EUROPOS
KOMISIJA

Briuselis, 2020 06 23
COM(2020) 255 final

ANNEX

PRIEDAS

prie

Pasiūlymo dėl Tarybos sprendimo

dėl pozicijos, kurios Europos Sąjungos vardu turi būti laikomasi Europos Sąjungos ir Šveicarijos Konfederacijos susitarimu dėl jų šiltnamio efektą sukeliančių dujų apyvartinių taršos leidimų prekybos sistemų susiejimo įsteigtame Jungtiniame komitete, dėl bendrų darbo procedūrų patvirtinimo

EUROPOS SĄJUNGOS IR ŠVEICARIJOS KONFEDERACIJOS SUSITARIMU DĖL JŲ ŠILTNAMIO EFEKTĄ SUKELIANČIŲ DUJŲ APYVARTINIŲ TARŠOS LEIDIMŲ PREKYBOS SISTEMŲ SUSIEJIMO ĮSTEIGTO JUNGTINIO KOMITETO SPRENDIMAS Nr. 1/2020

... m. .... d.

dėl bendrų darbo procedūrų (BDP)

JUNGTINIS KOMITETAS

atsižvelgdamas į Europos Sąjungos ir Šveicarijos Konfederacijos susitarimą dėl jų šiltnamio efektą sukeliančių dujų apyvartinių taršos leidimų prekybos sistemų susiejimo[1] (toliau – Susitarimas), ypač į jo 3 straipsnį,

kadangi:

(1) 2019 m. gruodžio 5 d. Jungtinio komiteto sprendimu Nr. 2/2019 Susitarimo I ir II priedai buvo iš dalies pakeisti ir taip buvo įvykdytos Susitarime nustatytos susiejimo sąlygos;

(2) Jungtiniam komitetui priėmus Sprendimą Nr. 2/2019, Susitarimo šalys, vadovaudamosi Susitarimo 21 straipsnio 3 dalimi, apsikeitė ratifikavimo arba patvirtinimo dokumentais, nes, jų manymu, visos Susitarime apibrėžtos susiejimo sąlygos buvo įvykdytos;

(3) pagal Susitarimo 21 straipsnio 4 dalį Susitarimas įsigaliojo 2020 m. sausio 1 d.;

(4) pagal Susitarimo 3 straipsnio 6 dalį Šveicarijos registro administratorius ir Sąjungos vyriausiasis administratorius, atsižvelgdami į Šalių vidaus teisės prioritetus, turėtų nustatyti bendras darbo procedūras (toliau – BDP), susijusias su techniniais ar kitais klausimais, kurie yra būtini jungties tarp Sąjungos registro Europos Sąjungos sandorių žurnalo (ESSŽ) ir Šveicarijos registro Šveicarijos papildomų sandorių žurnalo (angl. *Swiss Supplementary Transaction Log*, SSTL) veikimui užtikrinti. BDP turėtų įsigalioti, kai jas sprendimu patvirtina Jungtinis komitetas;

(5) pagal Susitarimo 13 straipsnio 1 dalį Jungtinis komitetas, atsižvelgdamas į Šalių vidaus teisės prioritetus, turėtų susitarti dėl techninių gairių, kuriomis būtų užtikrintas tinkamas Susitarimo įgyvendinimas, įskaitant techninius ar kitus klausimus, būtinus jungties veikimui užtikrinti. Technines gaires gali parengti pagal Susitarimo 12 straipsnio 5 dalį sudaryta darbo grupė. Į darbo grupę turėtų būti įtraukti bent Šveicarijos registro administratorius ir Sąjungos registro vyriausiasis administratorius; ji turėtų padėti Jungtiniam komitetui vykdyti Susitarimo 13 straipsnyje nurodytas funkcijas;

(6) atsižvelgiant į techninį gairių pobūdį ir tai, kad jas reikės koreguoti atsižvelgiant į vykstančius pokyčius, Šveicarijos registro administratoriaus ir Sąjungos vyriausiojo administratoriaus parengtos techninės gairės turėtų būti teikiamos Jungtiniam komitetui susipažinti arba, jei reikia, patvirtinti,

PRIĖMĖ ŠĮ SPRENDIMĄ:

1 straipsnis

Prie šio sprendimo pridėtos bendros darbo procedūros (toliau – BDP) yra patvirtinamos.

[1] OL L 322, 2017 12 7, p. 3.

2 straipsnis

Vadovaujantis Susitarimo 12 straipsnio 5 dalimi, sudaroma darbo grupė. Ji padeda Jungtiniam komitetui užtikrinti tinkamą Susitarimo įgyvendinimą, tarp kitų dalykų – parengti BDP įgyvendinti reikalingas technines gaires.

Į darbo grupę įtraukiamas bent Šveicarijos registro administratorius ir Sąjungos registro vyriausiasis administratorius.

3 straipsnis

Šis sprendimas įsigalioja jo priėmimo dieną.

Priimta anglų kalba Briuselyje 2020 m. ... d.

Jungtinio komiteto vardu

Europos Sąjungos sekretorius	*Pirmininkas*	*Šveicarijos sekretorius*

PRIEDĖLIS

PRIEDAS

BENDROS DARBO PROCEDŪROS (BDP)

pagal Europos Sąjungos ir Šveicarijos Konfederacijos susitarimo dėl jų šiltnamio efektą sukeliančių dujų apyvartinių taršos leidimų prekybos sistemų susiejimo 3 straipsnio 6 dalį
Laikino sprendimo įgyvendinimo procedūros

1. SĄVOKŲ ŽODYNĖLIS

1-1 lentelė. Santrumpos ir apibrėžtys

Santrumpa arba sąvoka	Apibrėžtis
Skaitmeninį sertifikatą teikianti organizacija	Skaitmeninius sertifikatus išduodantis subjektas
ŠK	Šveicarijos Konfederacija
ATLPS	Apyvartinių taršos leidimų prekybos sistema
ES	Europos Sąjunga
IVG	Incidentų valdymo grupė
Informacijos išteklius	Įmonei arba organizacijai vertingas informacijos vienetas.
IT	Informacinės technologijos
ITIB	Informacinių technologijų infrastruktūros biblioteka
ITPV	IT paslaugų valdymas
STS	Susiejimo techniniai standartai
Registras	Pagal ATLPS išduotų apyvartinių taršos leidimų apskaitos sistema, kurioje registruojami elektroninėse sąskaitose laikomų leidimų turėtojai
PkU	Pakeitimo užklausa
NIS	Neskelbtinos informacijos sąrašas
PslU	Paslaugos užklausa
Vikis	Interneto svetainė, kurioje naudotojai gali keistis informacija ir duomenimis pildydami arba koreguodami turinį tiesiogiai interneto svetainės naršyklėje.

2. ĮŽANGA

2017 m. lapkričio 23 d. Europos Sąjungos ir Šveicarijos Konfederacijos susitarime dėl jų šiltnamio efektą sukeliančių dujų apyvartinių taršos leidimų prekybos sistemų susiejimo (toliau – Susitarimas) numatytas abipusis apyvartinių taršos leidimų, kuriuos galima naudoti atitikčiai užtikrinti pagal Europos Sąjungos apyvartinių taršos leidimų prekybos sistemą (ES ATLPS) arba Šveicarijos apyvartinių taršos leidimų prekybos sistemą (Šveicarijos ATLPS), pripažinimas. ES ATLPS ir Šveicarijos ATLPS susiejimas praktiškai įgyvendinamas sukuriant tiesioginę jungtį tarp Sąjungos registro Europos Sąjungos sandorių žurnalo (ESSŽ) ir Šveicarijos registro Šveicarijos papildomų sandorių žurnalo (angl. *Swiss Supplementary Transaction Log*, SSTL), kad pagal bet kurią iš šių dviejų ATLPS išduoti apyvartiniai taršos leidimai galėtų būti perkelti iš vieno registro į kitą (Susitarimo 3 straipsnio 2 dalis). Siekiant praktiškai susieti ES ATLPS ir Šveicarijos ATLPS, 2020 m. gegužės mėn. arba kuo anksčiau po šios datos pradedamas taikyti laikinas sprendimas. Šalys bendradarbiauja siekdamos kuo anksčiau pakeisti šį laikiną sprendimą nuolatine registro jungtimi (Susitarimo II priedas).

Pagal Susitarimo 3 straipsnio 6 dalį Šveicarijos registro administratorius ir Sąjungos vyriausiasis administratorius, atsižvelgdami į Šalių vidaus teisės prioritetus, nustato su techniniais ar kitais klausimais, būtinais jungties veikimui užtikrinti, susijusias bendras darbo procedūras (BDP). Administratorių parengtos BDP įsigalioja, kai jas sprendimu patvirtina Jungtinis komitetas.

Šiame dokumente išdėstytas BDP sprendimu Nr. 1/2020 turi patvirtinti Jungtinis komitetas. Pagal šį sprendimą Jungtinis komitetas prašo Šveicarijos registro administratoriaus ir Sąjungos vyriausiojo administratoriaus parengti išsamesnes susiejimo praktinio įgyvendinimo technines gaires ir užtikrinti, kad jos būtų nuolat tikslinamos atsižvelgiant į technikos pažangą ir naujus reikalavimus, susijusius su jungties sauga ir saugumu ir jos veiksmingu ir efektyviu veikimu.

2.1. Taikymo sritis

Šiame dokumente įtvirtintas bendras Susitarimo šalių susitarimas dėl jungties tarp ES ATLPS ir Šveicarijos APTLPS registrų kūrimo procedūrinių pagrindų. Nors šiame dokumente yra išdėstyti bendri procedūriniai jungties veikimo reikalavimai, tam, kad jungtis būtų įgyvendinta praktiškai, bus reikalingos tam tikros papildomos techninės gairės.

Kad jungtis tinkamai veiktų, bus reikalingos techninės jungties praktinio įgyvendinimo specifikacijos. Pagal Susitarimo 3 straipsnio 7 dalį šie aspektai aprašomi Jungtinio komiteto sprendimu atskirai priimtuose susiejimo techniniuose standartuose (toliau – STS).

BDP paskirtis – užtikrinti, kad su jungties tarp ES ATLPS ir Šveicarijos ATLPS registrų veikimu susijusios IT paslaugos būtų teikiamos veiksmingai ir efektyviai, ypač užtikrinti, kad paslaugų užklausos būtų vykdomos, aptarnavimo sutrikimai ir problemos būtų šalinami ir eilinės darbo užduotys būtų vykdomos pagal tarptautinius IT paslaugų valdymo standartus.

Pagal laikiną sprendimą, dėl kurio susitarta, bus reikalingos tik šios šiame dokumente aprašytos BDP:

- incidentų valdymas;
- problemų valdymas;
- užklausų vykdymas;
- pakeitimų valdymas;
- versijų valdymas;

- saugumo incidentų valdymas;
- informacijos saugumo valdymas.

Ateityje, kai bus įdiegta nuolatinė registrų jungtis, reikiamas BDP nuostatas reikės patikslinti ir papildyti.

2.2. Adresatai

Šios BDP yra skirtos ES ir Šveicarijos registrų priežiūros grupėms.

3. METODIKA IR STANDARTAI

Visoms BDP taikomas principas:

- ES ir ŠK susitaria šias BDP aprašyti remiantis ITIB (Informacinių technologijų infrastruktūros biblioteka, 3 versija). Šiame standarte apibrėžta praktika naudojama ir pritaikoma pagal konkrečius su laikinu sprendimu susijusius poreikius.
- Abi Šalys ryšį palaiko ir BDP vykdymą koordinuoja, kai tai yra reikalinga BDP vykdyti, per ŠK ir ES registrų aptarnavimo centrus. Užduotys visada skiriamos vienos Šalies struktūroje.
- Jeigu dėl BDP tvarkymo nesutariama, nesutarimą analizuoja ir sprendžia abu aptarnavimo centrai. Jeigu susitarti nepavyksta, kreipiamasi į aukštesnį sprendimų lygmenį dėl bendro sprendimo priėmimo.

Sprendimų lygmenys	**ES**	**ŠK**
1-asis lygmuo	ES aptarnavimo centras	ŠK aptarnavimo centras
2-asis lygmuo	ES operacijų valdytojas	ŠK registro taikomosios programos valdytojas
3-asis lygmuo	Jungtinis komitetas (jis šią atsakomybę gali deleguoti pagal Susitarimo 12 straipsnio 5 dalį)	
4-asis lygmuo	ngtinis komitetas, jeigu 3-iojo lygmens atsakomybė yra deleguojama	

- Kiekviena Šalis, atsižvelgdama į šių BDP reikalavimus ir su šiomis BDP susijusias sąsajas, nustato savo registro sistemos veikimo procedūras.
- BDP palaikyti yra naudojama IT paslaugų valdymo priemonė, konkrečiai incidentų valdymo, problemų valdymo ir užklausų vykdymo moduliai, taip pat Šalys tuo tikslu palaiko tarpusavio ryšį.
- Taip pat leidžiama keistis informacija e. paštu.
- Abi Šalys užtikrina, kad būtų laikomasi tvarkymo instrukcijose nustatytų informacijos saugumo reikalavimų.

4. INCIDENTŲ VALDYMAS

Incidentų valdymo proceso paskirtis – kuo greičiau ir kuo mažiau trukdant veiklai atkurti įprastą IT paslaugų lygį.

Incidentų valdymo specialistai taip pat turėtų tvarkyti incidentų registrą – jis reikalingas atskaitomybės tikslais, juo taip pat būtų remiamasi per kitus procesus, kad juos būtų galima nuolat tobulinti.

- Incidentų valdymą bendrai sudaro ši veikla:
- incidentų nustatymas ir registravimas;
- klasifikavimas ir pradinė pagalba;
- tyrimas ir problemos nustatymas;
- sprendimas ir atkūrimas;
- incidento užbaigimo procedūra.

Per visą incidento gyvavimo ciklą incidentų valdymo proceso specialistai turi nuolat prižiūrėti, kas atsakingas už vykdomas užduotis, vykdyti stebėseną, sekti, kaip vykdomos užduotys, ir palaikyti ryšį.

4.1. Incidentų nustatymas ir registravimas

Incidentą gali nustatyti priežiūros grupė, jis gali būti nustatytas automatinėmis stebėsenos priemonėmis arba jį gali nustatyti įprastą stebėseną vykdantys techniniai darbuotojai.

Incidentą nustačius, jis registruojamas ir jam suteikiama unikali identifikavimo žyma, kad incidentą būtų galima tinkamai sekti ir stebėti. Unikali incidento identifikavimo žyma – tai žyma, kurią incidentą užfiksavusios Šalies (ES arba ŠK) aptarnavimo centras priskiria bendroje pagalbos prašymų sistemoje (angl. *ticketing system*) ir kuri turi būti naudojama visoje su incidentu susijusioje komunikacijoje.

Visais atvejais kontaktinio centro funkcijas atlieka pagalbos prašymą užregistravusios Šalies aptarnavimo centras.

4.2. Klasifikavimas ir pradinė pagalba

Incidentų klasifikavimo paskirtis – padėti suprasti ir nustatyti, kuriai sistemai ir (arba) paslaugai padarytas poveikis ir kokio dydžio tas poveikis yra. Kad klasifikavimas būtų veiksmingas, juo remiantis incidentas turi būti nukreipiamas spręsti į reikiamą padalinį iš karto, kad incidentą būtų galima išspręsti greičiau.

Klasifikavimo etapu incidentas priskiriamas kuriai nors kategorijai ir pagal incidento poveikį bei sprendimo skubumą jam priskiriamas prioritetas, kad incidentas būtų sprendžiamas laikantis tą prioritetą atitinkančių terminų.

Jeigu dėl incidento gali būti padarytas poveikis neskelbtinų duomenų konfidencialumui, vientisumui ir (arba) sistemos prieinamumui, incidentas taip pat pripažįstamas saugumo incidentu ir valdomas laikantis šio dokumento skyriuje „Saugumo incidentų valdymas“ aprašyta tvarka.

Jeigu tai įmanoma, pirminį įvertinimą atlieka ir problemą nustato pagalbos prašymą užregistravęs aptarnavimo centras. Tai darydamas aptarnavimo centras analizuoja, ar incidentas kilo dėl jau žinomos klaidos. Jeigu incidentas kilo dėl jau žinomos klaidos, incidento sprendimo būdas arba aplinkinis sprendimas jau yra žinomi ir užfiksuoti dokumentuose.

Jeigu aptarnavimo centrui incidentą pavyksta sėkmingai išspręsti, jis atlieka incidento užbaigimo procedūrą, nes pagrindinis incidentų valdymo tikslas (būtent – greitai atkurti paslaugas galutiniam naudotojui) buvo pasiektas. Jeigu incidento išspręsti nepavyksta, aptarnavimo centras kreipiasi dėl incidento sprendimo į atitinkamą incidentų šalinimo grupę, kad ši išnagrinėtų incidentą ir nustatytų problemą.

4.3. Tyrimas ir problemos nustatymas

Incidento tyrimo ir problemos nustatymo procedūros vykdomos, kai aptarnavimo centrui incidento išspręsti per pradinį incidento įvertinimą nepavyksta ir dėl to incidentą spręsti perduodama kitam sprendimų lygmeniui. Incidento perdavimas spręsti kitam sprendimų lygmeniui yra atskira tyrimo ir problemos nustatymo proceso dalis.

Įprastai šiuo tyrimo ir problemos nustatymo etapu yra bandoma incidentą atkurti kontroliuojamomis sąlygomis. Incidentą tiriant ir nustatant problemą svarbu tinkamai suprasti įvykių, dėl kurių įvyko incidentas, seką.

Jeigu incidentas perduodamas spręsti kitam sprendimų lygmeniui, yra pripažįstama, kad incidento pradiniu pagalbos lygmeniu išspręsti nepavyko ir kad incidento sprendimą reikia perduoti aukštesnio lygmens pagalbos grupei arba kitai Šaliai. Incidento sprendimas kitam sprendimų lygmeniui gali būti perduodamas dviem kryptimis: horizontaliai (pagal funkcijas) arba vertikaliai (pagal hierarchiją).

Aptarnavimo centras, kuris užregistravo incidentą ir inicijavo jo sprendimą, yra atsakingas už incidento sprendimo perdavimą atitinkamam padaliniui ir už bendros incidento sprendimo būklės ir jo perdavimo stebėjimą.

Šalis, kuriai incidentas perduotas spręsti, yra atsakinga už reikiamų veiksmų įgyvendinimą laiku ir grįžtamosios informacijos pateikimą savo Šalies aptarnavimo centrui.

4.4. Sprendimas ir atkūrimas

Incidentą visapusiškai išsiaiškinus, jis išsprendžiamas ir padėtis atkuriama. Incidento išsprendimas reiškia, kad randamas būdas, kaip ištaisyti atsiradusią problemą. Padėties atkūrimas – tai sprendimo būdo pritaikymas.

Kai atitinkamas padalinys paslaugų sutrikimą pašalina, informacija apie incidentą vėl perduodama atitinkamam incidentą užregistravusiam aptarnavimo centrui, o šis susisiekia su apie incidentą pranešusiu asmeniu ir įsitikina, kad klaida ištaisyta ir kad galima atlikti incidento užbaigimo procedūras. Per incidento sprendimo procesą padarytos išvados yra užregistruojamos, kad jomis būtų galima pasinaudoti ateityje.

Atkūrimo darbus gali atlikti IT priežiūros specialistai arba galutiniam naudotojui gali būti pateiktos instrukcijos, kaip tai padaryti.

4.5. Incidento užbaigimo procedūra

Incidento užbaigimo procedūra – tai paskutinis incidentų valdymo proceso etapas, vykdomas iškart po to, kai incidentas išsprendžiamas.

Svarbiausi veiksmai, įtraukti į incidento užbaigimo veiksmų kontrolinį sąrašą:

- pradinės kategorijos, prie kurios buvo priskirtas incidentas, patikrinimas;
- tinkamas visos informacijos apie incidentą surinkimas;
- tinkamas incidento dokumentavimas ir žinių bazės atnaujinimas;
- tinkamas komunikavimas su kiekvienu suinteresuotuoju subjektu, kuriam incidentas yra tiesiogiai arba netiesiogiai aktualus.

Aptarnavimo centrui atlikus incidento užbaigimo procedūras ir informaciją apie tai perdavus kitai Šaliai, incidentas oficialiai užbaigiamas.

Atlikus incidento užbaigimo procedūras jis nebeatnaujinamas. Jeigu incidentas netrukus pasikartoja, registruojamas naujas incidentas, o ankstesnis incidentas nėra atnaujinamas.

Jeigu incidentą stebi ir ES, ir ŠK aptarnavimo centrai, už galutines incidento užbaigimo procedūras yra atsakingas pagalbos prašymą užregistravęs aptarnavimo centras.

5. PROBLEMŲ VALDYMAS

Šią procedūrą reikėtų vykdyti kaskart, kai nustatoma problema, taigi, kai atsiranda pagrindas vykdyti problemų valdymo procesą. Pagrindinis problemų valdymo proceso tikslas – gerinti kokybę ir mažinti kylančių incidentų skaičių. Problemos priežastis gali būti vienas arba keli incidentai. Kai gaunamas pranešimas apie incidentą, incidentų valdymo specialistai siekia paslaugas atkurti kuo greičiau, jeigu galima – pasinaudodami aplinkiniais sprendimo būdais. Iškilus problemai, stengiamasi išsiaiškinti jos pagrindinę priežastį ir nustatyti, ką reikia pakeisti, kad problema ir su ja susiję incidentai ateityje nesikartotų.

5.1. Problemos nustatymas ir registravimas

Sprendžiant su problema susijusius klausimus kontaktinio centro funkcijas atlieka pagalbos prašymą užregistravęs ES arba ŠK aptarnavimo centras.

Problemos unikali identifikavimo žyma – tai per IT paslaugų valdymo procesą suteikta identifikavimo žyma. Ją reikia nurodyti visuose su šia problema susijusiuose pranešimuose.

Problema gali atsirasti dėl incidento arba būti iškelta savo iniciatyva siekiant ištaisyti kuriuo nors etapu pastebėtus sistemos sutrikimus.

5.2. Prioriteto priskyrimas problemai

Kad problemas būtų lengviau sekti, jas galima suskirstyti į kategorijas pagal problemos rimtumą ir pirmumą tokiu pačiu būdu kaip incidentus, atsižvelgiant į su problema susijusių incidentų poveikį ir dažnumą.

5.3. Problemos tyrimas ir įvertinimas

Problemą gali iškelti kiekviena Šalis. Už problemos registravimą, jos perdavimą spręsti atitinkamam padaliniui ir bendrą būklės stebėjimą yra atsakingas problemos sprendimą inicijavusios Šalies aptarnavimo centras.

Problemos sprendimo grupė, kuriai perduota spręsti problemą, yra atsakinga už problemos išsprendimą laiku ir už ryšio su aptarnavimo centru palaikymą.

Gavusios prašymą, abi Šalys yra atsakingos už pavestų veiksmų įgyvendinimą ir grįžtamosios informacijos pateikimą savo Šalies aptarnavimo centrui.

5.4. Sprendimas

Problemos sprendimo grupė, kuriai pavesta spręsti problemą, yra atsakinga už problemos išsprendimą ir atitinkamos informacijos pateikimą savo Šalies aptarnavimo centrui.

Sprendžiant problemą padarytos išvados užregistruojamos, kad jomis būtų galima pasinaudoti ateityje.

5.5. Problemos užbaigimas

Kai atliekami reikiami pakeitimai ir problema išsprendžiama, problema oficialiai užbaigiama. Problemos užbaigimo procedūras atlieka aptarnavimo centras, kuris problemą užregistravo ir informavo apie ją kitos Šalies aptarnavimo centrą.

6. UŽKLAUSŲ VYKDYMAS

Užklausų vykdymo procesas – tai viso užklausos dėl naujos arba esamos paslaugos ciklo valdymas nuo to momento, kai užklausa užregistruojama ir patvirtinama, iki užklausos

vykdymo užbaigimo. Paslaugų užklausos paprastai būna smulkios, iš anksto apibrėžtos, pasikartojančios, dažnos, iš anksto patvirtintos ir procedūrinės.

Toliau aprašyti pagrindiniai etapai, kuriuos reikia atlikti.

6.1. Užklausos inicijavimas

Informacija, susijusi su paslaugos užklausa, pateikiama ES arba ŠK aptarnavimo centrui e. paštu, telefonu, naudojantis IT paslaugų valdymo priemone arba kitu sutartu ryšio kanalu.

6.2. Užklausos registravimas ir analizė

Visais paslaugų užklausų atvejais kontaktinio centro funkcijas turėtų atlikti ES arba ŠK aptarnavimo centras, priklausomai nuo to, kuri Šalis pateikė paslaugos užklausą. Šis aptarnavimo centras bus atsakingas už paslaugos užklausos registravimą ir reikiamo nuodugnumo analizę.

6.3. Užklausos patvirtinimas

Paslaugos užklausą pateikusios Šalies aptarnavimo centro specialistas patikrina, ar iš kitos Šalies reikia gauti kokius nors patvirtinimus ir, jei reikia, imasi veiksmų, kad juos gautų. Jeigu paslaugos užklausa nepatvirtinama, aptarnavimo centras atnaujina informaciją ir užbaigia užklausą.

6.4. Užklausos vykdymas

Šis etapas skirtas paslaugų užklausoms efektyviai ir veiksmingai sutvarkyti. Atvejai skirstomi į šias kategorijas:

- paslaugos užklausos vykdymas aktualus tik vienai Šaliai. Šiuo atveju Šalis parengia darbo nurodymus ir koordinuoja, kaip jie vykdomi;
- paslaugos užklausos vykdymas aktualus ir ES, ir ŠK. Šiuo atveju aptarnavimo centrai parengia darbo nurodymus savo atsakomybės srityse. Abu aptarnavimo centrai koordinuoja, kaip vykdoma paslaugų užklausa. Visa atsakomybė tenka aptarnavimo centrui, kuris priėmė paslaugos užklausą ir inicijavo jos vykdymą.

Kai paslaugos užklausa įvykdoma, jos būklė pakeičiama į įvykdytą.

6.5. Užklausos perdavimas kitam sprendimų lygmeniui

Jeigu reikia, aptarnavimo centras gali perduoti neįvykdytą paslaugos užklausą atitinkamiems kito lygmens padaliniams (trečiajai šaliai).

Paslaugos užklausos vykdymas perduodamas atitinkamoms trečiosioms šalims, t. y. ES aptarnavimo centras turės kreiptis į ŠK aptarnavimo centrą, jeigu paslaugos užklausos vykdymą reikės perduoti ŠK trečiajai šaliai, ir atvirkščiai.

Trečioji šalis, kuriai paslaugos užklausa perduodama vykdyti, yra atsakinga už tai, kad paslaugos užklausa būtų įvykdyta laiku, ir kad su aptarnavimo centru, kuris perdavė paslaugos užklausą, būtų palaikomas ryšys.

Aptarnavimo centras, kuris užregistravo paslaugos užklausą, yra atsakingas už paslaugos užklausos bendros būklės stebėjimą ir perdavimą.

6.6. Užklausų vykdymo peržiūra

Atsakingas aptarnavimo centras, prieš atlikdamas paslaugos užklausos vykdymo užbaigimo procedūras, pateikia paslaugos užklausos įrašą galutinei kokybės kontrolei atlikti. Taip siekiama užtikrinti, kad paslaugos užklausa būtų faktiškai sutvarkyta ir kad visa informacija,

kuri yra reikalinga užklausos ciklui aprašyti, būtų pateikta ir būtų pakankamai išsami. Be to, per užklausos tvarkymo ciklą padarytos išvados yra užregistruojamos, kad jomis būtų galima pasinaudoti ateityje.

6.7. Užklausos vykdymo užbaigimas

Jeigu Šalys, kurioms paslaugos užklausa buvo perduota, sutinka, kad užklausa yra įvykdyta, o prašymo pateikėjas pripažįsta, kad klausimas išspręstas, užklausos būklė pakeičiama į „užbaigta“.

Paslaugos užklausos vykdymas oficialiai užbaigiamas, kai paslaugos užklausą užregistravęs aptarnavimo centras atlieka užklausos vykdymo užbaigimo procedūras ir informuoja kitos Šalies aptarnavimo centrą.

7. PAKEITIMŲ VALDYMAS

Tikslas – užtikrinti, kad visi IT infrastruktūros valdymo pakeitimai būtų tvarkomi efektyviai ir greitai pagal standartizuotus metodus ir procedūras ir taip būtų užtikrinta, kad su jais susijusių incidentų kiltų kuo mažiau ir visų atitinkamų incidentų poveikis paslaugoms būtų kuo mažesnis. IT infrastruktūra gali būti keičiama reaguojant į problemas arba į išorės reikalavimus, pvz., teisės aktų pakeitimus, pakeitimai taip pat gali būti įgyvendinami savo iniciatyva, siekiant didesnio veiksmingumo ir efektyvumo arba tam, kad būtų galima įgyvendinti verslo iniciatyvas ar kad į jas būtų atsižvelgta.

Pakeitimų valdymo procesą sudaro įvairūs etapai, kuriais visi pakeitimo užklausos aspektai yra užregistruojami, kad ateityje juos būtų galima atsekti. Per šiuos procesus užtikrinama, kad prieš pakeitimą pradedant taikyti praktiškai, jis būtų patvirtintas ir ištestuotas. Versijų valdymo procesu užtikrinamas sėkmingas įdiegimas.

7.1. Pakeitimo užklausa

Pakeitimo užklausa teikiama pakeitimų valdymo grupei tikrinti ir tvirtinti. Visų pakeitimų užklausų atvejais kontaktinio centro funkcijas atlieka ES arba ŠK aptarnavimo centras, priklausomai nuo to, kuri Šalis pateikė užklausą. Šis aptarnavimo centras bus atsakingas už užklausos registravimą ir reikiamo nuodugnumo analizę.

Galimos pakeitimų užklausų priežastys:

- incidentas, dėl kurio atsirado pakeitimo poreikis;
- esama problema, dėl kurios reikalingas pakeitimas;
- galutinio naudotojo užklausa dėl naujo pakeitimo;
- pakeitimo poreikis atsiranda vykdant nuolatinę techninę priežiūrą;
- teisės aktų pakeitimai.

7.2. Pakeitimų vertinimas ir planavimas

Šiuo etapu atliekama pakeitimo vertinimo ir planavimo veikla. Jis apima prioritetų priskyrimo ir planavimo veiklą, kad rizika ir poveikis būtų kuo mažesni.

Jeigu pakeitimo užklausos vykdymas yra aktualus ir ES, ir ŠK, pakeitimo užklausą užregistravusi Šalis pakeitimo įvertinimą ir planą sutikrina su kita Šalimi.

7.3. Pakeitimo patvirtinimas

Visos užregistruotos pakeitimų užklausos turi būti patvirtintos atitinkamu sprendimų lygmeniu.

7.4. Pakeitimų įgyvendinimas

Pakeitimai įgyvendinami versijų valdymo procesu. Abiejų Šalių versijų valdymo grupės vykdo savo procesus, apimančius planavimą ir testavimą. Pakeitimų peržiūra vykdoma užbaigus įgyvendinimą. Siekiant užtikrinti, kad viskas būtų daroma pagal planą, esamas pakeitimų valdymo procesas yra nuolat peržiūrimas ir prireikus atnaujinamas.

8. VERSIJŲ VALDYMAS

Versija – tai vienas arba keli į vieną versijos planą įtraukti IT paslaugos pakeitimai, dėl kurių turės būti gautas leidimas, kurie turės būti parengti, sudėti į visumą, ištestuoti ir įdiegti visi kartu. Vienos versijos paskirtis gali būti ištaisyti klaidą, atlikti aparatinės įrangos arba kitų komponentų pakeitimus, atlikti programinės įrangos pakeitimus, atnaujinti taikomosios programos versijas, atlikti dokumentų ir (arba) procesų pakeitimus. Kiekvienos versijos turinys yra valdomas, testuojamas ir diegiamas kaip vienas procesas.

Versijos planavimo paskirtis – suplanuoti, sudėti į visumą, ištestuoti, patvirtinti ir parengti apibrėžtoms paslaugoms teikti reikalingus pajėgumus ir taip įvykdyti suinteresuotųjų subjektų reikalavimus bei pasiekti užsibrėžtus tikslus. Visų paslaugos pakeitimų priėmimo kriterijai bus apibrėžti ir dokumentuoti projekto derinimo etapu ir pateikti versijų valdymo grupėms.

Versiją paprastai sudaro keletas problemos ištaisymų ir paslaugos patobulinimų. Į ją įtraukiama nauja arba pakeista programinė įranga ir nauja arba pakeista aparatinė įranga, kurios yra reikalingos patvirtintiems pakeitimais įgyvendinti.

8.1. Versijos planavimas

Pirmuoju šio proceso etapu pakeitimai, dėl kurių gautas leidimas, suskirstomi į versijų paketus, apibrėžiama versijų apimtis ir turinys. Remdamasis šia informacija, Versijų planavimo padalinys parengia versijos sukūrimo, testavimo ir diegimo tvarkaraštį.

Planavimo padalinys turėtų apibrėžti:

- versijos apimtį ir turinį;
- versijos rizikos įvertinimą ir rizikos pobūdį;
- klientus (naudotojus), kuriems versija aktuali;
- už versiją atsakingą grupę;
- versijos parengimo ir diegimo strategiją;
- versijai sudaryti ir diegti reikalingus išteklius.

Abi Šalys viena kitą informuoja apie versijų planavimo ir techninės priežiūros laikotarpius. Jeigu versija yra aktuali ir ES, ir ŠK, Šalys koordinuoja planus ir nustato bendrą techninės priežiūros laikotarpį.

8.2. Versijos paketo kūrimas ir testavimas

Versijų valdymo proceso etapu, kuris yra skirtas versijai sukurti ir testuoti, prieš pakeitimo įdiegimą pasirenkamas versijos arba versijos paketo kūrimo metodas, kontroliuojamos aplinkos palaikymo metodas, visi pakeitimai testuojami visose aplinkose, kuriose jie bus diegiami.

Jeigu versija yra aktuali ir ES, ir ŠK, Šalys koordinuoja parengimo planus ir testavimą. Koordinuojami šie aspektai:

- kaip ir kada bus parengti versijos moduliai ir paslaugos komponentai;

- kokie yra tipiniai vykdymo terminai; kas nutiks, jei bus vėluojama;
- kaip sekti vykdymo pažangą ir gauti patvirtinimą;
- stebėsenos parametrai ir parametrai, pagal kuriuos bus nustatoma, ar versija įdiegta sėkmingai;
- bendri svarbių funkcijų ir pakeitimų testavimo etapai.

Šio paprocesio pabaigoje visi reikalingi versijos komponentai turi būti parengti diegti praktiškai realioje aplinkoje.

8.3. Pasirengimas diegimui

Per pasirengimo paprocesį užtikrinama, kad būtų parengti tinkami komunikacijos planai ir pranešimai, kurie bus siunčiami visiems suinteresuotiesiems subjektams ir galutiniams naudotojams, kuriems tai aktualu, ir kad versija būtų įtraukta į pakeitimų valdymo procesą siekiant užtikrinti, kad visi pakeitimai būtų atliekami kontroliuojamu būdu ir kad dėl jų būtų gauti reikiamo lygmens patvirtinimai.

Jeigu versija yra aktuali ir ES, ir ŠK, Šalys koordinuoja šią veiklą:

- pakeitimo užklausos įrašo, kuriuo nustatomas diegimo tvarkaraštis ir pasirengiama diegimui darbinėje aplinkoje, sukūrimą;
- įgyvendinimo plano sukūrimą;
- ankstesnės būklės atkūrimo metodą, kad tuo atveju, jei diegimas nepavyktų, būtų galima atkurti ankstesnę būseną;
- visoms reikiamoms Šalims siunčiamus pranešimus;
- leidimo diegti versiją gavimą iš atitinkamo sprendimų lygmens.

8.4. Ankstesnės versijos atkūrimas

Jeigu versijos įdiegti nepavyksta arba jeigu atliekant testavimą paaiškėja, kad diegimas buvo nesėkmingas arba kad jis neatitinka suderintų priėmimo ir (arba) kokybės kriterijų, abiejų Šalių versijų valdymo grupės turės atkurti ankstesnę būklę. Reikės informuoti visus reikiamus suinteresuotuosius subjektus, įskaitant galutinius naudotojus, kuriems tai aktualu, ir (arba) tikslinius galutinius naudotojus. Kol negautas patvirtinimas, procesą galima atnaujinti bet kuriame ankstesniame etape.

8.5. Versijos peržiūra ir užbaigimo procedūra

Atliekant diegimo peržiūrą, reikėtų atlikti šiuos veiksmus:

- surinkti grįžtamąją informaciją apie tai, ar atlikus diegimo darbus patenkinti vartotojų, naudotojų lūkesčiai ir lūkesčiai dėl paslaugos teikimo (surinkti grįžtamąją informaciją ir ją išnagrinėti, kad paslaugą būtų galima nuolat tobulinti);
- peržiūrėti visus neįvykdytus kokybės kriterijus;
- patikrinti, ar visi veiksmai, reikalingi pataisymai ir pakeitimai yra užbaigti;
- įsitikinti, kad diegimo pabaigoje neliko jokių pajėgumų, išteklių, gebėjimų arba veikimo problemų;

- patikrinti, ar visos problemos, žinomos klaidos ir aplinkiniai sprendimai yra dokumentuoti ir ar klientas, galutiniai naudotojai, operacijų palaikymo specialistai ir kitos Šalys, kurioms tai aktualu, jiems pritarė;
- stebėti incidentus ir problemas, kurių kilo atliekant diegimo darbus (iš anksto suteikti pagalbą operacijų specialistams, jeigu dėl versijos padidėtų darbo apimtys);
- atnaujinti pagalbinius dokumentus (t. y. techninės informacijos dokumentus);
- oficialiai perduoti įdiegtą versiją aptarnavimo operacijų specialistams;
- dokumentuoti įgytą patirtį;
- iš įgyvendinimo grupių gauti versijos santraukos dokumentą;
- patikrinti pakeitimo užklausos įrašą ir oficialiai atlikti versijos užbaigimo procedūras.

9. SAUGUMO INCIDENTŲ VALDYMAS

Saugumo incidentų valdymas – tai saugumo incidentų tvarkymo procesas, suteikiantis galimybę pranešti apie incidentą suinteresuotiesiems subjektams, kuriems tai gali būti aktualu; incidento vertinimas ir prioriteto jam priskyrimas; reagavimas į incidentą siekiant ištaisyti visus faktinius, įtariamus arba galimus konfidencialumo, neskelbtinos informacijos išteklių prieinamumo arba vientisumo pažeidimus.

9.1. Informacijos saugumo incidentų skirstymas į kategorijas

Visi incidentai, darantys poveikį Sąjungos registro ir Šveicarijos registro jungčiai, yra analizuojami siekiant nustatyti galimus visos neskelbtinos informacijos, įtrauktos į neskelbtinos informacijos sąrašą (NIS), konfidencialumo, vientisumo arba prieinamumo pažeidimus.

Jeigu tokį poveikį darantis incidentas įvyksta, jis laikomas informacijos saugumo incidentu, nedelsiant užregistruojamas naudojantis IT paslaugų valdymo priemone ir tvarkomas kaip toks incidentas.

9.2. Informacijos saugumo incidentų tvarkymas

Atsakomybė už saugumo incidentus yra priskirta 3-iajam sprendimų lygmeniui. Incidentus sprendžia speciali incidentų valdymo grupė.

Incidentų valdymo grupė atsakinga už tai, kad būtų:

- atlikta pirminė analizė, nustatyta incidento kategorija ir rimtumas;
- koordinuojami visų suinteresuotųjų subjektų veiksmai, įskaitant visą incidento analizės dokumentavimą, priimtus sprendimus siekiant pašalinti incidentą ir galimas nustatytas silpnąsias vietas;
- priklausomai nuo saugumo incidento dydžio, laiku perduota informacija apie incidentą atitinkamam sprendimų lygmeniui siekiant jį informuoti ir (arba) kad tuo lygmeniu būtų priimtas sprendimas.

Per informacijos saugumo valdymo procesą visa informacija apie incidentus klasifikuojama aukščiausiu informacijos slaptumo lygmeniu, tačiau bet kuriuo atveju ne žemesniu negu „ETS SENSITIVE“ (neskelbtina) lygmeniu.

Jeigu tyrimas dar vykdomas ir (arba) silpnoji vieta dar nėra pašalinta ir ja gali būti pasinaudota, iki spragos ištaisymo informacija priskiriama kategorijai „ETS CRITICAL“ (ypatingos svarbos).

9.3. Saugumo incidentų nustatymas

Atsižvelgdamas į saugumo įvykio pobūdį, informacijos saugumo specialistas nustato, kokias organizacijas įtraukti į Incidentų valdymo grupę.

9.4. Saugumo incidentų analizė

Incidentų valdymo grupė susisiekia su visomis įtrauktomis organizacijomis ir atitinkamais savo grupių nariais, kad incidentas būtų peržiūrėtas. Atliekant analizę nustatomas ištekliaus konfidencialumo, vientisumo arba prieinamumo praradimo mastas ir įvertinami padariniai visoms paveiktoms organizacijoms. Paskui apibrėžiami pradiniai ir paskesni incidento sprendimo ir jo poveikio valdymo veiksmai, įskaitant šiems veiksmams atlikti reikalingus išteklius.

9.5. Saugumo incidento rimtumo įvertinimas, perdavimas spręsti kitam sprendimų lygmeniui ir atsiskaitymas

Incidentų valdymo grupė įvertina kiekvieno naujo saugumo incidento rimtumą nustatydama jo bruožus ir nedelsdama imasi reikiamų veiksmų atsižvelgdama į incidento rimtumą.

9.6. Pranešimas apie reagavimą į saugumo incidentą

Incidentų valdymo grupė įtraukia incidento sustabdymo ir pašalinimo rezultatus į reagavimo į informacijos saugumo incidentą ataskaitą. Ataskaita pateikiama 3-iojo sprendimų lygmens specialistams saugiu e. paštu arba kitomis abipusiai priimtinomis saugaus ryšio priemonėmis.

Atsakinga Šalis peržiūri incidento sustabdymo ir pašalinimo rezultatus ir:

- vėl prijungia registrą, jeigu prieš tai jis buvo atjungtas;
- pateikia informaciją apie incidentą registro grupėms;
- atlieka incidento užbaigimo procedūras.

Siekiant užtikrinti informacijos registravimo ir komunikacijos nuoseklumą, taip pat tam, kad būtų galima skubiai imtis reikiamų veiksmų incidentui sustabdyti, incidentų valdymo grupė turėtų į reagavimo į informacijos saugumo incidentą ataskaitą saugiai įtraukti atitinkamus duomenis. Incidentų valdymo grupė laiku pateikia parengtą reagavimo į informacijos saugumo incidentą ataskaitą.

9.7. Stebėsena, gebėjimų stiprinimas ir nuolatinis tobulinimas

Incidentų valdymo grupė visų saugumo incidentų ataskaitas pateikia 3-iojo sprendimų lygmens specialistams. Šiuo sprendimų lygmeniu ataskaitos analizuojamos ir nustatoma:

- silpnosios saugumo kontrolės vietos ir (arba) tai, kurias operacijas reikia stiprinti;
- galimi poreikiai tobulinti šią procedūrą, kad į incidentus būtų reaguojama efektyviau;
- mokymo ir gebėjimų stiprinimo galimybės siekiant toliau stiprinti registro sistemų informacijos saugumo patikimumą, mažinti incidentų skaičių ateityje ir kuo labiau sumažinti incidentų poveikį.

10. INFORMACIJOS SAUGUMO VALDYMAS

Informacijos saugumo valdymo tikslas – užtikrinti organizacijos neskelbtinos informacijos, duomenų ir IT paslaugų konfidencialumą, vientisumą ir prieinamumą. Tam, kad būtų įvykdyti laikino sprendimo saugumo reikalavimai, be techninių komponentų, įskaitant projektavimą ir testavimą (žr. STS), reikia atlikti toliau nurodytas bendras procedūras.

10.1. Informacijos slaptumo nustatymas

Informacijos slaptumas įvertinamas nustačius, kokį poveikį verslui gali padaryti su šia informacija susijęs saugumo pažeidimas (pvz., finansiniai nuostoliai, įvaizdžio pablogėjimas, įstatymų pažeidimas ir pan.).

Neskelbtinos informacijos ištekliai nustatomi pagal jų poveikį jungčiai.

Informacijos slaptumo lygis įvertinamas pagal šiai jungčiai taikytiną šio dokumento skirsnyje „Informacijos saugumo incidentų tvarkymas“ pateiktą slaptumo skalę.

10.2. Informacijos išteklių slaptumo lygiai

Tai nustačius, informacijos išteklius priskiriamas tam tikrai kategorijai, laikantis šių taisyklių:

- jeigu informacijos konfidencialumo, vientisumo arba prieinamumo lygis įvertinamas kaip „aukštas“, informacijos išteklius priskiriamas kategorijai „ETS CRITICAL“ (ypatingos svarbos);
- jeigu informacijos konfidencialumo, vientisumo arba prieinamumo lygis įvertinamas kaip „vidutinis“, informacijos išteklius priskiriamas kategorijai „ETS SENSITIVE“ (neskelbtina);
- jeigu informacijos konfidencialumo, vientisumo arba prieinamumo lygis įvertinamas tik kaip „žemas“, informacijos išteklius priskiriamas kategorijai „ETS LIMITED“ (riboto naudojimo).

10.3. Už informacijos išteklius atsakingo asmens paskyrimas

Turi būti paskirtas už kiekvieną informacijos išteklių atsakingas asmuo. ATLPS informacijos ištekliai, kurie priklauso ESSŽ ir SSTL jungčiai arba yra su ja susiję, turėtų būti įtraukti į abiejų Šalių tvarkomą bendrų išteklių sąrašą. ATLPS informacijos ištekliai, kurie nepriklauso ESSŽ ir SSTL jungčiai, turėtų būti įtraukti į atitinkamos Šalies tvarkomą išteklių sąrašą.

Abi Šalys susitaria dėl atsakomybės už kiekvieną informacijos išteklių, kuris priklauso ESSŽ ir SSTL jungčiai arba yra su ja susijęs. Už informacijos išteklių atsakingas asmuo atsako už informacijos slaptumo įvertinimą.

Atsakingo asmens pareigų lygis turėtų atitikti priskirto (-ų) ištekliaus (-ių) vertę. Dėl atsakingo asmens atsakomybės už išteklių (-ius) ir pareigos užtikrinti reikalingą konfidencialumo, vientisumo ir prieinamumo lygį turėtų būti susitarta ir susitarimas turi būti įformintas.

10.4. Neskelbtinos informacijos registravimas

Visa neskelbtina informacija registruojama neskelbtinos informacijos sąraše (NIS).

Jeigu reikia, atsižvelgiama į neskelbtinos informacijos grupę, kuri gali lemti didesnį poveikį negu pavienė informacija, ir tokia informacijos grupė yra registruojama NIS (pvz., informacijos rinkinys, saugomas sistemos duomenų bazėje).

NIS nėra statiškas. Su informacijos ištekliumi susijusių saugumo incidentų grėsmės, pažeidžiamos sritys, tikimybė arba padariniai gali keistis ir tai gali nebūti pastebėta, o į registro sistemų darbą gali būti įtraukiami nauji ištekliai.

Todėl NIS yra reguliariai peržiūrimas ir visa nauja informacija, kuri yra laikoma neskelbtina, nedelsiant įtraukiama į NIS.

Kiekvieną NIS įrašą sudaro bent ši informacija:

- informacijos aprašymas;
- už informaciją atsakingas asmuo;
- slaptumo lygis;
- pastaba, ar informacija apima asmens duomenis;
- jeigu reikia, papildoma informacija.

10.5. Neskelbtinos informacijos tvarkymas

Jeigu neskelbtina informacija yra tvarkoma ne Sąjungos registro ir Šveicarijos registro jungtyje, ji tvarkoma pagal tvarkymo instrukcijas.

Sąjungos registro ir Šveicarijos registro jungtyje informacija tvarkoma pagal Šalių saugumo reikalavimus.

10.6. Prieigos valdymas

Prieigos valdymo tikslas – suteikti įgaliotiems naudotojams teisę naudotis paslauga ir neleisti ja naudotis reikiamo leidimo neturintiems naudotojams. Prieigos valdymas kartais taip pat vadinamas teisių valdymu arba tapatybės valdymu.

Naudodamosi laikinu sprendimu ir vykdydamos operacijas pagal jį abi Šalys turi turėti prieigą prie šių komponentų:

- vikio – bendradarbiavimo aplinkos, kurioje keičiamasi bendra informacija, pavyzdžiui, versijų išleidimo planais;
- IT paslaugų valdymo priemonės, skirtos incidentams ir problemoms valdyti (žr. skyrių „Metodika ir standartai“);
- keitimosi pranešimais sistemos – kiekviena Šalis pasirūpina saugia keitimosi pranešimais ir pranešimų perdavimo sistema, kuria naudojantis būtų perduodami pranešimai su sandorio duomenimis.

Šveicarijos registro administratorius ir Sąjungos vyriausiasis administratorius užtikrina, kad prieiga būtų atnaujinta, ir prieigos valdymo tikslais atlieka savo Šalių kontaktinių centrų funkcijas. Prieigos užklausos yra tvarkomos pagal užklausų vykdymo procedūras.

10.7. Sertifikato ir (arba) rakto valdymas

Kiekviena Šalis yra atsakinga už savo sertifikato ir (arba) rakto valdymą (sukūrimą, registravimą, saugojimą, įdiegimą, naudojimą, atnaujinimą, panaikinimą, atsarginės kopijos išsaugojimą ir atkūrimą). Kaip nurodyta Susiejimo techniniuose standartuose (STS), naudojami tik skaitmeninį sertifikatą teikiančios organizacijos, kuria pasitiki abi Šalys, išduoti skaitmeniniai sertifikatai. Sertifikatai ir (arba) raktai saugomi laikantis tvarkymo instrukcijų nuostatų.

Visus sertifikatų ir raktų panaikinimo ir (arba) atnaujinimo atvejus suderina abi Šalys. Tai atliekama pagal užklausų vykdymo procedūras.

Šveicarijos registro administratorius ir Sąjungos vyriausiasis administratorius vienas kitam sertifikatus ir (arba) raktus perduoda saugiomis ryšio priemonėmis, laikydamiesi tvarkymo instrukcijose išdėstytų nuostatų.

Visokia sertifikatų ir (arba) raktų patikra tarp Šalių atliekama naudojantis atskiru duomenų perdavimo kanalu.