Europos Sąjungos
oficialusis leidinys

LT
L serija

2025/1550

2025 7 29

# KOMISIJOS ĮGYVENDINIMO REGLAMENTAS (ES) 2025/1550

## 2025 m. liepos 28 d.

## kuriuo nustatomos decentralizuotos IT sistemos, nurodytos Europos Parlamento ir Tarybos reglamente (ES) 2023/1543, techninės specifikacijos ir kiti reikalavimai

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo,

atsižvelgdama į 2023 m. liepos 12 d. Europos Parlamento ir Tarybos reglamentą (ES) 2023/1543 dėl Europos įrodymų pateikimo orderių ir Europos įrodymų saugojimo orderių elektroniniams įrodymams baudžiamajame procese ir laisvės atėmimo bausmių vykdymui pasibaigus baudžiamajam procesui ([1]), ypač į jo 25 straipsnio 1 dalies a, b, c ir d punktus,

kadangi:

(1) siekiant sukurti Reglamente (ES) 2023/1543 nurodytą decentralizuotą IT sistemą, būtina apibrėžti ir patvirtinti tos sistemos įgyvendinimo technines specifikacijas, priemones ir tikslus;

(2) pagal Reglamentą (ES) 2023/1543 decentralizuota IT sistema turėtų apimti valstybių narių ir Sąjungos agentūrų bei įstaigų IT sistemas ir sąveikius e. CODEX prieigos taškus, per kuriuos tos IT sistemos yra sujungtos. Atitinkamai decentralizuotos IT sistemos techninės specifikacijos ir kiti reikalavimai turėtų šią sistemą atspindėti;

(3) pagal Reglamentą (ES) 2023/1543 decentralizuotos IT sistemos prieigos taškai turėtų būti grindžiami patvirtintais e. CODEX prieigos taškais, apibrėžtais Europos Parlamento ir Tarybos reglamento (ES) 2022/850 3 straipsnio 3 punkte ([2]);

(4) valstybės narės gali nuspręsti naudoti Komisijos sukurtą bazinio sistemos modelio programinę įrangą kaip savo galinę sistemą vietoj nacionalinės IT sistemos. sąveikumo užtikrinimo tikslais nacionalinėms IT sistemoms ir bazinio sistemos modelio programinei įrangai turėtų būti taikomos tos pačios šiame reglamente nustatytos techninės specifikacijos ir reikalavimai;

(5) siekiant sumažinti galimas technines problemas, susijusias su decentralizuotos IT sistemos pajėgumu ir patikimumu, būtina nustatyti per tą sistemą perduodamų elektroninių įrodymų kiekio ribą. Sistemai pradėjus veikti, turėtų būti stebimas duomenų perdavimo dažnumas ir jų kiekis, o tam tikrais atvejais riba turėtų būti pakoreguota, kad būtų kuo labiau padidintas sistemos veiksmingumas;

(6) siekiant sustiprinti decentralizuotos IT sistemos sąveikumą ir veiksmingumą, turėtų būti nurodyta naudoti atitinkamus ETSI standartus. Reikėtų stebėti būsimus pokyčius ir prireikus apsvarstyti galimybę įtraukti papildomų ETSI standartų;

(7) Reglamentas (ES) 2023/1543 Airijai yra privalomas, todėl ji dalyvauja priimant šį reglamentą;

(8) pagal prie Europos Sąjungos sutarties ir Sutarties dėl Europos Sąjungos veikimo pridėto Protokolo Nr. 22 dėl Danijos pozicijos 1 ir 2 straipsnius, šis reglamentas Danijai nėra privalomas ar taikomas;

([1]) OL L 191, 2023 7 28, p. 118, ELI: http://data.europa.eu/eli/reg/2023/1543/oj.

([2]) 2022 m. gegužės 30 d. Europos Parlamento ir Tarybos reglamentas (ES) 2022/850 dėl tarpvalstybinio elektroninio keitimosi duomenimis teisminio bendradarbiavimo civilinėse ir baudžiamosiose bylose srityje kompiuterinės sistemos (sistemos e. CODEX), kuriuo iš dalies keičiamas Reglamentas (ES) 2018/1726 (OL L 150, 2022 6 1, p. 1, ELI: http://data.europa.eu/eli/reg/2022/850/oj).

(9) vadovaujantis Europos Parlamento ir Tarybos reglamento (ES) 2018/1725 ([3]) 42 straipsnio 1 dalimi, buvo konsultuojamasi su Europos duomenų apsaugos priežiūros pareigūnu ir 2025 m. birželio 25 d. jis pateikė nuomonę;

(10) šiame reglamente nustatytos priemonės atitinka pagal Reglamento (ES) 2023/1543 26 straipsnį įsteigto komiteto nuomonę,

PRIĖMĖ ŠĮ REGLAMENTĄ:

*1 straipsnis*

**Decentralizuotos IT sistemos techninės specifikacijos**

Reglamento (ES) 2023/1543 25 straipsnio 1 dalyje nurodytos decentralizuotos IT sistemos, skirtos ryšiams, kaip apibrėžta to reglamento 19 straipsnyje, techninės specifikacijos ir reikalavimai, priemonės ir tikslai nustatomi šio reglamento priede.

*2 straipsnis*

**Įsigaliojimas**

Šis reglamentas įsigalioja dvidešimtą dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje*.

Šis reglamentas pagal Sutartis privalomas visas ir tiesiogiai taikomas valstybėse narėse.

Priimta Briuselyje 2025 m. liepos 28 d.

*Komisijos vardu*
*Pirmininkė*
Ursula VON DER LEYEN

([3]) 2018 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1725 dėl fizinių asmenų apsaugos Sąjungos institucijoms, organams, tarnyboms ir agentūroms tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinamas Reglamentas (EB) Nr. 45/2001 ir Sprendimas Nr. 1247/2002/EB (OL L 295, 2018 11 21, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

*PRIEDAS*

**DECENTRALIZUOTOS IT SISTEMOS TECHNINĖS SPECIFIKACIJOS**

**(nurodytos 1 straipsnyje)**

1. **Įvadas ir taikymo sritis**

Šiame priede nustatomos decentralizuotos IT sistemos techninės specifikacijos, priemonės ir tikslai, susiję su procedūromis, vykdomomis pagal Reglamentą (ES) 2023/1543.

Pagal Reglamentą (ES) 2023/1543, visų pirma jo 19 straipsnį, decentralizuota IT sistema turi sudaryti sąlygas kompetentingų institucijų ir paskirtųjų įmonių arba teisinių atstovų rašytinei komunikacijai, taip pat kompetentingų institucijų ir kompetentingų Sąjungos agentūrų ar įstaigų rašytinei komunikacijai.

2. **Apibrėžtys**

2.1. Saugusis hiperteksto perdavimo protokolas (angl. *HyperText Transport Protocol Secure*) arba HTTPS – šifruotojo ryšio ir saugiojo perdavimo kanalai;

2.2. kilmės neginčijamumas – savybė, reiškianti, kad duomenų vientisumas ir kilmė įrodomi tokiomis priemonėmis kaip skaitmeninis sertifikavimas, viešojo rakto infrastruktūra, elektroniniai parašai ir elektroniniai spaudai;

2.3. informacijos gavimo neginčijamumas – savybė, reiškianti, kad duomenų, siųstų siuntėjo numatytajam gavėjui, gavimas įrodomas tokiomis priemonėmis kaip skaitmeninis sertifikavimas, viešojo rakto infrastruktūra ir elektroniniai parašai bei elektroniniai spaudai;

2.4. SOAP (angl. *Simple Object Access Protocol*) – kaip nustatyta Žiniatinklio konsorciumo standartuose, pranešimų protokolo specifikacija, kurioje nustatomi struktūrizuotos informacijos mainų, diegiant tinklo paslaugas kompiuteriniuose tinkluose, reikalavimai;

2.5. reprezentacinis valstybės perdavimas (REST) – architektūrinis stilius, skirtas tinklinėms taikomosioms programoms kurti, grindžiamas asmens be pilietybės, kliento ir serverio ryšio modeliu ir naudojant standartinius metodus operacijoms atlikti naudojant išteklius, kurie paprastai pateikiami struktūrizuotais formatais;

2.6. saityno paslauga – programinės įrangos sistema, suprojektuota įvairių kompiuterių sąveikai tinkle užtikrinti, turinti įdiegtą sąsają, aprašytą kompiuteriu galimu apdoroti formatu;

2.7. keitimasis duomenimis – keitimasis pranešimais, formomis, dokumentais ir elektroniniais įrodymais naudojantis decentralizuota IT sistema;

2.8. API – bendruoju keitimosi duomenimis standartu grindžiama taikomųjų programų sąsaja, leidžianti paslaugų teikėjams, kurie, keisdamiesi informacija ir duomenimis, susijusiais su prašymais dėl elektroninių įrodymų, naudojasi specialiais IT sprendimais, naudotis prieiga prie decentralizuotų IT sistemų automatinėmis priemonėmis;

2.9. internetinė sąsaja – per HTTPS internete prieinama naudotojo sąsaja, leidžianti paslaugų teikėjams rankiniu būdu prisijungti prie decentralizuotos IT sistemos, kad būtų galima saugiai bendrauti su valdžios institucijomis ir keistis informacija bei duomenimis, susijusiais su elektroninių įrodymų prašymais, nesusikūrus savo specialios infrastruktūros;

2.10. ETSI standartai – Europos telekomunikacijų standartų instituto (ETSI) parengtos techninės specifikacijos ir standartai, skirti informacinių ir ryšio technologijų sąveikai, saugumui ir veiksmingumui užtikrinti. Jose pateikiamos įvairių technologijų, įskaitant judriojo ryšio tinklus, radijo ryšius, kibernetinį saugumą ir interneto infrastruktūrą, sistemos, protokolai ir geriausios praktikos pavyzdžiai;

2.11. maišos santrumpa – fiksuoto ilgio išvestis, gauta naudojant kriptografinės maišos funkciją, kai ji taikoma savo nuožiūra nustatytam įvesties ilgiui. Kriptografinės maišos funkcija skirta pagrindinėms apsaugos savybėms, įskaitant atsparumą pirminiam vaizdui, papildomą atsparumą pirminiam vaizdui ir atsparumą susidūrimams, užtikrinti, kad ji būtų atspari inversijai ir susidūrimo atakoms;

2.12. sistema e. CODEX – sistema e. CODEX, apibrėžta Reglamento (ES) 2022/850 3 straipsnio 1 punkte;

2.13. ES e. teisingumo baziniai žodynai – ES e. teisingumo baziniai žodynai, apibrėžti Reglamento (ES) 2022/850 priedo 4 punkte;

2.14. „ebMS“ – ebXML pranešimų paslauga – tai pranešimų perdavimo protokolas, sukurtas pagal OASIS sistemą, kuriuo sudaromos sąlygos saugiai, patikimai ir sąveikiai keistis elektroniniais verslo dokumentais naudojant SOAP, remiant įmonių tarpusavio integraciją įvairiose sistemose;

2.15. AS4 – tai 4 pareiškimas dėl taikymo, OASIS standartas, kuriuo apibūdinamas „ebMS 3.0“; juo supaprastinami saugūs ir sąveikūs įmonių tarpusavio pranešimai, taikant atviruosius standartus, pvz., SOAP ir „WS-Security“;

2.16. atkūrimo laiko tikslas – ilgiausias priimtinas laikas paslaugai po incidento atkurti;

2.17. atkūrimo taško tikslas – didžiausias priimtinas prarastų duomenų kiekis gedimo atveju.

3. **Ryšio palaikymo elektroninėmis priemonėmis metodai**

3.1. Valstybių narių kompetentingų institucijų, kompetentingų institucijų ir paslaugų teikėjų paskirtųjų įmonių arba teisinių atstovų, taip pat kompetentingų institucijų ir Sąjungos agentūrų ar įstaigų rašytinės komunikacijos tikslais decentralizuota IT sistema naudoja paslaugomis grindžiamus ryšių metodus, pavyzdžiui, saityno paslaugas arba kitus daugkartinio naudojimo komponentus ir programinės įrangos sprendimus keitimosi duomenimis tikslais. Konkrečiai, tai apims ryšius per e. CODEX prieigos taškus, kaip nustatyta Reglamento (ES) 2022/850 5 straipsnio 2 dalyje. Todėl, siekiant užtikrinti veiksmingą ir sąveikų tarpvalstybinį keitimąsi duomenimis, decentralizuota IT sistema palaiko ryšį per sistemą e. CODEX.

3.2. Atsižvelgiant į numatomą didelį elektroninių įrodymų, kurie bus perduoti vykdant Europos įrodymų pateikimo orderį per decentralizuotą IT sistemą, kaip nurodyta Reglamento (ES) 2023/1543 19 straipsnio 1 ir 4 dalyse, kiekį, dėl kurio gali atsirasti techninių pajėgumų apribojimų, galinčių turėti neigiamos įtakos decentralizuotai IT sistemai, elektroniniai įrodymai perduodami per šią sistemą tik tuo atveju, jei jie neviršija 25 megabaitų (25 600 kilobaitų) ribos. Šią ribą viršijantys elektroniniai įrodymai perduodami pagal to reglamento 19 straipsnio 5 dalį.

3.3. Atsižvelgiant į Reglamento (ES) 2023/1543 19 straipsnio 6 dalį, jei perdavimas vykdomas alternatyviomis priemonėmis, kaip numatyta toje dalyje, nes dėl vienos iš to reglamento 19 straipsnio 5 dalyje nustatytų priežasčių neįmanoma naudotis decentralizuota IT sistema:

3.3.1. Jei perdavimas yra susijęs su kompetentingų institucijų ir paslaugų teikėjų rašytine komunikacija, įskaitant keitimąsi formomis, kaip apibrėžta Reglamento (ES) 2023/1543 19 straipsnio 1 dalyje, perdavimo iniciatorius užregistruoja perdavimą savo decentralizuotos IT sistemos dalyje. Įrašytą informaciją sudaro bent bylos numeris arba rinkmenos nuorodos numeris, jos data ir laikas, siuntėjas ir gavėjas, rinkmenos pavadinimas ir dydis.

3.3.2. Kai perduodama informacija raštu, įskaitant keitimąsi formomis, tarp kompetentingų institucijų, taip pat rašytinė komunikacija su kompetentingomis Sąjungos agentūromis ar įstaigomis, kaip tai suprantama Reglamento (ES) 2023/1543 19 straipsnio 4 dalyje, perdavimo rengėjas užregistruoja perdavimą decentralizuotoje IT sistemoje, visų pirma savo nacionalinėje IT sistemoje arba, kai taikytina, kompetentingos Sąjungos agentūros ar įstaigos valdomose IT sistemose. Įrašytą informaciją sudaro bent bylos numeris arba rinkmenos nuorodos numeris, perdavimo data ir laikas, siuntėjas ir gavėjas, rinkmenos pavadinimas ir dydis.

3.3.3. Kai elektroniniai įrodymai pagal Europos įrodymų pateikimo orderį perduodami alternatyviomis ryšio priemonėmis tarp paslaugų teikėjų ir išduodančiosios valstybės kompetentingų institucijų ([1]) arba kai elektroniniai įrodymai iš vykdančiosios institucijos alternatyviomis priemonėmis perduodami išduodančiosios valstybės kompetentingoms institucijoms pagal Reglamento (ES) 2023/1543 16 straipsnio 9 dalyje numatytą vykdymo procedūrą, rengėjas:

a) pildydamas deklaraciją, registruoja ir perduoda institucijai, kuriai buvo perduoti elektroniniai įrodymai arba suteikta galimybė su jais susipažinti, šią informaciją:

1) informaciją apie siuntėją ir gavėją;

2) metaduomenis, kuriais pateikti elektroniniai įrodymai susiejami su konkrečiu (-iais) Europos įrodymų pateikimo arba saugojimo orderiu (-ais);

3) perdavimo datą ir laiką arba nuorodą, kada elektroniniai įrodymai tapo prieinami gavėjui;

4) informaciją apie perdavimo priemones (pvz., saugaus ryšio, per kurį buvo pateikti elektroniniai įrodymai, įrašas, gavimo arba pristatymo iš pašto tarnybų įrodymas ir kt. ([2]));

5) visą elektroninių įrodymų, perduotų ar kitaip tapusių prieinamais numatytam gavėjui išduodančiojoje valstybėje, rinkmenos pavadinimą (-us);

6) elektroninių įrodymų, perduotų ar kitaip suteiktų numatytam gavėjui išduodančiojoje valstybėje, duomenų dydį;

7) bent viena persiųstų ar suteiktų duomenų maišos santrumpa ir naudoto (-ų) maišos algoritmo (-ų) nuoroda. Šiai (-ioms) maišos santrumpai (-oms) apskaičiuoti naudotas (-i) maišos algoritmas (-ai) turi būti kriptografiškai stiprus (-ūs) bendrai naudojamas (-i) algoritmas (-ai), kuriam (-iems) netaikomi viešai atskleisti trūkumai, pvz., susidūrimai (pvz., SHA-512, SHA3-512, BLAKE2 arba RIPEMD-160, bet galbūt stipresnis algoritmas (-ai), priklausomai nuo technologinės plėtros);

b) kai taikytina, a punkte nurodytoje deklaracijoje nurodoma data ir laikas, iki kurių elektroniniai įrodymai išliks prieinami. Šiuo laikotarpiu išduodančiosios valstybės kompetentingai institucijai suteikiamas pagrįstas terminas elektroniniams įrodymams gauti, kuris yra ne trumpesnis kaip 10 kalendorinių dienų ir ne ilgesnis kaip 45 kalendorinės dienos nuo to momento, kai elektroniniai įrodymai tapo prieinami. Išduodančiosios valstybės kompetentingos institucijos prašymu iniciatoriaus nurodytas laikotarpis konkrečiu atveju gali būti pratęstas;

c) gali įrašyti ir perduoti bet kokią su byla susijusią papildomą informaciją ar pastabas institucijai, kuriai buvo perduoti elektroniniai įrodymai arba suteikta galimybė jais naudotis, kaip a punkte nurodytos deklaracijos dalį.

3.4. Atsižvelgiant į Reglamento (ES) 2023/1543 28 straipsnį, bazinio sistemos modelio programinė įranga programiškai renka, perduoda arba kitaip suteikia prieigą prie to straipsnio 2 dalyje nurodytų statistinių duomenų tiek struktūrizuotais (pvz., XML), tiek nestruktūrizuotais (pvz., PDF) duomenų formatais. Pagal Reglamento (ES) 2023/1543 28 straipsnio 3 dalį valstybių narių valdomi nacionaliniai portalai, jei jie techniškai pritaikyti ([3]), taip pat gali perduoti arba teikti šiuos statistinius duomenis Komisijai taikant automatizuotą procesą. Komisija paskelbia gaires dėl duomenų struktūros ir šių statistinių duomenų rinkimo ir perdavimo metodo.

([1]) Siekiant didesnio aiškumo, nuorodos į kompetentingas nacionalines institucijas *mutatis mutandis* taip pat suprantamos kaip taikomos Eurojusto nacionaliniams nariams, Europos prokurorams ir Europos deleguotiesiems prokurorams, jei jie yra įgalioti vykdyti tas pačias funkcijas pagal ES teisę ir nacionalinę teisę.

([2]) Reikėtų priminti, kad pagal 19 straipsnio 5 dalį perdavimas tokiomis alternatyviomis ryšio priemonėmis turi atitikti greito, saugaus ir patikimo ryšio reikalavimus, leidžiančius gavėjui nustatyti autentiškumą.

([3]) „Nacionaliniai portalai“ turėtų būti suprantami kaip nacionalinės IT sistemos, kurios yra decentralizuotos IT sistemos dalis, kaip apibrėžta Reglamento (ES) 2023/1543 3 straipsnio 21 punkte.

4. **Ryšių protokolai**

4.1. Decentralizuota IT sistema naudoja saugius interneto protokolus, skirtus:

a) kompetentingų institucijų ryšiams decentralizuotoje IT sistemoje;

b) kompetentingų institucijų ir Sąjungos agentūrų bei įstaigų ryšiams decentralizuotoje IT sistemoje;

c) kompetentingų institucijų ir paslaugų teikėjų ryšiams per API ir internetinę sąsają ir

d) ryšiams su teismų duomenų baze.

4.2. Siekiant apibrėžti ir perduoti struktūrizuotus duomenis ir metaduomenis, decentralizuotos IT sistemos komponentai grindžiami išsamiais ir visuotinai pripažintais pramonės standartais ir protokolais, pavyzdžiui, SOAP ir REST, visų pirma tais, kuriais remiasi Europos standartizacijos organizacijos, pavyzdžiui, ETSI.

4.3. Perdavimo ir pranešimų protokolų atveju decentralizuota IT sistema grindžiama saugių standartų protokolais, pavyzdžiui:

a) AS4 profilis, skirtas tarpvalstybiniam keitimuisi duomenimis, užtikrinant saugų ir patikimą keitimąsi pranešimais su šifravimu ir neginčijimu;

b) HTTPS/RESTful API, skirtas JSON ir XML formatams palaikyti;

c) SOAP, skirtas didelio patikimumo sąveikai, įskaitant „WS-Security“ tapatumo nustatymui ir šifravimui.

4.4. Siekiant sklandžiai ir sąveikiai keistis duomenimis, decentralizuotos IT sistemos naudojami ryšių protokolai turi atitikti susijusius sąveikumo standartus.

4.5. Kai taikytina, e. įrodymų XML schemoje naudojami atitinkami standartai arba žodynai, būtini siekiant tinkamai patvirtinti šioje schemoje apibrėžtus elementus ir tipus. Tai gali būti:

a) ES e. teisingumo pagrindinis žodynas;

b) besąlyginiai duomenų tipai;

c) Europos Sąjungos kalbų kodų sąrašas.

Be to, kai taikytina, į XML schemą gali būti įtraukti atitinkami ETSI standartai, kad būtų galima naudoti jų apibrėžtis.

4.6. Komisija apibrėžia bendros API specifikacijas, kurias vykdymo užtikrinimo valstybės pateikia paslaugų teikėjams kaip prieigos prie decentralizuotos IT sistemos priemonę. Kiek tai įmanoma ir pagrįsta, ši API grindžiama ETSI TS 104 144 („E. įrodymų reglamento (ES) 2023/1543 sąsajos apibrėžtis nacionalinėms institucijoms ir paslaugų teikėjams“).

4.7. Saugumo ir tapatumo nustatymo protokolų atveju decentralizuota IT sistema grindžiama standartais pagrįstais protokolais, pavyzdžiui:

a) TLS (transporto lygmens saugumas) užšifruotiems ir tapatumo nustatymu pagrįstiems ryšiams tinklais, palaikant abipusį tapatumo nustatymą naudojant X.509 skaitmeninius sertifikatus;

b) „Oauth / OpenID Connect“ (OIDC) saugiam tapatumo nustatymui ir leidimų suteikimui;

c) viešojo rakto infrastruktūra ir skaitmeniniai parašai saugiems raktų mainams ir pranešimų vientisumo tikrinimui, naudojant patikimų sertifikavimo institucijų (SI) išduotus skaitmeninius sertifikatus (X.509).

5. **Informacijos saugumo tikslai ir atitinkamos techninės priemonės**

5.1. Keičiantis informacija per decentralizuotą IT sistemą, techninės priemonės, kuriomis užtikrinami būtiniausi informacinių technologijų saugumo standartai, apima:

a) priemones, kuriomis užtikrinamas informacijos konfidencialumas, be kita ko, naudojant saugius ryšio kanalus;

b) priemones, kuriomis užtikrinamas duomenų (pranešimų, formų, dokumentų ir elektroninių įrodymų) vientisumas saugojimo ir perdavimo metu;

c) priemones, kuriomis užtikrinama, kad decentralizuotoje IT sistemoje nebūtų galima išsižadėti informacijos siuntėjo kilmės ir kad nebūtų galima išsižadėti informacijos gavimo;

d) priemones, kuriomis užtikrinamas prieinamumas užtikrinant nuolatinę prieigą prie paslaugų ir duomenų, užkertant kelią sutrikimams dėl kibernetinių išpuolių ar gedimų;

e) priemones, skirtos užtikrinti, kad saugumo įvykiai būtų registruojami laikantis pripažintų tarptautinių rekomendacijų dėl informacinių technologijų saugumo standartų;

f) priemones, kuriomis užtikrinamas naudotojo autentiškumo patvirtinimas ir leidimas, ir priemonės, skirtos prie decentralizuotos IT sistemos prijungtų sistemų tapatybei patikrinti.

5.2. Decentralizuotos IT sistemos komponentai užtikrina saugų ryšį ir duomenų perdavimą, naudodami šifravimą, viešojo rakto infrastruktūrą su skaitmeniniais tapatumo nustatymo ir saugaus keitimosi raktais sertifikatais ir saugius pranešimų siuntimo protokolus, pavyzdžiui, AS4 („ebMS“), RESTful API ir SOAP, kad būtų išlaikytas pranešimų konfidencialumas ir vientisumas.

5.3. Decentralizuotos IT sistemos komponentai kuriami laikantis pritaikytosios ir standartizuotosios duomenų apsaugos principo ir įgyvendinamos tinkamos administracinės, organizacinės ir techninės priemonės aukštam kibernetinio saugumo lygiui užtikrinti.

5.4. Komisija projektuoja, plėtoja ir prižiūri bazinio sistemos modelio programinę įrangą laikydamasi Reglamente (ES) 2018/1725 nustatytų duomenų apsaugos reikalavimų ir principų. Komisijos teikiama bazinio sistemos modelio programinė įranga sudaro sąlygas valstybėms narėms vykdyti savo pareigas pagal atitinkamai Europos Parlamento ir Tarybos reglamentą (ES) 2016/679 ([4]) ir Europos Parlamento ir Tarybos direktyvą (ES) 2016/680 ([5]), priklausomai nuo to, kuris teisės aktas taikomas.

5.5. Valstybės narės, kurios naudoja nacionalinę IT sistemą, kuri nėra bazinio sistemos modelio programinė įranga, įgyvendina priemones, būtinas užtikrinti, kad ji atitiktų atitinkamai Reglamento (ES) 2016/679 ir Direktyvos (ES) 2016/680 reikalavimus.

5.6. Atsižvelgdami į savo dalyvavimą decentralizuotoje IT sistemoje, Eurojustas ir Europos prokuratūra įgyvendina priemones, būtinas užtikrinti, kad jų atitinkamos IT sistemos atitiktų Reglamento (ES) 2018/1725 ir jų steigimo aktų reikalavimus.

5.7. Valstybės narės, Eurojustas ir Europos prokuratūra, laikydamiesi savo atitinkamos politikos, nustato patikimus grėsmių nustatymo ir reagavimo į incidentus mechanizmus, skirtus decentralizuotai IT sistemai priklausančioms IT sistemoms, už kurias jie yra atsakingi, kad būtų užtikrintas savalaikis saugumo incidentų nustatymas, padarinių sušvelninimas ir atkūrimas po jų.

6. **Elektroninių įrodymų** ([6]) **šifravimas**

6.1. Nedarant poveikio decentralizuotos IT sistemos nustatytoms saugumo priemonėms, kompetentingos institucijos, išduodamos Europos įrodymų pateikimo orderį, gali papildomai pateikti specialų X.509 viešąjį sertifikatą asimetriniam elektroninių įrodymų šifravimui.

([4]) 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (OL L 119, 2016 5 4, p. 1).

([5]) 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuriuo panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR (OL L 119, 2016 5 4, p. 89).

([6]) Siekiant išvengti abejonių, terminas „elektroniniai įrodymai“ apima tik Reglamento (ES) 2023/1543 3 straipsnio 8 punkte pateiktą apibrėžtį.

6.2. Už 6.1 punkte nurodytų sertifikatų išdavimą, valdymą, tikrinimą ir visus susijusius aspektus kartu su atitinkama viešojo rakto infrastruktūra atsako tik išduodančioji valstybė narė.

6.3. Nedarant poveikio būsimai technologinei raidai, viešaisiais sertifikatais remiami sektoriaus standartiniai šifravimo algoritmai, pvz., RSA (Rivest–Shamir–Adleman) arba ECDH Diffie-Hellman elipsinė kreivė), skirti ECC (kriptografijos elipsinė kreivė).

6.4. Viešieji sertifikatai turi turėti atitinkamą „keyUsage“ plėtinį, pvz., „keyEncipherment“ arba „dataEncipherment“, skirtą RSA grindžiamiems sertifikatams, ir „keyAgreement“, skirtą ECC grindžiamiems sertifikatams. Sertifikatai pateikiami slaptojo pašto (angl. *Privacy-Enhanced Mail*, PEM) arba išskirtinių kodavimo taisyklių (angl. *Distinguished Encoding Rules*, DER) formatu.

6.5. Jeigu išduodančioji institucija pateikė X.509 viešąjį sertifikatą ir jeigu paslaugų teikėjas siunčia pateikiamus elektroninius įrodymus pagal Europos įrodymų pateikimo orderį, teikėjas, prieš siųsdamas tuos duomenis per decentralizuotą IT sistemą, užšifruoja elektroninius įrodymus, naudodamas atitinkamą X.509 viešąjį sertifikatą, pateiktą išduodančiosios valstybės.

6.6. Jeigu išduodančioji institucija pateikė X.509 viešąjį sertifikatą, tačiau elektroninių įrodymų perduoti šifruota forma neįmanoma dėl techninių ar kitų pateisinamų priežasčių ir nedarant poveikio Reglamento (ES) 2023/1543 19 straipsnio 5 dalies nuostatai, paslaugų teikėjas gali perduoti duomenis be turinio šifravimo. Tokiais atvejais paslaugų teikėjas išduodančiajai institucijai pateikia pagrįstą paaiškinimą.

7. **Minimalūs prieinamumo tikslai**

7.1. Valstybės narės, Eurojustas ir Europos prokuratūra užtikrina galimybę 24 valandas ir 7 dienas per savaitę naudotis decentralizuotos IT sistemos, už kurią jie yra atsakingi, komponentais, o tikslinė techninio prieinamumo norma yra bent 98 % per metus, išskyrus planinę techninę priežiūrą.

7.2. Komisija užtikrina, kad teismų duomenų bazė būtų prieinama 24 valandas, 7 dienas per savaitę, o tikslinė techninio prieinamumo norma būtų didesnė nei 99 % per metus, išskyrus planinę techninę priežiūrą.

7.3. Kiek tai įmanoma, darbo dienomis techninės priežiūros operacijos planuojamos nuo 20.00 iki 7.00 val. Vidurio Europos laiku (CET).

7.4. Valstybės narės, Eurojustas ir Europos prokuratūra praneša Komisijai ir kitoms valstybėms narėms apie techninės priežiūros veiklą tokia tvarka:

a) apie techninės priežiūros operacijas, dėl kurių gali būti neprieinama iki 4 valandų, – prieš 5 darbo dienas;

b) apie techninės priežiūros operacijas, dėl kurių paslaugomis gali būti neįmanoma naudotis 4–12 valandų – prieš 10 darbo dienų;

c) apie techninės priežiūros operacijas, dėl kurių paslaugomis gali būti neįmanoma naudotis daugiau kaip 12 valandų – prieš 30 darbo dienų;

7.5. Jei valstybės narės, Eurojustas ar Europos prokuratūra yra nustačiusios konkrečius reguliarios techninės priežiūros laikotarpius, jie informuoja Komisiją ir decentralizuotos IT sistemos dalyvius apie laiką ir dieną (-as), kada planuojami tokie konkretūs reguliarūs techninės priežiūros laikotarpiai. Nepaisant 7.4 punkte nustatytų įpareigojimų, jei tokiu reguliariu konkrečiu laikotarpiu nebūtų galima naudotis decentralizuotos IT sistemos, už kurią atsakingos valstybės narės, Eurojustas ar Europos prokuratūra, komponentais, jie gali nuspręsti nepranešti Komisijai kiekvienu atveju.

7.6. Decentralizuotos IT sistemos komponentų, už kuriuos atsakingos valstybės narės, Eurojustas ar Europos prokuratūra, netikėto techninio gedimo atveju jos nedelsdamos informuoja Komisiją ir decentralizuotos IT sistemos dalyvius apie šį gedimą ir, jei žinoma, apie numatomą atkūrimo laikotarpį.

7.7. Jei valstybė narė yra atsakinga už decentralizuotos IT sistemos komponentų techninės priežiūros veiklą arba netikėtą techninį gedimą, kuris daro neigiamą poveikį paslaugų teikėjų API ir (arba) internetinės sąsajos prieinamumui, atitinkama valstybė narė nedelsdama paskelbia šią informaciją interneto svetainėje ir (arba) perduoda ją jos teritorijoje veikiantiems paslaugų teikėjams.

7.8. Netikėto teismų duomenų bazės techninio gedimo atveju Komisija nedelsdama informuoja valstybes nares, Eurojustą ir Europos prokuratūrą apie duomenų bazės neprieinamumą ir, jei žinoma, numatomą atkūrimo laikotarpį.

7.9. Paslaugų teikimo sutrikimo atveju valstybės narės, Eurojustas ir Europos prokuratūra užtikrina, kad paslaugos būtų greitai atkurtos, o duomenų nuostoliai būtų minimalūs, kaip nustatyta atkūrimo laiko tikslu ir atkūrimo taško tikslu.

7.10. Valstybės narės, Eurojustas ir Europos prokuratūra įgyvendina tinkamas priemones pirmiau nurodytiems prieinamumo tikslams pasiekti ir nustato veiksmingo reagavimo į incidentus procedūras.

8. **Kompetentingų institucijų / teismų duomenų bazė (CDB)**

8.1. Atsižvelgiant į Reglamento (ES) 2023/1543 19 straipsnį, decentralizuotos IT sistemos veikimo tikslais labai svarbu sukurti patikimą paslaugų teikėjų ir kompetentingų institucijų duomenų bazę.

8.2. Kompetentingų institucijų patikimoje duomenų bazėje struktūrizuotu formatu pateikiama ši informacija:

a) Reglamento (ES) 2023/1543 19 straipsnio taikymo tikslais – informacija apie kompetentingas institucijas, apie kurias pranešta pagal to reglamento 31 straipsnio 1 dalies a–c punktus, įskaitant informaciją apie:

1) Eurojusto nacionalinius narius, kartu nurodant, ar pagal nacionalinę teisę jie yra įgalioti išduoti Europos įrodymų pateikimo orderius ir Europos įrodymų saugojimo orderius, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (ES) 2018/1727 8 straipsnio 3 ir 4 dalyse ([7]);

2) Europos deleguotuosius prokurorus ir Europos prokurorus, apie kuriuos valstybės narės pranešė pagal Tarybos reglamento (ES) 2017/1939 ([8]) 105 straipsnio 3 dalį kaip kompetentinga išduodančioji institucija pagal Reglamentą (ES) 2023/1543;

b) kai tinkama, informacija, būtina institucijų kompetencijos geografinėms sritims nustatyti, arba kiti atitinkami kriterijai, būtini jų kompetencijai nustatyti;

c) informacija, būtina tinkamam duomenų mainų ir techninių žinučių nukreipimui decentralizuotoje IT sistemoje veikimui užtikrinti.

8.2.1. 8.2 punkto c papunktyje nurodyta informacija apima:

a) informaciją apie valstybę narę, kurioje įsisteigusi paslaugų teikėjo paskirtoji įmonė arba kurioje gyvena jo teisinis atstovas:

1) valstybės narės pavadinimą;

2) centrinę instituciją;

([7]) 2018 m. lapkričio 14 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1727 dėl Europos Sąjungos bendradarbiavimo baudžiamosios teisenos srityje agentūros (Eurojusto) ir kuriuo pakeičiamas ir panaikinamas Tarybos sprendimas 2002/187/TVR (OL L 295, 2018 11 21, p. 138).

([8]) 2017 m. spalio 12 d. Tarybos reglamentas (ES) 2017/1939, kuriuo įgyvendinamas tvirtesnis bendradarbiavimas Europos prokuratūros įsteigimo srityje (OL L 283, 2017 10 31, p. 1).

b) informaciją apie paslaugų teikėją:

1) pavadinimą arba vardą, pavardę;

2) adresą / buveinę;

3) registracijos numerį;

4) teisinę formą;

5) telefono numerį;

6) e. pašto adresą;

c) informaciją apie paskirtąją įmonę / teisinį atstovą:

1) subjekto rūšį (paskirtasis padalinys / teisinis atstovas);

2) pavadinimą arba vardą, pavardę;

3) adresą / buveinę;

4) telefono numerį;

5) e. pašto adresą;

6) bendrą kontaktinį asmenį / subjektą;

7) paslaugų teikėjui / paskirtajai įmonei / teisiniam atstovui priimtiną (-as) oficialiąją (-ąsias) kalbą (-as);

8) Europos Parlamento ir Tarybos direktyvos (ES) 2023/1544 ([9]) 2 straipsnio 1 dalyje nurodytos paslaugos, siūlomos Sąjungoje;

9) ES teisinių priemonių, dėl kurių paskirtas paskirtasis padalinys / teisinis atstovas, rūšį (tais atvejais, kai valstybės narės nedalyvauja įgyvendinant visus atitinkamus ES teisės aktus);

10) teritorinę paskyrimo taikymo sritį;

d) informacijos autentiškumo patvirtinimą:

1) įgaliotojo atstovo vardą ir pavardę;

2) pareigų pavadinimą;

3) adresą;

4) telefono numerį;

5) e. pašto adresą;

6) datą.

8.2.2. 8.2 punkto c papunktyje nurodyta informacija, jei turima, gali apimti:

a) informaciją apie paslaugų teikėją:

1) kontaktinį asmenį, teikiantį užklausas dėl pranešimų (jei tai nėra pasirašantysis asmuo);

2) interneto svetainę;

b) turimų duomenų tipus:

1) kiekvienai susijusiai paslaugai:

— turimų duomenų tipus,

— duomenų kategoriją,

— identifikatorių,

— turimų duomenų laikotarpį;

([9]) 2023 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva (ES) 2023/1544, kuria nustatomos paskirtųjų įmonių ir teisinių atstovų skyrimo elektroniniams įrodymams baudžiamosiose bylose rinkti suderintos taisyklės (OL L 191, 2023 7 28, p. 181, ELI: http://data.europa.eu/eli/dir/2023/1544/oj).

2) papildomą informaciją apie duomenis;

3) papildomą informaciją apie paslaugą (pvz., subrangos santykiai);

c) informaciją apie paskirtąją įmonę / teisinį atstovą:

1) kiti paslaugų teikėjai, kuriems paskirta ši paskirtoji įmonė arba teisinis atstovas;

2) techninės pagalbos kontaktinę informaciją;

3) kontaktinį asmenį skubiais atvejais;

d) techninę informaciją:

1) techninio kontaktinio punkto pavadinimą;

2) techninio kontaktinio punkto telefono numerį;

3) techninio kontaktinio punkto e. pašto adresą;

4) API URL, kad būtų galima dinamiškai gauti informaciją apie duomenų rūšis;

5) prisijungimo prie nacionalinės IT sistemos tipą:

— internetinę sąsają,

— API,

— pranešimų API URL.

8.3. Atsižvelgiant į decentralizuotos IT sistemos veiklos poreikius:

a) Komisija yra atsakinga už patikimos duomenų bazės kūrimą, priežiūrą, veikimą ir palaikymą;

b) Komisija suteikia prieigą prie patikimos duomenų bazės, kuri gali būti prieinama kompetentingoms institucijoms, Eurojustui ir Europos prokuratūrai per API, kad jie galėtų dalyvauti decentralizuotoje IT sistemoje;

c) valstybės narės užtikrina, kad patikimoje duomenų bazėje 8.2 punkto a ir b papunkčiuose nurodyta informacija apie jų kompetentingas institucijas būtų išsami, tiksli ir nuolat atnaujinama;

d) patikima duomenų bazė suteikia valstybėms narėms galimybę teikti ir atnaujinti informaciją apie savo paslaugų teikėjus, o decentralizuotoje IT sistemoje dalyvaujančios institucijos – programiškai susipažinti su ta informacija ir ją gauti;

e) valstybės narės ir paslaugų teikėjai užtikrina, kad patikimoje duomenų bazėje 8.2 punkto c papunktyje nurodyta informacija būtų išsami, tiksli ir nuolat atnaujinama.