



ЕВРОПЕЙСКИ СЪЮЗ

ЕВРОПЕЙСКИ ПАРЛАМЕНТ

СЪВЕТ

Страсбург, 14 ноември 2018 г.
(OR. en)

2017/0228 (COD)
LEX 1838

PE-CONS 53/1/18
REV 1

TELECOM 213
COMPET 496
MI 511
DATAPROTECT 145
JAI 723
CODEC 1211

РЕГЛАМЕНТ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА ОТНОСНО РАМКА ЗА СВОБОДНОТО ДВИЖЕНИЕ НА НЕЛИЧНИ ДАННИ В ЕВРОПЕЙСКИЯ СЪЮЗ

РЕГЛАМЕНТ (ЕС) 2018/...
НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

от 14 ноември 2018 година

**относно рамка за свободното движение на нелични данни
в Европейския съюз**

(текст от значение за ЕИП)

ЕВРОПЕЙСКИЯТ ПАРЛАМЕНТ И СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

като взеха предвид Договора за функционирането на Европейския съюз, и по-специално член 114 от него,

като взеха предвид предложението на Европейската комисия,

след предаване на проекта на законодателния акт на националните парламенти,

като взеха предвид становището на Европейския икономически и социален комитет¹,

след консултация с Комитета на регионите,

в съответствие с обикновената законодателна процедура²,

¹ ОВ С 227, 28.6.2018 г., стр. 78.

² Позиция на Европейския парламент от 4 октомври 2018 г. все още непубликувана в Официален вестник) и решение на Съвета от 6 ноември 2018 г.

като имат предвид, че:

- (1) Цифровизацията на икономиката се ускорява. Информационните и комуникационните технологии вече не са отделен сектор, а представляват основата на всички модерни иновативни икономически системи и общества. Електронните данни са в центъра на тези системи и могат да генерират висока стойност при анализи или в комбинация с услуги и продукти. В същото време бързото развитие на основаната на данни икономика и нововъзникващите технологии, като например изкуственият интелект, продуктите и услугите, свързани с „интернет на предметите“, автономните системи и 5G, водят до възникването на нови правни проблеми, свързани с въпросите относно достъпа до данни и тяхната повторна употреба, отговорността, етичното измерение и солидарността. Следва да се обръща внимание на работата върху проблемите, свързани с отговорността, по-специално чрез прилагането на кодекси за саморегулиране и други най-добри практики, като се отчитат препоръките, решенията и действията, предприемани без човешка намеса по цялата верига на създаване на стойност, при обработването на данните. Тази работа би могла да включва също и подходящи механизми за определяне на отговорността, за прехвърляне на отговорност между сътрудническите си служби, за застраховане и за одитиране.

- (2) Веригите на стойността на данните са изградени на основата на различни дейности: създаване и събиране на данни; обобщаване и организиране на данни; обработване на данни; анализ, маркетинг и разпространение на данни; използване и повторно използване на данни. Ефективното и ефикасното функциониране на обработването на данни е в основата на всяка верига на стойност на данните. Ефективното и ефикасното функциониране на обработването на данни и развитието на основаната на данни икономика в Съюза обаче са затруднени, по-специално от два типа пречки пред мобилността на данните и пред вътрешния пазар: изискванията за локализиране на данни, установени от органите на държавите членки и практиките на създаване на зависимост от конкретен доставчик на услуги в частния сектор.
- (3) Свободата на установяване и свободата на предоставяне на услуги съгласно Договора за функционирането на Европейския съюз („ДФЕС“) се прилагат към услугите за обработване на данни. Предоставянето на тези услуги обаче се затруднява или понякога осуetyава от определени национални, регионални или местни изисквания за локализиране на данни в определена територия.

- (4) Подобни пречки за свободното движение на услугите за обработване на данни и за упражняването на правото на установяване на доставчиците на услуги произтичат от изисквания в правото на държавите членки за локализиране на данни в определен географски район или територия за целите на обработването им. Други правила или административни практики постигат равностойно въздействие чрез налагането на конкретни изисквания, които затрудняват обработването на данни извън конкретен географски район или територия в Съюза, като например изисквания за използване на технологични съоръжения, които са сертифицирани или одобрени в определена държава членка. 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. Настоящият регламент по никакъв начин не ограничава свободата на предприятията да сключват договори, определящи къде да се локализируют данни. Настоящият регламент цели единствено да защитава тази свобода, като гарантира, че договореното местоположение на данните може да бъде навсякъде в рамките на Съюза.
- (5) Същевременно мобилността на данните в Съюза се възпрепятства и от частни ограничения: правни, договорни или технически проблеми затрудняват или пречат на ползвателите на услуги за обработване на данни да пренасят данните си от един доставчик на услуги към друг или обратно към собствените си информационни системи, включително при прекратяване на договора им с доставчик на услуги.

- (6) Комбинацията от тези пречки води до липса на конкуренция между доставчиците на облачни услуги в Съюза, до различни практики на създаване на зависимост от конкретен доставчик на услуги и до сериозна липса на мобилност на данните. Също така политиките на локализиране на данни засегнаха негативно способността на дружествата за изследователска и развойна дейност да подпомагат сътрудничеството между предприятия, университети и други научноизследователски организации с цел стимулиране на иновациите.
- (7) От съображения за правна сигурност и поради необходимостта от еднакви условия на конкуренция в Съюза наличието на единен набор от правила за всички участници на пазара е ключов елемент за функционирането на вътрешния пазар. Следователно, за да се отстранят пречките пред търговията и нарушенията на конкуренцията в резултат на различията между националните правни уредби, както и за да се предотврати появата на нови възможни пречки пред търговията и съществени нарушения на конкуренцията, е необходимо да се приемат единни правила, приложими във всички държави членки.

- (8) Правната рамка относно защитата на физическите лица във връзка с обработването на лични данни и относно зачитането на неприкосновеността на личния живот и защитата на личните данни в електронните съобщения и особено Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета¹, и директиви (ЕС) 2016/680² и 2002/58/ЕО³ на Европейския парламент и на Съвета, не са засегнати от настоящия регламент.
- (9) Развиващият се „интернет на предметите“, изкуственият интелект и машинното учене са основни източници на нелични данни, например в резултат на тяхното използване в автоматизирани производствени процеси в промишлеността. Конкретни примери за нелични данни включват агрегирани и анонимизирани набори от данни, използвани за анализ на големи информационни масиви, данни за прецизно земеделие, които могат да помогнат за наблюдение и оптимизиране на употребата на пестициди и вода, или данни относно нуждите от поддръжка на промишлени машини. Ако напредъкът в технологичното развитие направи възможно превръщането на анонимизираните данни в лични данни, тези данни трябва да се третираят като лични данни и Регламент (ЕС) 2016/679 трябва да се прилага съответно.

¹ 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).

² 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).

³ 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).

- (10) Съгласно Регламент (ЕС) 2016/679 държавите членки не могат нито да ограничават, нито да забраняват свободното движение на лични данни в Съюза по причини, свързани със защитата на физическите лица по отношение на обработването на лични данни. Настоящият регламент установява същия принцип на свободно движение на нелични данни в Съюза, освен когато ограничението или забраната са оправдани от съображения за обществената сигурност. Регламент (ЕС) 2016/679 и настоящият регламент осигуряват съгласуван набор от правила, които дават възможност за свободното движение на различни видове данни. Освен това настоящият регламент не налага задължение за отделно съхраняване на различните видове данни.
- (11) За да се създаде рамка за свободното движение на нелични данни в Съюза и да се изгради база за развитието на основаната на данни икономика и за повишаването на конкурентоспособността на промишлеността на Съюза, е необходимо да се създаде ясна, цялостна и предсказуема правна рамка за обработването на данни, различни от личните данни, във вътрешния пазар. Прилагането на основан на принципи подход, предвиждащ сътрудничество между държавите членки, както и саморегулиране, следва да гарантира, че рамката е достатъчно гъвкава, за да може да взема предвид променящите се нужди на ползвателите, доставчиците на услуги и националните органи в Съюза. За да се избегне рискът от припокриване със съществуващи механизми, като при това се избегне създаването на по-голяма тежест както за държавите членки, така и за предприятията, следва да не се установяват подробни технически правила.

- (12) Настоящият регламент следва да не засяга обработването на данни, доколкото то се извършва като част от дейности, попадащи извън обхвата на правото на Съюза. По-специално, следва да се припомни, че в съответствие с член 4 от Договора за Европейския съюз („ДЕС“) националната сигурност е отговорност изцяло на отделните държави членки.
- (13) Свободното движение на данни в рамките на Съюза ще играе важна роля за постигането на основан на данните растеж и иновации. Заедно с бизнеса и потребителите, публичните органи и публичноправните организации на държавите членки също ще извлекат ползи от по-голямата свобода на избор по отношение на доставчиците на основани на данни услуги, от по-конкурентните цени и от по-ефикасното предоставяне на услуги на гражданите. Като се има предвид огромното количество данни, с които публичните органи и публичноправните организации работят, от първостепенно значение е те да дадат добър пример като въведат услуги за обработване на данни и да се въздържат от поставянето на ограничения по отношение на локализирането на данни, когато използват услуги за обработване на данни. Следователно публичните органи и публичноправните организации следва да бъдат обхванати от настоящия регламент. В това отношение принципът на свободно движение на нелични данни, предвиден в настоящия регламент, следва да се прилага също и за общи и последователни административни практики и за други изисквания за локализиране на данни в областта на обществените поръчки, без да се засяга Директива 2014/24/ЕС на Европейския парламент и на Съвета¹.

¹ 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).

- (14) Както е в случая с Директива 2014/24/ЕС, настоящият регламент не засяга законовите, подзаконовите и административните разпоредби, които са свързани с вътрешната организация на държавите членки и които разпределят на публичните органи и публичноправните организации, правомощия и 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. Въпреки че публичните органи и публичноправните организации, се насърчават да вземат предвид икономическите и други ползи от възлагането на изпълнението на външни доставчици на услуги, те могат да имат основателни причини да изберат самопредоставяне на услуги или вътрешно предоставяне на услуги. Следователно настоящият регламент не задължава по никакъв начин държавите членки да сключват външни договори или да възлагат на външни изпълнители предоставянето на услуги, които те желаят да предоставят сами или да организират предоставянето им по начин, различен от обществените поръчки.
- (15) Настоящият регламент следва да се прилага по отношение на физическите и юридическите лица, които предоставят услуги за обработване на данни на ползватели, които пребивават или са установени в Съюза, включително такива доставчици на услуги за обработване на данни, които предоставят услуги за обработване на данни в Съюза, без да са установени в Съюза. Поради това настоящият регламент следва да не се прилага за услуги за обработване на данни, които се извършват извън Съюза, и за изисквания за локализиране, свързани с такива данни.

- (16) Настоящият регламент не съдържа правила относно определянето на приложимото право по търговски въпроси и следователно не засяга Регламент (ЕО) № 593/2008 на Европейския парламент и на Съвета¹. По-специално, доколкото приложимото към договора право не е било избрано в съответствие с посочения Регламент, договорът за предоставяне на услуги по принцип се урежда от правото на държавата, в която е обичайното пребиваване на доставчика на услуги.
- (17) Настоящият регламент следва да се прилага при обработването на данни в най-широкия смисъл, което включва използването на всички видове информационни системи, независимо дали те се намират в помещенията на ползвателя или изпълнението е възложено на доставчик на услуги. Настоящият регламент следва да обхваща обработването на данни с различни нива на интензитет, от тяхното съхранение („инфраструктура като услуга“ — IaaS), до обработването на данни на платформи („платформа като услуга“ — PaaS) или в приложения („софтуер като услуга“ — SaaS).
- (18) Изискванията за локализиране на данни представляват явна пречка пред свободното предоставяне на услуги за обработване на данни в целия Съюз и пред вътрешния пазар. Поради това те следва да бъдат забранени, освен когато са оправдани от съображения за обществена сигурност, както е предвидено в правото на Съюза, особено по смисъла на член 52 от ДФЕС, и удовлетворяват принципа на пропорционалност, уреден в член 5 от ДЕС. За да бъде приложен принципът на свободно трансгранично движение на нелични данни, за да се гарантира бързото отстраняване на съществуващите изисквания за локализиране на данни и да се даде възможност за обработване на данни на множество местоположения в Съюза поради оперативни съображения, и тъй като настоящият регламент предвижда мерки, които гарантират наличието на данни за целите на регулаторния контрол, държавите членки следва да могат да се позовават само на съображения за обществената сигурност като основание за налагане на изисквания за локализиране на данни.

¹ Регламент (ЕО) № 593/2008 на Европейския парламент и на Съвета от 17 юни 2008 г. относно приложимото право към договорни задължения (Рим I) (ОВ L 177, 4.7.2008 г., стр. 6).

- (19) Концепцията за „обществена сигурност“ по смисъла на член 52 от ДФЕС и съгласно тълкуването на тази концепция от Съда обхваща както вътрешната, така и външната сигурност на дадена държава членка, 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, 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. В съответствие с принципа на пропорционалност изискванията за локализиране на данните, които са оправдани от съображения, свързани с обществената сигурност, следва да бъдат подходящи за постигане на преследваната цел и следва да не надхвърлят необходимото за постигането на тази цел.
- (20) За да се осигури ефективното прилагане на принципа на свободното трансгранично движение на нелични данни и да се предотврати възникването на нови пречки за доброто функциониране на вътрешния пазар, държавите членки следва да съобщават незабавно на Комисията за всеки проект на акт, който въвежда ново изискване за локализиране на данни или изменя съществуващи изисквания за локализиране. Тези проекти на актове следва да бъдат представяни и оценявани в съответствие с Директива (ЕС) 2015/1535 на Европейския парламент и на Съвета¹.

¹ Директива (ЕС) 2015/1535 на Европейския парламент и на Съвета от 9 септември 2015 г. установяваща процедура за предоставянето на информация в сферата на техническите регламенти и правила относно услугите на информационното общество (ОВ L 241, 17.9.2015 г., стр. 1).

- (21) Освен това, за да се премахнат евентуални съществуващи пречки, по време на преходен период от 24 месеца от датата на прилагане на настоящия регламент, държавите членки следва да извършат преглед на действащите закони, подзаконови или административни разпоредби, с които се установяват изисквания за локализиране на данни и да съобщят на Комисията кои изисквания за локализиране на данни считат за съответстващи на настоящия регламент, като представят обосновка за тях. Това следва да позволи на Комисията да прецени съответствието на всички останали изисквания за локализиране на данни. Комисията следва да може, когато е уместно, да отправя коментари до въпросната държава членка. Тези коментари могат да включват препоръка за изменение или отмяна на изискването за локализиране на данни.
- (22) Задълженията за съобщаване на Комисията за съществуващи изисквания за локализиране на данни и на проектите на актове, установени с настоящия регламент, следва да се прилагат за регулаторните изисквания за локализиране на данни и за проектите на актове от общ характер, а не за решения, адресирани до конкретно физическо или юридическо лице.

- (23) За да се гарантира прозрачността на изискванията за локализиране на данните в държавите членки, установени в законова, подзаконова или административна разпоредба от общ характер за физически и юридически лица, като например доставчици на услуги и ползватели на услуги за обработване на данни, държавите членки следва да публикуват информация относно тези изисквания на национална единна информационна точка онлайн и редовно да актуализират тази информация. Като алтернатива, държавите членки следва да предоставят актуализирана информация относно тези изисквания на централна информационна точка, създадена съгласно друг акт на Съюза. За да бъдат надлежно информирани физическите и юридическите лица за изискванията за локализиране на данни в Съюза, държавите членки следва да съобщават на Комисията адресите на тези единни информационни точки. Комисията следва да публикува тази информация на своя собствен уебсайт, заедно с редовно актуализиран консолидиран списък на всички изисквания за локализиране на данните, които са в сила в държавите членки, включително обобщена информация относно тези изисквания.
- (24) Изискванията за локализиране на данни често са мотивирани от липса на доверие в трансграничното обработване на данни, произтичаща от предположението, че данните няма да са на разположение за целите на компетентните органи на държавите членки, например при инспекция или одит с цел регулаторен контрол или надзор. Тази липса на доверие не може да бъде преодоляна единствено чрез обявяването за нищожни на договорните условия, които забраняват законния достъп до данни на компетентните органи за изпълнението на техните служебни задължения. Поради това настоящият регламент следва категорично да предвижда, че с него не се засягат правомощията на компетентните органи да изискват или получават достъп до данни в съответствие с правото на Съюза или националното право, и че на компетентните органи не може да бъде отказан достъп до данни на основание, че данните се обработват в друга държава членка. Компетентните органи могат да налагат функционални изисквания за подпомагане на достъпа до данни, като например изискване описанията на системата да бъдат съхранявани в съответната държава членка.

- (25) Физическите или юридически лица, които са задължени да предоставят данни на компетентните органи, могат да изпълнят тези свои задължения като предоставят и гарантират на компетентните органи ефективен и навременен електронен достъп до данните, независимо от държавата членка, на чиято територия се обработват тези данни. Такъв достъп може да бъде осигурен чрез конкретни условия в договори между физическото или юридическо лице, задължено да предоставя достъп, и доставчика на услуга.
- (26) Когато дадено физическо или юридическо лице е задължено да предоставя данни и не изпълни това задължение, компетентният орган следва да може да потърси съдействие от компетентните органи на други държави членки. В такива случаи компетентните органи следва да използват конкретни инструменти за сътрудничество, предвидени в правото на Съюза или международни споразумения, в зависимост от предмета във всеки отделен случай, например полицейско сътрудничество, гражданско или наказателно право, или съответно административни въпроси, Рамково решение 2006/960/ПВР на Съвета¹, Директива 2014/41/ЕС на Европейския парламент и на Съвета², Конвенцията на Съвета на Европа за престъпленията в кибернетичното пространство³, Регламент (ЕО) № 1206/2001 на Съвета⁴, Директива 2006/112/ЕО⁵ и Регламент (ЕС) № 904/2010 на Съвета⁶. При липсата на такива специфични механизми за сътрудничество компетентните органи следва да си сътрудничат с оглед осигуряването на търсения достъп до данни чрез определени единни звена за контакт.

¹ Рамково решение 2006/960/ПВР на Съвета от 18 декември 2006 г. за опростяване обмена на информация и сведения между правоприлагащите органи на държавите — членки на Европейския съюз (ОВ L 386, 29.12.2006 г., стр. 89).

² Директива 2014/41/ЕС на Европейския парламент и на Съвета от 3 април 2014 г. относно Европейска заповед за разследване по наказателноправни въпроси (ОВ L 130, 1.5.2014 г., стр. 1).

³ Конвенция за престъпленията в кибернетичното пространство на Съвета на Европа, CETS № 185.

⁴ Регламент (ЕО) № 1206/2001 на Съвета от 28 май 2001 г. относно сътрудничеството между съдилища на държавите членки при събирането на доказателства по граждански или търговски дела (ОВ L 174, 27.6.2001 г., стр. 1).

⁵ Директива 2006/112/ЕО на Съвета от 28 ноември 2006 г. относно общата система на данъка върху добавената стойност (ОВ L 347, 11.12.2006 г., стр. 1).

⁶ Регламент (ЕС) № 904/2010 на Съвета от 7 октомври 2010 г. относно административното сътрудничество и борбата с измамите в областта на данъка върху добавената стойност (ОВ L 268, 12.10.2010 г., стр. 1).

- (27) Когато искането за съдействие предполага получаване на достъп до всички помещения на физическо или юридическо лице, включително всякакво оборудване и всякакви средства за обработване на данни от страна на запитания орган, този достъп се осъществява в съответствие с правото на Съюза или с националното процесуалното право, включително евентуални изисквания за получаване на предварително съдебно разрешение.
- (28) Настоящият регламент не следва да позволява на ползвателите да се опитват да избягват прилагането на националното право. Поради това следва да бъде предвидено налагането от страна на държавите членки на ефективни, пропорционални и възпиращи санкции за ползвателите, които възпрепятстват компетентните органи да получават достъп до техните данни, необходими за изпълнението на официалните задължения на компетентните органи съгласно правото на Съюза и националното право. В спешни случаи, когато ползвател злоупотребява с това право, държавите членки следва да могат да налагат стриктно пропорционални временни мерки. Всички временни мерки, които изискват повторно локализиране на данни за срок, по-дълъг от 180 дни след повторното локализиране, биха се отклонили от принципа за свободно движение на данни за значителен период от време и поради това следва да бъдат съобщавани на Комисията за преценка на тяхната съвместимост с правото на Съюза.

- (29) Възможността за безпрепятствено пренасяне на данни е ключов фактор за улесняване на избора на ползвателите и за ефективната конкуренция на пазарите на услуги за обработване на данни. Реалните или предполагаемите затруднения за трансгранично пренасяне на данни също така подкопават доверието на професионалните ползватели при приемането на трансгранични оферти, а оттам и доверието им във вътрешния пазар. Докато индивидуалните потребители могат да се възползват от действащото право на Съюза, то не улеснява възможността за смяна на доставчиците на услуги за тези ползватели, които упражняват стопанска или професионална дейност. Съгласуваността на техническите изисквания в целия Съюз, било то във връзка с техническата хармонизация, взаимното признаване или доброволното хармонизиране, допринася също за изграждането на конкурентен вътрешен пазар на услугите за обработване на данни.
- (30) За да се възползват напълно от конкурентната среда, професионалните ползватели следва да са в състояние да правят информиран избор и да сравняват лесно отделните компоненти на различните услуги за обработване на данни, предлагани на вътрешния пазар, включително и по отношение на договорните условия за пренасяне на данни при прекратяването на договор. С цел изравняване с иновационния потенциал на пазара и отчитане на опита и експертните знания на доставчиците на услуги и професионалните ползватели на услуги за обработване на данни, подробната информация и оперативните изисквания за пренасянето на данни следва да бъдат определени от участниците на пазара чрез саморегулиране, насърчавано, подпомагано и наблюдавано от Комисията, под формата на кодекси за поведение на равнището на Съюза, които може да включват примерни договорни условия.

- (31) За да бъдат ефективни и да улесняват смяната на доставчиците на услуги и пренасянето на данни, тези кодекси за поведение следва да бъдат подробни и да обхващат най-малко основните аспекти, които са важни при процеса на пренасяне на данни, като например начина на създаване и местоположението на резервните копия на данните, наличните формати и помощни средства, изискваната ИТ конфигурация и минималната ширина на честотната лента за мрежата, времето, необходимо преди започване на процеса по пренасяне на данни и времето, през което данните ще останат на разположение за пренасяне, както и гаранциите за достъп до данните в случай на несъстоятелност на доставчика на услуги. Кодексите за поведение следва също така да посочват ясно, че зависимостта от конкретен доставчик не е приемлива стопанска практика, да предвиждат повишаващи доверието технологии и да бъдат актуализирани редовно, за да не се изостава от развитието на технологиите. Комисията следва да гарантира, че по време на целия процес се провеждат консултации с всички заинтересовани страни, включително сдруженията на малки и средни предприятия (МСП) и стартиращи предприятия, ползватели и доставчици на облачни услуги. Комисията следва да извърши оценка на разработването и на ефективността на прилагането на тези кодекси за поведение.

- (32) Когато компетентен орган в дадена държава членка поиска съдействие от друга държава членка, за да получи достъп до данни съгласно настоящия регламент, той следва да внесе чрез определено единно звено за контакт надлежно обосновано искане до определеното единно звено за контакт на тази държава членка, което следва да включва писмено обяснение относно причините, както и правните основания за искане на достъп до данни. Единното звено за контакт, определено от държавата членка, от която е поискано съдействие, следва да осигури препращането на искането до съответния компетентен орган в запитаната държава членка. За да осигури ефективно сътрудничество, органът, на когото е предадено искането, следва незабавно да окаже съдействие в отговор на дадено искане или да предостави информация за трудностите при изпълнението на такова искане или за мотивите си за отказ.
- (33) 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. То следва да също да подобри и правната сигурност за дружествата относно спазването на приложимите изисквания за сигурност, когато те възлагат изпълнението на своите дейности по обработване на данни на доставчици на услуги, включително на доставчици на услуги в други държави членки.

- (34) Всички изисквания за сигурност, свързани с обработване на данни, които се прилагат обосновано и пропорционално на основата на правото на Съюза или националното право и в съответствие с правото на Съюза в държавата членка, където пребивава или е установено физическото или юридическото лице, чиито данни са засегнати, следва да продължат да се прилагат към обработването на данни в друга държава членка. Тези физически или юридически лица следва да имат възможност да изпълнят тези изисквания или лично, или чрез договорни клаузи в договори с доставчици на услуги.
- (35) Изискванията за сигурност, определени на национално равнище, следва да бъдат необходими и пропорционални на рисковете, пред които е изправено обработването на данните в обхвата на националното право, в което са залегнали тези изисквания.
- (36) Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета¹ предвижда правни мерки за повишаване на цялостното равнище на киберсигурността в Съюза. Услугите за обработване на данни съставляват една от цифровите услуги, обхванати от посочената директива. Съгласно посочената директива държавите членки трябва да гарантират, че доставчиците на цифрови услуги определят и предприемат подходящи и пропорционални технически и организационни мерки за управление на рисковете, пред които е изправена сигурността на мрежовите и информационните системи, които използват. Такива мерки следва да гарантират ниво на сигурност, отговарящо на съществуващия риск, и следва да вземат предвид сигурността на системите и съоръженията, реагирането на инциденти, управлението на непрекъснатостта на дейностите, мониторинга, одита и изпитванията, както и съответствието с международните стандарти. Тези елементи трябва да бъдат допълнително уточнени от Комисията в актове за изпълнение съгласно посочената директива.

¹ Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 г. относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза (ОВ L 194, 19.7.2016 г., стр. 1).

- (37) Комисията следва да представи доклад относно прилагането на настоящия регламент, по-специално с цел да провери необходимостта от изменения в контекста на промените в технологичните или пазарните условия. В този доклад следва по-специално да се направи оценка на настоящия регламент, особено на прилагането му по отношение на наборите от данни, съставени както от лични, така и от нелични данни, както и на прилагането на изключението, свързано с обществената сигурност. Преди настоящият регламент да започне да се прилага, Комисията следва също така да публикува информативни насоки за начина на третиране на наборите от данни, съставени както от лични, така и от нелични данни, за да могат дружествата, включително МСП, да разберат по-добре взаимодействието между настоящия регламент и Регламент (ЕС) 2016/679 и да гарантират спазването и на двата регламента.
- (38) Настоящият регламент зачита основните права и съблюдава принципите, признати по-специално от Хартата на основните права на Европейския съюз, и следва да се тълкува и прилага в съответствие с тези права и принципи, включително правото на защита на личните данни, свободата на изразяване на мнение и свободата на информация и свободата на стопанска инициатива.
- (39) Доколкото целта на настоящия регламент, а именно да осигури свободното в Съюза, движение на данни, различни от личните данни, не може да бъде постигната в достатъчна степен от държавите членки, а поради обхвата и последиците си може да бъде по-добре постигната на равнището на Съюза, Съюзът може да приеме мерки в съответствие с принципа на субсидиарност, уреден в член 5 от ДЕС. В съответствие с принципа на пропорционалност, уреден в същия член, настоящият регламент не надхвърля необходимото за постигането на тази цел,

ПРИЕХА НАСТОЯЩИЯ РЕГЛАМЕНТ:

Член 1
Предмет

Настоящият регламент има за цел да гарантира свободното движение на данни, различни от личните данни, в рамките на Съюза, като определи правила, свързани с изискванията за локализирането на данните, наличието на данни за компетентните органи и пренасянето на данни за професионалните ползватели.

Член 2
Обхват

1. Настоящият регламент се прилага за обработването на електронни данни, различни от личните данни, в Съюза, което се:
 - а) извършва като услуга за ползвателите, пребиваващи или установени в Съюза, независимо дали доставчикът на услуги е установен в Съюза или не, или
 - б) извършва от физическо или юридическо лице, което пребивава или е установено в Съюза за собствените си нужди.
2. 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.

3. Настоящият регламент не се прилага за дейност, попадаща извън обхвата на правото на Съюза.

Настоящия регламент не засяга закони, подзакони 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, правомощия и отговорности за обработването на данни, без заплащане на договорни възнаграждения на частни лица, както и законите, подзаконовите и административните разпоредби на държавите членки, които осигуряват изпълнението на тези правомощия и отговорности.

Член 3

Определения

За целите на настоящия регламент се прилагат следните определения:

- 1) „данни“ означава данни, различни от личните данни, определени в член 4, точка 1 от Регламент (ЕС) 2016/679;
- 2) „обработване“ означава всяка операция или съвкупност от операции, извършвани с данни или набор от данни в електронен формат чрез автоматични или неавтоматични средства, като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, привеждане в съответствие или комбиниране, ограничаване, изтриване или унищожаване;

- 3) „проект на акт“ означава текст, изготвен с цел да бъде въведен като законова, подзаконова или административна разпоредба от общ характер, като текстът е на етап от подготовката, в който все още могат да бъдат правени съществени изменения;
- 4) „доставчик на услуги“ означава всяко физическо или юридическо лице, което предоставя услуги за обработване на данни;
- 5) „изисквания за локализиране на данни“ означава 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;
- 6) „компетентен орган“ означава орган на дадена държава членка или всеки друг субект, оправомощен от националното право да изпълнява публична функция или да упражнява официална власт, който е оправомощен да получава достъп до данните, обработвани от физическо или юридическо лице, за изпълнението на служебните си задължения, както е предвидено в правото на Съюза или в националното право;
- 7) „ползвател“ означава всяко физическо или юридическо лице, включително публичен орган или публичноправна организация, което използва или изисква услуги за обработване на данни;
- 8) „професионален ползвател“ означава всяко физическо или 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.

Член 4

Свободно движение на данни в Съюза

1. Забраняват се изискванията за локализиране на данни, освен ако те са оправдани от съображения за обществена сигурност в съответствие с принципа на пропорционалност.

Първа алинея от настоящия параграф не засяга параграф 3 и изискванията за локализиране на данни, предвидени въз основа на действащото право на Съюза.

2. Държавите членки незабавно съобщават на Комисията за всеки проект на акт, който въвежда ново изискване за локализиране на данни или променя вече съществуващо такова изискване съгласно процедурите, определени в членове 5, 6 и 7 от Директива (ЕС) 2015/1535.
3. В срок до ...[24 месеца от датата на прилагане на настоящия регламент] държавите членки гарантират, че всяко съществуващо изискване за локализиране на данни, което е предвидено в закони, подзаконови или административни разпоредби от общ характер и което не съответства на параграф 1 от настоящия член, е отменено.

В срок до ...[24 месеца от датата на прилагане на настоящия регламент], ако дадена държава членка счита, че определена съществуваща мярка, съдържаща изискване за локализиране на данни, съответства на параграф 1 от настоящия член и следователно може да остане в сила, тя съобщава на Комисията тази мярка, като представя и обосновка за оставането ѝ в сила. Без да се засягат разпоредбите на член 258 от ДФЕС, Комисията, в срок от шест месеца от датата на получаване на такова съобщение, разглежда съответствието на тази мярка с параграф 1 от настоящия член и по целесъобразност отправя коментари към съответната държава членка, включително, когато е необходимо, препоръчва изменението или отмяната на мярката.

4. Държавите членки публикуват подробна информация за всички изисквания за локализиране на данни, предвидени в закони, подзаконови или административни разпоредби от общ характер и приложими на тяхната територия, посредством национална единна информационна точка онлайн, която редовно се актуализира, или предоставят подробна актуализирана информация относно всякакви изисквания за локализиране на данни на централна информационна точка, създадена съгласно друг акт на Съюза.
5. Държавите членки информират Комисията за адреса на своята единна информационна точка, посочена в параграф 4. Комисията публикува хипервръзката(ите) към тази/тези информационна(ни) точка(и) на своя уебсайт заедно с редовно актуализиран консолидиран списък на всички изисквания за локализиране на данни, посочени в параграф 4, включително обобщена информация относно тези изисквания.

Член 5

Достъп до данни за компетентните органи

1. Настоящият регламент не засяга правомощията на компетентните органи да изискват или да получават достъп до данни за изпълнението на служебните си задължения в съответствие с правото на Съюза или националното право. На компетентните органи не може да бъде отказан достъп до данни на основание, че тези данни се обработват в друга държава членка.
2. Когато даден компетентен орган, след поискване на достъп до данни на даден ползвател, не получи достъп и ако не съществува конкретен механизъм за сътрудничество съгласно правото на Съюза или международни споразумения за обмен на данни между компетентните органи на различните държави членки, този компетентен орган може да поиска съдействие от компетентния орган на държава членка в съответствие с процедурата, определена в член 7.
3. Когато искането за съдействие предполага получаване на достъп до всички помещения на физическо или юридическо лице, включително всякакво оборудване и всякакви средства за обработване на данни от страна на запитания орган, този достъп се осъществява в съответствие с правото на Съюза или националното процесуално право.
4. Държавите членки могат да налагат ефективни, пропорционални и възпиращи санкции за неизпълнение на задължение за предоставяне на данни в съответствие с правото на Съюза и националното право.

В случай на злоупотреба с права от страна на ползвател, съответната държава членка може, когато това е оправдано от неотложността на достъпа до данните и като се вземат предвид интересите на засегнатите страни, да наложи стриктно пропорционални временни мерки на този ползвател. Ако дадена временна мярка налага повторно локализиране на данните за срок, по-дълъг от 180 дни след повторното им локализиране, тя се съобщава на Комисията в рамките на този 180-дневен срок. Комисията във възможно най-кратък срок разглежда мярката и нейната съвместимост с правото на Съюза и предприема по целесъобразност необходимите мерки. Комисията обменя информация относно опита си в това отношение с единните звена за контакт на държавите членки, посочени в член 7.

Член 6

Пренасяне на данни

1. Комисията насърчава и улеснява разработването на кодекси за поведение на равнището на Съюза с цел саморегулиране („кодекси за поведение“), за да допринесе за конкурентоспособността на основаната на данни икономика, въз основа на принципите за прозрачност и за оперативна съвместимост и като взема предвид отворените стандарти, обхващащи, *inter alia*, следните аспекти:
 - а) най-добрите практики при улесняването на смяната на доставчици на услуги и пренасянето на данни в структуриран, широко използван и машинночетим формат, включително формати на отворени стандарти, когато такива се изискват или бъдат поискани от доставчика на услуги, който получава данните;

- б) минималните изисквания за информация с цел да се гарантира, че професионалните ползватели, преди сключването на договор за обработване на данни, разполагат с достатъчно подробна, ясна и прозрачна информация относно процесите, техническите изисквания, сроковете и таксите, които се прилагат, в случай че професионален ползвател иска да премине към друг доставчик на услуги или да прехвърли данни обратно в собствените си информационни системи;
 - в) подходи към схеми за сертифициране, улесняващи сравнението на продукти и услуги за обработване на данни за професионални ползватели, като се вземат предвид установените национални или международни норми и като се улеснява съпоставимостта на тези продукти и услуги. Такива подходи могат да включват, *inter alia*, управление на качеството, управление на информационната сигурност, управление на непрекъснатостта на дейността и управление на околната среда;
 - г) комуникационни пътни карти, в които се използва мултидисциплинарен подход за повишаване на осведомеността относно кодексите за поведение сред съответните заинтересовани страни.
2. Комисията гарантира, че кодексите за поведение са разработени в тясно сътрудничество с всички съответни заинтересовани страни, включително сдружения на МСП и стартиращи предприятия, ползватели и доставчици на облачни услуги.
3. Комисията насърчава доставчиците на услуги да приключат разработването на кодексите за поведение в срок до ... [12 месеца от датата на публикуване на настоящия регламент] и да ги приложат ефективно в срок до ... [18 месеца от датата на публикуване на настоящия регламент].

Член 7

Процедура за сътрудничество между органите

1. Всяка държава членка определя единно звено за контакт, което поддържа връзка с единните звена за контакт на другите държави членки и с Комисията по въпросите на прилагането на настоящия регламент. Държавите членки уведомяват Комисията за определените единни звена за контакт и за всякакви последващи промени в тях.
2. Когато компетентен орган в дадена държава членка поиска съдействие от друга държава членка съгласно член 5, параграф 2, за да получи достъп до данни, той внася надлежно обосновано искане до определеното единно звено за контакт на тази държава членка. Искането включва писмено обяснение на причините и на правните основания за искане на достъп до данните.
3. Единното звено за контакт определя съответния компетентен орган в своята държава членка и му предава полученото искане съгласно параграф 2.
4. Без ненужно забавяне и в рамките на сроковете, пропорционални на спешността на искането, съответният компетентен орган, от който е поискано съдействие представя отговор, в който съобщава за исканите данни или информира отпращаващото искането компетентен орган, че не счита, че условията за искане на съдействие съгласно настоящия регламент са изпълнени.

5. Всяка информация, обменена в контекста на поисканото и предоставеното съдействие по член 5, параграф 2, се използва единствено по отношение на въпросите, за които е поискана.
6. Единните звена за контакт предоставят на ползвателите обща информация относно настоящия регламент, включително относно кодексите на поведение.

Член 8

Оценка и насоки

1. Не по-късно от ... [48 месеца от датата на публикуване на настоящия регламент] Комисията представя доклад на Европейския парламент, на Съвета и на Европейския икономически и социален комитет, в който се съдържа оценка на прилагането на настоящия регламент, в частност по отношение на:
 - а) прилагането на настоящия регламент, особено по отношение на набори от данни, съставени както от лични, така и от нелични данни, в контекста на пазарното и технологичното развитие, което може да разшири възможностите за деанонимизиране на данните;
 - б) прилагането от страна на държавите членки на член 4, параграф 1, и по-специално на изключението, свързано с обществената сигурност; както и
 - в) разработването и ефективното прилагане на кодексите за поведение и ефективното предоставяне на информация от страна на доставчиците на услуги.
2. Държавите членки предоставят на Комисията информацията, която е необходима за изготвянето на посочения в параграф 1 доклад.

3. В срок до ... [6 месеца от датата на публикуване на настоящия регламент] Комисията публикува информативни насоки относно взаимодействието на настоящия регламент и Регламент (ЕС) 2016/679, особено по отношение на наборите от данни, съставени както от лични, така и от нелични данни.

Член 9

Заключителни разпоредби

Настоящият регламент влиза в сила на двадесетия ден след публикуването му в *Официален вестник на Европейския съюз*.

Настоящият регламент започва да се прилага шест месеца след публикуването му.

Настоящият регламент е задължителен в своята цялост и се прилага пряко във всички държави членки.

Съставено в Страсбург на

За Европейския парламент
Председател

За Съвета
Председател