2025/1550

29.7.2025 г.

РЕГЛАМЕНТ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2025/1550 НА КОМИСИЯТА

от 28 юли 2025 година

за определяне на техническите спецификации и други изисквания за децентрализираната информационна система, посочена в Регламент (ЕС) 2023/1543 на Европейския парламент и на Съвета

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид Регламент (ЕС) 2023/1543 на Европейския парламент и на Съвета от 12 юли 2023 г. относно европейските заповеди за предоставяне и европейските заповеди за запазване на електронни доказателства в рамките на наказателните производства и за изпълнението на наказания лишаване от свобода вследствие на наказателни производства ([1]), и по-специално член 25, параграф 1, букви а), букви а), б), в) и г) от него,

като има предвид, че:

(1) За да се създаде децентрализираната информационна система, посочена в Регламент (ЕС) 2023/1543, е необходимо да се определят и приемат технически спецификации, мерки и цели за въвеждането на тази система.

(2) Съгласно Регламент (ЕС) 2023/1543 децентрализираната информационна система следва да се състои от информационните системи на държавите членки и на агенциите и органите на Съюза и от оперативно съвместими точки за достъп до e-CODEX, чрез които тези информационни системи са свързани помежду си. В съответствие с това техническите спецификации и другите изисквания на децентрализираната информационна система следва да отразяват тази рамка.

(3) Съгласно Регламент (ЕС) 2023/1543 точките за достъп на децентрализираната информационна система следва да се основават на разрешени точки за достъп до e-CODEX, както е определено в член 3, параграф 3 от Регламент (ЕС) 2022/850 на Европейския парламент и на Съвета ([2]).

(4) Държавите членки могат да изберат да използват образеца на софтуерно приложение за свързване, разработен от Комисията, като поддържаща система вместо национална информационна система. За да се гарантира оперативната съвместимост, както националните информационни системи, така и образецът на софтуерно приложение за свързване следва да подлежат на едни и същи технически спецификации и изисквания, определени в настоящия регламент.

(5) За да се смекчат потенциалните технически проблеми, свързани с капацитета и надеждността на децентрализираната информационна система, е необходимо да се установи праг за обема на електронните доказателства, предавани чрез тази система. След пускането в действие на системата честотата и обемът на тези предавания следва да бъдат наблюдавани и прагът следва да бъде адаптиран, когато е целесъобразно, за да се постигне максимална ефикасност на системата.

(6) За да се засили оперативната съвместимост и ефикасността на децентрализираната информационна система, следва да се разпореди използването на подходящи стандарти на ETSI. Бъдещото развитие следва да бъде наблюдавано и, когато е необходимо, следва да се обмисли приемането на допълнителни стандарти на ETSI.

(7) Ирландия е обвързана от Регламент (ЕС) 2023/1543 и следователно участва в приемането на настоящия регламент.

(8) В съответствие с членове 1 и 2 от Протокол № 22 относно позицията на Дания, приложен към Договора за Европейския съюз и към Договора за функционирането на Европейския съюз, Дания не е обвързана от настоящия регламент, нито от неговото прилагане.

([1]) ОВ L 191, 28.7.2023 г., стр. 118, ELI: http://data.europa.eu/eli/reg/2023/1543/oj.

([2]) Регламент (ЕС) 2022/850 на Европейския парламент и на Съвета от 30 май 2022 г. относно компютризирана система за трансграничен електронен обмен на данни в областта на съдебното сътрудничество по гражданскоправни и наказателноправни въпроси (система e-CODEX) и за изменение на Регламент (ЕС) 2018/1726 (ОВ L 150, 1.6.2022 г., стр. 1, ELI: http://data.europa.eu/eli/reg/2022/850/oj).

(9) В съответствие с член 42, параграф 1 от Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета ([3]) беше проведена консултация с Европейския надзорен орган по защита на данните, който прие становище на 25 юни 2025 г.

(10) Мерките, предвидени в настоящия регламент, са в съответствие със становището на комитета, създаден по силата на член 26 от Регламент (ЕС) 2023/1543,

ПРИЕ НАСТОЯЩИЯ РЕГЛАМЕНТ:

Член 1

Технически спецификации на децентрализираната информационна система

Техническите спецификации и изискванията, мерките и целите на децентрализираната информационна система, посочена в член 25, параграф 1 от Регламент (ЕС) 2023/1543, за комуникация по смисъла на член 19 от същия регламент, са определени 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 в държавите членки в съответствие с Договорите.

Съставено в Брюксел на 28 юли 2025 година.

За Комисията
Председател
Ursula VON DER LEYEN

([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, 21.11.2018г., стр. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

ПРИЛОЖЕНИЕ

ТЕХНИЧЕСКИ СПЕЦИФИКАЦИИ НА ДЕЦЕНТРАЛИЗИРАНАТА ИНФОРМАЦИОННА СИСТЕМА

(посочени в член 1)

1. **Въведение и приложно поле**

В настоящото приложение се определят техническите спецификации, мерките и целите за въвеждането на децентрализираната информационна система по Регламент (ЕС) 2023/1543.

Съгласно Регламент (ЕС) 2023/1543, и по-специално член 19 от него, децентрализираната информационна система трябва да дава възможност за писмена комуникация между компетентните органи и определените форми на установяване или представителите, между компетентните органи, както и между компетентните органи и компетентните агенции или органи на Съюза.

2. **Определения**

2.1. „HyperText Transport Protocol Secure“ или „HTTPS“ означава криптирана комуникация и сигурни канали за връзка;

2.2. „невъзможност за заличаване на произхода“ означава мерките, предоставящи доказателство за целостта на данните и доказателство за произхода на данните чрез методи като цифрово удостоверяване, инфраструктура на публичния ключ и електронни подписи и електронни печати;

2.3. „невъзможност за отказване на получаването“ означава мерките, предоставящи на източника на предаването доказателство за получаването на данните от получателя, за когото са предназначени данните, чрез методи като цифрово удостоверяване, инфраструктура на публичния ключ и електронни подписи и електронни печати;

2.4. „SOAP“ означава, съгласно стандартите на World Wide Web Consortium, спецификация на протокол за съобщения за обмен на структурирана информация в изпълнение на уеб услуги в компютърни мрежи;

2.5. „Representational State Transfer“ (REST) означава архитектурен стил за проектиране на приложения в мрежа, като се разчита на модел за комуникация клиент-сървър, неустановен в определена държава, и се използват стандартни методи за извършване на операции с ресурси, които обикновено са представени в структурирани формати;

2.6. „уеб услуга“ означава софтуерна система, създадена да поддържа оперативната съвместимост на взаимодействието машина-машина в мрежа, разполагаща с интерфейс, описан в машинно обработваем формат;

2.7. „обмен на данни“ означава обмен на съобщения, формуляри, документи и електронни доказателства чрез децентрализираната информационна система;

2.8. „API“ означава приложно-програмен интерфейс, основан на общ стандарт за обмен на данни, който позволява на доставчиците на услуги, които използват специално разработени информационно-технологични решения за целите на обмена на информация и данни, свързани с искания за електронни доказателства, да получават достъп до децентрализираните информационни системи чрез автоматизирани средства;

2.9. „уеб базиран интерфейс“ означава потребителски интерфейс, достъпен чрез HTTPS в интернет, който позволява на доставчиците на услуги да имат ръчен достъп до децентрализираната информационна система, за да комуникират по сигурен начин с органите и да обменят информация и данни, свързани с искания за електронни доказателства, без да е необходимо да създават своя собствена специална инфраструктура;

2.10. „Стандарти на ETSI“ означава технически спецификации и стандарти, разработени от Европейския институт за стандарти в далекосъобщенията (ETSI) с цел осигуряване на оперативна съвместимост, сигурност и ефективност на информационните и комуникационните технологии. Те предоставят рамки, протоколи и най-добри практики за широк спектър от технологии, включително мобилни мрежи, радиокомуникации, киберсигурност и интернет инфраструктура;

2.11. „хеш резюме“ означава изходни данни с фиксирана дължина, генериран от криптографска хеш-функция, когато се прилага към входни данни с произволна дължина. Криптографската хеш-функция е проектирана да отговаря на основни характеристики за сигурност, включително устойчивост на предварително изображение, устойчивост на второ предварително изображение и устойчивост на сблъсък, като се гарантира нейната устойчивост срещу инверсия и сблъсък при посегателства;

2.12. „система e-CODEX“ означава системата e-CODEX, определена в член 3, параграф 1 от Регламент (ЕС) 2022/850;

2.13. „Основни речници на ЕС в областта на електронното правосъдие“ означава основните речници на ЕС в областта на електронното правосъдие съгласно определението в точка 4 от приложението към Регламент (ЕС) 2022/850;

2.14. „ebMS“ означава услугата ebXML Messaging Service, която представлява протокол за съобщения, разработен съгласно рамката OASIS, който дава възможност за сигурен, надежден и оперативно съвместим обмен на електронни бизнес документи чрез SOAP и подпомага интеграцията между предприятията в различни системи;

2.15. „AS4“ означава декларация за приложимост 4 — стандарт OASIS, който описва ebMS 3.0; като се има предвид, че с него се опростяват сигурните и оперативно съвместими съобщения между предприятията чрез използване на отворени стандарти като SOAP и WS-Security;

2.16. „Целево време за възстановяване“ означава максимално допустимото време за възстановяване на услугата след инцидент;

2.17. „Целева точка на възстановяване“ означава максимално допустимото количество загуба на данни в случай на неизправност.

3. **Методи за комуникация по електронен път**

3.1. За целите на писмената комуникация между компетентните органи на държавите членки, между компетентните органи и определените форми на установяване или представителите на доставчиците на услуги, както и между компетентните органи и агенциите или органите на Съюза децентрализираната информационна система използва основани на услугите методи за връзка, като например уеб услуги или други компоненти за многократна употреба и софтуерни решения за целите на обмена на данни. По-специално тя ще включва комуникация чрез точките за достъп до e-CODEX, както е посочено в член 5, параграф 2 от Регламент (ЕС) 2022/850. Поради това, за да се гарантира ефективен и оперативно съвместим трансграничен обмен на данни, децентрализираната информационна система поддържа комуникацията чрез системата e-CODEX.

3.2. Като се има предвид очакваният голям обем електронни доказателства, които ще бъдат предавани след издаване на европейска заповед за предоставяне чрез децентрализираната информационна система, както е посочено в член 19, параграфи 1 и 4 от Регламент (ЕС) 2023/1543, което може да доведе до ограничения на техническия капацитет, които биха могли да окажат отрицателно въздействие върху децентрализираната информационна система, електронните доказателства се предават чрез тази система, при условие че не надхвърлят прага от 25 мегабайта (25 600 килобайта). Предаването на електронни доказателства, надхвърлящи този праг, се извършва в съответствие с член 19, параграф 5 от посочения регламент.

3.3. Като се има предвид член 19, параграф 6 от Регламент (ЕС) 2023/1543, в случай че предаването се извършва чрез алтернативни средства, както е предвидено в същия параграф, поради невъзможност за използване на децентрализираната информационна система по една от причините, посочени в член 19, параграф 5 от посочения регламент:

3.3.1. Когато предаването се отнася до писмена комуникация, включително обмен на формуляри, между компетентните органи и доставчиците на услуги по смисъла на член 19, параграф 1 от Регламент (ЕС) 2023/1543, източникът на предаването записва предаването в своята национална информационна система, която е част от децентрализираната информационна система. Записаната информация включва като минимум референтен номер на делото или досието, датата и часа, подателя и получателя, името и размера на файла.

3.3.2. Когато предаването се отнася до писмена комуникация, включително обмен на формуляри, между компетентните органи, както и до писмена комуникация с компетентните агенции или органи на Съюза по смисъла на член 19, параграф 4 от Регламент (ЕС) 2023/1543, източникът на предаването го записва в децентрализираната информационна система, по-специално в рамките на своята национална информационна система или, когато е приложимо, в информационните системи, управлявани от компетентната агенция или орган на Съюза. Записаната информация включва като минимум референтен номер на делото или досието, датата и часа на предаване, подателя и получателя, името на файла и неговия размер.

3.3.3. Когато електронните доказателства съгласно европейска заповед за предоставяне са предадени чрез алтернативни средства за комуникация между доставчиците на услуги и компетентните органи в издаващата държава ([1]) или когато електронните доказателства се предават чрез алтернативни средства от изпълняващия орган на компетентните органи в издаващата държава съгласно процедурата по принудително изпълнение, предвидена в член 16, параграф 9 от Регламент (ЕС) 2023/1543, източникът на предаването:

а) записва и предава на органа, на който са предадени или предоставени електронните доказателства, следната информация като част от манифест:

1) информация за подателя и получателя;

2) метаданни, свързващи предоставените електронни доказателства с конкретна(и) европейска(и) заповед(и) за предоставяне или запазване;

3) датата и часа на предаването или датата, на която електронното доказателство е било предоставено на получателя;

4) информация относно средствата за предаване (напр. запис на защитената връзка, чрез която е предоставено електронното доказателство, доказателство за получаване или доставка от пощенски служби и др. ([2]));

5) пълните наименования на файловете с електронни доказателства, предадени или предоставени по друг начин на предвидения получател в издаващата държава;

6) размера на данните на електронното доказателство, предадено или предоставено по друг начин на предвидения получател в издаващата държава;

7) поне едно хеш резюме на данните, които са били предадени или предоставени, и указание за използваните алгоритми за хеширане. Алгоритмите за хеширане, използвани за изчисляване на хеш резюметата са криптографски силни, често срещани, и не подлежат на публично оповестени слабости, като например сблъсъци (например SHA-512, SHA3—512, BLAKE2 или RIPEMD-160, но потенциално по-силни, в зависимост от технологичното развитие);

б) когато е приложимо, посочва, като част от манифеста, посочен в буква а) по-горе, датата и часа, до които електронните доказателства ще останат достъпни. Този период предоставя на компетентния орган на издаващата държава разумен срок за извличане на електронните доказателства, който е не по-кратък от 10 календарни дни и не по-дълъг от 45 календарни дни от момента на предоставяне на електронните доказателства. По искане на компетентния орган на издаващата държава срокът, посочен от източника, може да бъде удължен в конкретен случай;

в) може да записва и предава всяка допълнителна информация или забележки, свързани със случая, на органа, на който са предадени или предоставени електронните доказателства, като част от манифеста, посочен в буква а) по-горе.

3.4. Като се има предвид член 28 от Регламент (ЕС) 2023/1543, в образеца на софтуерно приложение за свързване се събират, предават или се предоставя по друг начин достъп до статистическите данни, посочени в параграф 2 от същия член, както в структурирани (напр. XML), така и в неструктурирани (напр. PDF) формати на данни. В съответствие с член 28, параграф 3 от Регламент (ЕС) 2023/1543, когато са технически оборудвани, националните портали ([3]), управлявани от държавите членки, могат също така да предават или предоставят тези статистически данни на Комисията чрез автоматизиран процес. Комисията издава насоки относно структурата на данните и метода за събиране и съобщаване на тези статистически данни.

([1]) За по-голяма яснота позоваванията на компетентните национални органи се разбират *mutatis mutandis* и като отнасящи се до националните членове на Евроюст, европейските прокурори и европейските делегирани прокурори, доколкото те са оправомощени да изпълняват същите функции съгласно правото на ЕС и националното право.

([2]) Следва да се припомни, че в съответствие с член 19, параграф 5 предаването чрез такива алтернативни средства за комуникация трябва да отговаря на изискванията за бърз, сигурен и надежден обмен, който позволява на получателя да установи автентичността.

([3]) „Национални портали“ следва да се разбират като национални „информационни системи“, които са част от децентрализираната информационна система, както е определено в член 3, параграф 21 от Регламент (ЕС) 2023/1543.

4. **Протоколи за комуникация**

4.1. Децентрализираната информационна система използва защитени интернет протоколи за:

а) комуникация в рамките на децентрализираната информационна система между компетентните органи,

б) комуникация в рамките на децентрализираната информационна система между компетентните органи и агенциите и органите на Съюза,

в) комуникация между компетентните органи и доставчиците на услуги чрез API и уеб базирания интерфейс, и

г) комуникация с базата данни за съдилищата.

4.2. За определянето и предаването на структурирани данни и метаданни компонентите на децентрализираната информационна система се основават на всеобхватни и широко приети промишлени стандарти и протоколи, като SOAP и REST, и по-специално тези, на които се позовават европейските организации по стандартизация, като ETSI.

4.3. За протоколите за транспорт и съобщения децентрализираната информационна система се основава на сигурни, основани на стандарти протоколи, като например:

а) AS4 Профил за трансграничен обмен на данни, гарантиращ сигурни и надеждни съобщения с криптиране и невъзможност за отказване;

б) HTTPS/RESTful API за комуникация, поддържаща форматите JSON и XML;

в) SOAP за взаимодействия с висока степен на надеждност, включващ WS-Security за автентификация и криптиране.

4.4. За целите на безпрепятствения и оперативно съвместим обмен на данни комуникационните протоколи, използвани от децентрализираната информационна система, отговарят на съответните стандарти за оперативна съвместимост.

4.5. Когато е приложимо, XML схемите за електронни доказателства използват съответните стандарти или речници, които са необходими за правилното валидиране на елементите и типовете, определени в рамките на тази схема. Те може да включват:

а) Основен речник на ЕС в областта на електронното правосъдие;

б) Неквалифицирани видове данни;

в) Списък с кодове за езиците на Европейския съюз.

Също така, когато е приложимо, XML схемите могат да включват съответните стандарти на ETSI, за да се използват техните определения.

4.6. Комисията определя спецификациите за общия API, който се предоставя от прилагащите държави на доставчиците на услуги като средство за достъп до децентрализираната информационна система. Доколкото е възможно и разумно, този API се основава на ETSI TS 104 144 („Определение за интерфейс съгласно Регламент (ЕС) 2023/1543 относно електронните доказателства за националните органи и доставчиците на услуги“).

4.7. По отношение на протоколите за сигурност и автентификация децентрализираната информационна система се основава на протоколи, основани на стандарти, като например:

а) TLS (Transport Layer Security (сигурност на транспортния слой)) за криптирана и удостоверена комуникация по мрежи, подпомагаща взаимната автентификация чрез цифрови сертификати X.509;

б) OAuth/OpenID Connect (OIDC) за сигурна автентификация и оторизация;

в) Инфраструктура на публичния ключ и цифрови подписи за защитен обмен на ключове и проверка на целостта на съобщенията, като се използват цифрови сертификати (X.509), издадени от доверени сертифициращи органи (СО).

5. **Цели за сигурността на информацията и съответни технически мерки**

5.1. За обмена на информация чрез децентрализираната информационна система техническите мерки за гарантиране на минимални стандарти за сигурност на информационните технологии включват:

а) мерки, с които се гарантира поверителността на информацията, включително чрез използване на сигурни канали за комуникация;

б) мерки, с които се гарантира целостта на данните (съобщения, формуляри, документи и електронни доказателства) в покой и в процес на пренос;

в) мерки, с които се гарантира невъзможността за заличаване на произхода на подателя на информацията в децентрализираната информационна система и невъзможността за отказване на получаването на информацията;

г) мерки, с които се гарантира наличност чрез осигуряване на непрекъснат достъп до услуги и данни, предотвратяване на смущения, дължащи се на кибератаки или повреди;

д) мерки за осигуряване регистрирането на инцидентите, свързани със сигурността, в съответствие с приетите международни препоръки за стандарти за сигурност на информационните технологии;

е) мерки, с които се гарантират автентификацията и оторизацията на ползвателя, и мерки, с които се проверява идентификацията на системите, свързани с децентрализираната информационна система.

5.2. Компонентите на децентрализираната информационна система гарантират защитена комуникация и предаване на данни чрез използване на криптиране, инфраструктура на публичен ключ с цифрови сертификати за автентификация и защитен обмен на ключове, както и протоколи за сигурен обмен на съобщения като AS4 (ebMS), RESTful API и SOAP, за да се запазят поверителността и целостта на съобщенията.

5.3. Компонентите на децентрализираната информационна система се разработват в съответствие с принципа на защита на данните на етапа на проектирането и по подразбиране, и се прилагат подходящи административни, организационни и технически мерки, за да се гарантира високо ниво на киберсигурност.

5.4. Комисията проектира, разработва и поддържа образеца на софтуерно приложение за свързване в съответствие с изискванията и принципите за защита на данните, установени в Регламент (ЕС) 2018/1725. Образецът на софтуерно приложение за свързване, предоставен от Комисията, позволява на държавите членки да изпълняват задълженията си съответно съгласно Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета ([4]) и Директива (ЕС) 2016/680 на Европейския парламент и на Съвета ([5]), според случая.

5.5. Държавите членки, които използват национална информационна система, различна от образеца на софтуерно приложение за свързване, прилагат необходимите мерки, за да гарантират, че тя отговаря на изискванията на Регламент (ЕС) 2016/679 и Директива (ЕС) 2016/680, според случая.

5.6. Като вземат предвид участието си в децентрализираната информационна система, Евроюст и Европейската прокуратура прилагат необходимите мерки, за да гарантират, че съответните им информационни системи отговарят на изискванията на Регламент (ЕС) 2018/1725 и на техните учредителните актове.

5.7. За информационните системи, които са част от децентрализираната информационна система под тяхна отговорност, държавите членки, Евроюст и Европейската прокуратура създават стабилни механизми за откриване на заплахи и реагиране на инциденти, за да се гарантира своевременно идентифициране, смекчаване и възстановяване от инциденти, свързани със сигурността, в съответствие с техните съответни политики.

6. **Криптиране на електронни доказателства** ([6])

6.1. Без да се засягат мерките за сигурност, предвидени от децентрализираната информационна система, при издаването на европейска заповед за предоставяне компетентните органи могат допълнително да предоставят специален публичен сертификат X.509 за асиметрично криптиране на електронни доказателства.

([4]) 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).

([5]) Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни, и за отмяна на Рамково решение 2008/977/ПВР на Съвета (ОВ L 119, 4.5.2016 г., стр. 89).

([6]) За избягване на съмнения, понятието „електронни доказателства“ се ограничава до определението, предвидено в член 3, параграф 8 от Регламент (ЕС) 2023/1543.

6.2. Издаването, управлението, проверката и всички свързани аспекти на сертификатите, посочени в точка 6.1, заедно със съответната инфраструктура на публичния ключ, са отговорност единствено на издаващата държава.

6.3. Без да се засяга бъдещото технологично развитие, публичните сертификати трябва да поддържат стандартни за сектора алгоритми за криптиране, като например RSA (Rivest-Shamir-Adleman) или ECDH (Elliptic Curve Diffie-Hellman (Елиптична крива на Diffie-Hellman) за ECC (Elliptic Curve Cryptography (криптография по елиптична крива).

6.4. Публичните сертификати съдържат подходящото keyUsage разширение, като например keyEncipherment или dataEncipherment за сертификати, базирани на RSA, и keyAgreement за сертификати, базирани на ECC. Сертификатите се предоставят във формат PEM (Privacy-Enhanced Mail) или DER (Distinguished Encoding Rules).

6.5. Когато издаващият орган е предоставил публичен сертификат X.509 и когато доставчик на услуги изпраща предоставените електронни доказателства съгласно европейска заповед за предоставяне, преди предаването на тези данни чрез децентрализираната информационна система доставчикът криптира електронните доказателства, като използва съответния публичен сертификат X.509, осигурен от издаващата държава.

6.6. Когато издаващият орган е предоставил публичен сертификат X.509, но предаването на електронни доказателства в криптирана форма не е възможно поради технически или други основателни причини и без да се засяга разпоредбата на член 19, параграф 5 от Регламент (ЕС) 2023/1543, доставчикът на услуги може да предаде данните без криптиране на съдържанието. В такива случаи доставчикът на услуги предоставя мотивирано обяснение на издаващия орган.

7. **Цели за минимална наличност**

7.1. Държавите членки, Евроюст и Европейската прокуратура осигуряват наличност на компонентите на децентрализираната информационна система, за която отговарят, 24 часа, 7 дни в седмицата, с целеви процент на техническа наличност от най-малко 98 % годишно, с изключение на планираните дейности по поддръжка.

7.2. Комисията осигурява наличност на базата данни за съдилищата 24 часа, 7 дни в седмицата, с целева степен на техническа наличност от над 99 % годишно, с изключение на планираните дейности по поддръжка.

7.3. Доколкото е възможно, в работните дни операциите по поддръжка се планират между 20:00 и 7:00 часа централноевропейско време.

7.4. Държавите членки, Евроюст и Европейската прокуратура уведомяват Комисията и другите държави членки за дейностите по поддръжка, както следва:

а) 5 работни дни предварително за поддръжка, която може да блокира достъпа до системата за срок до 4 часа;

б) 10 работни дни предварително за поддръжка, която може да блокира достъпа до системата за срок между 4 и 12 часа;

в) 30 работни дни предварително за поддръжка, която може да блокира достъпа до системата за срок, по-дълъг от 12 часа;

7.5. Когато държавите членки, Евроюст или Европейската прокуратура имат фиксирани редовни периоди за поддръжка, те информират Комисията и участниците в децентрализираната информационна система за часа и деня (дните), в който (които) са планирани тези фиксирани редовни периоди. Независимо от задълженията, посочени в точка 7.4, в случай че компонентите на децентрализираната информационна система, за които отговарят държавите членки, Евроюст или Европейската прокуратура, станат недостъпни по време на такъв фиксиран редовен период, те могат да решат да не уведомяват Комисията всеки път.

7.6. В случай на неочаквана техническа неизправност на компонентите на децентрализираната информационна система, за която отговарят държавите членки, Евроюст или Европейската прокуратура, те незабавно информират Комисията и участниците в децентрализираната информационна система за тази неизправност и, ако е известен, за прогнозния срок за възстановяване.

7.7. В случай на дейности по поддръжка или неочаквана техническа неизправност на компонентите в децентрализираната информационна система, за която отговаря дадена държава членка, с неблагоприятно въздействие върху наличността на API и/или уеб базирания интерфейс за доставчиците на услуги, съответната държава членка незабавно предоставя тази информация на уебсайт и/или я съобщава на доставчиците на услуги, извършващи дейност на нейна територия, без ненужно забавяне.

7.8. В случай на неочаквана техническа неизправност на базата данни за съдилищата Комисията незабавно информира държавите членки, Евроюст и Европейската прокуратура за това, че не е налична и ако е известен, за прогнозния срок за възстановяване.

7.9. В случай на прекъсване на услугата държавите членки, Евроюст и Европейската прокуратура гарантират бързо възстановяване на услугата и минимална загуба на данни в съответствие с целевото време за възстановяване и целевата точка на възстановяване.

7.10. Държавите членки, Евроюст и Европейската прокуратура прилагат подходящи мерки за постигане на посочените по-горе цели относно наличността и установяват процедури за ефективно реагиране при инциденти.

8. **База данни за съдилищата/компетентните органи (CDB)**

8.1. Като се има предвид член 19 от Регламент (ЕС) № 2023/1543, за целите на функционирането на децентрализираната информационна система е от съществено значение да се създаде достоверна база данни за доставчиците на услуги и компетентните органи.

8.2. Достоверната база данни за компетентните органи включва следната информация в структуриран формат:

а) за целите на член 19 от Регламент (ЕС) 2023/1543 — информация за компетентните органи, нотифицирани съгласно член 31, параграф 1, буква а) — в) от него, включително по отношение на:

1) националните членове на Евроюст, заедно с указание за това дали са упълномощени съгласно националното право да издават европейски заповеди за предоставяне и европейски заповеди за запазване по смисъла на член 8, параграфи 3 и 4 от Регламент (ЕС) 2018/1727 на Европейския парламент и на Съвета ([7]);

2) европейските делегирани прокурори и европейските прокурори, когато са уведомени от държавите членки в съответствие с член 105, параграф 3 от Регламент (ЕС) 2017/1939 на Съвета ([8]) като компетентен издаващ орган по смисъла на Регламент (ЕС) 2023/1543;

б) когато е приложимо, информация, необходима за определяне на географските области на компетентност на органите, или други съответни критерии, необходими за установяване на тяхната компетентност;

в) информация, необходима за правилното функциониране на обмена на данни и за техническото маршрутизиране на съобщенията в рамките на децентрализираната информационна система.

8.2.1. Информацията, посочена в точка 8.2, буква в), включва следното:

а) информация за държавата членка, в която е установена определената форма на установяване на доставчика на услуги или в която пребивава неговият представител:

1) държава членка;

2) централен орган;

([7]) Регламент (ЕС) 2018/1727 на Европейския парламент и на Съвета от 14 ноември 2018 година относно Агенцията на Европейския съюз за сътрудничество в областта на наказателното правосъдие (Евроюст) и за замяна и отмяна на Решение 2002/187/ПВР на Съвета (ОВ L 295, 21.11.2018 г., стр. 138).

([8]) Регламент (ЕС) 2017/1939 на Съвета от 12 октомври 2017 година за установяване на засилено сътрудничество за създаване на Европейска прокуратура (ОВ L 283, 31.10.2017 г., стр. 1).

б) информация за доставчика на услуги:

1) наименование;

2) адрес/седалище;

3) регистрационен номер;

4) правна форма;

5) телефонен номер;

6) електронна поща;

в) информация за определената форма на установяване/представителя:

1) вид на образуването (определена форма на установяване/представител);

2) наименование;

3) адрес/седалище;

4) телефонен номер;

5) електронна поща;

6) лице/образувание за контакти;

7) официалните езици, приети от доставчика на услуги/определената форма на установяване/представителя;

8) услуги, посочени в член 2, параграф 1 от Директива (ЕС) 2023/1544 на Европейския парламент и на Съвета ([9]), предлагани в Съюза;

9) вид правни инструменти на ЕС, за които се определя определената форма на установяване/представителят (в случаите, когато държавите членки не участват във всички съответни правни инструменти на ЕС);

10) териториален обхват на определянето/назначаването;

г) автентификация на информацията:

1) име на упълномощения представител;

2) длъжност;

3) адрес;

4) телефонен номер;

5) електронна поща;

6) дата.

8.2.2. Когато е налична, информацията, посочена в точка 8.2, буква в), може да включва:

а) информация за доставчика на услуги:

1) лице за контакти за запитвания относно уведомленията (ако е различно от подписващото лице);

2) уебсайт;

б) видове налични данни:

1) за всяка засегната услуга:

— видове налични данни;

— категория на данните;

— идентификатори;

— период на наличност на данните;

([9]) Директива (ЕС) 2023/1544 на Европейския парламент и на Съвета от 12 юли 2023 година за установяване на хармонизирани правила относно определянето на определени форми на установяване и определянето на представители за целите на събирането на електронни доказателства по наказателни производства (ОВ L 191, 28.7.2023 г., стр. 181, ELI: http://data.europa.eu/eli/dir/2023/1544/oj).

2) допълнителна информация за данните;

3) допълнителна информация за услугата (напр. отношения с подизпълнители);

в) информация за определената форма на установяване/представителя:

1) други доставчици на услуги, за които е определена тази определена форма на установяване или представител;

2) информация за контакти за техническа помощ;

3) информация за контакт при извънредни ситуации;

г) техническа информация:

1) наименование на техническото звено за контакт;

2) телефонен номер на техническото звено за контакт;

3) електронна поща на техническото звено за контакт;

4) URL адрес на API за динамично извличане на информация за видовете данни;

(5) вид на връзката с националната информационна система:

— уеб базиран интерфейс;

— API;

— URL адрес на Push API (API за насочени известия).

8.3. С оглед на оперативните нужди на децентрализираната информационна система:

а) Комисията отговаря за разработването, поддръжката, експлоатацията и поддръжката на достоверната база данни;

б) Комисията осигурява възможността за достъп до достоверната база данни чрез API, предоставен на компетентните органи, Евроюст и Европейската прокуратура за целите на участието им в децентрализираната информационна система;

в) Държавите членки гарантират, че информацията за техните компетентни органи, посочена в точка 8.2, букви а) и б), в достоверната база данни е пълна, точна и актуална;

г) достоверната база данни дава възможност на държавите членки да предоставят и актуализират информацията за своите доставчици на услуги в нея, както и на органите, участващи в децентрализираната информационна система, да имат програмиран достъп до тази информация и да я извличат;

д) държавите членки и доставчиците на услуги гарантират, че информацията, посочена в точка 8.2, буква в) в достоверната база данни, е пълна, точна и актуална.