2025/1944

30.9.2025 г.

РЕГЛАМЕНТ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2025/1944 НА КОМИСИЯТА

от 29 септември 2025 година

за определяне на правила за прилагането на Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета по отношение на референтни стандарти за процесите на изпращане и получаване на данни при квалифицираните услуги за електронна препоръчана поща и по отношение на оперативната съвместимост на тези услуги

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 44, параграф 2 и член 44, параграф 2б от него,

като има предвид, че:

(1) Квалифицираните услуги за електронна препоръчана поща осигуряват сигурен канал за предаване на документи, включително на доказателство за изпращането и получаването на данните. Тяхна цел е сигурното идентифициране на адресата и висока степен на увереност при идентифицирането на изпращача.

(2) Презумпцията за съответствие, предвидена в член 44, параграф 1а от Регламент (ЕС) № 910/2014, следва да се прилага само когато квалифицираните удостоверителни услуги за предоставяне на квалифицирани услуги за електронна препоръчана поща отговарят на стандартите, определени в настоящия регламент. Тези стандарти следва да отразяват установените практики и да бъдат широко признати в съответните сектори. Те следва да бъдат адаптирани така, че да включват допълнителни проверки, гарантиращи сигурността и надеждността на квалифицираната удостоверителна услуга.

(3) Ако доставчик на удостоверителни услуги спазва изискванията, посочени в приложение I към настоящия регламент, надзорните органи следва да приемат, че са спазени съответните изисквания на Регламент (ЕС) № 910/2014, и надлежно да се съобразят с тази презумпция за предоставяне или потвърждаване на квалифицирания статус на удостоверителната услуга. Същевременно, доставчикът на квалифицирана удостоверителна услуга може да използва и други практики, за да докаже съответствие с изискванията на Регламент (ЕС) № 910/2014.

(4) Съгласно член 44, параграф 2а от Регламент (ЕС) № 910/2014, когато доставчиците на квалифицирани удостоверителни услуги се договорят да направят услугите си оперативно съвместими, е важно те да се придържат към подходящите стандарти и спецификации, определени в приложение II към настоящия регламент за изпълнение, за да могат лесно да предават електронни препоръчани данни между двама или повече доставчици на квалифицирани удостоверителни услуги и да насърчават лоялните практики на вътрешния пазар.

(5) Комисията редовно оценява нови технологии, практики, стандарти или технически спецификации. В съответствие със съображение 75 от Регламент (ЕС) 2024/1183 на Европейския парламент и на Съвета ([2]) Комисията следва да преразглежда и при необходимост да актуализира настоящия регламент, за да бъде той в съответствие с глобалното развитие, новите технологии, стандарти или технически спецификации 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) 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).

(6) Регламент (ЕС) 2016/679 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 всички дейности по обработване на лични данни съгласно настоящия регламент.

(7) Европейският надзорен орган по защита на данните беше консултиран в съответствие с член 42, параграф 1 от Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета ([5]) и прие своето становище на 6 юни 2025 г.

(8) 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

Референтни стандарти и спецификации за квалифицираните услуги за електронна препоръчана поща

Референтните стандарти и спецификации, посочени в член 44, параграф 2 от Регламент (ЕС) № 910/2014, са определени в приложение I към настоящия регламент.

Член 2

Референтни стандарти и спецификации за оперативната съвместимост между квалифицираните услуги за електронна препоръчана поща

Референтните стандарти и спецификации, посочени в член 44, параграф 2б от Регламент (ЕС) № 910/2014, са определени в приложение II към настоящия регламент.

Член 3

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 29 септември 2025 година.

За Комисията
Председател
Ursula VON DER LEYEN

([3]) 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).

([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]) 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).

ПРИЛОЖЕНИЕ I

Списък на референтните стандарти и спецификации, посочени в член 1

Прилага се стандартът ETSI EN 319 521 V1.1.1 (2019-02) („ETSI EN 319 521“) със следните адаптации:

1. За ETSI EN 319 521

1) 2.1 Нормативни препратки:

— [1] ETSI EN 319 401 V3.1.1 (2024-06) „Електронни подписи и инфраструктури (ESI); Общи изисквания на политиката за доставчиците на удостоверителни услуги“.

— [2] ETSI EN 319 411-1 V1.5.1 (2025-04) „Електронни подписи и инфраструктури (ESI); Изисквания на политиката и изисквания за сигурност за доставчиците на удостоверителни услуги, издаващи удостоверения; Част 1: Общи изисквания“.

— [3] ETSI EN 319 522-1 V1.2.1 (2024-01) „Електронни подписи и инфраструктури (ESI); Услуги за електронна препоръчана поща; Част 1: Рамка и архитектура“.

— [4] ETSI EN 319 522-2 V1.2.1 (2024-01) „Електронни подписи и инфраструктури (ESI); Услуги за електронна препоръчана поща; Част 2: Семантично съдържание“.

— [5] Европейска група за сертифициране на киберсигурността, подгрупа по криптография: „Договорени криптографски механизми“, публикувани от Агенцията на Европейския съюз за киберсигурност (ENISA) ([1]).

— [6] ISO/IEC 15408-1:2022 — Информационна сигурност, киберсигурност и защита на неприкосновеността. Критерии за оценяване на сигурността на информационните технологии.

— [7] Регламент за изпълнение (ЕС) 2024/482 на Комисията ([2]) за определяне на правила за прилагането на Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета по отношение на приемането на европейската схема за сертифициране на киберсигурността, основана на общи критерии (ЕССК).

— [8] Регламент за изпълнение (ЕС) 2024/3144 на Комисията ([3]) за изменение на Регламент за изпълнение (ЕС) 2024/482 по отношение на приложимите международни стандарти и за поправка на посочения регламент за изпълнение.

— [9] FIPS PUB 140-3 (2019) „Изисквания за сигурността на криптографските модули“.

2) 3.1 Термини

— Усъвършенстван електронен печат: Съгласно определението в Регламент (ЕС) 910/2014 [i.1].

— Усъвършенстван електронен подпис: Съгласно определението в Регламент (ЕС) 910/2014 [i.1].

— Квалифициран електронен печат: Съгласно определението в Регламент (ЕС) 910/2014 [i.1].

— Квалифициран електронен подпис: Съгласно определението в Регламент (ЕС) 910/2014 [i.1].

— защитено криптографско устройство: устройство, което държи частния ключ на ползвателя, защитава този ключ срещу компрометиране и изпълнява функции за подписване или декриптиране от името на потребителя.

([1]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.
([2]) ОВ L, 2024/482, 7.2.2024 г., ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([3]) ОВ L, 2024/3144, 19.12.2024 г., ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

3) 5.1.1 Общи разпоредби

— REQ-ERDS-5.1.1-01 ERDS трябва адекватно да гарантира разполагаемостта, целостта и поверителността на потребителското съдържание при обработването му от ERDS посредством избор на подходящи криптографски техники за цялост и поверителност, които са в съответствие с договорените криптографски механизми, одобрени от Европейската група за сертифициране на киберсигурността и публикувани от ENISA [5].

4) 5.2.1.1 Общи положения

— REQ-QERDS-5.2.1.1-01 QERDSP осигурява много висока степен на увереност при проверката на самоличността на получателя или пряко, или като разчита на трета страна и като използва едно от следните средства или комбинация от тях, според нуждата:

а) чрез физическото присъствие на физическото лице или на упълномощен представител на юридическото лице посредством подходящи доказателства и процедури, в съответствие с националното право;

б) дистанционно, чрез използване на средство за електронна идентификация, което отговаря на изискванията по член 8 от Регламент (ЕС) № 910/2014 [i.1] по отношение на ниво на осигуреност „високо“, или чрез европейския портфейл за цифрова самоличност;

в) чрез удостоверение за квалифициран електронен подпис или за квалифициран електронен печат;

г) чрез използване на други методи за идентификация, които гарантират, че физическото лице или упълномощеният представител на юридическото лице могат да бъдат идентифицирани с много висока степен на увереност. Гаранцията, че това идентифициране се извършва с много висока степен на увереност, се потвърждава от орган за оценяване на съответствието.

— REQ-QERDS-5.2.1.1-01A QERDSP проверява самоличността на изпращача чрез подходящи средства или пряко, или като разчита на трета страна, въз основа на един от следните методи или на комбинация от тях:

а) чрез физическото присъствие на физическото лице или на упълномощен представител на юридическото лице посредством подходящи доказателства и процедури, в съответствие с националното право;

б) дистанционно, чрез европейския портфейл за цифрова самоличност или средство за електронна идентификация, за което е извършено уведомяване, отговарящо на изискванията по член 8 от Регламент (ЕС) № 910/2014 [i.1] по отношение на ниво на осигуреност „значително“, при условие че то е било издадено въз основа на предходно физическо присъствие на физическото лице или на упълномощен представител на юридическото лице;

в) чрез удостоверение за усъвършенстван електронен подпис или усъвършенстван електронен печат, при условие че удостоверението е издадено на физическото лице или на упълномощен представител на юридическото лице съгласно стандартизираната политика за предоставяне на удостоверения (NCP), както е определено в ETSI EN 319 411-1 [2]; или

г) чрез използване на други методи за идентификация, които гарантират, че физическото лице или упълномощеният представител на юридическото лице могат да бъдат идентифицирани с много висока степен на увереност. Гаранцията, че това идентифициране се извършва с висока степен на увереност, се потвърждава от орган за оценяване на съответствието.

— БЕЛЕЖКА Следва да се отбележи, че третата страна, проверяваща самоличността на изпращача и получателя, може да бъде друг QERDSP, ако изпращачът и получателят са абонирани при различни QERDSP.

5) 5.2.1.2 Идентификация на получателя и предаване на потребителско съдържание

— REQ-QERDS-5.2.1.2-03 Ако идентификацията на получателя се основава на вътрешен процес в QERDS, QERDSP провежда целия процес в защитена и контролирана среда.

6) 5.2.2 Разпоредби относно автентификацията чрез QERDS в ЕС

— REQ-QERDS-5.2.2-03 [CONDITIONAL] Когато QERDSP свързва средство за автентификация с дадена самоличност на изпращач, проверена съгласно точка 5.2.1, трябва да бъде едно от следните:

а) механизми за двуфакторна автентификация;

б) европейски портфейл за цифрова самоличност или средство за електронна идентификация, за което е извършено уведомяване и което отговаря на изискванията по член 8 от Регламент (ЕС) № 910/2014 [i.1] по отношение на ниво на осигуреност „високо“ или „значително“;

в) взаимна TLS автентификация, която включва удостоверението, издадено на изпращача съгласно NCP, както е определено в ETSI EN 319 411-1 [2];

г) цифров подпис, подкрепен от удостоверение, издадено съгласно NCP, както е определено в ETSI EN 319 411-1 [2];

д) други средства, които гарантират автентификацията на идентифицирания изпращач. Съответствието на свързването се потвърждава от орган за оценяване на съответствието. Пример: Това може да включва използването на едно от горепосочените средства от букви а), б) и г) за регистриране на клиентски сертификат за TLS (сигурност на транспортния слой) за автоматизирано изпращане чрез взаимна TLS автентификация или за регистриране на сертификат за цифров печат, използван за подпечатване на твърдения за автентификация в ERDS. Могат да се прилагат и други механизми, при които идентифицираните изпращачи използват услугите на упълномощени трети страни.

— REQ-QERDS-5.2.2-03A [CONDITIONAL] Когато QERDSP свързва средство за автентификация с дадена самоличност на получател, проверена съгласно точка 5.2.1, то трябва да бъде едно от следните, при условие че средството, или всяка комбинация от средства, осигурява много висока степен на увереност по отношение на самоличността на автентифицирания получател:

а) механизъм за многофакторна автентификация;

б) европейски портфейл за цифрова самоличност или средство за електронна идентификация, за което е извършено уведомяване и което отговаря на изискванията по член 8 от Регламент (ЕС) № 910/2014 [i.1] по отношение на ниво на осигуреност „високо“ или „значително“;

в) удостоверение за квалифициран електронен подпис или за квалифициран електронен печат;

г) други средства, които гарантират автентификацията на идентифицирания получател. Съответствието на свързването се потвърждава от орган за оценяване на съответствието. Пример: Това може да включва използването на едно от горепосочените средства от букви а)—в) за регистриране на клиентски сертификат за TLS (сигурност на транспортния слой) за автоматизирано изпращане чрез взаимна TLS автентификация или за регистриране на сертификат за цифров печат, използван за подпечатване на твърдения за автентификация в ERDS. Могат да се прилагат и други механизми, при които идентифицираните изпращачи използват услугите на упълномощени трети страни.

— REQ-QERDS-5.2.2-04 [CONDITIONAL] Ако изпращачът се свърже с QERDS по защитена връзка, която изисква междумашинно взаимно удостоверяване на автентичността между машината на подателя и сървъра на QERDS въз основа на сертификати, издадени съгласно NCP, както е определено в ETSI EN 319 411-1 [2], след като бъде установена тази защитена връзка, за втория етап на автентификация на подателя могат да бъдат приети еднофакторни механизми за автентификация, ако въведените организационни процедури и мерки за сигурност гарантират доверие в автентификацията на подателя.

7) 5.4.1 Общи разпоредби

— REQ-ERDS-5.4.1-06 ERDS генерира и предоставя на разположение на законните заинтересовани страни доказателства от ERDS за събития, свързани с ЕПП, както е определено в точка 6 от ETSI EN 319 522-1 [3].

— REQ-ERDS-5.4.1-07 ERDSP архивира доказателствата и/или тяхна съкратена версия за всяко представено доказателство.

— REQ-ERDS-5.4.1-08 Доказателствата от ERDS, генерирани от ERDS, трябва да съответстват на семантиката на доказателствата, определена в точка 8 от ETSI EN 319 522-2 [4].

8) 7.2.1 Общи разпоредби

— REQ-ERDS-7.2.1-02 Персоналът на ERDSP с доверителни функции трябва да е способен да изпълни изискването за „експертни знания, опит и квалификации“ вследствие официално обучение и квалификация, или практически опит, или комбинация от двете.

— REQ-ERDS-7.2.1-03 Спазването на REQ-ERDS-7.2.1-02 включва редовни актуализации (най-малко на всеки 12 месеца) във връзка с новите заплахи и настоящите практики в областта на сигурността.

9) 7.3.2 Боравене с носители

— REQ-ERDS-7.3.1-02 Прилагат се всички изисквания на ETSI EN 319 401 [1], точка 7.3.3.

10) 7.5 Криптографски контрол

— REQ-ERDS-7.5-01A ERDS избира и използва подходящи криптографски техники, съответстващи на договорените криптографски механизми, одобрени от Европейската група за сертифициране на киберсигурността и публикувани от ENISA [5].

— REQ-ERDSP-7.5-03 Частният ключ за подпис на ERDS се съхранява и използва в рамките на защитено криптографско устройство, което е надеждна система, сертифицирана в съответствие със:

а) Общи критерии за оценяване на сигурността на информационните технологии, както са определени в ISO/IEC 15408 [6] или в Общи критерии за оценяване на сигурността на информационните технологии, версия CC:2002, части 1—5, публикувани от участниците в Споразумението за признаване на основани на общи критерии сертификати в областта на ИТ сигурността, и сертифицирана като EAL 4 или по-високо; или

б) Европейската схема за сертифициране на киберсигурността, основана на общи критерии (ЕССК) [7] [8], и сертифицирана като EAL 4 или по-високо; или

в) до 31.12.2030 г., FIPS PUB 140-3 [9] ниво 3.

Това сертифициране е спрямо целево ниво за сигурност или защитен профил, или документация за проект и сигурност на модула, която отговаря на изискванията на настоящия документ, въз основа на анализ на риска и като се вземат предвид физическите и други нетехнически мерки за сигурност.

Ако защитеното криптографско устройство е сертифицирано по ЕССК [7] [8], то се конфигурира и използва в съответствие с тази сертификация.

11) 7.8 Мрежова сигурност

— REQ-ERDSP-7.8-04 ERDSP използва най-съвременни протоколи и алгоритми за криптиране на ниво транспортен слой в съответствие с договорените криптографски механизми, одобрени от Европейската група за сертифициране на киберсигурността и публикувани от ENISA [5].

— REQ-ERDSP-7.8-06 Проверката на уязвимостта, изисквана по REQ-7.8-13 на ETSI EN 319 401 [1], се извършва поне веднъж на тримесечие.

— REQ-ERDSP-7.8-07 Проверката на изпитване за пробив, изисквана по REQ-7.8-17X на ETSI EN 319 401 [1], се извършва поне веднъж годишно.

— REQ-ERDSP-7.8-08 Защитните стени трябва да бъдат конфигурирани така, че да предотвратяват всякакви протоколи и достъп, които не са необходими за функционирането на доставчика на удостоверителни услуги.

12) 7.12 Планове за прекратяване на дейност на ERDSP и планове за осигуряване на непрекъснатост на обслужването на ERDS

— REQ-ERDS-7.12-03 Планът на ERDSP за осигуряване на непрекъснатост на обслужването е съобразен с изискванията, определени в актовете за изпълнение, приети съгласно член 24, параграф 5 от Регламент (ЕС) № 910/2014 [i.1].

13) 7.14 Верига на доставки

— REQ-ERDS-7.14-01 Прилагат се изискванията, посочени в ETSI EN 319 401 [1], точка 7.14.

ПРИЛОЖЕНИЕ II

Списък на референтните стандарти и спецификации, посочени в член 2

Прилагат се стандартите ETSI EN 319 522-1 V1.2.1 (2024-01) („ETSI EN 319 522-1“), ETSI EN 319 522-2 V1.2.1 (2024-01) („ETSI EN 319 522-2“), ETSI EN 319 522-3 V1.2.1 (2024-01) („ETSI EN 319 522-3“), ETSI EN 319 522-4-1 V1.2.1 (2019-01) („ETSI EN 319 522-4-1“), ETSI EN 319 522-4-2 V1.1.1 (2018-09) („ETSI EN 319 522-4-2“) и ETSI EN 319 522-4-3 V1.1.1 (2018-09) („ETSI EN 319 522-4-3“).