2025/2447

5.12.2025 г.

РЕГЛАМЕНТ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2025/2447 НА КОМИСИЯТА

от 4 декември 2025 година

за определяне на правилата за прилагане на Регламент (ЕС) 2018/1727 на Европейския парламент и на Съвета по отношение на техническите спецификации, мерки и други изисквания за създаването и използването на децентрализираната информационна система за сигурно обработване и съобщаване на информация

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид Регламент (ЕС) 2018/1727 на Европейския парламент и на Съвета от 14 ноември 2018 г. 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 ([1]), и по-специално член 22а, параграф 3 и член 22б, параграф 1, букви а), б), в) и г) от него,

като има предвид, че:

(1) С Регламент (ЕС) 2018/1727 се определя рамката за новата цифрова вътрешна инфраструктура на Евроюст и за създаването на децентрализирана система за сигурна цифрова комуникация между компетентните национални органи на държавите членки и Евроюст.

(2) Сигурната цифрова комуникация трябва да се осъществява чрез децентрализираната информационна система. За създаването на децентрализираната информационна система е необходимо да се определят технически спецификации, определящи методите за комуникация и протоколите за комуникация, технически мерки, с които се гарантират минимални стандарти за сигурност на информацията и киберсигурност, както и цели за минимална наличност за внедряването на тази система.

(3) В съответствие с член 22а, параграф 1 от Регламент (ЕС) 2018/1727 децентрализираната информационна система трябва да се състои от информационните системи на държавите членки и Евроюст, както и от оперативно съвместими точки за достъп до e-CODEX, чрез които тези информационни системи са свързани помежду си. Тази рамка следва да бъде взета предвид при техническите спецификации и другите определени в настоящия регламент изисквания за децентрализираната информационна система.

(4) Точките за достъп на децентрализираната информационна система следва да се основават на разрешените 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]).

(5) Тази децентрализирана информационна система се въвежда в рамките на по-голяма, основаваща се на e-CODEX, децентрализирана информационна система, наречена Justice Digital Exchange System (JUDEX). Поради това е необходимо да се гарантира ефективен обмен на информация относно хоризонталните разработки.

(6) В съответствие с член 22а, параграф 4 от Регламент (ЕС) 2018/1727 държавите членки и Евроюст могат да изберат да използват разработения от Комисията образец на софтуерно приложение за свързване като своя сървърна 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.

(7) Данните, свързани с терористични престъпления и тежка организирана престъпност, следва да се предават по структуриран начин, за да се подобрят качеството и относимостта на информацията, както и за да се гарантира, че информацията може да бъде по-ефикасно интегрирана в системата за управление на делата на Евроюст и по-добре подлагана на кръстосана проверка спрямо информацията, която вече се съхранява в тази система. По отношение на данните за пръстови отпечатъци и снимките, които могат да бъдат предавани на Евроюст с цел установяване на самоличността на лица, които са обект на наказателно производство, свързано с терористични престъпления, следва да се определят форматът и техническите стандарти за предаването.

([1]) ОВ L 295, 21.11.2018 г., стр. 138, ELI: http://data.europa.eu/eli/reg/2018/1727/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).

(8) Евроюст улеснява и подпомага издаването и изпълнението на исканията за съдебно сътрудничество, включително искания и решения, основани на инструменти, които привеждат в действие принципа на взаимно признаване. Националните компетентни органи следва да могат да търсят помощ и координация от Евроюст чрез децентрализираната информационна система.

(9) За да се гарантират ефикасност и съгласуваност, е важно техническите спецификации, които предстои да бъдат установени съгласно Регламент (ЕС) 2018/1727, да бъдат съвместими с техническите спецификации, установени съгласно регламенти (ЕС) 2023/2844 ([3]), (ЕС) 2023/1543 ([4]) и (ЕС) 2024/3011 на Европейския парламент и на Съвета ([5]), както и със свързаните с мандата на Евроюст бъдещи мерки за цифровизация, за да се подпомагат националните компетентни органи.

(10) Всяка друга комуникация между Евроюст и компетентните национални органи, като например съобщаването на информация за резултатите от обработването на информация, включително наличието на връзки със случаи, които вече са въведени в системата за управление на делата в съответствие с член 22 от Регламент (ЕС) 2018/1727, когато Евроюст действа по собствена инициатива, или на информация, предадена на Евроюст с цел запазване, анализиране и съхранение на доказателства, свързани с геноцид, престъпления против човечеството, военни престъпления и свързани престъпления, в съответствие с член 4, параграф 1, буква й) от посочения регламент, следва да бъде възможна и чрез децентрализираната информационна система.

(11) За да се гарантира, че с настоящия регламент се отчитат оперативните нужди на Евроюст, бяха проведени консултации с Евроюст в съответствие с член 22а, параграф 3 от Регламент (ЕС) 2018/1727.

(12) В съответствие с член 4 от Протокол № 21 относно позицията на Обединеното кралство и Ирландия по отношение на пространството на свобода, сигурност и правосъдие, приложен към Договора за Европейския съюз и към Договора за функционирането на Европейския съюз, Ирландия, с писмо от 9 септември 2019 г., е нотифицирала желанието си да приеме и да бъде обвързана от Регламент (ЕС) 2018/1727. С Решение (ЕС) 2019/2006 на Комисията ([6]) това участие беше потвърдено. Регламент (ЕС) 2018/1727 беше изменен с Регламент (ЕС) 2023/2131 на Европейския парламент и на Съвета ([7]), за да се даде възможност за създаване на сигурни цифрови канали за комуникация между Евроюст и компетентните национални органи, и с това се осигурява правното основание за настоящия регламент. При обстоятелства, при които Ирландия не е нотифицирала желанието си да участва в приемането и прилагането на Регламент (ЕС) 2023/2131 и не е нотифицирала желанието си да приеме и да бъде обвързана от посочения регламент, Ирландия, в съответствие с членове 1 и 2 и член 4а, параграф 1 от Протокол № 21, не е обвързана от Регламент (ЕС) 2023/2131, нито от неговото прилагане. Поради това Ирландия не участва в приемането на настоящия регламент.

(13) 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 участва в приемането на Регламент (ЕС) 2018/1727. Следователно Дания не е обвързана от настоящия регламент, нито от неговото прилагане.

([3]) Регламент (ЕС) 2023/2844 на Европейския парламент и на Съвета от 13 декември 2023 г. относно цифровизацията на съдебното сътрудничество и на достъпа до правосъдие по трансгранични гражданскоправни, търговскоправни и наказателноправни въпроси и за изменение на определени актове в областта на съдебното сътрудничество (ОВ L, 2023/2844, 27.12.2023 г., ELI: http://data.europa.eu/eli/reg/2023/2844/oj).

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

([5]) Регламент (ЕС) 2024/3011 на Европейския парламент и на Съвета от 27 ноември 2024 г. относно трансфера на производства по наказателни дела (ОВ L, 2024/3011, 18.12.2024 г., ELI: http://data.europa.eu/eli/reg/2024/3011/oj).

([6]) Решение (ЕС) 2019/2006 на Комисията от 29 ноември 2019 година относно участието на Ирландия в Регламент (ЕС) 2018/1727 на Европейския парламент и на Съвета относно Агенцията на Европейския съюз за сътрудничество в областта на наказателното правосъдие (Евроюст) (ОВ L 310, 2.12.2019 г., стр. 59, ELI: https://eur-lex.europa.eu/eli/dec/2019/2006/oj).

([7]) Регламент (ЕС) 2023/2131 на Европейския парламент и на Съвета от 4 октомври 2023 година за изменение на Регламент (ЕС) 2018/1727 на Европейския парламент и на Съвета и на Решение 2005/671/ПВР на Съвета по отношение на цифровия обмен на информация по дела за тероризъм (ОВ L, 2023/2131, 11.10.2023 г., ELI: https://eur-lex.europa.eu/eli/reg/2023/2131/oj).

(14) В съответствие с член 42, параграф 1 от Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета ([8]) беше проведена консултация с Европейския надзорен орган по защита на данните, който прие становище на 21 октомври 2025 г.

(15) Мерките, предвидени в настоящия регламент, са в съответствие със становището на комитета, създаден по силата на член 22в от Регламент (ЕС) 2018/1727,

ПРИЕ НАСТОЯЩИЯ РЕГЛАМЕНТ:

Член 1

Технически спецификации на децентрализираната информационна система

Техническите спецификации и мерки и целите на децентрализираната информационна система, посочени в член 22б, параграф 1, букви а), б), в) и г) от Регламент (ЕС) 2018/1727, са определени в приложение I към настоящия регламент.

Член 2

Цифрови процедурни стандарти

Цифровите процедурни стандарти, приложими за електронната комуникация чрез децентрализираната информационна система, посочени в член 22а, параграф 3 от Регламент (ЕС) 2018/1727, са определени в приложение II към настоящия регламент.

Член 3

Технически спецификации за предаването на пръстови отпечатъци и снимки

Техническите спецификации и форматът за предаването на пръстови отпечатъци и снимки, посочени в член 22а, параграф 3 от Регламент (ЕС) 2018/1727, са определени в приложение III към настоящия регламент.

Член 4

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 4 декември 2025 година.

За Комисията
Председател
Ursula VON DER LEYEN

([8]) 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

ТЕХНИЧЕСКИ СПЕЦИФИКАЦИИ, МЕРКИ И ЦЕЛИ НА ДЕЦЕНТРАЛИЗИРАНАТА ИНФОРМАЦИОННА СИСТЕМА

1. **Въведение и приложно поле**

В настоящото приложение се определят техническите спецификации, мерките и целите за децентрализираната информационна система за обмен на информация по Регламент (ЕС) 2018/1727.

Децентрализираният характер на информационната система дава възможност за пряк и сигурен обмен на данни между компетентните национални органи и Евроюст.

2. **Определения**

За целите на настоящото приложение се прилагат следните определения:

2.1. „Hypertext Transfer Protocol Secure“ или „HTTPS“ означава канали за сигурна връзка и криптирана комуникация;

2.2. „невъзможност за отричане на произхода“ означава мерките, предоставящи доказателство за цялостността 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 отричане 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, електронни подписи и електронни печати;

2.4. „SOAP“ (Simple Object Access Protocol) означава, съгласно стандартите на Консорциума на световната мрежа (World Wide Web Consortium), спецификация на протокол за съобщения за обмен на структурирана информация в изпълнение на уеб услуги в компютърни мрежи;

2.5. „REST“ (Representational State Transfer) 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 и документи чрез децентрализираната информационна система;

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

2.9. „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;

2.10. „ebMS“ се отнася до услугата ebXML Messaging Service — протокол за съобщения, разработен съгласно рамката OASIS, който дава възможност за сигурен, надежден и оперативно съвместим обмен на електронни бизнес документи чрез SOAP. С ebMS се подпомага интеграцията между предприятията в различни системи;

2.11. „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;

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

2.13. „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 обмена на съобщения и документи децентрализираната информационна система използва основани на услуги методи за комуникация, като например уеб услуги или други повторно използваеми компоненти и софтуерни решения.

3.2. По-специално децентрализираната информационна система 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.

4. **Протоколи за комуникация**

4.1. Децентрализираната информационна система използва сигурни интернет протоколи за:

а) комуникация в рамките на децентрализираната информационна система между компетентните органи и Евроюст;

б) комуникация с базата данни за компетентните органи/съдилища, както е посочено в точка 7.1.

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 RESTful.

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 отричане;

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 протоколите за комуникация, използвани от децентрализираната информационна система, отговарят на съответните стандарти за оперативна съвместимост.

4.5. Когато е приложимо, XML схемите използват съответните стандарти или речници, които са необходими за правилното валидиране на елементите и типовете, определени в рамките на схемата. Тези стандарти или речници могат 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.

4.6. 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 даване на права;

в) PKI (инфраструктура на публичен ключ) и цифрови подписи за защитен обмен на ключове и проверка на цялостността на съобщенията, като се използват цифрови сертификати (X.509), издадени от доверени сертифициращи органи.

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 следното:

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

б) мерки, с които се гарантира цялостността на данните в покой и в процес на пренос;

в) мерки, с които се гарантират невъзможността за отричане на произхода на подателя на информацията в децентрализираната информационна система и невъзможността за отричане на получаването на информацията;

г) мерки, с които се гарантира регистрирането на инцидентите, свързани със сигурността, в съответствие с признатите международни препоръки за стандарти за сигурност на информационните технологии ([1]);

д) мерки, с които се гарантират автентификацията и даването на права 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 публичния 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 цялостността на съобщенията.

5.3. Когато се използва TLS в контекста на децентрализираната информационна система, се използва последната стабилна версия на протокола или, ако това не е възможно, версия без известни уязвимости по отношение на сигурността. Допускат се само дължини на ключовете, които осигуряват адекватно равнище на криптографска сигурност, и не се използват поредици от шифри, за които е известно, че са несигурни или остарели.

5.4. Доколкото е възможно, цифровите PKI сертификати, използвани за целите на функционирането на децентрализираната информационна система, се издават от сертифициращите органи, признати за доставчици на квалифицирани удостоверителни услуги в съответствие с Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета ([2]). Прилагат се мерки, за да се гарантира, че тези сертификати се използват единствено за целите, за които са предназначени, при необходимото равнище на доверие и в съответствие с приложимите изисквания на Регламент (ЕС) № 910/2014.

5.5. 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.

5.6. 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 в съответствие с Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета ([3]) и Директива (ЕС) 2016/680, според случая.

([1]) Без да се засяга регистрирането за целите на сигурността, механизмите за регистриране, използвани от компонентите на децентрализираната информационна система, позволяват, когато е целесъобразно, да се гарантира спазването на изискванията, посочени в член 88 от Регламент (ЕС) 2018/1725 и, когато е приложимо, в член 25 отДиректива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 година 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, ELI: http://data.europa.eu/eli/dir/2016/680/oj).

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

([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).

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

5.8. Евроюст прилага необходимите мерки, за да гарантира, че нейната сървърна система или вариантът на образеца на софтуерно приложение за свързване, който внедрява, отговаря на изискванията на регламенти (ЕС) 2018/1725 и (ЕС) 2018/1727.

5.9. За информационните системи под тяхна отговорност, които са част от децентрализираната информационна система, държавите членки и Евроюст 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. **Цели за минимална наличност**

6.1. Евроюст и държавите членки осигуряват наличност на компонентите на децентрализираната информационна система, за които отговарят, 24 часа, 7 дни в седмицата, с целева степен на техническа наличност от най-малко 98 % годишно, с изключение на планираните дейности по поддръжка.

6.2. 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.

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

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

а) 5 работни дни предварително за операции по поддръжка, които могат да блокират достъпа до системата за срок до 4 часа;

б) 10 работни дни предварително за операции по поддръжка, които могат да блокират достъпа до системата за срок между 4 и 12 часа;

в) 30 работни дни предварително за операции по поддръжка, които могат да блокират достъпа до системата за срок, по-дълъг от 12 часа.

6.5. Когато държавите членки имат фиксирани редовни периоди за поддръжка, те информират Комисията, Евроюст и другите държави членки за часа и деня/дните, в който/които са планирани тези фиксирани редовни периоди. Чрез дерогация от задълженията, посочени в първото изречение, ако компонентите на децентрализираната информационна система, за които отговарят държавите членки, стават недостъпни по време на такъв фиксиран редовен период, държавите членки могат да решат да не уведомяват Комисията във всеки отделен случай.

6.6. В случай на неочаквана техническа неизправност на компонент на децентрализираната информационна система, за който отговарят държавите членки, държавите членки незабавно информират Комисията и другите държави членки за тази неизправност и, ако е известен, за прогнозния срок за възстановяване.

6.7. Евроюст уведомява Комисията и държавите членки за дейностите по поддръжка, както следва:

а) 5 работни дни предварително за операции по поддръжка, които могат да блокират достъпа до системата за срок до 4 часа;

б) 10 работни дни предварително за операции по поддръжка, които могат да блокират достъпа до системата за срок между 4 и 12 часа;

в) 30 работни дни предварително за операции по поддръжка, които могат да блокират достъпа до системата за срок, по-дълъг от 12 часа.

6.8. Когато Евроюст има фиксирани редовни периоди за поддръжка, агенцията информира Комисията и държавите членки за часа и деня/дните, в който/които са планирани тези фиксирани редовни периоди. Чрез дерогация от задълженията, посочени в първото изречение, ако компонентите на децентрализираната информационна система, за които отговаря Евроюст, станат недостъпни по време на такъв фиксиран редовен период, Евроюст може да реши да не уведомява Комисията във всеки отделен случай.

6.9. В случай на неочаквана техническа неизправност на компонент на децентрализираната информационна система, за който отговаря Евроюст, агенцията незабавно информира Комисията и държавите членки за тази неизправност и, ако е известен, за прогнозния срок за възстановяване.

6.10. В случай на неочаквана техническа неизправност на базата данни за компетентните органи/съдилища Комисията незабавно информира Евроюст и държавите членки за недостъпността и, ако е известен, за прогнозния срок за възстановяване.

6.11. В случай на прекъсване на услугата държавите членки и Евроюст гарантират, че услугата се възстановява бързо, а загубата на данни е минимална, в съответствие с целевото време за възстановяване и целевата точка на възстановяване.

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

7. **База данни за компетентните органи/съдилища**

7.1. Съгласно член 22а от Регламент (ЕС) 2018/1727 децентрализираната информационна система дава възможност за електронна комуникация между компетентните национални органи и Евроюст. Като се имат предвид задълженията за обмен на информация между компетентните национални органи и Евроюст съгласно членове 21, 21а и 22, както и ролята на Евроюст за улесняване и подкрепяне на издаването и изпълнението на искания за правна взаимопомощ или взаимно признаване в съответствие с член 8, параграф 1 от Регламент (ЕС) 2018/1727, участващите компетентни органи трябва да могат да бъдат ясно идентифицирани, когато използват децентрализираната информационна система. Поради това е от съществено значение да се създаде достоверна база данни с информация за тези органи за целите на децентрализираната информационна система.

7.2. Базата данни за компетентните органи/съдилища включва следната информация в структуриран формат:

а) за целите на член 8, параграфи 1, 3 и 4 и членове 21, 21a и 22 от Регламент (ЕС) 2018/1727 — информация относно компетентните национални органи, включително националните кореспонденти, посочени в член 20 от посочения регламент, както и националните членове в съответствие с член 7 ([4]) от посочения регламент;

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

в) информация, необходима за правилното техническо маршрутизиране на съобщенията в рамките на децентрализираната информационна система.

7.3. Комисията отговаря за разработването, поддръжката, експлоатацията и подпомагането на базата данни за компетентните органи/съдилища.

7.4. Базата данни за компетентните органи/съдилища дава възможност на държавите членки и Евроюст да актуализират информацията в нея, а на компетентните национални органи и националните членове, участващи в децентрализираната информационна система — да имат програмиран достъп до тази информация и да я извличат.

7.5. Достъпът до базата данни за компетентните органи/съдилища е възможен чрез общ протокол за комуникация, независимо дали компетентните органи, свързани с децентрализираната информационна система, управляват национална сървърна система, или са внедрили образеца на софтуерно приложение за свързване.

7.6. Държавите членки гарантират, че информацията относно техните компетентни органи в базата данни за компетентните органи/съдилища, посочена в точка 7.2, е пълна, точна и актуална.

([4]) Това не засяга делегирането на правомощия от националния член на неговия заместник, друг служител в националното бюро или оправомощен служител на Евроюст.

ПРИЛОЖЕНИЕ II

ЦИФРОВИ ПРОЦЕДУРНИ СТАНДАРТИ

В член 3, параграф 9 от Регламент (ЕС) 2022/850 цифровите процедурни стандарти се определят като техническите спецификации за моделите на работния процес и за схемите на данните, които спецификации определят електронната структура на данните, обменяни чрез системата e-CODEX.

В настоящото приложение се определят техническите спецификации за моделите на работния процес и техническите спецификации за схемите на данните.

1. **Технически спецификации за моделите на работния процес съгласно Регламент (ЕС) 2018/1727**

Техническите спецификации за моделите на работния процес са изложени в точки 1.1—1.5. В тях се определят ключовите аспекти, необходими за осигуряването на възможност за електронна комуникация за целите на Регламент (ЕС) 2018/1727 чрез децентрализираната информационна система.

Децентрализираната информационна система позволява обмен на информация само между компетентните национални органи на дадена държава членка и националния член от тази държава членка.

1.1. *Обмен на информация, свързана със Съдебния регистър в областта на борбата с тероризма (член 21а от Регламент (ЕС) 2018/1727)*

1.1.1. Модел за предаване на данни за Съдебния регистър в областта на борбата с тероризма:

компетентният национален орган предава на националния член данни за производства, свързани с тероризъм, за целите на Съдебния регистър в областта на борбата с тероризма.

1.1.2. Модел за получаване на данни за Съдебния регистър в областта на борбата с тероризма:

националният член получава данните за Съдебния регистър в областта на борбата с тероризма.

1.1.3. Модел за искане за съгласие:

националният член иска съгласието на своя компетентен национален орган.

1.1.4. Модел за получаване на искане за съгласие:

компетентният национален орган получава искането за съгласие.

1.1.5. Модел за изпращане на отговор на искане за съгласие:

компетентният национален орган изпраща отговор на искането за съгласие.

1.1.6. Модел за получаване на отговор на искане за съгласие:

националният член получава отговора на искането за съгласие.

1.1.7. Модел за информиране за връзка:

националният член информира компетентния национален орган за връзката с друг случай.

1.1.8. Модел за актуализиране на данни за Съдебния регистър в областта на борбата с тероризма:

компетентният национален орган предава на съответния си национален член данни, за които се изисква актуализиране или заличаване.

1.1.9. Модел за получаване на актуализирани данни за Съдебния регистър в областта на борбата с тероризма:

националният член получава данните за Съдебния регистър в областта на борбата с тероризма, за които се изисква актуализиране или заличаване.

1.2. *Обмен на информация, свързана с тежки престъпления (член 21 от Регламент (ЕС) 2018/1727)*

1.2.1. Модел за предаване на данни за тежка престъпност с трансгранично измерение:

националният компетентен орган предава на Евроюст данни за тежка престъпност с трансгранично измерение.

1.2.2. Модел за получаване на данни за тежка престъпност с трансгранично измерение:

националният член получава данните за тежка престъпност с трансгранично измерение.

1.2.3. Модел за искане за съгласие:

националният член иска съгласието на своя национален компетентен орган.

1.2.4. Модел за получаване на искане за съгласие:

компетентният национален орган получава искането за съгласие.

1.2.5. Модел за изпращане на отговор на искане за съгласие:

компетентният национален орган изпраща отговор на искането за съгласие.

1.2.6. Модел за получаване на отговор на искане за съгласие:

националният член получава отговора на искането за съгласие.

1.2.7. Модел за информиране за връзка:

националният член информира компетентния национален орган за връзката с друг случай.

1.2.8. Модел за актуализиране на данни за тежка престъпност с трансгранично измерение:

компетентният национален орган предава на съответния си национален член данни, за които се изисква актуализиране или заличаване.

1.2.9. Модел за получаване на актуализирани данни за тежка престъпност с трансгранично измерение:

националният член получава данните за тежка престъпност с трансгранично измерение, за които се изисква актуализиране или заличаване.

1.3. *Обмен на обща информация*

1.3.1. Модел за изпращане на информация:

националният член изпраща информация до компетентния национален орган или обратно.

1.3.2. Модел за получаване на информация:

компетентният национален орган или националният член получава информацията.

1.3.3. Модел за отговор на информация:

компетентният национален орган отговаря на информацията, получена от националния член, или обратно.

1.3.4. Модел за получаване на отговор:

националният член получава отговора от компетентния национален орган.

1.3.5. Модел за изпращане на информация:

компетентният национален орган изпраща информация на националния член.

1.3.6. Модел за получаване на информация:

националният член получава информацията.

1.3.7. Модел за отговор на информация:

националният член отговаря на информацията, получена от компетентния национален орган.

1.3.8. Модел за получаване на отговор:

компетентният национален орган получава отговора от компетентния националния член.

1.4. *Роля по улесняване и подкрепа (член 8, параграф 1 от Регламент (ЕС) 2018/1727)*

Бележка: Когато посочените в точка 1.5 модели за улесняване и подкрепа включват обмен на законоустановени формуляри, установени с правни актове на Съюза в областта на съдебното сътрудничество по наказателноправни въпроси, моделите използват, когато са налични, съответните разработени за тези актове представяния на структурирани данни и XML схеми, например създадените за целите на прилагането на Регламент (ЕС) 2023/2844 или други относими инструменти.

1.5. *Модел за искане за улесняване или подкрепа*

1.5.1. Модел за предаване на искане за улесняване или подкрепа:

националният компетентен орган предава на съответния си национален член искане за улесняване или искане за подкрепа.

1.5.2. Модел за получаване на искане за улесняване или подкрепа:

националният член получава искането за улесняване или подкрепа и го препраща на националния член на замолената държава членка извън JUDEX.

1.5.3. Модел за препращане на искане за улесняване или подкрепа до компетентния национален орган:

националният член на замолената държава членка изпраща искането до съответния компетентен национален орган.

1.5.4. Модел за получаване на искане за улесняване или подкрепа:

компетентният национален орган получава искането за улесняване или подкрепа.

1.5.5. Модел за изпращане на отговор на искане за улесняване или подкрепа:

компетентният национален орган изпраща отговор на искането или информация във връзка с него до националния член на замолената държава членка.

1.5.6. Модел за получаване на отговор на искане за улесняване или подкрепа:

националният член получава отговора на искането за улесняване или подкрепа или информация във връзка с него от компетентния национален орган и го/я споделя с националния член на молещата държава членка извън JUDEX.

1.5.7. Модел за отговор на искане за улесняване или подкрепа:

националният член на молещата държава членка отговаря на информацията във връзка с искането за улесняване или подкрепа от компетентния национален орган или я споделя.

1.5.8. Модел за получаване на отговор:

компетентният национален орган получава отговора на искането за улесняване или подкрепа или информацията във връзка с него.

2. **Технически спецификации за схемите на данните**

Техническите спецификации, които трябва да послужат като основа за разработването на дефиниции на XML схемите (XML Schema Definitions (XSD)) за цифровизацията на Регламент (ЕС) 2018/1727, са посочени в точки 2.1 и 2.2 от настоящото приложение. В настоящите спецификации се определят ключовите компоненти и всякаква друга информация, за да се предостави изчерпателно описание за изготвянето на тези схеми.

Описанието е предвидено да бъде общо и да позволява да се изменят и разширяват изготвените XSD, без да са необходими съществени промени в тези спецификации.

Спецификациите се прилагат за законоустановената форма на схемите съгласно приложеното към Регламент (ЕС) 2018/1727, за всички предварително определени съобщения или за всички съобщения със свободен текст, използвани при обмена съгласно посочения регламент.

2.1. *Общи съображения*

За всички схеми, които трябва да бъдат предоставени, се прилагат следните разпоредби:

2.1.1. Версии

Включва се атрибут за версия, който улеснява управлението на версиите на схемата и позволява схемата да бъде актуализирана при бъдещи варианти съгласно изискванията на работния процес. В атрибута за версия се посочва дали новата версия е съвместима с предходните версии, когато се въвеждат нови функции или подобрения.

2.1.2. Декларация за схемата и метаданни

— Когато е приложимо, схемата използва съответните изисквани от e-CODEX с цел осигуряване на оперативната съвместимост стандарти или речници, които са необходими за правилното валидиране на елементите и типовете, дефинирани в рамките на тази схема. Това може да включва следното:

  — Основен речник на ЕС в областта на електронното правосъдие;

  — Неквалифицирани видове данни;

  — Списък с кодове за езиците на Европейския съюз.

— Също така, когато е приложимо, схемата може да включва съответните стандарти на ETSI, за да се използват техните определения.

2.1.3. Анотации и документация

— **Анотации**: Всеки елемент в схемата обикновено се придружава от анотации. С анотациите се предоставя четима от човека информация за елемента, като често по ясен и кратък начин се определят целта или използването му.

2.1.4. Използване и адаптивност

Схемата следва правилата, определени в букви а)—г):

а) **Модулна структура**: всеки раздел се разработва със специфични функции и може да се използва повторно или да се адаптира независимо от останалите. Това прави схемата лесна за персонализиране за различните случаи на използване.

б) **Възможност за разширяване**: схемата се разработва така, че да поддържа включването на нови елементи или атрибути, ако в бъдеще е необходима допълнителна информация. Това се постига чрез използването на незадължителни елементи и поредици, които могат да бъдат разширявани, без да се нарушават съществуващите приложения.

в) **Приспособима структура**: схемата се разработва по начин, който позволява добавянето или изменянето на елементи или видове данни, ако е необходимо. Структурата на схемата се приспособява към промените в изискванията, без да е необходимо значително преработване.

г) **Незадължителни елементи**: елементите в рамките на схемата могат да бъдат обозначени като незадължителни, т.е. могат да бъдат включени или пропуснати въз основа на конкретни обстоятелства.

Схемата се разработва така, че да поддържа събирането на структурирани данни за конкретни искания.

2.1.5. Изменения

Разработката на схемата се характеризира с гъвкавост, модулност и възможност за лесно адаптиране. Сложните видове и незадължителните елементи се включват в разработката по такъв начин, че тя да може да се справя с различни сценарии, като същевременно остава лесна за изменяне и разширяване.

2.2. *Обмен на структурирани данни*

Структурираните данни, посочени в точки 2.2.1 и 2.2.2, се предоставят в съответствие с член 22а, параграф 3 от Регламент (ЕС) 2018/1727. Схемата позволява също така да се посочат наборите от данни, които трябва да бъдат заличени при бъдещи актуализации.

2.2.1. Данни за Съдебния регистър в областта на борбата с тероризма

Със следните технически спецификации за схемата на данните се установява структурирана рамка за създаване на схемата във формат XML.

а) Раздел от най-високо ниво

Този раздел от най-високо ниво съответства на информацията, посочена в приложение III към Регламент (ЕС) 2018/1727, за Съдебния регистър в областта на борбата с тероризма.

б) Структура на съобщението:

Структурата на данните за Съдебния регистър в областта на борбата с тероризма се състои от поредица от елементи и включва най-малко следното:

i) информация за установяване на самоличността на физически лица:

— фамилия (фамилно име);

— собствени имена (лични имена);

— всякакви псевдоними;

— дата на раждане;

— място на раждане (град и държава);

— гражданство на една или повече държави;

— документ за самоличност (вид и номер на документа);

— пол;

— място на пребиваване;

ii) информация за идентификация на юридически лица:

— наименование на предприятието;

— правна форма;

— местонахождение на седалището;

iii) информация за установяване на самоличността на физически лица и за идентификация на юридически лица:

— телефонни номера;

— адреси на електронна поща;

— данни за сметки в банки или в други финансови институции;

— качество в производството;

iv) информация за престъплението:

— информация за юридическите лица, участващи в подготовката или извършването на терористично престъпление;

— правна квалификация на престъплението съгласно националното право;

— приложим вид тежко престъпление от списъка в приложение I;

— всякаква принадлежност към терористична група;

— вид тероризъм, например джихадски, сепаратистки, ляв или десен;

— кратко резюме на делото;

v) информация за националните производства:

— етап на производството;

— отговорна прокуратура;

— номер на делото;

— дата на откриване на официалното съдебно производство;

— връзки с други имащи отношение дела;

vi) поле за допълнителна информация (свободен текст)

vii) код за предварително разрешение

2.2.2. Данни, предадени в съответствие с член 21 от Регламент (ЕС) 2018/1727

a) член 21, параграф 4 от Регламент (ЕС) 2018/1727 за създаване на съвместни екипи за разследване (СЕР)

i) Раздел от най-високо ниво

Този раздел от най-високо ниво съответства на информацията, посочена в член 21, параграф 4 от Регламент (ЕС) 2018/1727, относно създаването на СЕР.

ii) Структура на съобщението

Структурата на данните се състои от поредица от елементи и включва най-малко следното:

— национален съдебен орган, отговарящ за наказателното производство

— национален референтен номер на наказателното производство

— етап на наказателното производство

— престъпления, предмет на разследване

— други държави, участващи в случая

— дали делото вече се подкрепя от Евроюст

— ако отговорът е „да“ — идентификационен номер на делото в Евроюст

— ако отговорът е „не“ — дали това е искане за подкрепа

— дали делото се подкрепя от Европол

— ако отговорът е „да“ — оперативна работна група (ОРГ) и/или мрежовото приложение за защитен обмен на информация (SIENA)?

— споразумение за СЕР:

— участващи държави

— страни по СЕР (национални органи, отговарящи за разследванията)

— национален референтен номер на наказателното производство, обхванато от СЕР

— дата на подписване

— продължителност

— престъпления, предмет на разследване

— кратко резюме на делото

— основни заподозрени в наказателното производство, обхванато от СЕР (име, фамилия, дата и място на раждане и евентуално други относими и необходими категории данни съгласно приложение II)

— резултати от работата на СЕР:

— трудности/закъснения при:

— създаването на СЕР

— искането/споделянето на доказателства в рамките на СЕР

— договарянето/прилагането на обща стратегия за наказателно преследване

— допустимост/недопустимост/оценка на доказателствата на СЕР в национални производства

— резултат от съдебните производства (успешни/неуспешни наказателни преследвания и осъдителни/оправдателни присъди)

iii) Код за предварително разрешение

б) член 21, параграф 5 от Регламент (ЕС) 2018/1727, тежки сложни дела

i) Раздел от най-високо ниво

Този раздел от най-високо ниво съответства на информацията, посочена в член 21, параграф 5 от Регламента за Евроюст, т.е. за тежките сложни дела

ii) Структура на съобщението

Структурата на данните се състои от поредица от елементи и включва най-малко следното:

— национален съдебен орган, отговарящ за наказателното производство

— национален референтен номер на наказателното производство

— етап на наказателното производство

— престъпления, предмет на разследване

— други държави, участващи в случая

— дали делото вече се подкрепя от Евроюст

— ако отговорът е „да“ — идентификационен номер на делото в Евроюст

— ако отговорът е „не“ — дали това е искане за подкрепа

— дали делото се подкрепя от Европол

— ако отговорът е „да“ — оперативна работна група и/или SIENA?

— приложим вид тежко престъпление

— участие на организирана престъпна група

— от мафиотски тип

— трансгранична организирана престъпна група

— отражение на равнището на ЕС

— основни заподозрени в наказателното производство (име, фамилия, дата и място на раждане и евентуално други относими и необходими категории данни съгласно приложение II)

— кратко резюме на делото

— други участващи държави

— държави, с които вече съществува сътрудничество

— компетентни органи, вземащи участие в други държави

— използвани инструменти за съдебно сътрудничество

— брой на изпратените/получените искания

— наличие на свързани разследвания

— държави, с които ще бъде задействано сътрудничество/евентуално засегнати държави

— вид на необходимото сътрудничество (напр. екстрадиция, събиране на доказателства, друго сътрудничество)

— наличие на свързани разследвания

iii) Код за предварително разрешение

в) член 21, параграф 6, буква а) от Регламент (ЕС) 2018/1727, спорове за компетентност

i) Раздел от най-високо ниво

Този раздел от най-високо ниво съответства на информацията, посочена в член 21, параграф 6, буква а) от Регламент (ЕС) 2018/1727, т.е. за споровете за компетентност.

ii) Структура на съобщението

Структурата на данните се състои от поредица от елементи и включва най-малко следното:

— национален съдебен орган, отговарящ за наказателното производство

— национален референтен номер на наказателното производство

— етап на наказателното производство (напр. разследване, наказателно преследване, съдебен процес)

— престъпления, предмет на разследване

— други държави, участващи в случая

— дали делото вече се подкрепя от Евроюст

— ако отговорът е „да“ — идентификационен номер на делото в Евроюст

— ако отговорът е „не“ — дали това е искане за подкрепа

— дали делото се подкрепя от Европол

— ако отговорът е „да“ — оперативна работна група и/или SIENA?

— други участващи държави

— компетентни национални органи в другата държава, ако са известни

— национален референтен номер на наказателното производство в друга държава

— етап на производството в друга държава, ако е известен

— положителен или отрицателен спор

— действителен или потенциален спор

— вече предприети дейности по координация (напр. консултации съгласно Рамково решение 2009/948/ПВР на Съвета ([1]))

— кратко резюме на делото

— основни общи заподозрени (име, фамилия, дата и място на раждане и евентуално други относими и необходими категории данни съгласно приложение II)

iii) Код за предварително разрешение

г) член 21, параграф 6, буква б), контролирани доставки

i) Раздел от най-високо ниво

Този раздел от най-високо ниво съответства на информацията, посочена в член 21, параграф 6, буква б) от Регламент (ЕС) 2018/1727: контролирани доставки

ii) Структура на съобщението

Структурата на данните се състои от поредица от елементи и включва най-малко следното:

— национален съдебен орган, отговарящ за наказателното производство

— национален референтен номер на наказателното производство

— етап на наказателното производство (напр. разследване, наказателно преследване, съдебен процес)

— престъпления, предмет на разследване

— други държави, участващи в случая

— дали делото вече се подкрепя от Евроюст

— ако отговорът е „да“ — идентификационен номер на делото в Евроюст

— ако отговорът е „не“ — дали това е искане за подкрепа

— дали делото се подкрепя от Европол

— ако отговорът е „да“ — оперативна работна група и/или SIENA?

— други участващи държави

— държава на произход/транзит/крайно местоназначение

— компетентни национални органи в други държави

— наличие на свързани разследвания в други държави

([1]) Рамково решение 2009/948/ПВР на Съвета от 30 ноември 2009 година относно предотвратяване и уреждане на спорове за упражняване на компетентност при наказателни производства (ОВ L 328, 15.12.2009 г., стр. 42, ELI: https://eur-lex.europa.eu/eli/dec_framw/2009/948/oj).

— вид на доставените стоки (напр. наркотици и вид/пари/оръжия/цигари/други)

— статус на контролираната доставка (напр. планирана, текуща, завършена)

— резултат от контролираната доставка, ако вече е изпълнена

— използван инструмент за съдебно сътрудничество

— основни общи заподозрени (име, фамилия, дата и място на раждане и евентуално други относими и необходими категории данни съгласно приложение II)

iii) Код за предварително разрешение

д) член 21, параграф 6, буква в) от Регламент (ЕС) 2018/1727, системни проблеми с инструментите за съдебно сътрудничество

i) Раздел от най-високо ниво

Този раздел от най-високо ниво съответства на информацията, посочена в член 21, параграф 6, буква в) от Регламент (ЕС) 2018/1727: системни проблеми с инструментите за съдебно сътрудничество

ii) Структура на съобщението

Структурата на данните се състои от поредица от елементи и включва най-малко следното:

— национален съдебен орган, отговарящ за наказателното производство

— национален референтен номер на наказателното производство

— етап на наказателното производство (напр. разследване, наказателно преследване, съдебен процес)

— престъпления, предмет на разследване

— други държави, участващи в случая

— дали делото вече се подкрепя от Евроюст

— ако отговорът е „да“ — идентификационен номер на делото в Евроюст

— ако отговорът е „не“ — дали това е искане за подкрепа

— дали делото се подкрепя от Европол

— ако отговорът е „да“ — оперативна работна група и/или SIENA?

— други участващи държави

— компетентни национални органи, ако са известни

— действащи като издаващ или изпълняващ орган

— използван инструмент за съдебно сътрудничество (напр. ЕЗА, ЕЗР, обезпечаване и конфискация)

— съответно конкретно искане (т.е. какво действие по разследване, какъв вид обезпечаване, ЕЗА за изпълнение на присъда или за наказателно преследване)

— отказ или системно затруднение

— ако става въпрос за отказ — какво конкретно основание е изтъкнато

— кратко описание на проблема

— други национални органи, засегнати от същия проблем, ако има такива

iii) Код за предварително разрешение

2.3. *Кодове за предварително разрешение*

Когато обменят данни с Евроюст чрез JUDEX, компетентните национални органи посочват чрез кодове за предварително разрешение по-нататъшното обработване на данните, достъпа до тях и предаването им след установяването на връзка. В кодовете за предварително разрешение се посочва дали и до каква степен информацията, свързана с връзката, може да бъде споделяна с други компетентни национални органи, други агенции и органи на Съюза, трети държави или международни организации.

2.4. *Предварително определени съобщения*

Предварително определените съобщения са разновидност на обмена, установен с Регламент (ЕС) 2018/1727, за която обаче не е предвидена специална форма в правния акт. Техният вид и брой се определят в рамките на анализ на работния процес и технически анализ.

Дефинициите на XML схема (XML Schema Definitions (XSD)) за предварително определените съобщения се изготвят така, че да се гарантират последователност, структура и съответствие с нуждите, свързани с работния процес.

По отношение на тези схеми се прилага следното:

а) разделът от най-високо ниво в тази схема се наименува според конкретния вид съобщение, който се определя;

б) в рамките на тази структура се добавят и определят необходимите полета, които се изискват за конкретния вид съобщение, като се гарантира подходящо представяне на елементите от данни.

2.5. *Съобщения със свободен текст*

Съобщенията със свободен текст са разновидност на обмен, която дава възможност за неструктурирано или частично структурирано съдържание, позволяващо гъвкавост, като същевременно се спазват регулаторните изисквания и изискванията на работния процес. XSD за съобщенията със свободен текст се изготвят така, че да се гарантират последователност и правилно форматиране.

По отношение на тези схеми се прилага следното:

а) разделът от най-високо ниво в схемата се наименува според конкретния вид съобщение със свободен текст, който се определя;

б) със схемата се определя необходимата структура за съобщението със свободен текст, като същевременно се дава възможност за подходящо подреждане на елементите съгласно изискванията;

в) в рамките на тази структура се добавят и определят необходимите полета, които се изискват за конкретния вид съобщение със свободен текст, като се гарантира подходящо представяне на елемента от данни.

ПРИЛОЖЕНИЕ III

ТЕХНИЧЕСКИ СПЕЦИФИКАЦИИ ЗА ПРЪСТОВИ ОТПЕЧАТЪЦИ И СНИМКИ

Съобщенията, обменяни чрез децентрализираната информационна система, могат да се придружават от приложения, включително от файлове на Националния институт за стандарти и технологии (NIST), съдържащи пръстови отпечатъци и снимки, в съответствие с техническите спецификации, посочени в точки 1 и 2.

1. **Пръстови отпечатъци**

Пръстовите отпечатъци, които могат да бъдат споделяни с Евроюст с цел надеждно установяване на самоличността на лица, които са обект на наказателно производство, свързано с терористични престъпления, отговарят на следните условия:

а) пръстовите отпечатъци се предоставят в един файл, съдържащ цифрови изображения за пръстовите отпечатъци (NIST файл за пръстови отпечатъци), и се предоставят в съответствие със стандарта ANSI/NIST ITL 1-2011 Update 2015 (или по-нова версия);

б) NIST файлът за пръстови отпечатъци се състои от до десет отделни пръстови отпечатъка: по обиколката на пръста, плоски или и двете;

в) всички пръстови отпечатъци са обозначени;

г) пръстовите отпечатъци се снемат чрез сканиране или чрез отпечатване с мастило върху хартия, при условие че пръстовите отпечатъци, снети с мастило върху хартия, са сканирани с необходимата разделителна способност и със същото качество;

д) в NIST файла за пръстови отпечатъци е възможно да се включи допълнителна информация, като например условията на регистриране на пръстови отпечатъци и методът, използван за снемане на отделни изображения на пръстови отпечатъци;

е) пръстовите отпечатъци имат номинална разделителна способност 500 или 1 000 ppi [1] (с допустимо отклонение от +/– 10 ppi) с 256 нива на сивото;

ж) алгоритъмът за компресиране на пръстови отпечатъци, който трябва да се използва, следва препоръките на Националния институт за стандарти и технологии (NIST). Данните за пръстови отпечатъци с разделителна способност 500 ppi се компресират с помощта на алгоритъма WSQ (ISO/IEC 19794-5:2005). Данните за пръстови отпечатъци с разделителна способност 1 000 ppi се компресират с помощта на стандарта за компресиране на изображения JPEG 2000 (ISO/IEC 15444-1) и система за кодиране. Целевият коефициент на компресия е 15:1.

2. **Снимки**

Снимките, които могат да бъдат споделяни с Евроюст с цел надеждно установяване на самоличността на лица, които са обект на наказателно производство, свързано с терористични престъпления, отговарят на следните условия:

а) във файл за снимка (NIST файла за снимка) се предоставя само една портретна снимка, която се въвежда в съответствие със стандарта ANSI/NIST-ITL 1-2011 Update 2015 или всяка по-нова налична версия;

б) снимките са в сивата скала, цветни или в близост до инфрачервения спектър;

в) качеството на снимките се основава на изискванията за изображенията на ISO/IEC 19794-5:2011 Frontal image type или всяка по-нова налична версия;

г) NIST файлът за снимка позволява включването на допълнителна информация, включително датата, на която е направена снимката;

[1] Пиксела на инч.

д) снимките в портретен режим са с минимална разделителна способност от 600 пиксела на 800 пиксела и максимална разделителна способност от 1 200 пиксела на 1 600 пиксела;

е) лицето заема пространство в рамките на снимката, което осигурява минимум 120 пиксела между центъра на всяко око;

ж) използваният алгоритъм за компресиране на снимки следва препоръките на Националния институт за стандарти и технологии (NIST). Снимките се компресират само веднъж със стандарт за компресия на изображения JPG (ISO/IEC 10918) или JPEG 2000 (ISO/IEC 15444) и система за кодиране, при максимално допустим коефициент на компресия на изображението 20:1.