2025/1550

29.7.2025.

PROVEDBENA UREDBA KOMISIJE (EU) 2025/1550

od 28. srpnja 2025.

o utvrđivanju tehničkih specifikacija i drugih zahtjeva za decentralizirani IT sustav iz Uredbe (EU) 2023/1543 Europskog parlamenta i Vijeća

EUROPSKA KOMISIJA,

uzimajući u obzir Ugovor o funkcioniranju Europske unije,

uzimajući u obzir Uredbu (EU) 2023/1543 Europskog parlamenta i Vijeća od 12. srpnja 2023. o europskim nalozima za dostavljanje i europskim nalozima za čuvanje elektroničkih dokaza u kaznenim postupcima i za izvršenje kazni zatvora nakon kaznenog postupka ([1]), a posebno njezin članak 25. stavak 1. točke (a), (b), (c) i (d),

budući da:

(1) Kako bi se uspostavio decentralizirani IT sustav iz Uredbe (EU) 2023/1543, treba utvrditi i donijeti tehničke specifikacije, mjere i ciljeve za njegovu primjenu.

(2) U skladu s Uredbom (EU) 2023/1543 decentralizirani IT sustav trebao bi se sastojati od IT sustava država članica, agencija i tijela Unije te od interoperabilnih pristupnih točaka e-CODEX-a koje povezuju te IT sustave. Stoga bi tehničke specifikacije i drugi zahtjevi za decentralizirani IT sustav trebali biti u skladu s tim okvirom.

(3) U skladu s Uredbom (EU) 2023/1543 pristupne točke decentraliziranog IT sustava trebale bi se temeljiti na odobrenim pristupnim točkama e-CODEX-a kako su definirane u članku 3. točki 3. Uredbe (EU) 2022/850 Europskog parlamenta i Vijeća ([2]).

(4) Države članice mogu umjesto nacionalnog IT sustava za svoj pozadinski sustav koristiti referentni implementacijski softver koji je razvila Komisija. Da bi se osigurala interoperabilnost, nacionalni IT sustavi i referentni implementacijski softver trebali bi biti sukladni s istim tehničkim specifikacijama i zahtjevima utvrđenima u ovoj Uredbi.

(5) Da bi se smanjili potencijalni tehnički problemi s kapacitetom i pouzdanosti decentraliziranog IT sustava, potrebno je odrediti gornju vrijednost veličine elektroničkih dokaza koji se prenose sustavom. Nakon što sustav počne raditi, trebalo bi pratiti učestalost i količinu prenošenja elektroničkih dokaza pa bi na temelju toga prema potrebi trebalo prilagoditi gornju vrijednost radi maksimiziranja učinkovitosti sustava.

(6) Da bi se poboljšalo interoperabilnost i učinkovitost decentraliziranog IT sustava, trebalo bi propisati obavezno korištenje odgovarajućih normi Europskog instituta za telekomunikacijske norme (ETSI). Trebalo bi pratiti buduće razvoje pa prema potrebi razmotriti donošenje dodatnih ETSI-jevih normi.

(7) Uredba (EU) 2023/1543 obvezujuća je za Irsku te ona stoga sudjeluje u donošenju ove Odluke.

(8) U skladu s člancima 1. i 2. Protokola br. 22 o stajalištu Danske, priloženog Ugovoru o Europskoj uniji i Ugovoru o funkcioniranju Europske unije, ova Uredba nije obvezujuća za Dansku niti se na nju primjenjuje.

([1]) SL L 191, 28.7.2023., str. 118., ELI: http://data.europa.eu/eli/reg/2023/1543/oj.
([2]) Uredba (EU) 2022/850 Europskog parlamenta i Vijeća od 30. svibnja 2022. o računalnom sustavu za prekograničnu elektroničku razmjenu podataka u području pravosudne suradnje u građanskim i kaznenim stvarima (sustav e-CODEX) i izmjeni Uredbe (EU) 2018/1726 (SL L 150, 1.6.2022., str. 1., ELI: http://data.europa.eu/eli/reg/2022/850/oj).

(9) Provedeno je savjetovanje s Europskim nadzornikom za zaštitu podataka u skladu s člankom 42. stavkom 1. Uredbe (EU) 2018/1725 Europskog parlamenta i Vijeća ([3]) te je on dao mišljenje 25. lipnja 2025.

(10) Mjere predviđene u ovoj Uredbi u skladu su s mišljenjem Odbora osnovanog člankom 26. Uredbe (EU) 2023/1543,

DONIJELA JE OVU UREDBU:

Članak 1.

Tehničke specifikacije decentraliziranog IT sustava

Tehničke specifikacije i zahtjevi, mjere i ciljevi decentraliziranog IT sustava iz članka 25. stavka 1. Uredbe (EU) 2023/1543 za komunikaciju u smislu članka 19. te uredbe utvrđeni su u Prilogu ovoj Uredbi.

Članak 2.

Stupanje na snagu

Ova Uredba stupa na snagu dvadesetog dana od dana objave u *Službenom listu Europske unije*.

Ova je Uredba u cijelosti obvezujuća i izravno se primjenjuje u državama članicama u skladu s Ugovorima.

Sastavljeno u Bruxellesu 28. srpnja 2025.

Za Komisiju
Predsjednica
Ursula VON DER LEYEN

([3]) Uredba (EU) 2018/1725 Europskog parlamenta i Vijeća od 23. listopada 2018. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama, tijelima, uredima i agencijama Unije i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Uredbe (EZ) br. 45/2001 i Odluke br. 1247/2002/EZ (SL L 295, 21.11.2018., str. 39., ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

PRILOG

TEHNIČKE SPECIFIKACIJE DECENTRALIZIRANOG IT SUSTAVA

(iz članka 1.)

1. Uvod i područje primjene

U ovom se Prilogu utvrđuju tehničke specifikacije, mjere i ciljevi decentraliziranog IT sustava za postupke na temelju Uredbe (EU) 2023/1543.

U skladu s Uredbom (EU) 2023/1543, a posebno njezinim člankom 19., decentralizirani IT sustav omogućuje pisanu komunikaciju između nadležnih tijela i imenovanih subjekata koji imaju poslovni nastan ili pravnih zastupnika, pisanu komunikaciju među nadležnim tijelima te pisanu komunikaciju s nadležnim agencijama ili tijelima Unije.

2. Definicije

2.1 „HyperText Transport Protocol Secure" odnosno „HTTPS" znači šifrirani komunikacijski kanali sa sigurnom vezom;

2.2 „neosporivost podrijetla" znači dokazivanje cjelovitosti i podrijetla podataka metodama kao što su digitalna certifikacija, infrastruktura javnih ključeva te elektronički potpisi i pečati;

2.3 „neosporivost primitka podataka" znači dokazivanje osobi od koje prijenos potječe da je predviđeni primatelj primio podatke metodama kao što su digitalna certifikacija, infrastruktura javnih ključeva te elektronički potpisi i pečati;

2.4 „SOAP" znači, prema standardima konzorcija World Wide Web, specifikacija protokola za prijenos poruka radi razmjene strukturiranih informacija prilikom provedbe *web*-usluga u računalnim mrežama;

2.5 „REST" (Representational State Transfer) znači vrstu arhitekture za projektiranje umreženih aplikacija koja se temelji na modelu komunikacije između korisnika i poslužitelja bez očuvanja stanja i standardnim metodama za obavljanje operacija nad resursima, koji su obično u strukturiranim formatima;

2.6 „*web*-usluga" znači softverski sustav projektiran tako da podržava interoperabilne mrežne interakcije stroj-stroj i koji ima sučelje opisano u strojno obradivom obliku;

2.7 „razmjena podataka" znači razmjena poruka, obrazaca, dokumenata i elektroničkih dokaza decentraliziranim IT sustavom;

2.8 „API" znači aplikacijsko programsko sučelje utemeljeno na zajedničkom standardu za razmjenu podataka koje omogućuje automatizirani pristup decentraliziranim IT sustavima pružateljima usluga koji koriste vlastita IT rješenja za razmjenu informacija i podataka povezanih sa zahtjevima za elektroničke dokaze;

2.9 „internetsko sučelje" znači korisničko sučelje dostupno kroz HTTPS na internetu koje pružateljima usluga omogućuje da ručno pristupe decentraliziranom IT sustavu kako bi sigurno komunicirali s tijelima radi razmjene informacija i podataka povezanih sa zahtjevima za elektroničke dokaze bez uspostavljanja vlastite namjenske infrastrukture;

2.10 „ETSI-jeve norme" znači tehničke specifikacije i norme koje je razvio Europski institut za telekomunikacijske norme (ETSI) za potrebe interoperabilnosti, sigurnosti i učinkovitosti informacijskih i komunikacijskih tehnologija. U njima su sadržani okviri, protokoli i primjeri najbolje prakse za puno različitih tehnologija, uključujući mobilne mreže, radijsku komunikaciju, kibernetičku sigurnost i internetsku infrastrukturu;

2.11 „*hash*” znači izlazni podatak fiksne duljine dobiven kriptografskom funkcijom za generiranje *hasha* čiji ulazni podatak može biti proizvoljne duljine. Kriptografska funkcija za generiranje *hasha* osmišljena je tako da zadovoljava temeljna sigurnosna svojstva, uključujući prvu i drugu domensku otpornost i otpornost na kolizije, čime se osigurava njezina otpornost na napade koji se temelje na inverziji i koliziji;

2.12 „e-CODEX” znači sustav e-CODEX definiran u članku 3. stavku 1. Uredbe (EU) 2022/850;

2.13 „temeljni rječnici e-pravosuđa EU-a” znači temeljni rječnici e-pravosuđa EU-a kako su definirani u točki 4. Priloga Uredbi (EU) 2022/850;

2.14 „ebMS” znači ebXML Message Service, što je protokol za razmjenu poruka razvijen u okviru OASIS-a koji omogućuje sigurnu, pouzdanu i interoperabilnu razmjenu elektroničkih poslovnih dokumenata SOAP-om, čime se podupire integracija među poduzećima u različitim sustavima;

2.15 „AS4” znači Applicability Statement 4, standard OASIS-a na temelju kojeg je definiran protokol ebMS 3.0, kojim se pojednostavnjuje sigurna i interoperabilna razmjenu poruka među poduzećima korištenjem otvorenih standarda kao što su SOAP i WS-Security;

2.16 „ciljano vrijeme oporavka” znači maksimalno dopušteno vrijeme da se usluga ponovno uspostavi nakon incidenta;

2.17 „ciljana točka oporavka” znači maksimalna prihvatljiva količina gubitka podataka u slučaju kvara.

3. **Načini komunikacije elektroničkim sredstvima**

3.1 Za potrebe pisane komunikacije među nadležnim tijelima država članica između nadležnih tijela i imenovanih subjekata koji imaju poslovni nastan ili pravnih zastupnika pružatelja usluga te između nadležnih tijela i agencija ili tijela Unije decentralizirani IT sustav mora biti zasnovan na komunikacijskim metodama koje se temelje na uslugama, npr. na *web*-uslugama ili drugim ponovno iskoristivim komponentama i softverima za razmjenu podataka. Sustav će konkretno komunicirati komunikaciju preko pristupnih točaka e-CODEX-a, kako je utvrđeno u članku 5. stavku 2. Uredbe (EU) 2022/850. Kako bi se osigurala djelotvorna i interoperabilna prekogranična razmjena podataka, decentralizirani IT sustav mora podržavati komunikaciju e-CODEX-om.

3.2 Budući da se predviđa da će količina elektroničkih dokaza koji će se nakon izdavanja europskog naloga za dostavljanje razmjenjivati decentraliziranim IT sustavom, kako je navedeno u članku 19. stavcima 1. i 4. Uredbe (EU) 2023/1543, biti velika i da to može dovesti do tehničkih ograničenja kapaciteta koja bi mogla nepovoljno utjecati na decentralizirani IT sustav, gornja granica veličine elektroničkih dokaza koji se smiju prenositi tim sustavom trebala bi biti 25 megabajta (25 600 kilobajta). Prijenos elektroničkih dokaza veličine veće od te gornje vrijednosti obavlja se u skladu s člankom 19. stavkom 5. te uredbe.

3.3 Uzimajući u obzir članak 19. stavak 6. Uredbe (EU) 2023/1543, kad se radi o prijenosu koji se obavlja alternativnim sredstvima kako je predviđeno u tom stavku jer upotreba decentraliziranog IT sustava nije moguća zbog jednog od razloga navedenih u članku 19. stavku 5. te uredbe:

3.3.1 ako se prijenos odnosi na pisanu komunikaciju, uključujući razmjenu obrazaca, između nadležnih tijela i pružatelja usluga u smislu članka 19. stavka 1. Uredbe (EU) 2023/1543, osoba od koje prijenos potječe bilježi prijenos u svojem nacionalnom IT sustavu koji je dio decentraliziranog IT sustava. Među zabilježenim podacima moraju biti barem referentni broj predmeta ili datoteke, datum i vrijeme prijenosa, pošiljatelj i primatelj te ime i veličina datoteke;

3.3.2 ako se prijenos odnosi na pisanu komunikaciju, uključujući razmjenu obrazaca, među nadležnim tijelima te na pisanu komunikaciju s nadležnim agencijama ili tijelima Unije u smislu članka 19. stavka 4. Uredbe (EU) 2023/1543, osoba od koje prijenos potječe bilježi prijenos u decentraliziranom IT sustavu, odnosno u svojem nacionalnom IT sustavu ili, ako je primjenjivo, u IT sustavima kojima upravlja nadležna agencija ili nadležno tijelo Unije. Među zabilježenim podacima moraju biti barem referentni broj predmeta ili datoteke, datum i vrijeme prijenosa, pošiljatelj i primatelj te ime i veličina datoteke;

3.3.3 ako se elektronički dokazi na temelju europskog naloga za dostavljanje prenose alternativnim sredstvima komunikacije između pružatelja usluga i nadležnih tijela u državi izdavateljici ([1]) ili ako tijelo izvršitelj alternativnim sredstvima prenosi elektroničke dokaze nadležnim tijelima u državi izdavateljici u okviru postupka izvršenja kako je predviđeno u članku 16. stavku 9. Uredbe (EU) 2023/1543, osoba od koje prijenos potječe:

(a) bilježi i dostavlja tijelu kojem su elektronički dokazi preneseni ili stavljeni na raspolaganje sljedeće informacije u manifestu:

(1) pošiljatelja i primatelja;

(2) metapodatke na temelju kojih se dostavljeni elektronički dokazi povezuju s određenim europskim nalogom ili nalozima za dostavljanje ili europskim nalogom ili nalozima za čuvanje;

(3) datum i vrijeme prijenosa ili informacije o tome kad su elektronički dokazi stavljeni na raspolaganje primatelju;

(4) informacije o načinu prijenosa (npr. zapis sigurne poveznice kojom su elektronički dokazi stavljeni na raspolaganje, dokaz poštanske službe o primitku ili dostavi itd. ([2]));

(5) puna imena datoteka s elektroničkim dokazima koje se dostavljaju ili na drugi način stavljaju na raspolaganje predviđenom primatelju u državi izdavateljici;

(6) veličinu podataka elektroničkih dokaza koji se dostavljaju ili na drugi način stavljaju na raspolaganje predviđenom primatelju u državi izdavateljici;

(7) barem jedan *hash* podataka koji su preneseni ili stavljeni na raspolaganje te podatak o korištenom algoritmu za generiranje *hasha*. Algoritmi za generiranje *hasheva* koji služe za izračunavanje tih *hasheva* moraju biti kriptografski pouzdani, uobičajeno korišteni i otporni na javno objavljene slabosti kao što su kolizije (primjeri takvih algoritama su SHA-512, SHA3-512, BLAKE2 ili RIPEMD-160, ali se mogu koristiti i pouzdaniji algoritmi, ovisno o tehnološkim novostima);

(b) ako je primjenjivo, u manifestu iz točke (a) navodi do kad će (vrijeme i datum) elektronički dokazi biti dostupni. Taj rok ne smije biti kraći od 10 kalendarskih dana ni dulji od 45 kalendarskih dana od datuma stavljanja na raspolaganje elektroničkih dokaza te mora nadležnom tijelu u državi izdavateljici dati razumno vrijeme za preuzimanje elektroničkih dokaza. Na zahtjev nadležnog tijela države izdavateljice rok koji je navela osoba od koje prijenos potječe može se u pojedinom slučaju produljiti;

(c) može zabilježiti sve dodatne informacije ili primjedbe relevantne za predmet i dostaviti ih tijelu kojem su elektronički dokazi preneseni ili stavljeni na raspolaganje u manifestu iz točke (a).

3.4 Uzimajući u obzir članak 28. Uredbe (EU) 2023/1543, referentni implementacijski softver programski prikuplja i prenosi statističke podatke iz stavka 2. tog članka, ili na drugi način omogućuje pristup tim podacima i u strukturiranom (npr. XML) i u nestrukturiranom (npr. PDF) formatu podataka. U skladu s člankom 28. stavkom 3. Uredbe (EU) 2023/1543 nacionalni portali ([3]) kojima upravljaju države članice mogu, ako su tehnički sposobni, te statističke podatke automatiziranim procesom prenositi ili dostavljati i Komisiji. Komisija izdaje smjernice o strukturi podataka i načinima prikupljanja i priopćavanja tih statističkih podataka.

([1]) Radi veće jasnoće smatra se da se upućivanja na nadležna nacionalna tijela *mutatis mutandis* odnose i na nacionalne članove Eurojusta, europske tužitelje i delegirane europske tužitelje, u mjeri u kojoj su ovlašteni obavljati iste funkcije u skladu s pravom EU-a i nacionalnim pravom.

([2]) Treba podsjetiti da u skladu s člankom 19. stavkom 5. prijenos takvim alternativnim sredstvima komunikacije mora biti brz, siguran i pouzdan i omogućiti primatelju da utvrdi autentičnost.

([3]) „Nacionalni portali" trebali bi se tumačiti kao nacionalni „IT sustavi" koji su dio decentraliziranog IT sustava, kako je definiran u članku 3. stavku 21. Uredbe (EU) 2023/1543.

4. **Komunikacijski protokoli**

4.1 Decentralizirani IT sustav mora koristiti sigurne internetske protokole za:

(a) komunikaciju među nadležnim tijelima unutar decentraliziranog IT sustava;

(b) komunikaciju između nadležnih tijela i agencija i tijela Unije unutar decentraliziranog IT sustava;

(c) komunikaciju između nadležnih tijela i pružatelja usluga kroz API i internetske sučelje; i

(d) komunikaciju s bazom podataka sudova.

4.2 U kontekstu definiranja i prenošenja strukturiranih podataka i metapodataka komponente decentraliziranog IT sustava moraju se temeljiti na sveobuhvatnim i opće prihvaćenim industrijskim standardima i protokolima, kao što su SOAP i REST, posebno na onima na koje upućuju europske organizacije za normizaciju, kao što je ETSI.

4.3 Protokoli koje decentralizirani IT sustav koristi za prijenos podataka i razmjenu poruka moraju se temeljiti na sigurnim protokolima na standardima kao što su:

(a) AS4 Profile za prekograničnu razmjenu podataka, koji jamči sigurnu i pouzdanu razmjenu poruka sa šifriranjem i neosporivosti;

(b) API-ji HTTPS/RESTful za komunikaciju u formatima JSON i XML;

(c) SOAP za interakcije visoke pouzdanosti sa standardom WS-Security za autentifikaciju i šifriranje.

4.4 Da bi razmjena podataka bila glatka i interoperabilna, komunikacijski protokoli decentraliziranog IT sustava moraju biti u skladu s relevantnim standardima za interoperabilnost.

4.5 Ako je primjenjivo, XML sheme e-dokaza koriste relevantne standarde ili rječnike potrebne za pravilno potvrđivanje valjanosti elemenata i vrsta definiranih u ovoj shemi. To može uključivati:

(a) temeljni rječnik e-pravosuđa EU-a;

(b) nekvalificirane vrste podataka;

(c) popis oznaka za oznake jezika Europske unije.

Osim toga, ako je primjenjivo, XML sheme mogu uključivati relevantne ETSI-jeve norme kako bi se iskoristile njihove definicije.

4.6 Komisija utvrđuje specifikacije za zajednički API, koji države izvršiteljice stavljaju na raspolaganje pružateljima usluga kao način pristupa decentraliziranom IT sustavu. U mjeri u kojoj je to moguće i razumno, taj se API mora temeljiti na normi ETSI TS 104 144 („Definicija sučelja za Uredbu (EU) 2023/1543 o e-dokazima za nacionalna tijela i pružatelje usluga”).

4.7 Protokoli koje decentralizirani IT sustav koristi za sigurnost i autentifikaciju moraju se temeljiti na protokolima na standardima kao što su:

(a) TLS (Transport Layer Security) za šifriranu i autentificiranu mrežnu komunikaciju, koji podržava uzajamnu autentifikaciju na temelju digitalnih certifikata X.509;

(b) OAuth/OpenID Connect (OIDC) za sigurnu autentifikaciju i autorizaciju;

(c) infrastruktura javnih ključeva i digitalni potpisi za sigurnu razmjenu ključeva i provjeru cjelovitosti poruka na temelju digitalnih certifikata (X.509) koje su izdala pouzdana certifikacijska tijela.

5. **Ciljevi informacijske sigurnosti i relevantne tehničke mjere**

5.1 Tehničke mjere za potrebe ispunjavanja minimalnih sigurnosnih standarda informacijske tehnologije u razmjeni informacija decentraliziranim IT sustava obuhvaćaju:

(a) mjere za osiguravanje povjerljivosti informacija, među ostalim korištenje sigurnih komunikacijskih kanala;

(b) mjere za osiguravanje cjelovitosti podataka (poruke, obrasci, dokumenti i elektronički dokazi) u mirovanju i u prijenosu;

(c) mjere za osiguravanje neosporivosti podrijetla pošiljatelja informacija unutar decentraliziranog IT sustava i neosporivosti primitka informacija;

(d) mjere za osiguravanje dostupnosti omogućavanjem stalnog pristupa uslugama i podacima kojima se sprečavaju poremećaji u radu zbog kibernetičkih napada ili kvarova;

(e) mjere za osiguravanje bilježenja sigurnosnih događaja u skladu s priznatim međunarodnim preporukama za sigurnosne standarde informacijske tehnologije;

(f) mjere za osiguravanje autentifikacije i autorizacije korisnika te mjere za provjeru identiteta sustava povezanih s decentraliziranim IT sustavom.

5.2 Komponente decentraliziranog IT sustava moraju omogućavati sigurnu komunikaciju i prijenos podataka koji se temelje na šifriranju, infrastrukturi javnih ključeva s digitalnim certifikatima za autentifikaciju i sigurnu razmjenu ključeva te sigurnim protokolima za razmjenu poruka, kao što su AS4 (ebMS), API-ji RESTful i SOAP, kako bi se održala povjerljivost i cjelovitost poruka.

5.3 Komponente decentraliziranog IT sustava moraju biti razvijene u skladu s načelom tehničke i integrirane zaštite podataka te moraju postojati odgovarajuće administrativne, organizacijske i tehničke mjere kako bi se osigurala visoka razina kibernetičke sigurnosti.

5.4 Komisija izrađuje, razvija i održava referentni implementacijski softver u skladu sa zahtjevima i načelima za zaštitu podataka utvrđenima u Uredbi (EU) 2018/1725. Referentni implementacijski softver koji Komisija daje mora državama članicama omogućavati da ispune svoje obveze u skladu s Uredbom (EU) 2016/679 Europskog parlamenta i Vijeća ([4]), odnosno Direktivom (EU) 2016/680 Europskog parlamenta i Vijeća ([5]), kako je primjenjivo.

5.5 Države članice koje upotrebljavaju nacionalni IT sustav koji nije referentni implementacijski softver dužne su primjenjivati mjere potrebne za njegovu sukladnost sa zahtjevima iz Uredbe (EU) 2016/679 i Direktive (EU) 2016/680, ovisno o slučaju.

5.6 Uzimajući u obzir njihovo sudjelovanje u decentraliziranom IT sustavu, Eurojust i Ured europskog javnog tužitelja dužni su primjenjivati mjere potrebne da njihovi IT sustavi budu sukladni sa zahtjevima iz Uredbe (EU) 2018/1725 i akata o njihovu osnivanju.

5.7 Države članice, Eurojust i Ured europskog javnog tužitelja dužni su uspostaviti pouzdane mehanizme za otkrivanje prijetnji i odgovaranje na incidente radi pravovremenog utvrđivanja, ublažavanja i oporavka od sigurnosnih incidenata, u skladu sa svojim relevantnim politikama za IT sustave koji su dio decentraliziranog IT sustava za koje su odgovorni.

6. **Šifriranje elektroničkih dokaza** ([6])

6.1 Ne dovodeći u pitanje sigurnosne mjere decentraliziranog IT sustava, kad izdaju europski nalog za dostavljanje, nadležna tijela mogu uz njega dati namjenski javni certifikat X.509 za asimetrično šifriranje elektroničkih dokaza.

([4]) Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (SL L 119, 4.5.2016., str. 1.).

([5]) Direktiva (EU) 2016/680 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP (SL L 119, 4.5.2016., str. 89.).

([6]) Kako bi se izbjegla dvojbe, pojam „elektronički dokazi” ograničen je na definiciju iz članka 3. stavka 8. Uredbe (EU) 2023/1543.

6.2 Za izdavanje, upravljanje, provjeru i sve povezane aspekte certifikata iz točke 6.1. te za odgovarajuću infrastrukturu javnih ključeva isključivo je odgovorna država izdavateljica.

6.3 Ne dovodeći u pitanje budući tehnološki razvoj, javni certifikati moraju podržavati standardne algoritme šifriranja u sektoru, npr. RSA (Rivest-Shamir-Adleman) ili ECDH (Diffie-Hellmanov protokol na temelju eliptičnih krivulja) za kriptografiju na temelju eliptične krivulje (ECC).

6.4 Javni certifikati moraju imati primjerene „keyUsage" ekstenzije, npr. „keyEncipherment" i „dataEncipherment" za certifikate na temelju RSA odnosno „keyAgreement" za certifikate na temelju ECC-a. Ti se certifikati stavljaju na raspolaganje u formatu PEM (Privacy-Enhanced Mail) ili DER (Distinguished Encoding Rules).

6.5 Ako je tijelo izdavatelj dalo javni certifikat X.509 i ako pružatelj usluga šalje elektroničke dokaze na temelju europskog naloga za dostavljanje, pružatelj usluga, prije nego što će prenijeti podatke decentraliziranim IT sustavom, šifrira elektroničke dokaze odgovarajućim javnim certifikatom X.509 koji je dala država izdavateljica.

6.6 Ako je tijelo izdavatelj dalo javni certifikat X.509, ali prijenos elektroničkih dokaza u šifriranom obliku nije moguć zbog tehničkih ili drugih opravdanih razloga, i ne dovodeći u pitanje odredbu iz članka 19. stavka 5. Uredbe (EU) 2023/1543, pružatelj usluga može prenijeti podatke bez šifriranja sadržaja. U takvim slučajevima pružatelj usluga dostavlja obrazloženje tijelu izdavatelju.

7. **Minimalni ciljevi dostupnosti**

7.1 Države članice, Eurojust i Ured europskog javnog tužitelja dužni su se pobrinuti da komponente decentraliziranog IT sustava za koje su odgovorni budu dostupne 0-24, pri čemu ciljana tehnička dostupnost na godišnjoj razini mora biti najmanje 98 %, ne računajući planirano održavanje.

7.2 Komisija se dužna pobrinuti da baza podataka sudova bude dostupna 0-24, pri čemu ciljana tehnička dostupnost na godišnjoj razini mora biti veća od 99 %, ne računajući planirano održavanje.

7.3 U mjeri u kojoj je to moguće, aktivnosti održavanja zakazuju se izvan radnog vremena (između 20 sati i 7 sati po srednjoeuropskom vremenu).

7.4 Države članice, Eurojust i Ured europskog javnog tužitelja obavješćuju Komisiju i druge države članice o aktivnostima održavanja kako slijedi:

(a) 5 radnih dana unaprijed za aktivnosti održavanja koje mogu uzrokovati nedostupnost od do 4 sata;

(b) 10 radnih dana unaprijed za aktivnosti održavanja koje mogu uzrokovati nedostupnost od 4 do 12 sati;

(c) 30 radnih dana unaprijed za aktivnosti održavanja koje mogu uzrokovati nedostupnost dulju od 12 sati.

7.5 Ako države članice, Eurojust ili Ured europskog javnog tužitelja imaju fiksna razdoblja unutar kojih vrše redovno održavanje, obavješćuju Komisiju i sudionike u decentraliziranom IT sustavu o vremenu takvih redovitih fiksnih razdoblja. Neovisno o obvezama utvrđenima u točki 7.4., ako komponente decentraliziranog IT sustava za koje su odgovorni države članice, Eurojust ili Ured europskog javnog tužitelja u takvom redovitom fiksnom razdoblju budu nedostupne, mogu odlučiti da neće o tome svaki put obavijestiti Komisiju.

7.6 U slučaju neočekivanog tehničkog kvara komponenata decentraliziranog IT sustava za koje su odgovorni, države članice, Eurojust ili Ured europskog javnog tužitelja o tom kvaru i o predviđenom roku za oporavak, ako je poznat, bez odgode obavješćuju Komisiju i sudionike u decentraliziranom IT sustavu.

7.7 U slučaju aktivnosti održavanja ili neočekivanog tehničkog kvara komponenata u decentraliziranom IT sustavu za koje je odgovorna država članica čija je posljedica negativan utjecaj na dostupnost API-ja i/ili internetskog sučelja za pružatelje usluga, ta država članica bez odgode objavljuje te informacije na internetskim stranicama i/ili ih javlja pružateljima usluga koji rade na njezinu državnom području.

7.8 U slučaju neočekivanog tehničkog kvara u bazi podataka sudova Komisija bez odgode obavješćuje države članice, Eurojust i Ured europskog javnog tužitelja o toj nedostupnosti i o predviđenom roku za oporavak, ako je poznat.

7.9 U slučaju prekida pružanja usluga države članice, Eurojust i Ured europskog javnog tužitelja dužni su se pobrinuti za brzo ponovno uspostavljanje usluge s minimalnim gubitkom podataka, u skladu s ciljanim vremenom oporavka i ciljanom točkom oporavka.

7.10 Države članice, Eurojust i Ured europskog javnog tužitelja dužne su uvesti odgovarajuće mjere za postizanje prethodno navedenih ciljeva dostupnosti i uspostaviti postupke za djelotvoran odgovor na incidente.

8. **Baza podataka nadležnih tijela/sudova (CDB)**

8.1 Uzimajući u obzir članak 19. Uredbe (EU) 2023/1543, za potrebe funkcioniranja decentraliziranog IT sustava važno je uspostaviti mjerodavnu bazu podataka o pružateljima usluga i nadležnim tijelima.

8.2 Mjerodavna baza podataka nadležnih tijela mora sadržavati sljedeće informacije u strukturiranom obliku:

(a) za potrebe članka 19. Uredbe (EU) 2023/1543, informacije o nadležnim tijelima prijavljenima u skladu s njezinim člankom 31. stavkom 1. točkama od (a) do (c), među ostalim informacije o:

(1) nacionalnim članovima Eurojusta i podatkom mogu li u skladu s nacionalnim pravom izdavati europske naloge za dostavljanje i europske naloge za čuvanje u skladu s člankom 8. stavcima 3. i 4. Uredbe (EU) 2018/1727 Europskog parlamenta i Vijeća ([7]);

(2) delegiranim europskim tužiteljima i europskim tužiteljima, ako su države članice, u skladu s člankom 105. stavkom 3. Uredbe Vijeća (EU) 2017/1939 ([8]), priopćile da su nadležno tijelo izdavatelj u smislu Uredbe (EU) 2023/1543;

(b) informacije potrebne za određivanje geografskih područja nadležnosti tijela ili druge relevantne kriterije potrebne za utvrđivanje njihove nadležnosti, prema potrebi;

(c) informacije potrebne za pravilno funkcioniranje razmjene podataka i tehničko usmjeravanje poruka u okviru te razmjene unutar decentraliziranog IT sustava.

8.2.1 Informacije iz točke 8.2. podtočke (c) uključuju sljedeće:

(a) informacije o državi članici u kojoj imenovani subjekt koji ima poslovni nastan pružatelja usluga ima poslovni nastan ili u kojoj njegov pravni zastupnik ima boravište:

(1) država članica;

(2) središnje tijelo;

([7]) Uredba (EU) 2018/1727 Europskog parlamenta i Vijeća od 14. studenog 2018. o Agenciji Europske unije za suradnju u kaznenom pravosuđu (Eurojust) te zamjeni i stavljanju izvan snage Odluke Vijeća 2002/187/PUP (SL L 295, 21.11.2018., str. 138.).

([8]) Uredba Vijeća (EU) 2017/1939 od 12. listopada 2017. o provedbi pojačane suradnje u vezi s osnivanjem Ureda europskog javnog tužitelja („EPPO”) (SL L 283, 31.10.2017., str. 1.).

(b) informacije o pružatelju usluga:

(1) ime;

(2) adresa/sjedište;

(3) broj upisa u registar;

(4) pravni oblik;

(5) telefonski broj;

(6) e-adresa;

(c) informacije o imenovanom subjektu koji ima poslovni nastan / pravnom zastupniku:

(1) vrsta subjekta (imenovani subjekt koji ima poslovni nastan / pravni zastupnik);

(2) ime;

(3) adresa/sjedište;

(4) telefonski broj;

(5) e-adresa;

(6) osoba/subjekt za kontakt za opće predmete;

(7) službeni jezici koje prihvaća pružatelj usluga/imenovani subjekt koji ima poslovni nastan/pravni zastupnik;

(8) usluge iz članka 2. stavka 1. Direktive (EU) 2023/1544 Europskog parlamenta i Vijeća ([9]) koje se nude u Uniji;

(9) vrsta pravnih instrumenata EU-a za koje je imenovani subjekt koji ima poslovni nastan/pravni predstavnik imenovan (u situacijama u kojima države članice ne sudjeluju u svim relevantnim pravnim instrumentima EU-a);

(10) teritorijalno područje imenovanja;

(d) autentifikacija informacija:

(1) ime ovlaštenog zastupnika;

(2) naziv radnog mjesta;

(3) adresa;

(4) telefonski broj;

(5) e-adresa;

(6) datum.

8.2.2. Informacije iz točke 8.2. podtočke (c) mogu uključivati i sljedeće, ako je poznato:

(a) informacije o pružatelju usluga:

(1) osoba za kontakt za upite o obavijestima (ako nije potpisnik);

(2) internetske stranice;

(b) vrste dostupnih podataka:

(1) za svaku predmetnu uslugu:

— vrste dostupnih podataka,

— kategorija podataka,

— identifikacijske oznake,

— razdoblje dostupnosti podataka;

([9]) Direktiva (EU) 2023/1544 Europskog parlamenta i Vijeća od 12. srpnja 2023. o utvrđivanju usklađenih pravila za imenovanje imenovanih subjekata s poslovnim nastanom i za imenovanje pravnih zastupnika za potrebe prikupljanja elektroničkih dokaza u kaznenim postupcima (SL L 191, 28.7.2023., str. 181., ELI: http://data.europa.eu/eli/dir/2023/1544/oj).

(2) dodatne informacije o podacima;

(3) dodatne informacije o usluzi (npr. odnosi podugovaranja);

(c) informacije o imenovanom subjektu koji ima poslovni nastan / pravnom zastupniku:

(1) drugi pružatelji usluga za koje je imenovan imenovani subjekt koji ima poslovni nastan ili pravni zastupnik;

(2) kontakt za tehničku pomoć;

(3) kontakt za hitne slučajeve;

(d) tehničke informacije:

(1) ime tehničke kontaktne točke;

(2) telefonski broj tehničke kontaktne točke;

(3) e-adresa tehničke kontaktne točke;

(4) URL API-ja za dinamičko preuzimanje informacija o vrstama podataka;

(5) vrsta povezivanja s nacionalnim IT sustavom:

— internetsko sučelje,

— API,

— URL Push API-ja.

8.3 Kad je riječ o operativnim potrebama decentraliziranog IT sustava:

(a) Komisija je odgovorna za razvoj, održavanje, rad i potporu mjerodavne baze podataka;

(b) Komisija omogućuje pristup mjerodavnoj bazi podataka API-jem koji je dostupan nadležnim tijelima, Eurojustu i Uredu europskog javnog tužitelja za potrebe njihova sudjelovanja u decentraliziranom IT sustavu;

(c) države članice osiguravaju da su informacije o njihovim nadležnim tijelima utvrđene u točki 8.2. podtočkama (a) i (b) u mjerodavnoj bazi podataka potpune, točne i ažurne;

(d) mjerodavna baza podataka državama članicama omogućuje da unose i ažuriraju informacije o svojim pružateljima usluga sadržane u toj bazi podataka, a tijelima koja sudjeluju u decentraliziranom IT sustavu omogućuje programski pristup tim informacijama i preuzimanje tih informacija;

(e) države članice i pružatelji usluga osiguravaju da su informacije utvrđene u točki 8.2. podtočki (c) u mjerodavnoj bazi podataka potpune, točne i ažurne.