ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 12.6.2019 г.
COM(2019) 250 final/3

CORRIGENDUM
This document corrects document COM(2019) 250 final of 29.5.2019.
Concerns the Bulgarian language version.
Reference error in the last sentence of the third paragraph in the introduction.
The text shall read as follows:

СЪОБЩЕНИЕ НА КОМИСИЯТА ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И СЪВЕТА

Насоки във връзка с Регламента относно рамка за свободното движение на нелични данни в Европейския съюз

Съдържание

Настоящият документ се предоставя от Комисията само с информационна цел. Той не съдържа каквото и да е авторитетно тълкуване на Регламент (ЕС) 2018/1807 на Европейския парламент и на Съвета от 14 ноември 2018 г. относно рамка за свободното движение на нелични данни в Европейския съюз и не съставлява решение или позиция на Европейската комисия. Той не засяга което и да е решение или позиция на Европейската комисия в тази област, нито правомощията на Съда на Европейския съюз да тълкува регламента в съответствие с Договорите на ЕС.

1 Въведение

В икономика, която е движена във все по-голяма степен от данните, потоците от данни са в центъра на стопанските процеси в предприятията от всякакъв мащаб и във всички сектори. Новите цифрови технологии разкриват нови възможности за широката общественост, предприятията и органите на публичната администрация в Европейския съюз („ЕС“).

За да се увеличи още повече презграничният обмен на данни и да се стимулира основаната на данни икономика, през ноември 2018 г. Европейският парламент и Съветът приеха Регламент (ЕС) 2018/1807 относно рамка за свободното движение на нелични данни в Европейския съюз[1] („Регламента за свободното движение на нелични данни“) въз основа на предложение на Европейската комисия („Комисията“). Регламентът се прилага от 28 май 2019 г. Принципът на свободно движение на лични данни вече е залегнал в Регламент (ЕС) 2016/679 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 („Общия регламент относно защитата на данните“)[2]. В резултат на това днес съществува широкообхватна рамка за общо европейско пространство на данни и свободно движение на всички данни на територията на Европейския съюз[3].

Регламентът за свободното движение на нелични данни създава правна сигурност за предприятията, така че да могат да обработват своите данни където пожелаят в ЕС, повишава доверието в услугите за обработване на данни и се бори с практиките на създаване на зависимост от конкретен доставчик на услуги. Това ще разшири избора на клиентите, ще подобри ефикасността и ще стимулира приемането на облачни технологии, което ще доведе до значителни икономии за предприятията в ЕС. Едно проучване показва, че предприятията в ЕС могат да спестят 20 — 50 % от своите разходи за информационни технологии, като преминат към облачни услуги[4].

Благодарение на двата регламента данните могат да се движат свободно между държавите членки, което позволява на ползвателите на услуги за обработване на данни да използват данните, събрани на различни пазари на ЕС, за да подобрят своята производителност и конкурентоспособност. По този начин ползвателите могат да се възползват в пълна степен от икономиите от мащаба, предоставяни от големия пазар на

[1] Регламент (ЕС) 2018/1807 на Европейския парламент и на Съвета от 14 ноември 2018 г. относно рамка за свободното движение на нелични данни в Европейския съюз, ОВ L 303, 28.11.2018 г., стр. 59.

[2] 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 (Общ регламент относно защитата на данните), ОВ L 119, 4.5.2016 г., стр. 1.

[3] Общият регламент относно защитата на данните обхваща и Европейското икономическо пространство (ЕИП), което включва Исландия, Лихтенщайн и Норвегия. В допълнение Регламентът за свободното движение на нелични данни е обозначен като текст от значение за ЕИП.

[4] Deloitte: Measuring the economic impact of cloud computing in Europe („Измерване на икономическото въздействие на изчисленията в облак в Европа“), SMART 2014/0031, 2016 г. Публикувано в интернет на адрес: http://ec.europa.eu/newsroom/document.cfm?doc_id=41184.

ЕС, като подобряват своята конкурентоспособност в световен план и увеличават взаимосвързаността на основаната на данни европейска икономика.

Регламентът за свободното движение на нелични данни има три важни характеристики:

- Той предвижда принципна забрана за държавите членки да налагат изисквания относно това къде следва да се локализират данни. Изключения от това правило могат да бъдат оправдани единствено на основания, свързани с обществената сигурност, в съответствие с принципа на пропорционалност.
- С регламента се създава механизъм за сътрудничество, за да се гарантира, че компетентните органи ще могат и занапред да упражняват всички предоставени им права за достъп до данни, които се обработват в друга държава членка.
- Той предвижда стимули за промишлеността да разработи, с подкрепата на Комисията, кодекси за поведение с цел саморегулиране при смяната на доставчици на услуги и пренасянето на данни.

Цел на настоящите насоки

С настоящите насоки се изпълнява член 8, параграф 3 от Регламента за свободното движение на нелични данни, който изисква Комисията да публикува насоки относно взаимодействието на този регламент и Общия регламент относно защитата на данните, „особено по отношение на наборите от данни, съставени както от лични, така и от нелични данни“.

Целта на настоящите насоки е да се помогне на ползвателите — по-специално на малките и средните предприятия — да разберат взаимодействието между Регламента за свободното движение на нелични данни и Общия регламент относно защитата на данните[5]. Поради това в насоките се разглеждат по-специално: i) понятията за нелични данни и лични данни; ii) принципите на свободно движение на данни и забраната на изискванията за локализиране на данни, предвидени в двата регламента; и iii) понятието за преносимост на данните съгласно Регламента за свободното движение на нелични данни. Те обхващат също така изискванията за саморегулиране, определени в двата регламента.

Регламентът за свободното движение на нелични данни обхваща само „данни, различни от личните данни“, както са определени в Общия регламент относно защитата на данните. Общият регламент относно защитата на данните урежда обработването на лични данни, което е съществена част от рамката на ЕС за защита на данните[6]. Той

[5] Съображение 37 от Регламент (ЕС) 2018/1807 на Европейския парламент и на Съвета от 14 ноември 2018 г. относно рамка за свободното движение на нелични данни в Европейския съюз.

[6]
– 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 (Общ регламент относно защитата на данните), ОВ L 119/1, 4.5.2016 г., стр. 1.
– Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета от 23 октомври 2018 г. относно защитата на физическите лица във връзка с обработването на лични данни от институциите, органите, службите и агенциите на Съюза и относно свободното движение на такива данни и за

влезе в сила в държавите членки на 25 май 2018 г. В регламента са определени хармонизирани правила за защита на хората в ЕС/ЕИП, що се отнася до обработването на техните лични данни и свободното движение на такива данни. В Общия регламент относно защитата на данните: i) е посочено коя информация представлява лични данни; ii) са установени правните основания за нейното обработване; и iii) са определени правата и задълженията, които да бъдат спазвани при обработването на тези данни[7], наред с други разпоредби. Във връзка с принципа на свободно движение на лични данни член 1, параграф 3 от Общия регламент относно защитата на данните предвижда, че „[с]вободното движение на лични данни в рамките на Съюза не се ограничава, нито се забранява по причини, свързани със защитата на физическите лица във връзка с обработването на лични данни“.

В повечето ситуации от реалния живот е много вероятно наборът от данни да е съставен както от лични, така и от нелични данни. Това често се нарича „набор от смесени данни“. В раздел 2.2 по-долу е допълнително обяснено взаимодействието между Регламента за свободното движение на нелични данни и Общия регламент относно защитата на данните по отношение на наборите от смесени данни.

За по-голяма яснота не съществуват противоречащи си задължения съгласно Общия регламент относно защитата на данните и Регламента за свободното движение на нелични данни.

отмяна на Регламент (ЕО) № 45/2001 и Решение № 1247/2002/ЕО, ОВ L 295, 21.11.2018 г., стр. 39.

– Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни, и за отмяна на Рамково решение 2008/977/ПВР на Съвета, ОВ L 119, 4.5.2016 г., стр. 89.

– Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 г. относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронни комуникации), ОВ L 201, 31.7.2002 г., стр. 37 (понастоящем се преразглежда).

[7] За допълнителни насоки относно различните аспекти на 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 (Общ регламент относно защитата на данните) и европейската нормативна уредба в областта на защитата на данните, разгледайте интернет страницата на Европейския комитет по защита на данните, който е публикувал редица насоки в съответствие с член 70 от Общия регламент относно защитата на данните, достъпна на адрес: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_bg. На съответната интернет страница има също препратки и към насоки, препоръки и други документи, публикувани от предшественика на Европейския комитет по защита на данните — Работната група за защита на личните данни по член 29 („Работната група по член 29“). Освен това, с цел повишаване на осведомеността на гражданите и предприятията относно 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 (ОРЗД), Комисията публикува съобщение относно защитата на данните — насоки относно прякото прилагане на ОРЗД (COM/2018/043 final), на разположение на адрес: https://eur-lex.europa.eu/legal-content/BG/TXT/?qid=1517578296944&uri=CELEX%3A52018DC0043

2 Взаимодействие между Регламента за свободното движение на нелични данни и Общия регламент относно защитата на данните — набори от смесени данни

2.1 Понятието „нелични данни“ в Регламента за свободното движение на нелични данни

Регламентът за свободното движение на нелични данни[8] има за цел да гарантира свободното движение на данни, различни от личните данни. Навсякъде в текста на регламента се използва понятието „данни“, което следва да се разбира като „данни, различни от личните данни, определени в член 4, точка 1 от Регламент (ЕС) 2016/679“ [Общия регламент относно защитата на данните][9]. Тези данни, наричани още „**нелични данни**“ в настоящия документ, се определят чрез противопоставяне (*a contrario*) на личните данни, както са определени в Общия регламент относно защитата на данните.

Лични данни

Общият регламент относно защитата на данните гласи: „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“.

Определението за лични данни умишлено е формулирано в широк смисъл и по същество остава непроменено в Общия регламент относно защитата на данните в сравнение с предшестващото го законодателство[10]. Различни аспекти на определението на понятието „лични данни“, като например „всяка информация“, „свързана с“, „идентифицирано“ или „което може да бъде идентифицирано“, вече са разгледани от Работната група по член 29[11] в нейното Становище 4/2007 относно понятието „лични данни“ от 20 юни 2007 г. (WP136).

---

[8] Член 1 от Регламент (ЕС) 2018/1807 на Европейския парламент и на Съвета от 14 ноември 2018 г. относно рамка за свободното движение на нелични данни в Европейския съюз.

[9] Вж. член 3, параграф 1 от Регламент (ЕС) 2018/1807 на Европейския парламент и на Съвета от 14 ноември 2018 г. относно рамка за свободното движение на нелични данни в Европейския съюз.

[10] Вж. член 2, буква а) от Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 г. за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни (дата на изтичане на срока на валидност: 24 май 2018 г., отменена с Общия регламент относно защитата на данните). Вж. също съдебната практика на Съда относно определението на понятието „лични данни“, в която се признава широкото тълкуване на понятието, например в решение от 29 януари 2009 г. по дело *Productores de Música de España (Promusicae)*/*Telefónica de España SAU*, C-275/06, ECLI:EU:C:2008:54; решение от 24 ноември 2011 г. по дело *Scarlet Extended SA*/*Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, C-70/10, ECLI:EU:C:2011:771; решение от 19 октомври 2016 г. по дело *Patrick Breyer*/*Bundersrepublik Deutschland*, C-582/14, ECLI:EU:C:2016:779.

[11] Работната група по член 29 беше консултативен орган, който предоставяше на Комисията съвети по въпроси, свързани със защитата на данните, и помагаше при разработването на хармонизирани

Обща практика в области като научните изследвания, например, е личните данни да се псевдонимизират с цел да се скрие самоличността на съответното лице. **Псевдонимизация** означава обработването на лични данни по такъв начин, че те да не могат повече да бъдат свързвани с конкретно лице, без да се използва допълнителна информация. Тази допълнителна информация се съхранява отделно и е защитена чрез организационни или технически мерки (например криптиране)[12, 13]. Независимо от това данните, които са били псевдонимизирани, все пак се считат за информация относно лице, което може да бъде идентифицирано, ако те могат да бъдат свързани с това лице чрез използването на допълнителна информация[14]. Такива данни **представляват лични данни** в съответствие с Общия регламент относно защитата на данните.

Нелични данни

Когато данните не са „лични данни“ съгласно определението в Общия регламент относно защитата на данните, те са **нелични данни**. По своя произход неличните данни могат да бъдат категоризирани по следния начин:

- първо, данни, които първоначално не са били свързани с идентифицирано или подлежащо на идентифициране физическо лице, като например данни относно метеорологичните условия, генерирани чрез датчици, монтирани върху вятърни турбини, или данни относно необходимостта от техническа поддръжка на производствени машини;

- второ, данни, които първоначално са били лични данни, но по-късно са били **анонимизирани**[15]. „Анонимизацията“ на лични данни се различава от псевдонимизацията (вж. по-горе), тъй като надлежно анонимизираните лични данни

политики за защита на данните в рамките на ЕС. След влизането в сила на Общия регламент относно защитата на данните на 25 май 2018 г. функциите на Работната група по член 29 бяха поети от Европейския комитет по защита на данните.

[12] Вж. член 4, параграф 5 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 (ОРЗД), където е дадено определение на понятието „псевдонимизация“.

[13] Така например, проучване на въздействията на ново лекарство ще бъде определено като псевдонимизация, ако личните данни на участниците в проучването бъдат заменени с уникални идентификатори (например номер или код) в документацията на изследването и тези техни лични данни се съхраняват отделно от присвоените им уникални идентификатори в защитен документ (например в защитена с парола база данни).

[14] Вж. съображение 26 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 (Общ регламент относно защитата на данните).

[15] Вж. съображение 26 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 (Общ регламент относно защитата на данните), което предвижда, че „[п]оради това принципите на защита на данните не следва да се прилагат по отношение на анонимна информация, т.е. информация, която не е свързана с идентифицирано или подлежащо на идентифициране физическо лице, или по отношение на лични данни, които са анонимизирани по такъв начин, че субектът на данните да не може или вече не може да бъде идентифициран“.

не могат да бъдат свързани с конкретно лице дори и чрез използването на допълнителна информация[16] и следователно са нелични данни.

Оценката на това дали данните са надлежно анонимизирани зависи от конкретните и уникални обстоятелства на всеки отделен случай[17]. Няколко примера на повторно идентифициране на набори от данни, за които се е предполагало, че са били анонимизирани, показват, че такава оценка може да представлява предизвикателство[18]. За да се определи дали дадено физическо лице може да бъде идентифицирано, следва да се вземат предвид всички средства, с които съществува разумна вероятност да си послужи администраторът или друго лице, за да идентифицира пряко или непряко даденото физическо лице[19].

Примери за нелични данни:

- Данните, които са агрегирани до ниво, на което събитията, касаещи отделни лица (като например отделните пътувания на дадено лице в чужбина или моделите на пътуване, които биха могли да представляват лични данни), вече не подлежат на идентифициране, могат да бъдат квалифицирани като анонимни данни[20]. Анонимните данни се използват например в статистиката или в

[16] Вж. решение от 19 октомври 2016 г., *Patrick Breyer/Bundesrepublik Deutschland*, C-582/14, ECLI:EU:C:2016:779. Съдът е определил, че динамичният адрес по интернет протокол (IP адрес) може да съставлява лични данни, дори ако трето лице (например доставчик на интернет услуги) разполага с допълнителна информация, която би направила възможно идентифицирането на съответното лице. Възможността за идентифициране на лицето трябва да представлява средство, за което съществува разумна вероятност да бъде използвано с цел идентифицирането на даденото лице, независимо дали пряко или косвено.

[17] Анонимизацията на данните следва винаги да се извършва с най-новите и модерни технически способи за анонимизация.

[18] За примери за повторно идентифициране на данни, за които се предполага, че са били анонимизирани, разгледайте проучването на бъдещите потоци от данни, извършено за комисията по промишленост, изследвания и енергетика (ITRE) на Европейския парламент от Blackman, C. и Forge, S.: *Data Flows — Future Scenarios: In-Depth Analysis for the ITRE Committee (Потоците от данни — сценарии за бъдещето: задълбочен анализ за комисията ITRE),* 2017 г., стр. 22, каре 2. Публикувано в интернет на адрес: http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/607362/IPOL_IDA(2017)607362_EN.pdf

[19] Вж. съображение 26 от Регламент (ЕС) 2016/679 (Общия регламент относно защитата на данните), в съответствие с което „[з]а да се установи дали има достатъчна вероятност дадени средства да бъдат използвани за идентифициране на физическото лице, следва да се вземат предвид всички обективни фактори, като разходите и количеството време, необходими за идентифицирането, като се отчитат наличните към момента на обработване на данните технологии и технологичните развития“.

[20] Вж. Работна група по член 29: *Становище 05/2014 относно техническите способи за анонимизиране*, прието на 10 април 2014 г., WP216, стр 9: „Полученият масив от данни може да бъде квалифициран като анонимен само ако администраторът на данни агрегира данните до ниво, на което събитията, касаещи отделни лица, вече не подлежат на идентифициране. Например: ако дадена организация събира данни относно индивидуални пътувания, индивидуалните модели на пътуване на равнището на събитието ще продължават да бъдат лични данни за всяка страна, при условие че администраторът на данни (или всяко друго лице) продължава да има достъп до първоначалните необработени данни, дори когато преките признаци за идентифициране са отстранени от масива, предоставен на трети лица. Ако обаче администраторът на данни заличи необработените данни и предостави на трети лица само агрегираните статистически данни на по-високо равнище, като например „всеки понеделник по маршрута X преминават 160 % повече пътници в сравнение с вторник“, тези данни биха се считали за анонимни.“

докладите за продажби (например с цел изчисляване на популярността на даден продукт и неговите характеристики).

- Данни в областта високочестотната търговия във финансовия сектор или данни за прецизно земеделие, които помагат за наблюдението и оптимизирането на употребата на пестициди, хранителни вещества и вода.

Ако обаче неличните данни могат по някакъв начин да бъдат свързани с физическо лице, което го прави пряко или непряко подлежащо на идентифициране, данните трябва да се считат за лични.

Например ако доклад за контрола на качеството на производствена линия направи възможно свързването на данните с конкретни работници от фабриката (например онези, които задават параметрите на производството), тогава данните ще се квалифицират като лични данни и трябва да се приложи Общият регламент относно защитата на данните. Същите правила са в сила, когато напредъкът в технологичното развитие и анализа на данни направят възможно превръщането на анонимизираните данни в лични данни. [21]

Тъй като определението на понятието „лични данни“ се отнася за „физически лица“, наборите от данни, съдържащи наименования и данни за връзка на юридически лица, по принцип са нелични данни[22]. В някои ситуации обаче те могат да бъдат лични данни[23]. Такъв ще бъде случаят, ако например наименованието на юридическото лице е същото като на физическото лице, което го притежава, или ако информацията е свързана с идентифицирано или подлежащо на идентифициране физическо лице[24].

[21] Ако личните данни са обработвани незаконосъобразно или обработването по друг начин нарушава Общия регламент относно защитата на данните, субектите на данни (физическите лица) имат право съгласно Общия регламент относно защитата на данните да подадат жалба до национален надзорен орган (орган за защита на данните) в ЕС или да потърсят ефективна съдебна защита пред национален съд. Задачите, компетентностите и правомощията на националните надзорни органи са уредени в глава VI, раздел 2 от Общия регламент относно защитата на данните.

[22] Съображение 14 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 (Общ регламент относно защитата на данните) гласи, че „[н]астоящият регламент не обхваща обработването на лични данни, които засягат юридически лица, и по-специално предприятия, установени като юридически лица, включително наименованието и правната форма на юридическото лице и данните за връзка на юридическото лице.“ Това обаче трябва да се тълкува в светлината на определението на понятието„лични данни“, посочено в член 4, параграф 1 от Общия регламент относно защитата на данните.

[23] Вж. решение от 9 ноември 2010 г. по съединени дела *Volker und Markus Schecke GbR*, C-92/09, и *Hartmut Eifert/Land Hessen*, C-93/09, ECLI:EU:C:2010:662, точка 52.

[24] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-data-protection-rules-apply-data-about-company_bg

2.2 Набори от смесени данни

Регламентът за свободното движение на нелични данни и Общият регламент относно защитата на данните разглеждат свободното движение на данни в ЕС от две различни перспективи.

Регламентът за свободното движение на нелични данни (РСДНД) установява обща забрана срещу изискванията за локализиране на нелични данни. Съгласно член 4, параграф 1 от РСДНД се забраняват изискванията за локализиране на данни, освен ако те са оправдани от съображения за обществена сигурност в съответствие с принципа на пропорционалност.

В допълнение към гарантирането на висока степен на защита на личните данни, Общият регламент относно защитата на данните (ОРЗД) гарантира свободното движение на лични данни. В съответствие с член 1, параграф 3 от ОРЗД свободното движение на лични данни „не се ограничава, нито се забранява по причини, свързани със защитата на физическите лица във връзка с обработването на лични данни“. Заедно двата регламента предвиждат свободното движение на „всички“ данни в рамките на ЕС. Конкретните разпоредби са допълнително разгледани в раздели 3.1 и 3.2.

Наборът от смесени данни се състои както от лични, така и от нелични данни. Наборите от смесени данни представляват по-голямата част от наборите от данни в основаната на данни икономика и са често срещани в следствие на технологичното развитие, като например „интернет на предметите“ (т.е. цифровото свързване на предмети), изкуствения интелект и технологиите, които позволяват извършването на анализ на големи информационни масиви.

Примери за набори от смесени данни:

- данни на дружество в данъчния регистър, които съдържат името и телефонния номер на изпълнителния директор на дружеството;
- набори от данни в банка, по-специално онези, които съдържат информация за клиента и данни за трансакцията, като например платежни услуги (кредитни и дебитни карти), приложения за управление на връзките с партньори (PRM) и договори за кредит, документи, съдържащи смесени данни относно физически и юридически лица;
- анонимизирани статистически данни на научноизследователски институт и първоначално събраните необработени данни, като например отговорите на отделните респонденти на въпроси от статистическо проучване;
- база данни от знания на дружество относно проблеми, свързани с информационните технологии и тяхното решение, въз основа на доклади за отделни инциденти, свързани с информационните технологии;
- данни, свързани с „интернет на предметите“, когато някои данни позволяват да бъдат направени предположения относно подлежащи на идентифициране физически лица (например присъствие на определен адрес и модели на използване); и

- анализ на данните от експлоатационния дневник на производствено оборудване в преработващата промишленост.

Пример: услуги за управление на връзките с клиенти

Някои банки използват услуги за управление на връзките с клиенти (CRM), предоставяни от трети страни, които изискват предоставянето на данни за клиента на софтуера за CRM. Данните, съхранявани в рамките на услугата за CRM, ще включват цялата необходима информация за ефективното управление на взаимодействието с клиента, като например неговия пощенски адрес и адрес на електронна поща, телефонния му номер, продуктите и услугите, които купува, както и отчетите за продажби, включително агрегираните данни. Следователно тези данни могат да включват както лични, така и нелични данни за клиентите.

По отношение на наборите от смесени данни Регламентът за свободното движение на нелични данни[25] предвижда следното:

„В случая на набори от данни, съставени както от лични, така и от нелични данни, настоящият регламент се прилага към частта от набора на данни, съдържаща нелични данни. Когато личните и неличните данни в набор от смесени данни са неразривно свързани, настоящият регламент не засяга прилагането на Регламент (ЕС) 2016/679.“.

Това означава, че в случай на набор от данни, съставен както от лични, така и от нелични данни:

- Регламентът за свободното движение на нелични данни се прилага към частта от набора от данни, съдържаща нелични данни;
- разпоредбата относно свободното движение на данни, предвидена в Общия регламент относно защитата на данните[26], се прилага към частта от набора от данни, съдържаща лични данни; и
- ако частта, съдържаща нелични данни, и тази, съдържаща лични данни, са „неразривно свързани“, правата и задълженията за защита на данните, произтичащи от Общия регламент относно защитата на данните, се прилагат в пълна степен за целия набор от смесени данни и тогава, когато личните данни представляват само малка част от набора от данни[27].

---

[25] Член 2, параграф 2 от него.

[26] Член 1, параграф 3 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 (Общ регламент относно защитата на данните). Вж. също раздел 3.2 от настоящия документ.

[27] Както се припомня в *Работен документ на службите на Комисията „Оценка на въздействието“, придружаващ предложение за Регламент на Европейския парламент и на Съвета относно рамка за свободното движение на нелични данни в Европейския съюз (Commission Staff Working Document, Impact Assessment accompanying the document Proposal for a Regulation of the European*

Това тълкуване е в съответствие с правото на защита на личните данни, гарантирано от Хартата на основните права на Европейския съюз[28] и със съображение 8 от Регламента за свободното движение на нелични данни[29]. Съображение 8 от него предвижда, че „правната рамка относно защитата на физическите лица във връзка с обработването на лични данни [...], и особено [Общият регламент относно защитата на данните] [...] и директиви (ЕС) 2016/680 и 2002/58/ЕО [...], не са засегнати от настоящия регламент.“

Практически пример:

Дружество, извършващо дейност в ЕС, предлага услугите си чрез платформа. Предприятията (клиентите) качват на платформата своите документи, които съдържат набори от смесени данни. В качеството си на „администратор“ предприятието, което качва документите, трябва да се увери, че обработването е в съответствие с разпоредбите на Общия регламент относно защитата на данните. Като обработва набора от данни от името на администратора, дружеството, което предлага услугите („обработващият лични данни“), трябва да съхранява и обработва данните в съответствие с Общия регламент относно защитата на данните, например за да се увери, че е гарантирано подходящо ниво на сигурност по отношение на данните, включително чрез криптиране.

В нито един от двата регламента не е дадено определение на понятието „неразривно свързани“[30]. От практическа гледна точка то може да се отнася до ситуация, в която набор от данни съдържа както лични, така и нелични данни и разделянето им би било невъзможно или считано от администратора за икономически неефективно или технически неосъществимо. Например при купуването на CRM системи и системи за отчитане на продажби дружеството ще трябва да удвои разходите си за софтуер, като купи отделен софтуер за системата за CRM (лични данни) и системата за отчитане на продажбите (агрегирани/нелични данни), основана на данните за CRM.

С разделянето на набора от данни също така е вероятно неговата стойност значително да се намали. Освен това променящият се характер на данните (вж. раздел 2.1) прави по-трудно ясното разграничаване на различните категории данни и съответно тяхното разделяне.

Важно е да се отбележи, че нито един от двата регламента не задължава предприятията да разделят наборите от данни, които администрират или обработват.

Parliament and of the Council on a framework for the free flow of non-personal data in the European Union) (SWD(2017) 304), част 1/2, стр. 3: „независимо каква част от личните данни е включена в наборите от смесени данни, разпоредбите на ОРЗД [Общият регламент относно защитата на данните] трябва да се спазват в пълна степен по отношение на частта от набора, съдържаща лични данни.“

[28] Харта на основните права на Европейския съюз, ОВ С 362, 26.10.2012 г., стр. 391.

[29] Съображение 8 от него

[30] Регламентът за свободното движение на нелични данни и Общият регламент относно защитата на данните.

Следователно наборът от смесени данни по принцип е предмет на задълженията на администраторите на данни и обработващите данни и зачита правата на субектите на данни, установени от Общия регламент относно защитата на данните.

Обработване на данни за здравословното състояние

Данните за здравословното състояние могат да бъдат част от набор от смесени данни. Някои примери са електронните здравни досиета, клиничните изпитвания или набори от данни, събирани от различни мобилни приложения за здравето и благосъстоянието (като например приложения за измерване на здравния ни статус, за напомняне за приемане на лекарства или за проследяване на напредъка ни към постигане на добра форма)[31]. С развитието на технологиите точното разделение между лични и нелични данни в тези набори от данни става все по-неясно. Следователно тяхното обработване трябва да съответства на разпоредбите на Общия регламент относно защитата на данните, по-специално (тъй като данните за здравословното състояние представляват специална категория данни съгласно регламента) с член 9, който установява обща забрана за обработване на специални категории данни и изключения от тази забрана.

Данните в наборите от смесени данни, съдържащи данни за здравословното състояние, могат да бъдат ценен източник на информация, например за допълнителни медицински изследвания, за измерване на страничните ефекти от предписан лекарствен продукт, за целите на статистиката в областта на заболяванията или за разработване на нови здравни услуги или видове лечение. Общият регламент относно защитата на данните обаче трябва да се спазва при извършването както на първоначалните дейности по обработване, така и на допълнителни дейности по обработване. Следователно всяко такова обработване на данни за здравословното състояние трябва да има валидно правно основание[32] и подходяща обосновка, както и да бъде защитено и да осигурява достатъчни гаранции.

И накрая, от съществено значение е физическите лица и дружествата да имат правна сигурност и доверие по отношение на обработването на данни. Това е жизнено важно и за основаната на данни икономика. Двата регламента гарантират това и имат за цел да не променят свободното движение на данни.

[31] Разработването и експлоатацията на мобилни приложения за здравето изискват стриктно спазване на правилата на Общия регламент относно защитата на данните. Тези изисквания ще бъдат допълнително уточнени в Кодекса за поведение относно правото на неприкосновеност на личния живот при мобилни приложения за здравето, който е в процес на изготвяне. За повече информация относно етапа на неговото разработване вж.: https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps

[32] Вж. член 6, параграф 1 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 (Общ регламент относно защитата на данните).

3 Свободно движение на данни и премахване на изискванията за локализиране на данни

В този раздел са обяснени по-подробно концепциите за изискванията за локализиране на данни съгласно Регламента за свободното движение на нелични данни и за принципа на свободно движение, заложен в Общия регламент относно защитата на данните. Въпреки че тези разпоредби са насочени към държавите членки, разделът може да бъде от полза за предприятията, за да придобият по-точна представа за начините, по които тези два регламента допринасят за свободното движение на всички данни в ЕС.

3.1 Свободно движение на нелични данни

Регламентът за свободното движение на нелични данни[33] предвижда следното: „[з]абраняват се изискванията за локализиране на данни, освен ако те са оправдани от съображения за обществена сигурност в съответствие с принципа на пропорционалност“.

Изискванията за локализиране на данни се определят[34] като „всяко задължение, забрана, условие, ограничение или друго изискване, което е предвидено в законовите, подзаконовите или административните разпоредби на държава членка или което е в резултат на общи и последователни административни практики на държава членка и на публичноправните организации, включително в областта на обществените поръчки, без да се засяга Директива 2014/24/ЕС, което налага обработването на данни да бъде на територията на конкретна държава членка или пречи на обработването на данни във всяка друга държава членка“[35].

Определението показва, че мерките, ограничаващи свободното движение на данни в ЕС, могат да приемат различни форми. Те могат да бъдат определени в законови, подзаконови или административни разпоредби или дори да са в резултат от общи и последователни административни практики. В допълнение забраната на изискванията за локализиране на данни обхваща както преките, така и непреките мерки, които биха ограничили свободното движение на нелични данни.

Преките изисквания за локализиране на данни могат да се състоят например от задължение за съхранение на данни в конкретно географско местоположение (например сървърите трябва да бъдат разположени в определена държава членка) или задължение за спазване на специфичните национални технически изисквания (например за данните трябва да се използват конкретни национални формати).

---

33 Член 4, параграф 1 от него

34 Член 3, параграф 5 от Регламент (ЕС) 2018/1807 на Европейския парламент и на Съвета от 14 ноември 2018 г. относно рамка за свободното движение на нелични данни в Европейския съюз.

35 Следва да се отбележи, че правната несигурност относно степента на законност на различните изисквания за локализиране на данни допълнително ограничава избора, предоставен на участниците на пазара и на обществения сектор във връзка с местоположението на обработването на данните (вж. съображение 4 от Регламент (ЕС) 2018/1807 на Европейския парламент и на Съвета от 14 ноември 2018 г. относно рамка за свободното движение на нелични данни в Европейския съюз).

Непреките изисквания за локализиране на данни, които биха пречили на обработването на нелични данни в коя да е друга държава членка, могат да съществуват в различни форми. Те могат да включват изисквания за използване на технологични съоръжения, които са сертифицирани или одобрени в определена държава членка, или други изисквания, които водят до затрудняване на обработването на данни извън конкретен географски район или територия в рамките на Европейския съюз[36, 37].

При оценката на това дали конкретна мярка представлява непряко изискване за локализиране на данни, трябва да се разгледат специфичните обстоятелства на всеки случай.

В Регламента за свободното движение на нелични данни[38] е посочено понятието „**обществена сигурност**“, изложено в съдебната практика на Съда на Европейския съюз. Обществената сигурност „обхваща както вътрешната, така и външната сигурност на държавата членка[39], както и въпросите, свързани с обществената безопасност, по-специално за да се улесни разследването, разкриването и наказателното преследване на престъпления. Тази концепция предполага наличието на действителна и достатъчно сериозна заплаха, която засяга някой от основните интереси на обществото[40], като заплаха за функционирането на институции и на основни обществени услуги и заплаха за оцеляването на населението, както и риск от сериозно смущаване на външните отношения или на мирното съвместно съществуване на народите или риск, свързан с военните интереси.“

Освен това всички изисквания за локализиране на данни, оправдани от съображения, свързани с обществената сигурност, трябва да бъдат пропорционални. В съответствие със съдебната практика на Съда на Европейския съюз принципът на пропорционалност

---

[36] Съображение 4 от Регламент (ЕС) 2018/1807 на Европейския парламент и на Съвета от 14 ноември 2018 г. относно рамка за свободното движение на нелични данни в Европейския съюз.

[37] Вж. две проучвания относно изискванията за локализиране на данни, проведени преди приемането на Регламента за свободното движение на нелични данни: 1) Godel, M. et al.: *Facilitating cross border data flows in the Digital Single Market („Улесняване на трансграничното свободно движение на данни на цифровия единен пазар“)*, SMART номер 2015/2016. Публикувано в интернет на адрес: http://ec.europa.eu/newsroom/document.cfm?doc_id=41185 и 2) Time.lex, Spark Legal Network и Tech4i2: *Cross-border data flow in the digital single market: study on data localisation restrictions*. („Трансгранично свободно движение на данни на цифровия единен пазар: *проучване относно ограниченията за локализиране на данни“)*, SMART номер 2015/0054. Публикувано в интернет на адрес: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=46695

[38] Съображение 19 от него

[39] Вж. например решение от 23 ноември 2010 г. по дело *Land Baden-Württemberg/Tsakouridis*, C-145/09, ECLI:EU:C:2010:708, точка 43 и решение от 4 април 2017 г. по дело *Sahar Fahimian/Bundesrepublik Deutschland*, C-544/15, ECLI:EU:C:2017:225, точка 39.

[40] Вж. например решение от 22 декември 2008 г. по дело *Комисия на Европейските общности/Република Австрия*, C-161/07, ECLI:EU:C:2008:759, точка 35 и цитираната в него съдебна практика, и решение от 26 март 2009 г. по дело *Комисия на Европейските общности/Република Италия*, C-326/07, ECLI:EC:C:2009:193, точка 70 и цитираната в него съдебна практика.

изисква приетите мерки да са пропорционални, за да се гарантира, че преследваната цел е постигната, и не надхвърлят необходимото за тази цел[41].

За по-голяма яснота забраната на изискванията за локализиране на данни не засяга вече съществуващите ограничения, установени от правото на ЕС[42].

Освен това Регламентът за свободното движение на нелични данни не налага задължения за предприятията, нито ограничава тяхната свобода на договаряне да решават къде да бъдат обработвани данните им.

От държавите членки се изисква да публикуват подробна информация за всички изисквания за локализиране на данни, приложими на тяхната територия, на **национална единна информационна точка онлайн** (националните уебсайтове). Те трябва да ги актуализират или да предоставят актуализирана подробна информация на централна информационна точка, създадена съгласно друг акт на ЕС[43]. За удобството на предприятията и за да им осигури лесен достъп до необходимата информация в целия ЕС, Комисията ще публикува препратки към тези информационни точки на портала „Вашата Европа“[44].

3.2 Свободно движение на лични данни

Общият регламент относно защитата на данните[45] предвижда, че „[с]вободното движение на лични данни в рамките на Съюза [не може да] се ограничава, нито забранява по причини, свързани със защитата на физическите лица във връзка с обработването на лични данни“.

Ако дадена държава членка наложи изисквания за локализиране на лични данни по причини, различни от защита на личните данни, те ще трябва да бъдат оценени спрямо разпоредбите относно основните свободи и разрешените основания за дерогация от

---

41 Вж. например решение от 8 юли 2010 г. по дело *Afton Chemical Limited/Secretary of State for Transport*, C-343/09, ECLI:EU:C:2010:419, точка 45, както и цитираната в него съдебна практика.

42 Вж. например член 245, параграф 2 от Директива 2006/112/ЕО от 28 ноември 2006 г. относно общата система на данъка върху добавената стойност, който предвижда, че „[д]ържавите членки могат да изискват от данъчнозадължените лица, установени на тяхна територия, да ги уведомяват за мястото на съхранение, ако то е извън тяхната територия“. Това изискване обаче трябва да се тълкува съгласно член 249, който гласи: „[к]огато данъчнозадължено лице съхранява фактури, които то издава или получава, чрез електронни средства, гарантиращи достъп в режим „онлайн“ до данните и когато мястото на съхранение е в държава членка, различна от тази, в която то е установено, компетентните органи в държавата членка, в която то е установено, имат правото, за целите на настоящата директива, на достъп до тези фактури по електронен път, за зареждането и използването им в рамките, установени от правилата на държавата-членка, в която е установено данъчнозадълженото лице и доколкото тези органи изискват това за целите на контрола.“.

43 Член 4, параграф 4 от Регламент (ЕС) 2018/1807 на Европейския парламент и на Съвета от 14 ноември 2018 г. относно рамка за свободното движение на нелични данни в Европейския съюз

44 https://europa.eu/youreurope/index.htm#bg

45 Член 1, параграф 3 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 (Общ регламент относно защитата на данните)

тези свободи, предвидени в Договора за функционирането на Европейския съюз[46,47], и съответното законодателство на ЕС, като Директивата за услугите[48] и Директивата за електронната търговия[49].

Пример:

Национално право изисква сметките, по които се изплащат трудови възнаграждения, да се намират в определена държава членка поради причини, свързани с регулаторния контрол, например от страна на националния данъчен орган. Тази национална разпоредба попада извън обхвата на член 1, параграф 3 от Общия регламент относно защитата на данните, тъй като причините са различни от защита на личните данни. Вместо това изискването ще трябва да бъде оценено спрямо разпоредбите относно основните свободи и разрешените основания за дерогация от тези свободи, предвидени в Договора за функционирането на Европейския съюз.

Общият регламент относно защитата на данните[50] признава, че държавите членки могат да налагат условия, включително и ограничения, по отношение на обработването на генетични данни, биометрични данни или данни за здравословното състояние. Както се посочва в съображение 53, тези национални ограничения не следва да възпрепятстват свободното движение на лични данни в рамките на Съюза, когато тези условия се прилагат за трансгранично обработване на такива данни. Това е в съответствие с член 16 от Договора за функционирането на Европейския съюз, в който е установено правното основание за приемането на правилата, свързани с правото на защита на личните данни, както и по отношение на свободното движение на тези данни.

3.3 Обхват на Регламента за свободното движение на нелични данни

Както вече беше споменато, Регламентът за свободното движение на нелични данни има за цел да гарантира свободното движение на нелични данни „в рамките на Съюза“[51]. Поради това той не се прилага за операции за обработване на данни, които се

[46] Консолидиран текст на Договора за функционирането на Европейския съюз, ОВ С 326, 26.10.2012 г., стр. 47—390.

[47] Вж. също решение от 19 юни 2008 г. по дело *Комисия на Европейските общности/Великото херцогство Люксембург,* C-319/06, ECLI:EU:C:2008:350, точки 90—91: Съдът счита, че задължението за държане на разположение и съхраняване на някои документи в определена държава членка представлява ограничение на свободното предоставяне на услуги; обосновката, че това „улеснява най-общо изпълнението на задължението за контрол на органите“ не е достатъчна.

[48] Директива 2006/123/ЕО на Европейския парламент и на Съвета от 12 декември 2006 г. относно услугите на вътрешния пазар, ОВ L 376, 27.12.2006 г., стр. 36—68.

[49] Директива 2000/31/ЕО на Европейския парламент и на Съвета от 8 юни 2000 г. за някои правни аспекти на услугите на информационното общество, и по-специално на електронната търговия на вътрешния пазар („Директива за електронната търговия“) ОВ L 178, 17.7.2000 г., стр. 1—16.

[50] Член 9, параграф 4 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 (Общ регламент относно защитата на данните)

[51] Вж. член 1от Регламент (ЕС) 2018/1807 на Европейския парламент и на Съвета от 14 ноември 2018 г. относно рамка за свободното движение на нелични данни в Европейския съюз.

извършват извън ЕС, и за изисквания за локализиране на данни, свързани с такова обработване[52, 53].

Следователно в съответствие с член 2, параграф 1 обхватът на Регламента е ограничен до обработването на електронни нелични данни в ЕС, което:

а) се извършва като услуга за ползвателите, пребиваващи или установени в ЕС, независимо дали доставчикът на услуги е установен в ЕС, или не; или
б) се извършва от физическо или юридическо лице, което пребивава или е установено в ЕС, за собствените му нужди.

Примери:

Член 2, параграф 1, буква а) от Регламента за свободното движение на нелични данни:

- Доставчик на облачни услуги, установен в САЩ, предоставя своите услуги за обработване на данни на клиенти, пребиваващи или установени в ЕС. Той управлява дейностите си чрез сървъри, които се намират на територията на ЕС, където данните на европейските му клиенти се съхраняват или обработват по друг начин. Не е необходимо доставчикът на облачни услуги да разполага с инфраструктура, базирана в ЕС, но може например също така да наеме място на сървър в ЕС. Регламентът за свободното движение на нелични данни се прилага за такава обработка на данни.
- Доставчик на облачни услуги, установен в Япония, предлага услугите си на европейски клиенти. Капацитетът за обработване е разположен в Япония и всички дейности по обработване се осъществяват там. В този случай Регламентът за свободното движение на нелични данни не се прилага, ако всички дейности по обработване се осъществяват извън ЕС[54].

Член 2, параграф 1, буква б) от Регламента за свободното движение на нелични данни:

[52] Виж съображение 15 от Регламент (ЕС) 2018/1807 на Европейския парламент и на Съвета от 14 ноември 2018 г. относно рамка за свободното движение на нелични данни в Европейския съюз.

[53] Понятието „обработване“ е определено в широк смисъл (член 3, параграф 2 от Регламент (ЕС) 2018/1807 на Европейския парламент и на Съвета от 14 ноември 2018 г. относно рамка за свободното движение на нелични данни в Европейския съюз), и както е подчертано в съображение 17, регламентът следва да се прилага при обработването в най-широкия смисъл, което включва използването на всички видове информационни системи.

[54] Следва да се отбележи, че Регламент (ЕС) 2018/1807 на Европейския парламент и на Съвета от 14 ноември 2018 г. относно рамка за свободното движение на нелични данни в Европейския съюз не се отнася до изискванията за локализиране на данни, налагани от държавите членки по отношение на съхранението на нелични данни в трети държави, и те могат да съществуват в националния правен ред. С цел по-голяма яснота Общият регламент относно защитата на данните се прилага за обработването на лични данни на субекти на данни, които се намират в Съюза, от администратор или обработващ лични данни, който не е установен в Съюза, когато дейностите по обработване на данни са свързани с: а) предлагането на стоки или услуги на такива субекти на данни в Съюза, независимо дали от субекта на данни се изисква плащане; или б) наблюдението на тяхното поведение, доколкото това поведение се проявява в рамките на Съюза (вж. член 3, параграф 2 от Общия регламент относно защитата на данните).

- Малко европейско стартиращо предприятие от държава членка А решава да разшири бизнеса си, като разкрие обект в държава членка Б. За да сведе до минимум разходите, това стартиращо предприятие избира да централизира съхранението и обработването на данните на новия обект на сървъра си, който се намира в държава членка А. Държавите членки не могат да забраняват такива дейности по централизация на информационните технологии, освен на основание обществена сигурност в съответствие с принципа на пропорционалност.

Въпреки че Регламентът за свободното движение на нелични данни не се прилага, ако всички дейности по обработване на нелични данни се извършват извън ЕС, трябва да се спазват изискванията на Общия регламент относно защитата на данните, когато личните данни са част от набора от данни. По-конкретно правилата за предаване на лични данни на трети държави или международни организации съгласно Общия регламент относно защитата на данните трябва да се спазват във всички случаи[55].

3.4 Дейности, свързани с вътрешната организация на държавите членки

Регламентът за свободното движение на нелични данни не задължава държавите членки да възлагат на външни изпълнители предоставянето на услуги, свързани с нелични данни, които те желаят да предоставят сами или чието предоставяне желаят да организират по начин, различен от обществени поръчки[56].

Член 2, параграф 3, втора алинея от Регламента за свободното движение на нелични данни гласи:

„Настоящият регламент не засяга законови, подзаконови и административни разпоредби, които са свързани с **вътрешната организация** на държавите членки и които разпределят сред публичните органи и публичноправните организации, съгласно определението в член 2, параграф 1, точка 4 от Директива 2014/24/ЕС[57], правомощия и

[55] Във връзка с предаването на лични данни на трети държави, разгледайте уебсайта на Комисията: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_bg и *Съобщение на Комисията до Европейския парламент и Съвета — Обмен и защита на личните данни в един глобализиран свят*, COM/2017/07, на разположение на адрес: https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=COM%3A2017%3A7%3AFIN. По отношение на Япония на 23 януари 2019 г. Комисията прие решението си относно адекватното ниво на защита, позволяващо личните данни да се движат свободно между двете икономики благодарение на солидни гаранции за защита.

[56] Съображение 14 от Регламент (ЕС) 2018/1807 на Европейския парламент и на Съвета от 14 ноември 2018 г. относно рамка за свободното движение на нелични данни в Европейския съюз.

[57] Член 2, параграф 1, четвърта алинея от Директива 2014/24/ЕС на Европейския парламент и на Съвета от 26 февруари 2014 г. за обществените поръчки и за отмяна на Директива 2004/18/ЕО, ОВ L 94, 28.3.2014 г., стр. 65—242 гласи: „Публичноправни организации“ означава организации, които имат всички характеристики, изброени по-долу: а) създадени са с конкретната цел да задоволяват нужди от общ интерес, които нямат промишлен или търговски характер; б) имат правосубектност; както и в) финансират се в по-голямата си част от държавни, регионални или местни органи или от други публичноправни организации; или са обект на управленски контрол от страна на тези органи или организации; или имат административен, управителен или надзорен орган, повечето от половината от членовете на който са назначени от държавните, регионалните или местните органи или от други публичноправни организации.“

отговорности за **обработването на данни, без заплащане на договорни възнаграждения на частни лица**, както и законовите, подзаконовите и административните разпоредби на държавите членки, които осигуряват изпълнението на тези правомощия и отговорности.“[58].

Може да има законни интереси, които ще гарантират избора на този вид „самопредоставяне“ на услуги за обработване на данни, като например „вътрешно предоставяне“ или насрещни договорености между публични администрации. Типични примери са използването на „правителствен облак“, или наемането от страна на правителството на централизирана агенция за информационни технологии, която да предоставя услуги за обработване на данни на публичните институции и органи.

Регламентът за свободното движение на нелични данни обаче насърчава държавите членки да вземат предвид икономическата ефективност и други предимства от използването външни доставчици на услуги[59,60]. Когато националните органи започнат да възлагат обработването на данни на външни изпълнители със заплащане на договорни възнаграждения на частни лица и обработването се извършва в ЕС, това обработване попада в обхвата на Регламента за свободното движение на нелични данни, което означава, че принципът на свободното движение на нелични данни се прилага за общите и административните практики на националните органи. По-конкретно те трябва да се въздържат от поставянето на ограничения по отношение на локализирането на данни, например при тръжните процедури за възлагане на обществени поръчки[61].

4 Подходи за саморегулиране в подкрепа на свободното движение на данни

Саморегулирането допринася за иновациите и изграждането на доверие между участниците на пазара и има потенциала да реагира по-добре на промените на пазара. Настоящият раздел представя общ преглед на инициативите за саморегулиране при обработването както на лични, така и на нелични данни.

4.1 Пренасяне на данни и смяна на доставчиците на облачни услуги

Една от целите на Регламента за свободното движение на нелични данни е да се избегнат практиките на създаване на зависимост от конкретен доставчик. Тези практики се появяват, когато ползвателите не могат да сменят доставчиците на услуги,

[58] Съображение 13 от Регламент (ЕС) 2018/1807 на Европейския парламент и на Съвета от 14 ноември 2018 г. относно рамка за свободното движение на нелични данни в Европейския съюз посочва, че регламентът не засяга Директива 2014/24/ЕС.

[59] Съображение 14 от Регламент (ЕС) 2018/1807 на Европейския парламент и на Съвета от 14 ноември 2018 г. относно рамка за свободното движение на нелични данни в Европейския съюз.

[60] Външен доставчик на услуги е всеки субект, който не представлява „публичноправна организация“, както е предвидено в член 2, параграф 1, четвърта алинея от Директива 2014/24/ЕС на Европейския парламент и на Съвета от 26 февруари 2014 г. за обществените поръчки и за отмяна на Директива 2004/18/ЕО, ОВ L 94, 28.3.2014 г., стр. 65—242.

[61] Съображение 13 от Регламент (ЕС) 2018/1807 на Европейския парламент и на Съвета от 14 ноември 2018 г. относно рамка за свободното движение на нелични данни в Европейския съюз.

тъй като техните данни са „заключени“ в системата на доставчика, например поради специален формат на данните или договорни условия, и не могат да бъдат прехвърлени извън информационната система на доставчика. Безпрепятственото пренасяне на данни е важно, за да се даде възможност на ползвателите да избират свободно доставчиците на услуги за обработване на данни и по този начин да се гарантира ефективната конкуренция на пазара.

Преносимостта на данните между предприятията придобива все по-голямо значение в широк кръг от цифрови отрасли, включително облачните услуги.

В съответствие с член 6 от Регламента за свободното движение на нелични данни Комисията насърчава и улеснява разработването на кодекси за поведение на равнището на ЕС с цел саморегулиране („кодекси за поведение“), за да допринесе за конкурентоспособността на основаната на данни икономика Той предоставя основа на промишлеността да разработи кодекси за поведение с цел саморегулиране относно смяната на доставчици на услуги и пренасянето на данни между различни информационни системи.

При разработването на такива кодекси за поведение относно пренасянето на данни следва да се вземат предвид редица аспекти, по-специално:

- **най-добрите практики** при улесняването на смяната на доставчици на услуги и пренасянето на данни в структуриран, широко използван и машинночетим формат;
- **минималните изисквания за информация** с цел да се гарантира, че преди сключването на договор за обработване на данни, професионалните ползватели разполагат с достатъчно подробна и ясна информация относно процесите, техническите изисквания и сроковете и таксите, които се прилагат, в случай че професионален ползвател иска да премине към друг доставчик на услуги или да пренесе данните обратно в собствените си информационни системи;
- **подходи към схеми за сертифициране** с цел по-добра съпоставимост на облачните услуги; и
- **комуникационни пътни карти** за повишаване на осведомеността относно кодексите за поведение.

На пазара на облачни услуги Комисията започна да подпомага дейността на работните групи от заинтересовани страни в областта на облачните услуги на цифровия единен пазар, която обединява експерти в областта на облачните услуги и професионални ползватели, включително малки и средни предприятия. На този етап една подгрупа разработва кодекс за поведение с цел саморегулиране относно пренасянето на данни и смяната на доставчиците на облачни услуги (работна група SWIPO)[62], а друга подгрупа

[62] Работната група за смяна на доставчиците на облачни услуги и пренасяне на данни

работи по въпросите на сертифицирането за сигурност на облачните услуги (работна група CSPCERT)[63].

Работната група SWIPO разработва кодекси за поведение, в които е обхванат целият спектър от облачни услуги: инфраструктура като услуга (IaaS), платформа като услуга (PaaS) и софтуер като услуга (SaaS).

Комисията очаква различните кодекси за поведение да бъдат допълвани от **примерни договорни клаузи**[64]. Те ще позволят достатъчна техническа и правна специфика при изпълнението и прилагането на кодексите за поведение на практика, което ще бъде от особено значение за малките и средните предприятия. Изготвянето на примерните договорни клаузи се планира след разработването на кодексите за поведение (което следва да завърши до 29 ноември 2019 г.).

В съответствие с член 8 от Регламента за свободното движение на нелични данни Комисията ще извърши оценка на прилагането на регламента до 29 ноември 2022 г. Това ще предостави възможност за оценка на: i) отражението върху свободното движение на данни в Европа; ii) прилагането на регламента, особено към набори от смесени данни; iii) степента, в която държавите членки ефективно са отменили съществуващи неоправдани ограничения по отношение на локализирането на данни; и iv) пазарната ефективност на кодексите за поведение в областта на пренасянето на данни и смяната на доставчиците на облачни услуги.

Понятието „преносимост“ и взаимодействието с Общия регламент относно защитата на данните

И двата регламента[65] се отнасят до преносимостта на данните и целта им е да улеснят пренасянето на данни от една информационна среда до друга, тоест или до други системи на доставчик, или до системи на място. Това предотвратява създаването на зависимост от конкретен доставчик и насърчава конкуренцията между доставчиците на услуги. Що се отнася до връзката между целевите заинтересовани групи и правния характер на разпоредбите обаче регламентите се различават по своите подходи към преносимостта.

Правото на преносимост на личните данни съгласно член 20 от Общия регламент относно защитата на данните се фокусира върху отношенията между субекта на данни и администратора. Той се отнася до правото на субекта на данни да получи личните данни, които е предоставил на администратора, в структуриран, широко използван и

[63] Европейската работна група за сертифициране на доставчици на облачни услуги. Вж. също раздел 4.3

[64] Виж съображение 30 от Регламент (ЕС) 2018/1807 на Европейския парламент и на Съвета от 14 ноември 2018 г. относно рамка за свободното движение на нелични данни в Европейския съюз.

[65] Член 6 от Регламент (ЕС) 2018/1807 на Европейския парламент и на Съвета от 14 ноември 2018 г. относно рамка за свободното движение на нелични данни в Европейския съюз и член 20 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 (Общ регламент относно защитата на данните).

пригоден за машинно четене формат и да прехвърли тези данни на друг администратор или на собствения си капацитет за съхранение без администраторът, на когото личните данни са предоставени, да го възпрепятства[66]. Обикновено при тези отношения субектите на данни са потребители на различни онлайн услуги, които желаят да сменят тези доставчици на услуги.

Член 6 от Регламента за свободното движение на нелични данни не предвижда право за професионалните ползватели да пренасят данни, но съдържа подход за саморегулиране с доброволни кодекси за поведение за промишлеността. В същото време той е насочен към ситуация, при която професионален ползвател е възложил обработването на данните си на трета страна, която предлага услуги за обработване на данни[67]. В съответствие с член 3, параграф 8 от Регламента за свободното движение на нелични данни понятието „професионален ползвател“ може да включва както физическо, така и юридическо лице, „включително публичен орган или публичноправна организация, което използва или изисква услуга за обработване на данни за цели, свързани с неговата търговска или стопанска дейност, занаят, професия или задача“.

На практика преносимостта съгласно член 6 от Регламента за свободното движение на нелични данни се отнася до работните отношения между професионален ползвател (който може да се квалифицира като „администратор“ в съответствие с Общия регламент относно защитата на данните в случаи, които включват обработването на лични данни) и доставчик на услуги (по подобен начин в някои случаи може да се квалифицира като „обработващ лични данни“).

Въпреки различията, могат да възникнат ситуации, в които при смесени набори от данни пренасянето на данни би било обхванато както от Регламента за свободното движение на нелични данни, така и от Общия регламент относно защитата на данните.

Пример:

Предприятие, което използва облачни услуги, решава да смени доставчика си на облачни услуги и да пренесе всички данни на нов доставчик. Смяната на доставчика на услуги и пренасянето на данни са обхванати в договора между клиента и доставчика на облачни услуги. Ако старият доставчик на облачни услуги се придържа към кодексите за поведение, разработени съгласно Регламента за свободното движение на нелични данни, пренасянето на данни трябва да се извърши в съответствие с изискванията, уточнени в кодексите.

[66] Вж. Работна група по член 29: *Насоки относно правото на преносимост на данните.* WP 242 rev.01, приети на 13 декември 2016 г., последно преразгледани и приети на 5 април 2017 г.

[67] Съображение 29 от Регламент (ЕС) 2018/1807 на Европейския парламент и на Съвета от 14 ноември 2018 г. относно рамка за свободното движение на нелични данни в Европейския съюз гласи: „Докато индивидуалните потребители могат да се възползват от действащото право на Съюза [т.е. Общия регламент относно защитата на данните], то не улеснява възможността за смяна на доставчиците на услуги за тези ползватели, които упражняват стопанска или професионална дейност.“

Ако личните данни също са част от пренесените набори от данни, пренасянето трябва да съответства на всички имащи отношение разпоредби на Общия регламент относно защитата на данните, по-специално гарантирането, че новият доставчик на облачни услуги изпълнява приложимите изисквания, например по отношение на сигурността[68].

Пример:

Ако дадена банка реши да промени доставчика си на управление на връзките с клиенти (CRM), е възможно да се наложи някои (лични и нелични) данни да бъдат пренесени от стария на новия доставчик. Тогава тези данни ще подлежат на различни регулаторни изисквания, някои от които произтичат от Общия регламент относно защитата на данните, а други от Регламента за свободното движение на нелични данни.

4.2 Кодекси за поведение и механизми за сертифициране за защита на личните данни

За доказване на спазването на задълженията съгласно Общия регламент относно защитата на данните могат да се използват кодекси за поведение и механизми за сертифициране (вж. член 24, параграф 3 и член 28, параграф 5).

В съответствие с член 40, параграф 1 и член 42, параграф 1 от Общия регламент относно защитата на данните държавите членки, надзорните органи, Европейският комитет по защита на данните и Комисията насърчават промишлеността да изготвя кодекси за поведение и да създава механизми за сертифициране за защита на данните.

Сдружения или други органи, представляващи определена категория администратори или обработващи лични данни, могат да изготвят кодекс за поведение за конкретния сектор. На съответния надзорен орган, компетентен да издава одобрения, трябва да бъде представен проект на кодекса[69]. Ако проектът на кодекса за поведение се отнася до дейности по обработване на данни в няколко държави членки, надзорният орган трябва да го представи пред Европейския комитет по защита на данните, преди да го одобри. След това Комитетът ще даде своето становище за това дали проектът на кодекса е в съответствие с Общия регламент относно защитата на данните.

Европейският комитет по защита на данните публикува своите Насоки 1/2019 относно кодексите за поведение и органите за наблюдение съгласно Общия регламент относно защитата на данните[70]. Насоките съдържат информация за изготвянето на кодекси за

[68] Вж. Работна група по член 29: *Становище 05/2012 относно изчисленията в облак*, прието на 1 юли 2012 г. WP196, в което състоянието и задълженията на ползвателите на облачни услуги и доставчиците на облачни услуги във връзка с обработването на лични данни са допълнително уточнени.

[69] Вж. член 40, параграф 5 и член 55 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 (Общ регламент относно защитата на данните).

[70] Европейски комитет по защита на данните: *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 („Насоки 1/2019 относно кодексите за поведение и органите за*

поведение, критерии за тяхното одобряване и друга полезна информация. По подобен начин Насоките на Европейският комитет по защита на данните 1/2018 относно сертифицирането и определянето на критерии за сертифициране в съответствие с членове 42 и 43 от Общия регламент относно защитата на данните предоставят информация за сертифицирането в съответствие с този регламент и разработването и одобряването на критерии за сертифициране[71].

Примери на кодекси за поведение, разработени от сектора на облачните услуги:

Кодексът на ЕС за поведение в областта на облачните услуги, чието разработване беше подпомогнато от Комисията, беше изготвен в сътрудничество с Cloud Select Industry Group (C-SIG) въз основа на Директивата за защита на личните данни[72] и в последствие на Общия регламент относно защитата на данните. Кодексът на ЕС за поведение в областта на облачните услуги обхваща пълния спектър от облачни услуги — софтуер като услуга (SaaS), платформа като услуга (PaaS) и инфраструктура като услуга (IaaS)[73].

Кодексът за поведение на доставчиците на инфраструктура за услуги в облак в Европа (CISPE)[74] е съсредоточен върху доставчиците на инфраструктура като услуга (IaaS). Кодексът за поведение на CISPE се състои от изисквания относно доставчиците на IaaS, които изпълняват функцията на обработващи лични данни съгласно Общия регламент относно защитата на данните. В него са предвидени също така разпоредби за управленската структура за изпълнение и прилагане на кодекса.

Кодексът за поведение на Алианса за облачна сигурност (Cloud Security Alliance — CSA) за съответствие с ОРЗД е насочен към всички заинтересовани страни в сферата на изчисленията в облак и европейското законодателство в областта на личните данни, като доставчици на облачни услуги, клиенти и потенциални клиенти на облачни услуги, одитори и брокери на облачни услуги. Кодексът за поведение обхваща пълния спектър на доставчиците на облачни услуги[75].

наблюдение съгласно Регламент 2016/679), приети на 12 февруари 2019 г., версия за обществена консултация, на разположение на адрес: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-under_en

[71] Европейски комитет по защита на данните: *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679 („Насоки 1/2018 относно сертифицирането и определянето на критерии за сертифициране в съответствие с членове 42 и 43 от Регламент 2016/679)*, приети на 23 януари 2019 г., версия за обществена консултация, на разположение на адрес: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_en

[72] Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 г. за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни (дата на изтичане на срока на валидност: 24 май 2018 г.).

[73] За допълнителна информация относно Кодекса на ЕС за поведение в областта на облачните услуги вж.: https://eucoc.cloud/en/home.html

[74] За допълнителна информация относно Кодекса за поведение на CISPE вж.: https://cispe.cloud/code-of-conduct/

[75] За допълнителна информация относно Кодекса за поведение на CSA вж.: https://gdpr.cloudsecurityalliance.org/

4.3 Повишаване на доверието в трансграничното обработване на данни — сертифициране на механизмите за сигурност

Както е посочено в съображение 33 от Регламента за свободното движение на нелични данни, повишаването на доверието в сигурността на трансграничното обработване на данни следва да намали склонността на участниците на пазара и на обществения сектор да използват локализирането на данни като метод за постигане на сигурността на данните. Едновременно със законодателния пакет в областта на киберсигурността, предложен от Комисията през 2017 г.[76], работната група CSPCERT разработва препоръки за целите на създаването на европейска схема за сертифициране на облачните услуги, които ще бъдат представени на Комисията. Тази схема има потенциала да улесни свободното движение на данни, да даде възможност за по-добра съпоставимост на облачните услуги и да насърчи тяхното навлизане. Комисията може да поиска от Агенцията на Европейския съюз за киберсигурност (ENISA) да разработи предложение за схема в съответствие с приложимите разпоредби на Акта за киберсигурността[77]. Тази схема може да е насочена както към лични, така и към нелични данни. В допълнение към Акта за киберсигурността и както е подчертано в раздел 4.2, ОРЗД може също така да бъде използван за доказване на наличието на подходящи гаранции относно сигурността на данните[78].

Заключителни бележки

Правната сигурност и доверието в обработването на данни са от решаващо значение за способността на ЕС да използва възможно най-пълноценно данните, така че веригите за създаване на стойност да могат да се развиват във всички сектори и пресичайки границите. Двата регламента осигуряват това, като и двата преследват целта за свободно движение на данни. Взети заедно, Регламентът за свободното движение на нелични данни и Общият регламент относно защитата на данните създават основата за свободното движение на всички данни в рамките на Европейския съюз и за високо конкурентна основана на данни европейска икономика.

---

[76] За допълнителна информация вж.: https://ec.europa.eu/digital-single-market/en/cyber-security

[77] Регламент на Европейския парламент и на Съвета от 17 април 2019 г. относно ENISA (Агенцията на Европейския съюз за киберсигурност) и относно сертифицирането на киберсигурността на информационните и комуникационните технологии и за отмяна на Регламент (ЕС) № 526/2013 („Акт за киберсигурността“)

[78] Вж. съображение 74 от Акта за киберсигурността.