, специализирани в автоматизираното обработване на лични данни, внедряването на автоматизирани системи като приложно-програмни интерфейси (API)[27] може да улесни обмена на информация със субекта на данните, а оттам и да намали потенциалната тежест, произтичаща от повтарящи се искания. Следователно би трябвало да има много малко случаи, в които администраторът на данни да може да обоснове отказа да предостави поисканата информация, дори по отношение на многократни искания за преносимост на данните.

Освен това общите разходи по процесите, които са създадени, за да се отговори на исканията за преносимост на данните, не следва да се вземат предвид при определянето на прекомерността на дадено искане. Всъщност член 12 от ОРЗД се отнася до исканията, отправени от един субект на данните, а не до общия брой искания, получени от администратора на данни. По тази причина общите разходи за внедряването на системата не следва нито да се налагат на субектите на данните, нито да се използват, за да се обоснове отказ да се изпълнят искания за преносимост.

V. Как трябва да се предоставят преносимите данни?

- Какви средства се очаква да бъдат внедрени от страна на администратора на данни за целите на предоставянето на данни?

В член 20, параграф 1 от ОРЗД е предвидено, че субектите на данни имат правото да прехвърлят данните на друг администратор без възпрепятстване от администратора, на когото личните данни са предоставени.

Подобно възпрепятстване може да бъде определено като всякакви правни, технически или финансови пречки, отбелязани от администратора на данни, за да се въздържи или да забави достъпа, предаването или повторното използване от субекта на данните или от друг администратор на данни. Такова възпрепятстване би било например: да се искат такси за предоставяне на данните, липса на оперативна съвместимост или достъп до формата на данните или API, или предоставеният формат на данните, прекомерното забавяне или сложността при извличането на пълния набор данни, умишленото объркване на наборите данни или специфични, безпричинни или прекомерни изисквания за секторно страндартизиране или акредитиране[28].

Съгласно член 20, параграф 2 администраторите на данни са задължени също така да предават преносимите данни направо на други администратори на данни, „когато това е технически осъществимо“.

[27] Приложно-програмен интерфейс (API) означава интерфейсите на приложения или интернет услуги, предоставяни от администраторите на данни, за да може други системи или приложения да се свързват и да работят с техните системи.

[28] Възможно е все пак да възникнат някои основателни пречки, които са свързани с правата и свободите на други лица, посочени в член 20, параграф 4, или които се отнасят до сигурността на собствените системи на администраторите на данни. Администраторът на данни следва да носи отговорност за обосноваване на причините защо въпросните пречки са основателни и защо не представляват възпрепятстване по смисъла на член 20, параграф 1.

Техническата осъществимост на предаването от един администратор на данни към друг, осъществявано под контрола на субекта на данните, следва да се преценява на база конкретен случай. В съображение 68 допълнително са пояснени границите на това какво е „технически осъществимо“, като е посочено, че това „не следва да поражда задължение за администраторите да възприемат или поддържат технически съвместими системи за обработване“.

От администраторите на данни се очаква да предават личните данни в оперативно съвместим формат, макар че това не поражда задължения за другите администратори на данни да поддържат тези формати. Следователно пряко предаване от един администратор на данни към друг би могло да се осъществи, когато е възможна комуникация между двете системи по сигурен начин[29] и когато получаващата система от техническа гледна точка може да получи входящите данни. Ако има технически пречки, които да не позволяват пряко предаване, администраторът на данни следва да обясни на субектите на данните какви са тези пречки, тъй като в противен случай последиците от неговото решение ще са аналогични на отказ да предприеме действия във връзка с искане на субект на данните (член 12, параграф 4).

На техническо ниво администраторите на данни следва да разгледат и преценят два различни и допълващи се варианта на предоставяне на преносимите данни на разположение на субектите на данни или на други администратори на данни:

- пряко предаване на целия набор от преносими данни (или няколко извадки от части от общ набор данни);
- автоматизиран инструмент, позволяващ извличането на релевантните данни.

Администраторите на данни може да предпочитат втория вариант в случаи, касаещи сложни и големи набори данни, тъй като при него е възможно извличането на всяка част от набора данни, която е от значение за субекта на данните в контекста на неговото искане, може да допринесе за намаляването на риска до минимум и евентуално да позволи използването на механизми за синхронизиране на данни[30] (например в рамките на редовна комуникация между администраторите на данни). За „новия“ администратор на данни това може да е по-добрият начин да се осигури съответствие, а за първоначалния администратор на данни би било добра практика за намаляване на рисковете за неприкосновеността на личния живот.

Тези два различни и евентуално допълващи се начина за предоставяне на релевантните преносими данни може да бъдат приложени чрез предоставянето на данните на разположение посредством различни средства, например като сигурни съобщения, SFTP сървър, сигурен WebAPI или WebPortal. Субектите на данни следва да имат възможност да използват персонално хранилище за данни, персонална система за управление на информация[31] или други видове доверени трети страни, да държат и

[29] Посредством съобщение с установяване на автентичност и с необходимото ниво на криптиране на данните.

[30] Механизмът за синхронизиране може да спомогне да се изпълнят общите задължения по член 5 от ОРЗД, в който се казва, че „[л]ичните данни са (…) точни и при необходимост да бъдат поддържани в актуален вид“.

[31] Относно персоналните системи за управление на информация (PIMS) вж. например Становище 9/2016 на ЕНОЗД, което е на разположение на:

съхраняват личните данни и да дават разрешение на администраторите на данни за достъп и обработване на личните данни, когато това е необходимо.

- **Какъв е очакваният формат на данните?**

С ОРЗД за администраторите на данни се поставят изисквания да предоставят личните данни, които са поискани от дадено физическо лице, във формат, позволяващ тяхната повторна употреба. По-специално в член 20, параграф 1 от ОРЗД се казва, че личните данни трябва да се предоставят „в структуриран, широко използван и пригоден за машинно четене формат“. В съображение 68 е дадено допълнително пояснение, че този формат следва да бъде оперативно съвместим — термин, който в ЕС се определя[32] като:

> *способността на различни и разнообразни по своя характер организации да си взаимодействат за постигане на взаимноизгодни и съгласувани общи цели, което включва обмен на информация и знания между организациите чрез стопанските процеси, които те поддържат, посредством обмен на данни между съответните им системи на ИКТ.*

Термините „структуриран“, „широко използван“ и „пригоден за машинно четене“ представляват набор от минимални изисквания, които следва да улеснят оперативната съвместимост на формата на данните, в който администраторът на данни ги предоставя. По този начин „структуриран, широко използван и пригоден за машинно четене“ са спецификации за средствата, а оперативната съвместимост е желаният резултат.

В съображение 21 от Директива 2013/37/ЕС[33,34] „машинночетим“ е определен като:

> *файлов формат, който е структуриран по начин, по който софтуерните приложения да могат лесно да идентифицират, разпознават и извличат специфични данни, включително отделни факти и тяхната вътрешна структура. Данните, кодирани във файлове, които са структурирани в машинночетим формат, са машинночетими данни. Машинночетимите формати могат да бъдат отворени или да бъдат защитени от право на собственост; те могат да бъдат официални стандарти или не. Документи, кодирани във файлов формат, който ограничава автоматичната обработка поради факта, че данните не могат въобще или не могат лесно да бъдат извлечени от тези документи, не следва да се считат за такива в машинночетим формат. Държавите членки, по целесъобразност, следва да насърчават използването на отворени, машинночетими формати.*

Като се има предвид широкият диапазон от потенциални типове данни, които може да бъдат обработвани от даден администратор на данни, ОРЗД не налага конкретни

---

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-10-20_PIMS_opinion_EN.pdf.

[32] Член 2 от Решение № 922/2009/ЕО на Европейския парламент и на Съвета от 16 септември 2009 г. за решения за оперативна съвместимост за европейските публични администрации (ISA) (ОВ L 260, 3.10.2009 г., стр. 20).

[33] Директива 2013/37/ЕС за изменение на Директива 2003/98/ЕО относно повторната употреба на информацията в обществения сектор.

[34] В речника на ЕС (http://eur-lex.europa.eu/eli-register/glossary.html) са дадени допълнителни пояснения относно очакванията, свързани с понятията, които са използвани в настоящите насоки, като *пригоден за машинно четене, оперативна съвместимост, отворен формат, стандарт, метаданни*.

препоръки относно формата на предоставяните лични данни. В различните сектори най-подходящият формат е различен и може вече да съществуват подходящи формати, които винаги следва да се избират, за да се постигне целта за оперативна съвместимост и да се осигури за субекта на данните висока степен на преносимост на данните. Форматите, които подлежат на скъпоструващи лицензионни ограничения, не биха били приети като подходящ подход.

В съображение 68 се пояснява, че *„[п]равото на субекта на данни да предава или получава отнасящи се до него лични данни не следва да поражда задължение за администраторите да възприемат или поддържат технически съвместими системи за обработване“*. **Следователно с преносимостта се цели създаването на оперативно съвместими системи, а не на съвместими системи**[35]**.**

Очаква се личните данни да се предоставят във формати с високо ниво на абстракция от всеки вътрешен или собствен формат. В това качество преносимостта на данните предполага допълнителен слой на обработване на данните от администраторите на данни, за да бъдат извлечени данните от платформата и личните данни да бъдат филтрирани извън обхвата на преносимостта, като например логически изведени данни или данни, свързани със сигурността на системите. По този начин администраторите на данни се насърчават предварително да идентифицират в техните собствени системи данните, които попадат в обхвата на преносимостта. Това допълнително обработване на данните ще се счита за допълнително към основното обработване на данните, тъй като то не се извършва с оглед на постигането на нова цел, определена от администратора на данни.

Когато в даден отрасъл или в даден контекст няма широко използвани формати, **администраторите на данни следва да предоставят личните данни в широко използвани отворени формати (например XML, JSON, CSV и др.) заедно с** полезни **метаданни с възможно най-подходящата степен на детайлност,** като се запази високо ниво абстракция. В тази връзка следва да се използват подходящи метаданни, за да се опише точното значение на обменяната информация. Тези метаданни трябва да са достатъчни, за да се позволи функционирането и повторното използване на данните, но, разбира се, без да се разкриват търговски тайни. Следователно, малка е вероятността, ако на физическо лице се предоставят версии в PDF на входящите електронни съобщения, те да са достатъчно структурирани или описателни, за да може данните за входящите електронни съобщения лесно да се използват повторно. Вместо това данните за електронните съобщения следва да бъдат предоставени във формат, в който се запазват всички метаданни, за да може данните ефективно да се използват повторно. Съответно, когато избира формата на данните, в който да предоставя личните данни, администраторът на данни следва да вземе предвид по какъв начин този формат ще повлияе или попречи на правото на физическото лице да използва данните повторно. В случаи, в които администраторът на данни може да даде избор на субекта на данните по отношение на предпочитания формат на личните данни, следва да бъде предоставено ясно обяснение за въздействието на избора. Все пак обработването на допълнителни метаданни с единствената цел, че те може да са нужни или желани, за да

[35] В ISO/IEC 2382-01 оперативната съвместимост е определена, както следва: „[с]пособността за общуване, изпълнение на програми или предаване на данни между различни функционални единици по начин, изискващ от потребителя малко или никакви знания относно уникалните характеристики на тези единици.“

се отговори на искане за преносимост на данните, не дава законно основание за такова обработване.

Работната група по член 29 силно препоръчва сътрудничество между заинтересованите страни от отрасъла и търговските органи за съвместна работа по общ набор от оперативно съвместими стандарти и формати, за да се изпълнят изискванията, свързани с правото на преносимост на данните. Това предизвикателство е било разгледано също така от Европейската рамка за оперативна съвместимост (EIF), по линия на която е разработен съгласуван подход към оперативната съвместимост за организации, които желаят съвместно да предоставят публични услуги. В обхвата на нейната приложимост рамката определя набор от общи елементи като речник, понятия, принципи, политики, насоки, препоръки, стандарти, спецификации и практики[36].

- **Как следва да се процедира със събирането на лични данни с голям обем или сложност?**

В ОРЗД не е посочено как да се подхожда към предизвикателството по отговаряне на искане в случай на събиране на данни с голям обем, със сложна структура или ако възникнат други технически въпроси, които може да породят трудности за администраторите на данни или за субектите на данните.

Във всички случаи обаче е съществено важно физическото лице да може напълно да разбере определението, схемата и структурата на личните данни, които може да бъдат предоставени от администратора на данни. Възможно е например първо данните да бъдат предоставени в обобщен вид, като се използват информационни таблици, позволяващи на субекта на данните да не пренася личните данни в пълен обем, а поднабори от тях. Администраторът на данни следва да направи обзор „в кратка, прозрачна, разбираема и лесно достъпна форма, на ясен и прост език“ (вж. член 12, параграф 1 от ОРЗД) по такъв начин, че субектът на данните винаги да разполага с ясна информация какви данни да свали или предаде на друг администратор на данни във връзка с дадена цел. Например субектите на данни следва да имат възможност да използват софтуерни приложения за лесното идентифициране, разпознаване и обработване на специфични данни от него.

Както е посочено по-горе, практичен начин, по който администраторът на данни може да отговаря на искания за преносимост на данните, може да бъде чрез предлагане на подходящ сигурен и документиран API. Това може да даде възможност на физическите лица да отправят към администратора на данни искания за техните лични данни чрез техния собствен софтуер или чрез софтуера на трета страна, или да предоставят разрешение други лица да направят това от тяхно име (включително друг администратор на данни), както е предвидено в член 20, параграф 2 от ОРЗД. Като се предоставя достъп до данни чрез API с външен достъп, може да е възможно също така да се предложи по-усъвършенствана система за достъп, позволяваща на физическите лица да отправят последващи искания за данни, независимо дали за пълно сваляне, или като делта функция, съдържаща само промени, направени след последното сваляне, без тези допълнителни искания да са в тежест за администратора на данни.

[36] Източник: http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf.

- **Как може да бъде гарантирана сигурността на преносимите данни?**

По принцип администраторите на данни следва да гарантират „подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки“ в съответствие с член 5, параграф 1, буква е) от ОРЗД.

Въпреки това при предаването на лични данни към субекта на данните също може да възникнат някои проблеми по сигурността:

Как администраторите на данни могат да гарантират сигурното предаване на личните данни към правилното лице?

Тъй като с преносимостта на данните се цели личните данни да бъдат извадени от информационната система на администратора на данни, предаването може да се превърне в потенциален източник на риск за тези данни (по-специално нарушение на сигурността на данните по време на предаването). Администраторът на данни е отговорен за предприемането на всички необходими мерки по сигурността, за да се гарантира не само сигурното предаване на личните данни (чрез използването на комплексни решения или криптиране на данните) до правилното местоназначение (чрез използването на сериозни мерки за установяване на автентичността), но също така да се запази защитата на личните данни, които остават в техните системи, както и прозрачни процедури за справяне с евентуални нарушения на сигурността на данните[37]. Следователно администраторите на данни следва да оценяват конкретните рискове, свързани с преносимостта на данните и да предприемат подходящи мерки за намаляване на рисковете.

Тези мерки за намаляване на риска може да включват: ако за субекта на данните вече е необходимо установяване на автентичността — използване на допълнителна информация за установяване на автентичността като споделена тайна или друг фактор за целта, като например еднократна парола; прекратяване или спиране на предаването, ако има съмнение, че акаунтът е бил компрометиран; в случаи на пряко предаване от един администратор на данни към друг администратор на данни, следва да се използва установяване на автентичността чрез предоставяне на мандат, като например установяване на автентичността чрез токен-устройство.

Тези мерки по сигурността не трябва да бъдат възпрепятстващи по своя характер и не трябва да пречат на потребителите да упражняват техните права, например като налагат допълнителни разходи.

Как може да се помогне на потребителите да имат сигурност при съхранението на техните лични данни в собствените им системи?

Когато извличат техните лични данни от дадена онлайн услуга, винаги има риск потребителите да ги съхранят в системи с по-ниско ниво на сигурност от предлаганото от услугата. Субектите на данните, които отправят искане за данни, носят отговорност за определяне на правилните мерки, за да се гарантира сигурността на личните данни в

[37] В съответствие с Директива (ЕС) 2016/1148 относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза.

тяхната собствена система. Потребителят обаче следва да бъде осведомен за това, за да може да предприеме стъпки за защита на информацията, която е получил. Като пример за водеща практика, администраторите на данни могат също така да препоръчват подходащ(и) формат(и), инструменти за криптиране и други мерки за сигурност, за да подпомогнат субектите на данните за постигането на тази цел.

* * *

Съставено в Брюксел на 13 декември 2016 г.

За Работната група
Председател
Isabelle FALQUE-PIERROTIN

Последно преразгледано и прието на 5 април 2017 г.

За Работната група
Председател
Isabelle FALQUE-PIERROTIN