2025/2531

17.12.2025 г.

РЕГЛАМЕНТ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2025/2531 НА КОМИСИЯТА

от 16 декември 2025 година

за определяне на правила за прилагането на Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета по отношение на референтни стандарти и спецификации за квалифицираните услуги за електронни регистри

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 45л, параграф 3 от него,

като има предвид, че:

(1) С Регламент (ЕС) 2024/1183 на Европейския парламент и на Съвета ([2]) в Регламент (ЕС) № 910/2014 беше включен списък на новите удостоверителни услуги и квалифицираните удостоверителни услуги, включително записването на електронни данни в квалифициран електронен регистър. Комисията трябва да състави списък с референтни стандарти и, ако е необходимо, да установи спецификации за този вид услуги.

(2) Електронният регистър е последователност от електронни записи на данни, която трябва да гарантира целостта на тези записи и точността на хронологичната подредба на тези записи. За да се гарантира, че записването на данни в квалифициран електронен регистър е хронологично подредено, последователно и надеждно, е необходимо да се установи общ набор от спецификации за записването на електронни данни в квалифициран електронен регистър.

(3) Презумпцията за съответствие, предвидена в член 45л, параграф 2 от Регламент (ЕС) № 910/2014, следва да е валидна само когато квалифицираните удостоверителни услуги за записване на електронни данни в квалифициран електронен регистър 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.

(4) Ако доставчик на удостоверителни услуги спазва изискванията, посочени в приложението 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 квалифицирани удостоверителни услуги може да използва и други практики, за да докаже съответствие с изискванията на Регламент (ЕС) № 910/2014.

(5) Комисията редовно оценява нови технологии, практики, стандарти или технически спецификации. В съответствие със съображение 75 от Регламент (ЕС) 2024/1183 Комисията следва да преразгледа и при необходимост да актуализира настоящия регламент, за да бъде той в съответствие с глобалното развитие, новите технологии, практики, 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 дейностите по обработване на лични данни съгласно настоящия регламент, като се вземат предвид Насоки 02/2025 на Европейския комитет по защита на данните относно обработването на лични данни посредством блокова верига ([5]).

(7) Беше проведена консултация с Европейския надзорен орган по защита на данните в съответствие с член 42, параграф 1 от Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета ([6]), който предостави своето становище на 21 октомври 2025 г. ([7])

(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

Референтните стандарти и спецификации, посочени в член 45л, параграф 3 от Регламент (ЕС) № 910/2014, са определени, по отношение на електронните регистри, в приложението към настоящия регламент.

Член 2

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 16 декември 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]) edpb_guidelines_202502_blockchain_en.pdf.

([6]) 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).

([7]) Официални коментари на ЕНОЗД по проекта за регламент за изпълнение за определяне на правила за прилагането на Регламент (ЕС) № 910/2014 по отношение на референтните стандарти и спецификации за квалифицирани електронни регистри.

ПРИЛОЖЕНИЕ

Списък на техническите спецификации и референтните стандарти за квалифицирани децентрализирани електронни регистри

1. За целите на настоящия регламент се прилагат следните определения:

   а) „окончателност“ означава състоянието на запис на данни в електронен регистър, при което записът е в окончателен вид и не може да бъде променен или премахнат;

   б) „децентрализиран електронен регистър“ означава електронен регистър, който е разположен в децентрализиран набор от възли, като при синхронизирането между тези възли се използва механизъм за консенсус;

   в) „възел на децентрализиран електронен регистър“ означава устройство или процес, който е част от мрежа на децентрализиран електронен регистър и съхранява пълно или частично копие на записите на данни в електронен регистър;

   г) „мрежа на децентрализиран електронен регистър“ означава мрежа от възли на децентрализиран електронен регистър, която изгражда система на децентрализиран електронен регистър;

   д) „система на децентрализиран електронен регистър“ означава система, която е техническа реализация на децентрализиран електронен регистър;

   е) „консенсус“ означава съгласие между възлите на децентрализиран електронен регистър относно валидността на трансакциите и поддържане на последователен и подреден набор от валидирани трансакции в системата на децентрализирания електронен регистър;

   ж) „механизъм за консенсус“ означава набор от правила и процедури, чрез които се постига консенсус;

   з) „правила за управление“ означава набор от протоколи, политики и механизми, които определят как функционира системата на децентрализирания електронен регистър, как се валидират и добавят данни в електронния регистър и как си взаимодействат участниците;

   и) „трансакция“ означава най-малката единица от работен процес в рамките на електронен регистър;

   й) „работен процес“ означава една или повече поредици от действия, необходими за постигане на резултат, който е в съответствие с правилата, по които функционира електронният регистър;

   к) „валидирана трансакция“ означава трансакция, за която изискваните цялостност, автентичност и специфични за проекта условия са били проверени в съответствие с приложимите правила на системата на децентрализирания електронен регистър;

   л) „криптографска връзка“ означава позоваване на данни, създадено с помощта на подходящи криптографски техники, за да се гарантира цялостността, автентичността или проследимостта на посочените данни и правилната последователност на записите на данни;

   м) „доклад от регистъра“ означава структурирано представяне на проверима информация, извлечена от записите на данни в електронен регистър, с което се предоставя информация за конкретни дейности, състояние или съответствие с предварително определени правила;

   н) „доставчик на квалифициран електронен регистър“ означава доставчик на квалифицирана удостоверителна услуга, която се състои в записване на данни в квалифициран електронен регистър;

   о) „квалифициран децентрализиран електронен регистър“ означава децентрализиран електронен регистър, който отговаря на изискванията за квалифициран електронен регистър.

2. Когато доставчикът на квалифицирани удостоверителни услуги трябва да изготви доклад от регистъра, той се изготвя по автоматизиран начин.

3. Доставчиците на квалифицирани електронни регистри създават, записват електронни данни в квалифициран електронен регистър, актуализират го и го поддържат в съответствие със спецификациите, установени в:

   а) За всички доставчици на квалифицирани електронни регистри, ETSI EN 319 401 v3.1.1 (2024-06) със следните адаптации:

      — 2.1. Нормативни препратки:

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

[2] IETF RFC 7515 (май 2015 г.): „JSON Web Signature (JWS)“.

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

[4] Регламент за изпълнение (ЕС) 2024/482 на Комисията от 31 януари 2024 година 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).

[5] Регламент за изпълнение (ЕС) 2024/3144 на Комисията от 18 декември 2024 година за изменение на Регламент за изпълнение (ЕС) 2024/482 по отношение на приложимите международни стандарти и за поправка на посочения регламент за изпълнение.

[6] ISO/IEC 15408:2022 (части 1—5): „Информационна сигурност, киберсигурност и защита на неприкосновеността на личния живот — критерии за оценка на сигурността на информационните технологии“.

— 6.1. Декларация за практиката при удостоверителните услуги:

  — REQ-6.1-12 Декларацията за практиката по отношение на електронния регистър включва най-малко следната информация:

    — функционалните и техническите възможности на платформата на електронния регистър и нейното използване през цялото време на предоставяне на записване на данни в квалифициран електронен регистър като квалифицирана удостоверителна услуга;

    — специфичните механизми за удостоверяване на произхода на данните, използвани при предоставянето на услугата;

    — специфичните механизми за подреждане в хронологичен ред, използвани при предоставянето на услугата;

    — когато е приложимо, криптографската връзка, използвана за осигуряване на последователността на записите на данни;

    — когато е приложимо, механизма за консенсус, който гарантира окончателност и цялостност на записите с данни и трансакциите, съхранявани в регистъра, включително всяко резервно време до постигането на окончателност и цялостност;

    — специфичните механизми за цялостност на данните, използвани при предоставянето на услугата.

— 6.2. Общи условия:

  — REQ-6.2-03 Абонатите и страните, които разчитат на удостоверителната услуга за електронно архивиране, се информират по ясен, изчерпателен и леснодостъпен начин, на публично достъпно място и поотделно, за конкретните общи условия, включително посочените по-горе елементи, преди да встъпят в договорни отношения.

— 6.3. Политика за сигурност на информацията

  — REQ-6.3-04X Доставчикът на удостоверителни услуги (TSP) установява процедури за уведомяване на надзорния орган за всички промени в предоставянето на удостоверителната услуга в съответствие със стопанските изисквания и съответните законови и подзаконови актове. TSP уведомява надзорния орган най-малко:

    — един месец преди извършването на каквато и да е промяна;

    — три месеца преди планираното прекратяване на предоставянето на удостоверителна услуга.

— 7.2. Човешки ресурси

  — REQ-7.2-04X Персоналът на TSP 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-7.2-05X Това включва редовни актуализации (най-малко на всеки 12 месеца) във връзка с новите заплахи и настоящите практики в областта на сигурността.

— 7.5. Криптографски контрол

— REQ-7.5-01X Въвеждат се подходящи механизми за контрол на сигурността за управлението на криптографски ключове, криптографски алгоритми и криптографски устройства през целия им жизнен цикъл, като се следва, когато е целесъобразно, подход на криптогъвкавост.

— REQ-7.5-02 За целите на предоставянето на своите удостоверителни услуги TSP избира и използва подходящи криптографски техники, съобразени с договорените криптографски механизми, одобрени от Европейската група за сертифициране на киберсигурността и публикувани от ENISA [1].

По-конкретно:

— REQ-7.5-03 Доставчиците на квалифицирани електронни регистри установяват произхода на записите на данни в електронния регистър. За тази цел те използват усъвършенствани електронни подписи въз основа на квалифицирани удостоверения или усъвършенствани електронни печати въз основа на квалифицирани удостоверения, създадени от потребителите на услугата в съответствие със следните стандарти и спецификации:

а) ETSI EN 319 122-1 V1.3.1 (2023-06). Електронни подписи и инфраструктура (ESI); CAdES цифрови подписи; Част 1: Градивни елементи и базови CAdES подписи.

б) ETSI EN 319 132-1 V1.3.1 (2024-07). Електронни подписи и доверителна инфраструктура за удостоверяване (ESI); XAdES цифрови подписи; Част 1: Градивни елементи и базови XAdES подписи.

в) ETSI TS 119 182-1 V1.2.1 (2024-07). Електронни подписи и доверителна инфраструктура за удостоверяване (ESI); JAdES цифрови подписи; Част 1: Градивни елементи и базови JAdES подписи със следната адаптация:

— 5.1.8. Параметърът header x5c (X.509 Удостоверителна верига)

— Параметърът header x5c, както е определен в точка 4.1.6 от IETF RFC 7515 [2], трябва да присъства в JAdES подписа като подписан или неподписан параметър header.

— Параметърът header x5c трябва да има семантиката, уточнена в IETF RFC 7515 [2], точка 4.1.6.

— Параметърът header x5c трябва да има синтаксиса, посочен в IETF RFC 7515 [2], точка 4.1.6.

— REQ-7.5-04: Доставчиците на квалифицирани електронни регистри гарантират уникалното подреждане в хронологичен ред на записите на данни в електронния регистър. За тази цел те използват криптографски връзки, основани на хеш списъци или хеш-дървета, като използват криптографски хеш функции, в съответствие със следните спецификации и стандарти:

а) SHA-256 или продукт с по-голям размер на хеша при спазване на съгласуваните криптографски механизми, одобрени от Европейската група за сертифициране на киберсигурността и публикувани от ENISA [1];

б) SHA3-256 или продукт с по-голям размер на хеша при спазване на съгласуваните криптографски механизми, одобрени от Европейската група за сертифициране на киберсигурността и публикувани от ENISA [1].

Като алтернатива, когато използват запис на времето, за да гарантират уникалното подреждане в хронологичен ред на записите на данни в електронния регистър, доставчиците на квалифицирани електронни регистри използват квалифицирани времеви печати.

— REQ-7.5-05 Доставчиците на квалифицирани електронни регистри гарантират цялостността на записите на данни, записвани в квалифициран електронен регистър. За тази цел те използват усъвършенствани електронни подписи въз основа на квалифицирани удостоверения или усъвършенствани електронни печати въз основа на квалифицирани удостоверения, в съответствие със следните стандарти и спецификации:

  а) всеки формат на подпис или печат, който спазва съгласуваните криптографски механизми, одобрени от Европейската група за сертифициране на киберсигурността и публикувани от ENISA [1];

  б) SHA-256 или по-високо за хеш размера на продукта при спазване на съгласуваните криптографски механизми, одобрени от Европейската група за сертифициране на киберсигурността и публикувани от ENISA [1];

  в) SHA3-256 или продукт с по-голям размер на хеша при спазване на съгласуваните криптографски механизми, одобрени от Европейската група за сертифициране на киберсигурността и публикувани от ENISA [1];

  г) Доставчиците на квалифицирани електронни регистри гарантират непосредственото засичане на всяка последваща промяна в данните, записани в квалифициран електронен регистър.

— REQ-7.5-06 Когато се използват механизми за цифров подпис, частните ключове за подпис на доставчика на квалифициран електронен регистър се съхраняват и използват 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 ([1]) [6] или в Общи критерии за оценяване на сигурността на информационните технологии, версия CC:2022, 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) ([2]) ([3]) [4] [5], и сертифицирана като EAL 4 или по-високо; или

  в) до 31.12.2030 г., FIPS PUB 140-3 ([4]) [3] 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 [4] [5], то се конфигурира и използва в съответствие с това сертифициране.

([1]) ISO/IEC 15408:2022 (части 1—5): „Информационна сигурност, киберсигурност и защита на неприкосновеността на личния живот — критерии за оценка на сигурността на информационните технологии“.

([2]) Регламент за изпълнение (ЕС) 2024/482 на Комисията от 31 януари 2024 г. 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) (ОВ L, 2024/482, 7.2.2024 г., ELI: http://data.europa.eu/eli/reg_impl/2024/482/2025-01-08).

([3]) Регламент за изпълнение (ЕС) 2024/3144 на Комисията от 18 декември 2024 година за изменение на Регламент за изпълнение (ЕС) 2024/482 по отношение на приложимите международни стандарти и за поправка на посочения регламент за изпълнение (ОВ L, 2024/3144, 19.12.2024 г., ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj).

([4]) FIPS PUB 140-3 (2019): „Изисквания за сигурност за криптографски модули“.

— 7.8. Мрежова сигурност:

— REQ-7.8-14X Проверката на уязвимостта, изисквана по REQ-7.8-13, се извършва поне веднъж на тримесечие.

— REQ-7.8-18X Изпитването за пробив, изисквано по REQ-7.8-17X, се извършва поне веднъж годишно.

— REQ-7.8-21X: Защитните стени трябва също да бъдат конфигурирани така, че да предотвратяват всякакви протоколи и достъп, които не са необходими за функционирането на доставчика на удостоверителни услуги.

— 7.9.1. Мониторинг и водене на регистри:

— При дейностите по мониторинг REQ-7.9.1-02X се взема предвид чувствителността на всяка информация, която се събира или анализира.

— 7.12. Прекратяване на дейност на TSP и планове на TSP за прекратяване:

— REQ-7.12-02A Планът на TSP за прекратяване е съобразен с изискванията, определени в актовете за изпълнение, приети съгласно член 24, параграф 5 от Регламент (ЕС) № 910/2014 [i.1].

б) Освен това за всички доставчици на квалифицирани електронни регистри, които използват технологии за децентрализиран електронен регистър:

1) ISO 23257:2022 Блокови вериги и технологии на децентрализирания регистър — Референтна архитектура, точка 9, предоставяща пълно описание на системата на технологията на децентрализирания електронен регистър, съответната мрежа от технологии на децентрализирания електронен регистър и възлите на технологията на децентрализирания електронен регистър;

2) ISO/TS 23635:2022. Блокови вериги и технологии на децентрализирания регистър — Насоки за управление по отношение на писмени и публично достъпни политики и практики, свързани със структурата на управление на предоставяната от тях услуга на електронен регистър.