2025/847

7.5.2025 г.

РЕГЛАМЕНТ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2025/847 НА КОМИСИЯТА

от 6 май 2025 година

за определяне на правила за прилагането на Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета по отношение на реакциите на пробиви в сигурността на европейските портфейли за цифрова самоличност

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 г. относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО ([1]), и по-специално член 5е параграф 5 от него,

като има предвид, че:

(1) Европейската рамка за цифрова самоличност, („рамката“) създадена с Регламент (ЕС) № 910/2014, е ключов компонент в изграждането на сигурна и оперативно съвместима екосистема на цифровата самоличност в Съюза. Тъй като европейските портфейли за цифрова самоличност („портфейли“) са крайъгълният камък на рамката, нейната цел е да се улесни достъпът до услуги в държавите членки, като същевременно се гарантира защитата на личните данни и неприкосновеността на личния живот.

(2) Регламенти (ЕС) 2016/679 ([2]) и (ЕС) 2018/1725 на Европейския парламент и на Съвета ([3]) и, когато е целесъобразно, Директива 2002/58/ЕО на Европейския парламент и на Съвета ([4]) се прилагат по отношение на дейностите по обработване на лични данни съгласно настоящия регламент. Правилата за оценка и предоставяне на информация, установени съгласно настоящия регламент, не засягат задължението за уведомяване на компетентния надзорен орган за нарушения на сигурността на личните данни, когато това е приложимо съгласно Регламент (ЕС) 2016/679 или Регламент (ЕС) 2018/1725, и задължението за уведомяване на субектите на данни за пробиви в сигурността на личните данни, когато това е приложимо съгласно тези регламенти.

(3) Комисията редовно оценява нови технологии, практики, стандарти и технически спецификации. С цел да се осигури най-високо равнище на хармонизация между държавите членки за разработването и сертифицирането на портфейлите, определените в настоящия регламент технически спецификации се основават на работата, извършена въз основа на Препоръка (ЕС) 2021/946 на Комисията ([5]), и по-специално рамката за техническа архитектура и технически справки, която е част от него. В съответствие със съображение 75 от Регламент (ЕС) 2024/1183 на Европейския парламент и на Съвета ([6]), Комисията следва да преразглежда и при необходимост да актуализира настоящия регламент, за да го поддържа в съответствие с глобалното развитие и с рамката за техническа архитектура и технически справки, и да следва най-добрите практики на вътрешния пазар.

([1]) ОВ L 257, 28.8.2014 г., стр. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([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, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([3]) 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 отмяна на Регламент (ЕО) № 45/2001 и Решение № 1247/2002/ЕО (ОВ L 295, 21.11.2018 г., стр. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([4]) 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, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([5]) Препоръка (ЕС) 2021/946 на Комисията от 3 юни 2021 г. относно общ инструментариум на Съюза за координиран подход към европейска рамка за цифрова самоличност (ОВ L 210, 14.6.2021 г., стр. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj).

([6]) Регламент (ЕС) 2024/1183 на Европейския парламент и на Съвета от 11 април 2024 г. за изменение на Регламент (ЕС) № 910/2014 по отношение на създаването на европейска рамка за цифрова самоличност (ОВ L, 2024/1183, 30.4.2024 г., ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(4) В случай на пробив или застрашаване на сигурността на решенията за портфейл или на механизмите за валидиране, посочени в член 5а, параграф 8 от Регламент (ЕС) № 910/2014, или на схемата за електронна идентификация, съгласно която се предоставят технологични решения за портфейл, реакциите на такива пробиви и застрашаване на сигурността трябва да са бързи и да протичат координирано и сигурно във всички държави членки, за да се защитят ползвателите и да се запази доверието в екосистемата на цифровата самоличност. Това не засяга Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета ([7]), регламенти (ЕС) 2019/88 ([8]) и (ЕС) 2024/2847 на Европейския парламент и на Съвета ([9]), по-специално по отношение на действията при инциденти или уязвимости и възприемането им като пробиви на сигурността. Поради това държавите членки следва да гарантират, че своевременно се спира предоставянето и използването на портфейли, засегнати от пробив или застрашаване на сигурността, или, когато е целесъобразно, тяхното оттегляне.

(5) За да се гарантира подходящ отговор при пробив или застрашаване на сигурността, държавите членки следва да преценят дали пробивът или застрашаването на сигурността на технологично решение за портфейл, на механизмите за валидиране, посочени в член 5а, параграф 8 от Регламент (ЕС) № 910/2014, или на схемата за електронна идентификация, съгласно която се предоставя технологично решение за портфейл, засяга надеждността на въпросното технологично решение за портфейл или на други технологични решения за портфейл. Тази преценка следва да се основава на единни критерии, като например броя и категорията на ползвателите на портфейли, на физическите лица и на засегнатите доверяващи се на портфейл страни, естеството на засегнатите данни, продължителността на застрашаването или пробива на сигурността, ограничената разполагаемост на дадена услуга и финансовите загуби, както и потенциалното застрашаване на лични данни. Тези критерии следва да предоставят на държавите членки гъвкавост и свобода да установяват по съразмерен начин дали е засегната надеждността на технологичното решение за портфейл и дали е целесъобразно временното спиране или, в случай че сериозността на пробива или застрашаването оправдават това — оттеглянето на технологичното решение за портфейл. Въпросните критерии не следва да водят до автоматично оттегляне на технологично решение за портфейл или до автоматично временно спиране на предоставянето и използването на технологично решение за портфейл, но те следва да бъдат надлежно взети предвид от държавите членки, когато решават дали е необходимо оттегляне или временно спиране на предоставянето и използването на технологично решение за портфейл.

(6) Поради въздействията и неудобствата, до които води временното спиране на използването на решения за портфейл, държавите членки ще трябва да преценят дали отмяната на удостоверенията за портфейлен блок или всякакви други допълнителни мерки са необходими като адекватен отговор на пробива или застрашаването на сигурността.

(7) За да информират ползвателите на портфейли за състоянието на техните портфейли, те трябва да ги уведомяват адекватно за пробиви или застрашаване на сигурността, засягащи техните портфейли. Тъй като регистрирани в Съюза доверяващи се на портфейл страни също могат да бъдат засегнати от пробиви на сигурността и застрашаване на сигурността, съответната информация за пробиви и застрашаване също трябва да бъде споделена с тях.

(8) За да се подобри прозрачността и да се изгради доверие в екосистемата на цифровата самоличност, информацията за пробив или застрашаване на сигурността, както и за последиците от това, следва най-малкото да включват информацията, изисквана съгласно настоящия регламент. Информацията относно пробиви или застрашаване на сигурността, споделяна с ползватели на портфейли и доверяващи се на портфейл страни, следва обаче да бъде внимателно прегледана, така че да се предотврати или ограничи рискът от това нападатели да се възползват от пробива или застрашаването.

([7]) Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 г. относно мерки за високо общо ниво на киберсигурност в Съюза, за изменение на Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148 (Директива за МИС 2) (ОВ L 333, 27.12.2022 г., стр. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

([8]) Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета от 17 април 2019 г. относно ENISA (Агенцията на Европейския съюз за киберсигурност) и сертифицирането на киберсигурността на информационните и комуникационните технологии, както и за отмяна на Регламент (ЕС) № 526/2013 (Акт за киберсигурността) (ОВ L 151, 7.6.2019 г., стр. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

([9]) Регламент (ЕС) 2024/2847 на Европейския парламент и на Съвета от 23 октомври 2024 г. относно хоризонтални изисквания за киберсигурност за продукти с цифрови елементи и за изменение на регламенти (ЕС) № 168/2013 и (ЕС) 2019/1020 и Директива (ЕС) 2020/1828 (Акт за киберустойчивост) (ОВ L, 2024/2847, 20.11.2024 г., ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

(9) За да се даде възможност на потребителите отново да имат достъп до своите портфейлни блокове след отстраняване на пробив или застрашаване на сигурността, държавата членка, която е предоставила технологичните решения за портфейл, ще трябва да възобнови предоставянето и използването на тези решения за портфейл без ненужно забавяне. Това може да се направи чрез възобновяване на портфейлните блокове, чрез издаване на портфейлни блокове, предоставени в рамките на нова версия на технологичните решения за портфейл, или чрез повторно издаване на нови валидни удостоверения за портфейлен блок. Засегнатите ползватели на портфейли, доверяващите се на портфейл страни, единните звена за контакт, посочени в съответствие с член 46в, параграф 1 от Регламент (ЕС) № 910/2014, и Комисията следва да бъдат съответно информирани.

(10) За да се гарантира оттеглянето на портфейлите, когато пробив или застрашаване на сигурността не е отстранено в срок от три месеца от временното спиране или когато това се налага поради сериозността на пробива или застрашаването на сигурността, държавата членка следва да гарантира отмяната на съответните удостоверения за портфейлен блок и че тяхната валидност не може да се възстанови, нито да бъдат издадени или предоставени на съществуващи портфейлни блокове. Освен това не следва да се предоставят нови портфейлни блокове в рамките на засегнатото технологично решение за портфейл. От съображения за прозрачност ползвателите, доверяващите се на портфейл страни, единните звена за контакт, посочени в съответствие с член 46в, параграф 1 от Регламент (ЕС) № 910/2014, и Комисията е необходимо да бъдат информирани за оттеглянето. Това включва описание на потенциалните отражения върху ползвателите на портфейла, и по-специално върху управлението на издадените удостоверения, или върху доверяващите се на портфейл страни.

(11) Периодът от три месеца след временното спиране на предоставянето и използването на технологичното решение за портфейл, по време на който трябва да се отстрани пробивът или застрашаването на сигурността, довели до това временно спиране, следва да осигурява срок, след който технологичното решение за портфейл трябва да бъде оттеглено, освен ако не е приложено подходящо решение за отстраняването на проблема. Държавите членки обаче са свободни да изискат пробивът или застрашаването на сигурността да бъдат отстранени в срок, по-кратък от три месеца, като се вземат предвид по-специално и когато е уместно, степента, продължителността и последиците от този пробив или застрашаване на сигурността. Когато пробивът или застрашаването на сигурността не бъдат или не може да бъдат отстранени в рамките на срока, определен от държавата членка, тя може да изиска технологичното решение за портфейл да бъде оттеглено преди изтичането на тримесечния срок. Държавите членки следва да използват срока, през който трябва да бъде отстранен пробивът или застрашаването на сигурността, довели до временното спиране на предоставянето и използването на решение за портфейл, за подготвяне на потенциалното оттегляне на това решение за портфейл и на свързаните с това съобщения.

(12) За да се намали административната тежест за държавите членки по отношение на информацията, която трябва да се изпраща в съответствие с настоящия регламент до Комисията и до други държави членки, държавите членки следва да използват съществуващите инструменти за уведомяване, като например системата за докладване и анализ на киберинциденти (CIRAS), управлявана от Агенцията на Европейския съюз за киберсигурност (ENISA). Ако се използват алтернативни канали или средства за уведомяване на ползвателите на портфейли, засегнати от пробив или застрашаване на сигурността, и на доверяващите се на портфейл страни, държавите членки следва да гарантират, че съответната информация се предоставя по ясен, изчерпателен и лесно достъпен начин. Каналите за предоставяне на такава информация на засегнатите ползватели на портфейл и доверяващите се на портфейл страни следва да включват подходящи решения за уеб-базирано предаване, проследяване в реално време на актуализациите на уебсайта и групиране на новини.

(13) Европейският надзорен орган по защита на данните беше консултиран в съответствие с член 42, параграф 1 от Регламент (ЕС) 2018/1725 и прие своето становище на 31 януари 2025 г.

(14) Мерките, предвидени в настоящия регламент, са в съответствие със становището на комитета, създаден съгласно член 48 от Регламент (ЕС) № 910/2014,

ПРИЕ НАСТОЯЩИЯ РЕГЛАМЕНТ:

Член 1

Предмет

С настоящия регламент се определят правила за отговор при пробив на сигурността на портфейлите, на механизмите за валидиране, посочени в член 5а, параграф 8 от Регламент (ЕС) № 910/2014, и на схемата за електронна идентификация, съгласно която се предоставят портфейлите.

Член 2

Определения

За целите на настоящия регламент се прилагат следните определения:

1) „технологично решение за портфейл“ означава съчетание от софтуер, хардуер, услуги, настройки и конфигурации, включително инстанции на портфейла, едно или повече защитени криптографски приложения на портфейла и едно или повече защитени криптографски устройства на портфейла;

2) „ползвател на портфейла“ означава ползвател, който управлява портфейлния блок;

3) „доверяваща се на портфейла страна“ означава доверяваща се страна, която възнамерява да разчита на портфейлни блокове за предоставянето на публични или частни услуги чрез цифрово взаимодействие;

4) „инстанция на портфейла“ означава приложението, инсталирано и конфигурирано на устройството или средата на ползвателя на портфейла, което е част от портфейлния блок и което ползвателят на портфейла използва за взаимодействие с портфейлния блок;

5) „защитено криптографско приложение на портфейла“ означава приложение, с което се управляват стратегически активи чрез свързване с и използване на криптографските и некриптографските функции, предоставяни от защитеното криптографско устройство на портфейла;

6) „защитено криптографско устройство на портфейла“ означава устойчиво на опити за подправяне устройство, осигуряващо среда, която е свързана с и използвана от защитеното криптографско приложение на портфейла за защита на стратегически активи и предоставяне на криптографски функции за сигурно изпълнение на операции от критично значение;

7) „доставчик на портфейл“ означава физическо или юридическо лице, което предоставя технологични решения за портфейла;

8) „портфейлен блок“ означава уникална конфигурация за технологично решение за портфейл, включваща инстанции на портфейла, защитени криптографски приложения на портфейла и защитени криптографски устройства на портфейла, предоставени от доставчик на портфейла на индивидуален ползвател на портфейла;

9) „стратегически активи“ означава активи в рамките на или във връзка с портфейлен блок от такова изключително значение, че тяхното извеждане от строя или унищожаване би имало много сериозен, отслабващ ефект върху способността да се разчита на портфейлния блок;

10) „удостоверение за портфейлен блок“ означава обект на данни, който описва компонентите на портфейла или позволява удостоверяване на автентичността и валидиране на тези компоненти.

Член 3

Установяване на пробив или застрашаване на сигурността

1. Без да се засягат разпоредбите на Директива (ЕС) 2022/2555 и регламенти (ЕС) 2019/881 и (ЕС) 2024/2847, държавите членки вземат надлежно предвид критериите, посочени в приложение I към настоящия регламент, за да преценят дали пробив на сигурността или застрашаване на технологично решение за портфейл, на механизмите за валидиране, посочени в член 5а, параграф 8 от Регламент (ЕС) № 910/2014, или на схемата за електронна идентификация, съгласно която се предоставя технологичното решение за портфейл, засяга тяхната надеждност или надеждността на други технологични решения за портфейл.

2. Когато въз основа на преценката, предвидена в параграф 1, държава членка установи, че пробив или застрашаване на сигурността засяга надеждността на технологичното решение за портфейл, и временно спре предоставянето и използването на това технологичното решение за портфейл, тази държава членка предприема мерките, посочени в членове 4 и 5. Когато държава членка оттегля технологичното решение за портфейл, тя предприема мерките, предвидени в членове 8 и 9.

3. Когато държава членка узнае информация за възможен пробив или застрашаване на сигурността, което може да засегне надеждността на едно или повече технологични решения за портфейл, предоставяни от друга държава членка, тази държава членка без ненужно забавяне съобщава това на Комисията и единните звена за контакт на засегнатите държави членки, определени съгласно член 46в, параграф 1 от Регламент (ЕС) № 910/2014. Съобщението включва информацията, посочена в член 5, параграф 2.

4. Държавата членка, която получава информация, предоставена по параграф 3, предприема без ненужно забавяне мерките, посочени в параграфи 1 и 2.

Член 4

Временно спиране на предоставянето и използването на портфейли и други корективни мерки

1. Държавите членки гарантират, че не се предоставят, използват или активират портфейлни блокове в рамките на временно спряно технологично решение за портфейл.

2. Държавите членки преценяват дали е необходимо да се отменят удостоверения за портфейлен блок за портфейлните блокове, засегнати от временното спиране на дадено технологично решение за портфейл, или е нужна някоя друга допълнителна корективна мярка, като адекватен отговор на пробива или застрашаването на сигурността.

3. Мерките, посочени в параграфи 1 и 2, се предприемат без ненужно забавяне и във всеки случай не по-късно от 24 часа след временното спиране на предоставянето и използването на технологичното решение за портфейл, обект на пробив или застрашаване на сигурността.

4. Мерките, посочени в параграфи 1 и 2, не засягат възможността засегнатите ползватели на портфейл да упражняват своето право на преносимост на данните, посочено в член 5а, параграф 4, буква ж) от Регламент (ЕС) № 910/2014. Това е така, при условие че това право може да бъде упражнено от ползвателите на портфейла, без да се накърнява сигурността на стратегическите активи на засегнатите портфейлни блокове, по-специално като се имат предвид причините за временното спиране и необходимостта да се гарантира ефективната защита на тези активи срещу злоупотреби.

Член 5

Информация за временни спирания и корективни мерки

1. Без ненужно забавяне и не по-късно от 24 часа след временното спиране на предоставянето и използването на технологичното решение за портфейл се предоставя ясна, изчерпателна и лесно достъпна информация за временното спиране на предоставянето и използването на въпросното решение. Тя се изпраща до:

а) единните точки за контакт, определени съгласно член 46в, параграф 1 от Регламент (ЕС) № 910/2014;

б) Комисията;

в) засегнатите ползватели на портфейли;

г) засегнатите доверяващи се на портфейла страни, регистрирани в съответствие с член 5б от Регламент (ЕС) № 910/2014.

2. Информацията, предоставена в съответствие с параграф 1, включва най-малко следното:

а) името на доставчика на технологичното решение за портфейл, чието предоставяне и използване е било временно спряно;

б) името и референтния идентификатор на това технологично решение за портфейл, както е посочено в списъка на сертифицираните портфейли, изготвен съгласно член 5г от Регламент (ЕС) № 910/2014, и, когато е приложимо, съответните версии;

в) датата и часа на установяване на пробива или застрашаването на сигурността;

г) ако са известни, датата и часа на пробива или застрашаването на сигурността въз основа на мрежови или системни регистри или други източници на данни;

д) датата и часа на временното спиране на технологичното решение за портфейл;

е) данните за контакт, включително най-малкото адрес на електронна поща и телефонен номер за уведомяващата държава членка и, когато са различни — данните за доставчика на портфейл, посочен в буква а);

ж) описание на пробива или застрашаването на сигурността;

з) описание на застрашените данни, включително, когато е приложимо, категориите лични данни, определени в член 9, параграф 1 и член 10 от Регламент (ЕС) 2016/679;

и) когато е възможно, приблизителен брой засегнати ползватели на портфейли и други засегнати физически лица;

й) описание на потенциалните въздействия върху доверяващите се на портфейл страни или върху ползвателите на портфейл, и във втория случай, когато е приложимо, всякакви указания за мерките, които ползвателите на портфейл могат да предприемат, за да смекчат тези потенциални въздействия;

к) описание на предприетите или планираните мерки за отстраняване на пробива или застрашаването на сигурността, заедно с план и краен срок за това отстраняване;

л) когато е приложимо и целесъобразно, описание на предприетите или планираните мерки за преминаване на засегнатите ползватели на портфейли към алтернативни технологични решения или услуги за портфейл.

Член 6

Възобновяване на предоставянето и използването на портфейлите

Когато е необходимо, за да се гарантира възобновяването на предоставянето, активирането и използването на технологично решение за портфейл, държавите членки без ненужно забавяне:

1) възобновяват предоставянето и използването на портфейлните блокове, предоставяни в рамките на това технологично решение за портфейл, като издават портфейлен блок, предоставен в рамките на нова версия на технологичното решение за портфейл, на всички засегнати потребители;

2) издават нови удостоверения за портфейлни блокове за нови портфейлни блокове или, когато е приложимо, за предходно издадени портфейлни блокове, при условие че тези портфейлни блокове отговарят на изискванията за сигурност, въведени след отстраняването на пробива или застрашаването на сигурността;

3) отменят всяка мярка, приложена съгласно член 4 и възпрепятстваща предоставянето на нови портфейлни блокове в рамките на засегнатото технологично решение за портфейл, когато тази мярка е свързана единствено с вече отстранения пробив или застрашаване на сигурността.

Член 7

Информация за възобновяването

Когато държава членка възобновява технологично решение за портфейл, тя гарантира, че:

1) информацията за това се предоставя без ненужно забавяне на всички страни, които са получили информация относно временното спиране на предоставянето и използването на въпросното технологично решение за портфейл в съответствие с член 5, параграф 1.

2) Информацията, изпратена съгласно точка 1, включва най-малко елементите, посочени в член 5, параграф 2, букви а), б) и е)—з), както и следното:

   а) датата и часа на отстраняване на пробива или застрашаването на сигурността;

   б) датата и часа на възобновяването на засегнатото технологично решение за портфейл и, когато е целесъобразно, на засегнатите портфейлни блокове, предоставяни в рамките на този портфейл;

   в) описание на мерките, които са били предприети за отстраняване на пробива или застрашаването на сигурността;

   г) описание на потенциалните остатъчни въздействия върху доверяващите се на портфейл страни или върху ползвателите на портфейл, и във втория случай, когато е приложимо, всякакви указания за мерките, които ползвателите на портфейл могат да предприемат, за да смекчат тези потенциални остатъчни въздействия;

Член 8

Оттегляне на портфейли

1. Когато пробив или застрашаване на сигурността, чието следствие е било временно спиране на предоставянето и използването на решение за портфейл, не се отстрани в срок от три месеца след датата на временното спиране на предоставянето и използването на това технологично решение за портфейл, държавата членка, която предоставя решението, гарантира, че засегнатото технологично решение за портфейл е оттеглено и валидността му е отменена без ненужно забавяне и при всички случаи в рамките на 72 часа след изтичането на тримесечния срок.

2. Когато държава членка оттегли технологично решение за портфейл, тя гарантира, че:

а) удостоверенията за портфейлен блок на портфейлния блок на засегнатото технологично решение за портфейл се отменят;

б) удостоверенията за портфейлен блок не могат да се върнат към състояние на валидност;

в) не може да се издаде удостоверение за нов портфейлен блок на съществуващи портфейлни блокове, предоставени в рамките на засегнатото технологично решение за портфейл;

г) не може да се предостави нов портфейлен блок в рамките на засегнатото технологично решение за портфейл.

3. Мерките, посочени в параграфи 1 и 2, не засягат възможността засегнатите ползватели на портфейл да упражняват своето право на преносимост на данните, посочено в член 5а, параграф 4, буква ж) от Регламент (ЕС) № 910/2014. Това е при условие че това право може да бъде упражнено от ползвателите на портфейла, без да се накърнява сигурността на стратегическите активи на засегнатите портфейлни блокове, по-специално като се имат предвид причините за оттеглянето и необходимостта да се гарантира ефективната защита на тези активи срещу злоупотреби.

Член 9

Информация за оттеглянето

1. Без ненужно забавяне и не по-късно от 24 часа след оттеглянето на технологичното решение за портфейл се предоставя ясна, изчерпателна и лесно достъпна информация за оттеглянето на въпросното решение. Тя се изпраща до:

а) единните точки за контакт, определени съгласно член 46в, параграф 1 от Регламент (ЕС) № 910/2014;

б) Комисията;

в) засегнатите ползватели на портфейли;

г) засегнатите доверяващи се на портфейла страни, регистрирани в съответствие с член 5б от Регламент (ЕС) № 910/2014.

2. Информацията, предоставена в съответствие с параграф 1, включва най-малко следното:

а) името на доставчика на технологичното решение за портфейл, което е било оттеглено;

б) името и референтния идентификатор на това технологично решение за портфейл, както е посочено в списъка на сертифицираните портфейли, изготвен съгласно член 5г от Регламент (ЕС) № 910/2014, и, когато е приложимо, съответните версии;

в) датата и часа на откриване на пробива или застрашаването на сигурността, довели до оттеглянето на засегнатото технологично решение за портфейл поради неговата сериозност или защото не е било отстранено в рамките на три месеца;

г) ако са известни, датата и часа на пробива или застрашаването на сигурността въз основа на мрежови или системни регистри или други източници на данни;

д) датата и часа на оттегляне на технологичното решение за портфейл и на ефективната отмяна на удостоверенията за портфейлни блокове на портфейлните блокове, предоставени в рамките на технологичното решение за портфейл;

е) дали оттеглянето е резултат от сериозността на пробива или застрашаването на сигурността или е следствие от неотстраняване на пробива или застрашаването на сигурността;

ж) данните за контакт, включително най-малкото адрес на електронна поща и телефонен номер за уведомяващата държава членка и, когато са различни — данните за доставчика на портфейл, посочен в буква (а);

з) описание на пробива или застрашаването на сигурността;

и) описание на застрашените данни, включително, когато е приложимо, категориите лични данни, определени в член 9, параграф 1 и член 10 от Регламент (ЕС) 2016/679;

й) когато е възможно, приблизителен брой засегнати ползватели на портфейли и други засегнати физически лица;

к) описание на потенциалните въздействия върху доверяващите се на портфейл страни или върху ползвателите на портфейл, и във втория случай, когато е приложимо, всякакви указания за мерките, които ползвателите на портфейл могат да предприемат, за да смекчат тези потенциални въздействия;

л) описание на предприетите или планираните мерки за преминаване на засегнатите ползватели на портфейли към алтернативни технологични решения за портфейл или, когато е приложимо и целесъобразно, към алтернативни услуги.

Член 10

Информационна система

Държавите членки изпращат информацията, посочена в членове 3, 5, 7 и 9, на Комисията и на единните звена за контакт на държавите членки, определени съгласно член 46в, параграф 1 от Регламент (ЕС) № 910/2014, чрез CIRAS, управлявана от ENISA, или чрез еквивалентна система, договорена между държавите членки и Комисията.

Член 11

Влизане в сила

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

Настоящият регламент е задължителен в своята цялост и се прилага пряко във всички държави членки, с изключение на член 10, който се прилага от 7 май 2026 г.

Съставено в Брюксел на 6 май 2025 година.

За Комисията
Председател
Ursula VON DER LEYEN

ПРИЛОЖЕНИЕ

Критерии за оценка на пробив или застрашаване на сигурността

1. Държавите членки оценяват пробива или застрашаването на сигурността като се опират на следните критерии:

   а) пробивът или застрашаването води или може да доведе до смърт или значително увреждане на здравето на физическо лице;

   б) налице е или може да бъде осъществен успешен, предполагаемо злонамерен или неразрешен достъп до мрежите и информационните системи на доставчик на технологично решение за портфейл, на доставчик на механизмите за валидиране, посочени в член 5а, параграф 8 от Регламент (ЕС) № 910/2014, или на доставчик на схемата за електронна идентификация, съгласно която се предоставя технологично решение за портфейл („засегнати субекти“) по начин, който може сериозно да обърка работата, и тези системи са критични компоненти на засегнатото технологично решение за портфейл, на засегнатите механизми за валидиране, посочени в член 5а, параграф 8 от Регламент (ЕС) № 910/2014, или на засегнатата схема за електронна идентификация, съгласно която се предоставя технологично решение за портфейл;

   в) технологично решение за портфейл, механизъм за валидиране, посочен в член 5а, параграф 8 от Регламент (ЕС) № 910/2014, или схема за електронна идентификация, съгласно която се предоставя решение за портфейл, или част от тях:

      — е напълно или се очаква да бъде напълно недостъпно за ползвателите на портфейла или за доверяващите се на портфейла страни в продължение на повече от 12 последователни часа;

      — е недостъпно или се очаква да бъде недостъпно за ползвателите на портфейла или доверяващите се на портфейла страни за повече от 16 часа, изчислено на база календарна седмица;

   г) предполага се, че ограничената наличност на технологичното решение за портфейл или на услугите, предоставяни от засегнати субекти по отношение на технологичното решение за портфейл, има или се очаква да има отражение върху над 1 % от ползвателите на портфейла или доверяващите се на портфейла страни;

   д) налице е възможност да бъде застрашен или е бил застрашен физическият достъп (ограничен до доверени служители на засегнатите субекти) или защитата на този физически достъп до едно или повече от местоположенията на мрежовите и информационните системи, поддържащи технологичното решение за портфейла, на предоставянето на механизмите за валидиране, посочени в член 5а, параграф 8 от Регламент (ЕС) № 910/2014, свързани с технологично решение за портфейл, или на схемата за електронна идентификация, съгласно която се предоставя технологично решение за портфейл;

   е) неприкосновеността на личния живот, целостта, поверителността или автентичността на данните, съхранявани, предавани или обработвани в технологичното решение за портфейл, са обект на застрашаване или може да бъдат обект на застрашаване, което:

      — има отражение върху над 1 % от ползвателите на портфейла на засегнатото технологично решение за портфейл или върху над 100 000 от ползвателите на портфейла, в зависимост от това кое от двете числа е по-малко;

      — е резултат от успешни, предполагаемо злонамерени действия;

      — е резултат или е вероятно да бъде резултат от една или повече известни уязвимости, включително такива, които са били обект на действия в съответствие с Регламент за изпълнение (ЕС) 2024/2981 на Комисията ([1]);

      — има вероятност да се отрази на личните данни по начин, който може да породи риск за правата и свободите на засегнатите физически лица, и по-специално в случай на пробив в сигурността на личните данни, както е определено в член 9, параграф 1 и член 10 от Регламент (ЕС) 2016/679;

([1]) Регламент за изпълнение (ЕС) 2024/2981 на Комисията от 28 ноември 2024 г. за определяне на правила за прилагането на Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета по отношение на сертифицирането на европейските портфейли за цифрова самоличност (ОВ L, 2024/2981, 4.12.2024 г., ELI: http://data.europa.eu/eli/reg_impl/2024/2981/oj).

— има вероятност да се отрази на личните електронни съобщения;

— има вероятност да изложи на висок риск правата и свободите на физически лица;

— има вероятност да се отрази на уязвими лица.

ж) сертифицирането на технологичното решение за портфейл е отменено или се очаква да бъде отменено;

з) пробивът или застрашаването води или може да доведе до пряка финансова загуба за засегнатия субект от над 500 000 EUR или 5 % от общия му годишен оборот през предходната финансова година, в зависимост от това коя от двете стойности е по-ниска.

2. Държавите членки не вземат предвид планирани последици от дейност по поддръжка, извършени от или от името на засегнатите субекти, при условие че тази дейност по поддръжка:

а) е била предварително заявена на потенциално засегнати ползватели на портфейла или доверяващи се на портфейла страни и съответните компетентни надзорни органи;

б) не отговаря на нито един от критериите, посочени в точка 1 от настоящото приложение.

3. Що се отнася до точка 1, буква (c), продължителността на инцидент, засягащ разполагаемостта, се измерва от момента на прекъсване на правилното предоставяне на засегнатата услуга до момента, в който услугата бъде възстановена и функционира отново. Когато засегнатият субект не е в състояние да определи момента, в който е започнало прекъсването, продължителността на инцидента се измерва от момента, в който инцидентът е бил засечен, или от момента, в който инцидентът е бил вписан в мрежовите или системните регистри или в други източници на данни, в зависимост от това кое от двете събития е настъпило първо. Пълната недостъпност на дадена услуга се измерва от момента, в който услугата е напълно недостъпна за ползвателите, до момента, в който редовните дейности или операции са възстановени до нивото на обслужване, предоставяно преди инцидента. Когато засегнатият субект не е в състояние да определи кога е започнала пълната недостъпност на услугата, недостъпността се измерва от момента, в който тя е била установена от този субект.

4. Що се отнася до параграф 1, буква (d), счита се, че е налице ограничена достъпност на услуга, по-специално когато услугата е значително по-бавна от средното време за отговор или когато не всички функционалности на услугата са достъпни. Когато е възможно, за оценка на закъсненията във времето за отговор се използват обективни критерии, основани на средното време за отговор на услугите.

5. За целите на определянето на преките финансови загуби, произтичащи от пробив или застрашаване съгласно точка 1, буква (h), засегнатите субекти вземат предвид всички финансови загуби, които са понесли в резултат на инцидента, като например разходи за замяна или преместване на софтуер, хардуер или инфраструктура, разходи за персонал, включително разходи, свързани със замяна или преместване на персонал, наемане на допълнителен персонал, възнаграждение за извънреден труд и възстановяване на изгубени или нарушени умения, такси поради неспазване на договорни задължения, разходи за правна защита и обезщетение на клиенти, загуби поради пропуснати приходи, разходи, свързани с вътрешна и външна комуникация, и разходи за консултации, включително разходи, свързани с правни консултации, криминалистични анализи и услуги за възстановяване. Разходите, необходими за ежедневното функциониране на предприятието, като например за обща поддръжка на инфраструктура, оборудване, хардуер и софтуер, подобрения и инициативи за оценка на риска, както и за застрахователни премии, не се считат за финансови загуби в резултат на инцидент. Засегнатите субекти изчисляват размера на финансовите загуби въз основа на наличните данни, а когато действителният размер на тези загуби не може да бъде определен, субектите го изчисляват приблизително.