2024/2982

4.12.2024 г.

РЕГЛАМЕНТ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2024/2982 НА КОМИСИЯТА

от 28 ноември 2024 година

за определяне на правила за прилагането на Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета по отношение на протоколите и интерфейсите, които трябва да се поддържат от европейската рамка 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 5а, параграф 23 от него,

като има предвид, че:

(1) Европейската рамка за цифрова самоличност, 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 за физически и юридически лица, като същевременно се гарантира защитата на личните данни и неприкосновеността на личния живот.

(2) Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета ([2]) и, когато е целесъобразно, Директива 2002/58/ЕО на Европейския парламент и на Съвета ([3]) се прилагат по отношение на всички дейности по обработване на лични данни съгласно посочения регламент.

(3) С член 5а, параграф 23 от Регламент (ЕС) № 910/2014 на Комисията се възлага, когато е необходимо, да установи съответните спецификации и процедури. Това се постига чрез четири регламента за изпълнение, отнасящи се до протоколите и интерфейсите: Регламент за изпълнение (ЕС) 2024/2982 на Комисията ([4]), целостта и основните функции: Регламент за изпълнение (ЕС) 2024/2979 на Комисията ([5]), данните за идентификация на лица и електронното удостоверение за атрибути: Регламент за изпълнение (ЕС) 2024/2977 на Комисията ([6]), както и уведомленията до Комисията: Регламент за изпълнение (ЕС) 2024/2980 на Комисията ([7]). В настоящия регламент се определят съответните изисквания за протоколите и интерфейсите.

([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]) 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.

([4]) Регламент за изпълнение (ЕС) 2024/2982 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 протоколите и интерфейсите, които трябва да се поддържат от европейската рамка за цифрова самоличност (ОВ L, 2024/2982, 4.12.2024 г., ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

([5]) Регламент за изпълнение (ЕС) 2024/2979 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 целостта и основните функции на европейските портфейли за цифрова самоличност (ОВ L, 2024/2979, 4.12.2024 г., ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

([6]) Регламент за изпълнение (ЕС) 2024/2977 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 данните за идентификация на лица и електронните удостоверения за атрибути, издадени за европейските портфейли за цифрова самоличност (ОВ L, 2024/2977, 4.12.2024 г., ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).

([7]) Регламент за изпълнение (ЕС) 2024/2980 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 уведомленията до Комисията относно екосистемата на европейските портфейли за цифрова самоличност (ОВ L, 2024/2980, 4.12.2024 г., ELI: http://data.europa.eu/eli/reg_impl/2024/2980/oj).

(4) Комисията редовно оценява нови технологии, практики, стандарти или 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 от 3 юни 2021 г. относно общ инструментариум на Съюза за координиран подход към европейска рамка за цифрова самоличност ([8]), и по-специално рамката за техническа архитектура и технически справки. В съответствие със съображение 75 от Регламент (ЕС) 2024/1183 на Европейския парламент и на Съвета ([9]) Комисията следва да преразглежда и при необходимост да актуализира настоящия регламент за изпълнение, за да бъде в съответствие с глобалното развитие, рамката за техническа архитектура и технически справки и да следва най-добрите практики на вътрешния пазар.

(5) За да се осигури прозрачност и надеждност за доверяващите се на портфейла страни спрямо ползвателите на портфейла, използваните от технологичните решения за портфейл протоколи и интерфейси следва да предоставят на ползвателите на портфейла надежден механизъм за удостоверяване на автентичността на доверяващи се на портфейла страни и на други портфейлни блокове. От друга страна, доставчиците на портфейли следва да предоставят механизъм за удостоверяване на автентичността и валидиране на портфейлните блокове, така че доверяващите се страни да могат да получат гаранции по отношение на надеждността и автентичността на портфейлните блокове. Освен това техническата инфраструктура на портфейлите също следва да бъде проектирана така, че да се извършва прехвърляне само на минимално необходимото количество данни единствено към оправомощени доверяващи се страни, като същевременно се запазва несвързаността между различните трансакции. С цел да се улесни издаването на данни за идентификация на лица и електронно удостоверение за атрибути, всички технологични решения за портфейл следва да поддържат минимален набор от протоколи и интерфейси.

(6) За да се гарантира използваемостта на технологичните решения за портфейл в държавите членки, всички технологични решения за портфейл следва да поддържат общи технически спецификации, когато данните за идентификация на лица и електронните удостоверения за атрибути се представят чрез портфейлите на доверяващите се страни както от разстояние, така и в близост. Освен това портфейлните блокове може да поддържат други протоколи и интерфейси за конкретни случаи на употреба.

(7) За да се гарантира защита на данните на етапа на проектирането и по подразбиране, портфейлите следва да бъдат снабдени с няколко функции за подобряване на неприкосновеността на личния живот с цел да се предотврати комбинирането от страна на доставчиците на средства за електронна идентификация и електронно удостоверение за атрибути на лични данни, получени при предоставяне на други услуги, с личните данни, обработвани с цел предоставяне на услуги, попадащи в обхвата на Регламент (ЕС) № 910/2014. Както е посочено в Регламент (ЕС) № 910/2014, по време на процеса на регистрация доверяващите се страни не трябва да изискват от ползвателите да предоставят каквито и да било данни, различни от посочените за предвидената употреба на портфейлите. Ползвателите на портфейла следва да имат възможност да проверяват по всяко време данните за регистрация на доверяващите се страни. Освен това портфейлните блокове следва да могат да показват на ползвателите удостоверенията за регистрация на доверяващи се на портфейла страни, когато има такива, като част от искане за атрибут. Това следва да даде възможност на ползвателите на портфейли да проверяват дали атрибутите, изисквани от доверяващата се на портфейла страна, попадат в обхвата на техните регистрирани атрибути, като така се предоставя увереност, че искането е законосъобразно и надеждно.

(8) За да защитят данните на ползвателите на портфейла, доставчиците на портфейли следва да гарантират, че преди портфейлните блокове да предоставят каквито и да било данни, те валидират искания от доверяващите се на портфейла страни или други портфейлни блокове. По същата причина и в съответствие с член 5а, параграф 4, буква г), точка ii) от Регламент (ЕС) № 910/2014, доставчиците на портфейли следва да гарантират, че портфейлните блокове позволяват на ползвателите на портфейла да отправят искания за изтриване на данни до доверяващите се на портфейла страни.

(9) С цел да се предостави възможност за бързи реакции в случай на опасения относно защитата на данните, свързани с член 5а, параграф 4, буква г), подточка iii) от Регламент (ЕС) № 910/2014, доставчиците на портфейли следва да гарантират, че технологичните решения за портфейл предоставят на доверяваща се страна механизми за докладване на компетентния национален орган за защита на данните. На доставчиците на портфейли и на органите за защита на данните следва да се осигури подходяща гъвкавост при установяването на подходящи механизми за взаимодействие с органите за защита на данните на държавите членки.

(10) С Европейския надзорен орган по защита на данните беше проведена консултация в съответствие с член 42, параграф 1 от Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета ([10]) и той прие своето становище на 30 септември 2024 г.

([8]) ОВ L 210, 14.6.2021 г., стр. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj.

([9]) 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.

([10]) 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).

(11) Предвидените в настоящия регламент мерки са в съответствие със становището на Комитета, посочен в член 48 от Регламент (ЕС) № 910/2014,

ПРИЕ НАСТОЯЩИЯ РЕГЛАМЕНТ:

Член 1

Предмет и приложно поле

С настоящия регламент се определят правилата относно протоколите и интерфейсите за технологичните решения за портфейл във връзка с:

1) издаването на данни за идентификация на лица и електронни удостоверения за атрибути на портфейлни блокове;

2) представянето на атрибути за данни за идентификация на лица и електронни удостоверения за атрибути на доверяващи се на портфейла страни и на други портфейлни блокове;

3) съобщаването на искания за изтриване на данни на доверяващи се на портфейла страни;

4) докладването на доверяващи се на портфейла страни пред надзорните органи, създадени съгласно член 51 от Регламент (ЕС) 2016/679.

Настоящият регламент се актуализира редовно, за да бъде в съответствие с развитието на технологиите и стандартите и с работата, извършена въз основа на Препоръка (ЕС) 2021/946 на Комисията, и по-специално рамката за техническа архитектура и технически справки.

Член 2

Определения

За целите на настоящия регламент се прилагат следните определения:

1) „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;

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

3) „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;

4) „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;

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

6) „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;

7) „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;

8) „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;

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 достъп на доверяваща се на портфейла страна“ означава удостоверение за електронни печати или подписи за удостоверяване на автентичността и валидиране на доверяваща се на портфейла страна, издадено от доставчик на удостоверения за достъп на доверяваща се на портфейла страна;

11) „доставчик на удостоверения за достъп на доверяваща се на портфейла страна“ означава физическо или юридическо лице, на което е възложено от държава членка да издава удостоверения за достъп на доверяваща се страна на регистрирани във въпросната държава членка доверяващи се на портфейла страни;

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

13) „включени политики за оповестяване“ означава набор от правила, включени при електронно удостоверение за атрибути от техния доставчик, посочващи условията, които доверяващата се на портфейла страна трябва да изпълни, за да получи достъп до електронното удостоверение за атрибути;

14) „удостоверение за регистрация на доверяваща се на портфейла страна“ означава обект на данни, който показва атрибутите, които доверяващата се страна е регистрирала с оглед на това те да бъдат изисквани от ползвателите;

15) „доставчик на данни за идентификация на лица“ означава физическо или юридическо лице, отговорно за издаването и отмяната на данните за идентификация на лица и гарантирането, че данните за идентификация на лице на ползвателя са свързани криптографски с портфейла;

16) „криптографско обвързване“ означава методът за свързване на данни за идентификация на лица или електронни удостоверения за атрибути с портфейлни блокове чрез криптографски средства.

Член 3

Общи разпоредби

По отношение на посочените в членове 4 и 5 протоколи и интерфейси, доставчиците на портфейли гарантират, че портфейлните блокове:

1) установяват автентичността и валидират удостоверенията за достъп на доверяваща се на портфейла страна, когато си взаимодействат с доверяващите се на портфейла страни;

2) установяват автентичността и валидират удостоверенията за портфейлен блок на други портфейлни блокове, когато си взаимодействат с други портфейлни блокове;

3) установяват автентичността и валидират искания, подадени с помощта на удостоверения за достъп на доверяваща се на портфейла страна или удостоверения за портфейлен блок от други портфейлни блокове, когато това е приложимо;

4) удостоверяват автентичността и валидират удостоверението за регистрация на доверяваща се на портфейла страна, когато е приложимо;

5) показват на ползвателите на портфейла информацията, съдържаща се в удостоверенията за достъп на доверяваща се на портфейла страна или в удостоверенията за портфейлен блок;

6) показват на ползвателите на портфейла, когато това е приложимо, удостоверенията, които ползвателите на портфейла са задължени да представят;

7) показват на ползвателите на портфейла, когато е приложимо, информацията, съдържаща се в удостоверението за регистрация на доверяващата се на портфейла страна;

8) представят удостоверения за портфейлен блок на портфейлния блок на доверяващите се на портфейла страни или на портфейлните блокове, които го изискват;

9) не представят на доверяващите се на портфейла страни или на портфейлните блокове каквито и да било поискани атрибути, докато не бъдат изпълнени следните изисквания:

   а) потвърждение, че защитеното криптографско приложение на портфейла е удостоверило самоличността на ползвателя на портфейла;

   б) потвърждение, че включените политики за разкриване на информация са обработени в рамките на портфейлния блок в съответствие с член 11 от Регламент за изпълнение (ЕС) 2024/2979, когато е приложимо;

   в) проверка дали ползвателите на портфейла частично или изцяло са одобрили представянето;

10) позволяват техники за запазване на поверителността, които гарантират несвързаност, при което електронните удостоверения за атрибути не изискват идентифициране на ползвателя на портфейла, когато представят удостоверения или данни за идентификация на лица между различни доверяващи се на портфейла страни.

Член 4

Издаване на данни за идентификация на лица и електронни удостоверения за атрибути на портфейлни блокове

1. Доставчиците на портфейли гарантират, че технологичните решения за портфейла поддържат протоколи и интерфейси за издаване на данни за идентификация на лица и електронни удостоверения за атрибути на портфейлни блокове.

2. Доставчиците на портфейли гарантират, че портфейлните блокове изискват издаване на данни за идентификация на лица и електронни удостоверения за атрибути само от страни, които имат автентично и валидно удостоверение за достъп на доверяваща се на портфейла страна, удостоверяващо ги като:

а) доставчик на данни за идентификация на лица;

б) доставчик на квалифицирано електронно удостоверение за атрибути;

в) доставчик на електронно удостоверение за атрибути, издадено от орган от публичния сектор, отговарящ за автентичен източник, или от името на такъв орган; или

г) доставчик на неквалифицирано електронно удостоверение за атрибути.

3. Във връзка с издаването на данни за идентификация на лица и електронни удостоверения за атрибути на портфейлния блок, доставчиците на портфейли гарантират, че са спазени следните изисквания:

а) когато ползвателите на портфейл използват своя портфейлен блок, за да поискат издаването на данни за идентификация на лица или електронни удостоверения за атрибути от доставчици на данни за идентификация на лица или доставчици на електронни удостоверения за атрибути, които позволяват издаването на данни за идентификация на лица или електронни удостоверения в повече от един формат, портфейлният блок ги изисква във всички формати, посочени в член 8 от Регламент за изпълнение (ЕС) 2024/2979 на Комисията за определяне на правила за прилагането на Регламент (ЕС) № 910/2014 по отношение на целостта и основните функции на европейските портфейли за цифрова самоличност;

б) когато ползвателите на портфейла използват своя портфейлен блок, за да взаимодействат с доставчици на данни за идентификация на лица или електронни удостоверения за атрибути, портфейлните блокове позволяват удостоверяване на автентичността и валидиране на компонентите на портфейлния блок, като представят на тези доставчици удостоверения за портфейлен блок при поискване от тяхна страна;

в) технологичните решения за портфейла поддържат механизми, които позволяват на доставчиците на данни за идентификация на лица да проверяват издаването, доставката и активирането в съответствие с изискванията за ниво на осигуреност „високо“, определено в Регламент за изпълнение (ЕС) 2015/1502 на Комисията ([11]);

г) портфейлните блокове проверяват автентичността и валидността на данните за идентификация на лица и електронните удостоверения за атрибути.

Член 5

Представяне на атрибути на доверяващи се на портфейла страни

1. Доставчиците на портфейли гарантират, че технологичните решения за портфейл поддържат протоколи и интерфейси за представяне на атрибути на доверяващи се на портфейла страни от разстояние и, когато е подходящо, в близост, в съответствие с посочените в приложението стандарти.

2. Доставчиците на портфейли гарантират, че по искане на ползвателите портфейлните блокове отговарят на успешно удостоверяване на автентичността и валидиране на заявки от доверяващи се на портфейла страни, посочени в член 3, в съответствие с посочените в приложението стандарти.

3. Доставчиците на портфейли гарантират, че портфейлните блокове поддържат доказване на притежанието на частни ключове, съответстващи на публичните ключове, използвани в криптографските обвързвания.

([11]) Регламент за изпълнение (ЕС) 2015/1502 на Комисията от 8 септември 2015 г. за определяне на минимални технически спецификации и процедури за нивата на осигуреност за средствата за електронна идентификация съгласно член 8, параграф 3 от Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар (ОВ L 235, 9.9.2015 г., стр. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

4. Доставчиците на портфейли гарантират, че технологичните решения за портфейл поддържат селективното оповестяване на атрибути на данни за идентификация на лица и електронни удостоверения за атрибути.

5. Параграфи 1—4 се прилагат *mutatis mutandis* за взаимодействията в близост между два портфейлни блока.

Член 6

Съобщаване на искания за изтриване на данни

1. Доставчиците на портфейли гарантират, че портфейлните блокове поддържат протоколи и интерфейси, позволяващи на ползвателите на портфейла да поискат от доверяващите се на портфейла страни, с които са взаимодействали чрез тези портфейлни блокове, да изтрият своите лични данни, предоставени чрез тези портфейлни блокове, в съответствие с член 17 от Регламент (ЕС) 2016/679.

2. Посочените в параграф 1 протоколи и интерфейси позволяват на ползвателите на портфейла да избират доверяващи се на портфейла страни, на които да се изпращат искания за изтриване на данни.

3. Портфейлните блокове ще показват на ползвателя на портфейла подадените преди това искания за изтриване на данни, направени чрез тези портфейлни блокове.

Член 7

Докладване на доверяващи се на портфейла страни пред надзорните органи, създадени съгласно член 51 от Регламент (ЕС) 2016/679

1. Доставчиците на портфейли гарантират, че портфейлните блокове позволяват на ползвателите на портфейла да докладват лесно доверяващите се на портфейла страни пред надзорните органи, създадени съгласно член 51 от Регламент (ЕС) 2016/679.

2. Доставчиците на портфейли прилагат протоколите и интерфейсите за докладване на доверяващите се на портфейла страни в съответствие с националните процесуални закони на държавите членки.

3. Доставчиците на портфейли гарантират, че портфейлните блокове позволяват на ползвателите на портфейла да обосноват докладите, включително чрез прикачване на подходяща информация за идентифициране на доверяващите се на портфейла страни и претенциите на ползвателите на портфейла в машинночетим формат.

Член 8

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.

Съставено в Брюксел на 28 ноември 2024 година.

За Комисията
Председател
Ursula VON DER LEYEN

ПРИЛОЖЕНИЕ

СТАНДАРТИ, ПОСОЧЕНИ В ЧЛЕН 5, ПАРАГРАФИ 1 И 2

— ISO/IEC 18013-5:2021

— ISO/IEC TS 18013-7:2024