EIROPAS
KOMISIJA

Briselē, 23.6.2020.
COM(2020) 255 final

ANNEX

PIELIKUMI

dokumentam

Priekšlikums Padomes Lēmumam

par nostāju, kas Eiropas Savienības vārdā jāieņem Apvienotajā komitejā, kura izveidota ar Nolīgumu starp Eiropas Savienību un Šveices Konfederāciju par siltumnīcefekta gāzu emisijas kvotu tirdzniecības sistēmu sasaisti, par kopējo darbības procedūru pieņemšanu

AR NOLĪGUMU STARP EIROPAS SAVIENĪBU UN ŠVEICES KONFEDERĀCIJU PAR SILTUMNĪCEFEKTA GĀZU EMISIJAS KVOTU TIRDZNIECĪBAS SISTĒMU SASAISTI IZVEIDOTĀS APVIENOTĀS KOMITEJAS LĒMUMS Nr. 1/2020

(…)

par kopējām darbības procedūrām

APVIENOTĀ KOMITEJA,

ņemot vērā Nolīgumu starp Eiropas Savienību un Šveices Konfederāciju par siltumnīcefekta gāzu emisijas kvotu tirdzniecības sistēmu sasaisti[1] (turpmāk "Nolīgums") un jo īpaši tā 3. pantu,

tā kā:

(1) Ar Apvienotās komitejas 2019. gada 5. decembra Lēmumu Nr. 2/2019 tika grozīts nolīguma I un II pielikums, tādējādi izpildot nolīgumā izklāstītos sasaistes nosacījumus.

(2) Pēc Apvienotās komitejas Lēmuma Nr. 2/2019 pieņemšanas un saskaņā ar nolīguma 21. panta 3. punktu puses apmainījās ar saviem ratifikācijas vai apstiprināšanas instrumentiem, jo tās uzskatīja, ka ir izpildīti visi nolīgumā noteiktie sasaistes nosacījumi.

(3) Saskaņā ar nolīguma 21. panta 4. punktu nolīgums stājās spēkā 2020. gada 1. janvārī.

(4) Saskaņā ar nolīguma 3. panta 6. punktu Šveices reģistra administratoram un Savienības centrālajam administratoram būtu jānosaka kopējās darbības procedūras (KDP), kas saistītas ar tehniskiem vai citiem jautājumiem un ir vajadzīgas, lai nodrošinātu sasaistes funkcionēšanu starp Savienības reģistra Eiropas Savienības darījumu žurnālu (*EUTL*) un Šveices reģistra Šveices papildu darījumu žurnālu (*SSTL*), tostarp ņemot vērā iekšējos tiesību aktos izklāstītās prioritātes. KDP būtu jāstājas spēkā, kad tās ir pieņemtas ar Apvienotās komitejas lēmumu.

(5) Saskaņā ar nolīguma 13. panta 1. punktu Apvienotajai komitejai būtu jāvienojas par tehniskajām vadlīnijām, kas vajadzīgas, lai nodrošinātu nolīguma pareizu īstenošanu, tostarp vadlīnijām par tehniskiem vai citiem jautājumiem, kas ir vajadzīgas, lai nodrošinātu sasaistes funkcionēšanu, tostarp ņemot vērā iekšējos tiesību aktos izklāstītās prioritātes. Tehniskās vadlīnijas var izstrādāt darba grupa, ko izveido saskaņā ar nolīguma 12. panta 5. punktu. Darba grupā būtu jāiekļauj vismaz Šveices reģistra administrators un Savienības centrālais administrators, un tai būtu jāpalīdz Apvienotajai komitejai veikt tās funkcijas saskaņā ar nolīguma 13. pantu,

(6) Ņemot vērā vadlīniju tehnisko raksturu un vajadzību tās pielāgot situācijas attīstībai, Šveices reģistra administratora un Savienības centrālā administratora izstrādātās tehniskās vadlīnijas būtu jāiesniedz Apvienotajai komitejai informēšanas vai — attiecīgā gadījumā — apstiprināšanas nolūkā,

IR PIEŅĒMUSI ŠO LĒMUMU.

1. pants

Ar šo pieņem kopējās darbības procedūras (KDP), kas pievienotas šim lēmumam.

[1] OV L 322, 7.12.2017., 3. lpp.

2. pants

Ar šo izveido darba grupu saskaņā ar nolīguma 12. panta 5. punktu. Tā palīdz Apvienotajai komitejai nodrošināt nolīguma pareizu īstenošanu, tostarp izstrādā KDP īstenošanas tehniskās vadlīnijas.

Darba grupā ietilpst vismaz Šveices reģistra administrators un Savienības centrālais administrators.

3. pants

Šis lēmums stājas spēkā tā pieņemšanas dienā.

Sagatavots angļu valodā Briselē 2020. gada XX.

Apvienotās komitejas vārdā –

sekretāre no Eiropas Savienības puses	*priekšsēdētājs*	*sekretāre no Šveices puses*

PAPILDINĀJUMS

PIELIKUMS

KOPĒJĀS DARBĪBAS PROCEDŪRAS

saskaņā ar 3. panta 6. punktu Nolīgumā starp Eiropas Savienību un Šveices Konfederāciju par siltumnīcefekta gāzu emisijas kvotu tirdzniecības sistēmu sasaisti - Pagaidu risinājuma procedūras

1. GLOSĀRIJS

1-1. tabula. Akronīmi un definīcijas

Akronīms/termins	Definīcija
Sertificētājs (*CA*)	Iestāde, kas izdod digitālos sertifikātus
CH	Šveices Konfederācija
ETS	Emisijas kvotu tirdzniecības sistēma
ES	Eiropas Savienība
IMT	Incidentu vadības vienība
Informācijas aktīvs	Uzņēmumam vai organizācijai vērtīga informācija
IT	Informācijas tehnoloģijas
ITIL	Informācijas tehnoloģiju infrastruktūras bibliotēka
ITSM	IT pakalpojumu vadība
STS	Sasaistes tehniskie standarti
Reģistrs	Uzskaites sistēma, kurā uzskaita ETS ietvaros iedalītās kvotas un kura ļauj izsekot elektroniskajos kontos turēto kvotu īpašumtiesībām.
RFC	Izmaiņas pieprasījums
SIL	Sensitīvas informācijas saraksts
SR	Pakalpojuma pieprasījums
Wiki	Tīmekļa vietne, kas dod iespēju lietotājiem dalīties informācijā un zināšanās, saturu papildinot vai pielāgojot tieši tīmekļa pārlūkprogrammā.

2. IEVADS

Nolīgums starp Eiropas Savienību un Šveices Konfederāciju par siltumnīcefekta gāzu emisijas kvotu tirdzniecības sistēmu sasaisti (turpmāk "Nolīgums") ir noslēgts 2017. gada

23. novembrī un paredz savstarpēji atzīt emisijas kvotas, ko var izmanot, lai panāktu atbilstību Eiropas Savienības emisijas kvotu tirdzniecības sistēmā (ES ETS) vai Šveices emisijas kvotu tirdzniecības sistēmā. Lai ES ETS un Šveices ETS sasaiste varētu darboties, starp Savienības reģistra Eiropas Savienības darījumu žurnālu (*EUTL*) un Šveices reģistra Šveices papildu darījumu žurnālu (*SSTL*) izveido tiešu sasaisti, kas dos iespēju katras ETS ietvaros izdotās kvotas pārskaitīt starp reģistriem (Nolīguma 3. panta 2. punkts). Lai ES ETS un Šveices ETS sasaiste varētu darboties, līdz 2020. gada maijam vai drīz pēc tam ievieš pagaidu risinājumu. Puses sadarbojas, lai reģistru pagaidu sasaistes risinājumu pēc iespējas drīzāk aizstātu ar pastāvīgu sasaisti (Nolīguma II pielikums).

Saskaņā ar Nolīguma 3. panta 6. punktu Šveices reģistra administrators un Savienības centrālais administrators nosaka kopējās darbības procedūras (KDP), kas saistītas ar tehniskiem vai citiem jautājumiem un ir vajadzīgas, lai nodrošinātu sasaistes funkcionēšanu, tostarp ņemot vērā iekšējos tiesību aktos izklāstītās prioritātes. Administratoru izstrādātās KDP stājas spēkā, kad tās ir pieņemtas ar Apvienotās komitejas lēmumu.

Šajā dokumentā izklāstītās KDP Apvienotā komiteja grasās pieņemt ar Lēmumu Nr. 1/2020. Saskaņā ar šo lēmumu Apvienotā komiteja prasa Šveices reģistra administratoram un Savienības centrālajam administratoram izstrādāt sīkākas tehniskās vadlīnijas, kas nepieciešamas, lai nodrošinātu sasaistes funkcionēšanu, tās pastāvīgu pielāgošanu tehnikas attīstībai un jaunām prasībām, kas saistītas ar sasaistes drošumu un drošību, un tās rezultatīvu un efektīvu darbību.

2.1. Darbības joma

Šis dokuments atspoguļo Nolīguma pušu kopīgo izpratni par ES ETS un Šveices ETS reģistru sasaistes procedurālā pamata izveidi. Tajā izklāstītas vispārējās procedurālās prasības attiecībā uz sasaistes operācijām, tomēr būs vajadzīgas arī sīkākas tehniskas vadlīnijas, lai sasaiste varētu darboties.

Lai sasaiste varētu pienācīgi funkcionēt, būs jānosaka sasaistes darbības tehniskās specifikācijas. Saskaņā ar Nolīguma 3. panta 7. punktu šie jautājumi tiks iztirzāti sasaistes tehnisko standartu (STS) dokumentā, ko Apvienotā komiteja pieņems atsevišķi ar attiecīgu lēmumu.

KDP mērķis ir nodrošināt, ka IT pakalpojumi, kas saistīti ar ES ETS un Šveices ETS reģistru sasaistes darbību, tiek sniegti rezultatīvi un efektīvi, proti, ka tiek izpildīti pakalpojuma pieprasījumi, novērstas pakalpojumu atteices, atrisinātas problēmas un ka rutīnas operacionālie uzdevumi tiek izpildīti saskaņā ar starptautiskajiem IT pakalpojumu vadības standartiem.

Ierosinātajam pagaidu risinājumam būs vajadzīgas tikai šādas KDP, kas ir daļa no šā dokumenta:

- Incidentu vadība
- Problēmu vadība
- Pieprasījuma izpilde
- Izmaiņu vadība
- Laidumu vadība
- Drošības incidentu vadība
- Informācijas drošības vadība

Kad vēlāk tiks izveidota pastāvīgā reģistru sasaiste, KDP ir vajadzības gadījumā jāpielāgo un jāpapildina.

2.2. Adresāti

KDP mērķauditorija ir ES un Šveices reģistru atbalsta vienības.

3. PIEEJA UN STANDARTI

Uz visām KDP attiecas šāds princips.

- ES un CH vienojas KDP definēt, pamatojoties uz *ITIL* (Informācijas tehnoloģiju infrastruktūras bibliotēka, 3. versija). Šajā standartā paredzēto praksi izmanto un pielāgo specifiskajām vajadzībām, kas saistītas ar pagaidu risinājumu.
- Saziņa un koordinācija, kas nepieciešama, lai KDP ieviestu abas puses, notiek ar CH un ES reģistru apkalpošanas dienestu starpniecību. Uzdevumus allaž piešķir vienas puses ietvaros.
- Ja rodas domstarpības par KDP izmantošanu, tās analizē un atrisina abi apkalpošanas dienesti savā starpā. Ja vienošanos panākt neizdodas, kopīga risinājuma meklēšanu nodod nākamajam līmenim.

Eskalācijas līmeņi	**ES**	**CH**
1. līmenis	ES apkalpošanas dienests	CH apkalpošanas dienests
2. līmenis	ES operāciju vadītājs	CH reģistra lietojumu vadītājs
3. līmenis	Apvienotā komiteja (kas šo atbildību var deleģēt saskaņā ar Nolīguma 12. panta 5. punktu)	
4. līmenis	pvienotā komiteja, ja 3. līmenī atbildība tikusi deleģēta.	

- Katra puse var noteikt savas reģistra sistēmas darbības procedūras, ņemot vērā ar šīm KDP saistītās prasības un saskarnes.
- KDP atbalstam, jo īpašu incidentu vadības, problēmu vadības un pieprasījumu izpildes aspektā, un saziņai starp abām pusēm izmanto IT pakalpojumu vadības (*ITSM*) rīku.
- Ir atļauta informācijas apmaiņa pa e-pastu.
- Abas puses nodrošina, ka tiek izpildītas informācijas drošības prasības saskaņā ar rīkošanās instrukcijām.

4. INCIDENTU VADĪBA

Incidentu vadības procesa mērķis ir panākt, ka IT pakalpojumi pēc iespējas ātrāk un ar minimāliem darbības traucējumiem atsāk darboties normālā pakalpojumu sniegšanas režīmā.

Incidentu vadības gaitā incidenti tiek fiksēti ziņošanas vajadzībām, un incidentu vadību integrē ar pārējiem procesiem, lai sekmētu pastāvīgus uzlabojumus.

- Vispārīgā skatījumā incidentu vadība sastāv no šādām darbībām:
- incidentu konstatēšana un reģistrēšana;

- klasificēšana un sākotnējais atbalsts;
- izmeklēšana un diagnostika;
- atrisināšana un atkopšana;
- incidenta noslēgšana.

Visā incidenta dzīves ciklā incidentu vadības procesam ir pastāvīgi jānodrošina īpašumtiesību apstrāde, monitorings, izsekošana un saziņa.

4.1. Incidentu konstatēšana un reģistrēšana

Incidentu var konstatēt atbalsta grupa, automatizēti monitoringa rīki vai tehniskais personāls, kas nodarbojas ar rutīnas pārraudzību.

Kad incidents ir konstatēts, tas ir jāreģistrē un tam jāpiešķir unikāls identifikators, lai būtu iespējama pienācīga incidenta izsekošana un monitorings. Incidenta unikālais identifikators ir identifikators, ko kopējā pretenziju sistēmā piešķir tās puses (ES vai CH) apkalpošanas dienests, kas signalizējusi par incidentu, un tas ir jāizmanto jebkādā saziņā par šo incidentu.

Visiem incidentiem kontaktpunkts ir tās puses apkalpošanas dienests, kas pretenziju reģistrējusi.

4.2. Klasificēšana un sākotnējais atbalsts

Incidentu klasificēšanas mērķis ir izprast un identificēt, kāda sistēma un/vai pakalpojums ir skarti un kādā mērā. Lai klasifikācija būtu lietderīga un paātrinātu incidenta atrisināšanu, tai jau ar pirmo mēģinājumu jānovirza incidents uz pareizo resursu.

Klasificēšanas posmā incidents jākategorizē un jāprioritizē atkarībā no ietekmes un steidzamības, lai to varētu risināt tā prioritātei atbilstošā termiņā.

Ja incidents var potenciāli ietekmēt sensitīvu datu konfidencialitāti vai integritāti un/vai ietekmēt sistēmas pieejamību, incidents jāklasificē arī kā drošības incidents un tā vadībai jānorit saskaņā ar procesu, kas definēts šā dokumenta nodaļā “Drošības incidentu vadība”.

Ja iespējams, sākotnējo diagnostiku veic apkalpošanas dienests, kas reģistrējis pretenziju. Lai to izdarītu, apkalpošanas dienests vispirms noskaidros, vai incidents nav jau zināma kļūda. Tādā gadījumā risināšanas gaita vai aprisinājums jau ir zināms un dokumentēts.

Ja apkalpošanas dienests incidentu ir sekmīgi atrisinājis, tas šajā brīdī faktiski incidentu slēdz, jo ir izpildīts incidentu vadības primārais uzdevums (proti, pakalpojuma nodrošināšana galalietotājam ir ātri atjaunota). Pretējā gadījumā apkalpošanas dienests incidentu eskalē līdz piemērotai risinātāju grupai turpmākai izmeklēšanai un diagnostikai.

4.3. Izmeklēšana un diagnostika

Incidentu izmeklēšanu un diagnostiku izmanto tad, kad incidentu nevar atrisināt apkalpošanas dienests sākotnējā diagnosticēšanā un tas tiek pienācīgi eskalēts. Incidentu eskalācija ir izmeklēšanas un diagnostikas procesa pilnvērtīga daļa.

Ierasta prakse izmeklēšanas un diagnostikas posmā ir mēģinājums reproducēt incidentu kontrolētos apstākļos. Incidenta izmeklēšanas un diagnostikas gaitā ir ļoti svarīgi izprast to notikumu secību, kas pie incidenta noveduši.

Eskalācija nozīmē atzīt, ka incidentu nevar atrisināt pašreizējā atbalsta līmenī un ka tas ir jānodod augstāka līmeņa atbalsta grupai vai otrai pusei. Eskalācija var būt divējāda: horizontāla (funkcionāla) vai vertikāla (hierarhiska).

Eskalēt incidentu līdz piemērotam resursam un sekot līdzi incidenta statusam un piešķiršanai ir incidentu reģistrējušā un ierosinājušā apkalpošanas dienesta pienākums.

Pienākums nodrošināt, ka prasītās darbības tiek veiktas savlaicīgi, un nodrošināt atgriezenisko saisti savam apkalpošanas dienestam, ir tās puses uzdevums, kurai incidents piešķirts.

4.4. Atrisināšana un atkopšana

Incidentu atrisināšana un atkopšana notiek, kad incidents ir pilnībā izprasts. Incidenta risinājuma atrašana nozīmē, ka ir uziets veids, kā problēmu novērst. Incidenta risinājuma piemērošana ir atkopšanas posms.

Kad attiecīgie resursi ir atrisinājuši pakalpojuma atteici, incidentu novirza atpakaļ attiecīgajam apkalpošanas dienestam, kurš incidentu reģistrējis, un tas vēršas pie incidenta iniciatora, lai pārliecinātos, ka kļūda ir novērsta un ka incidentu var noslēgt. Incidenta apstrādes gaitā izdarītie konstatējumi ir jāfiksē, jo tie varētu noderēt turpmāk.

Atkopšanu var veikt IT atbalsta darbinieki vai arī galalietotājs, kam dod norādījumus, kā to izdarīt.

4.5. Incidenta noslēgšana

Noslēgšana ir incidentu vadības pēdējais posms un notiek neilgi pēc incidenta atrisināšanas.

Noslēgšanas posmā ir jāveic virkne darbību, no kurām īpaši izceļamas šādas:

- verificēt incidentam sākotnēji piešķirto kategoriju;
- pienācīgi fiksēt visu informāciju par incidentu;
- pienācīgi dokumentēt incidentu un atjaunināt zināšanu bāzi;
- pienācīgi sazināties ar visām ieinteresētajām personām, ko tieši vai netieši skāris incidents.

Incidentu formāli noslēdz tad, kad apkalpošanas dienests ir pabeidzis incidenta noslēgšanas posmu un par to paziņojis otrai pusei.

Kad incidents ir noslēgts, to vairs neatver. Ja incidents pēc neilga laika atkārtojas, reģistrē jaunu incidentu, nevis vēlreiz atver sākotnējo incidentu.

Ja incidentam seko līdzi gan ES, gan CH apkalpošanas dienesti, incidenta galīgā noslēgšana ir tā apkalpošanas dienesta pienākums, kas pretenziju reģistrējis.

5. PROBLĒMU VADĪBA

Šī procedūra ir jāievēro ikreiz, kad tiek identificēta problēma, kas savukārt ierosina problēmu vadības procesu. Problēmu vadības galvenais uzdevums ir uzlabot kvalitāti un samazināt incidentu skaitu. Problēma var būt viena vai vairāku incidentu cēlonis. Kad tiek ziņots par incidentu, incidentu vadības mērķis ir pēc iespējas ātrāk atjaunot pakalpojumu, tostarp izmantojot aprisinājumus. Kad problēma reģistrēta, mērķis ir izpētīt problēmas pamatcēloni, lai noskaidrotu, kādas izmaiņas vajadzīgas, lai nodrošinātu, ka problēma un ar to saistītie incidenti vairs nenotiek.

5.1. Problēmas identificēšana un reģistrēšana

Atkarībā no tā, kura puse ierosinājusi pretenziju, kontaktpunkts ar problēmu saistītajos jautājumos būs ES vai CH apkalpošanas dienests.

Problēmas unikālais identifikators ir identifikators, ko piešķir IT pakalpojumu vadība (*ITSM*). To izmanto jebkādā saziņā par šo problēmu.

Problēmu var ierosināt incidents, vai arī to var ierosināt pēc pašu iniciatīvas, lai novērstu jebkurā sistēmas posmā atklātās nepilnības.

5.2. Problēmu prioritizēšana

Lai problēmām varētu vieglāk izsekot, tās var iedalīt kategorijās pēc to smaguma un prioritātes tādā pašā veidā kā incidentus, ņemot vērā saistīto incidentu ietekmi un biežumu.

5.3. Problēmas izmeklēšana un diagnostika

Katra puse var izvirzīt problēmu, un šīs puses apkalpošanas dienests būs atbildīgs par problēmas reģistrēšanu, tās novirzīšanu piemērotam resursam un sekošanu tās statusam kopumā.

Risinātāju grupa, kam problēma eskalēta, ir atbildīga par problēmas savlaicīgu risināšanu un saziņu ar apkalpošanas dienestu.

Pēc pieprasījuma — nodrošināt, ka piešķirtās darbības tiek veiktas, un nodrošināt atgriezenisko saiti savam apkalpošanas dienestam ir abu pušu uzdevums.

5.4. Atrisinājums

Par problēmas atrisināšanu ir atbildīga risinātāju grupa, kam problēma piešķirta, un tā ir atbildīga arī par to, ka grupas puses apkalpošanas dienestam tiek sniegta relevantā informācija.

Problēmas apstrādes gaitā izdarītie konstatējumi ir jāfiksē, jo tie varētu noderēt turpmāk.

5.5. Problēmas noslēgšana

Problēma tiek formāli noslēgta tad, kad tā ir novērsta, pateicoties ieviestām izmaiņām. Problēmas noslēgšanas posmu realizē tas apkalpošanas dienests, kas problēmu reģistrēja un informēja otras puses apkalpošanas dienestu.

6. PIEPRASĪJUMA IZPILDE

Pieprasījuma izpildes procesa ietvaros no sākuma līdz beigām tiek pārvaldīti pieprasījumi pēc jauna vai esoša pakalpojuma, proti, no brīža, kad pieprasījums tiek reģistrēts un apstiprināts, līdz brīdim, kad tas tiek noslēgts. Pakalpojuma pieprasījumi parasti ir nelieli, iepriekš definēti, atkārtojami, bieži, iepriekš apstiprināti un procedurāli pieprasījumi.

Galvenā darbību virkne ir šāda.

6.1. Pieprasījuma iniciēšana

Ar pakalpojuma pieprasījumu saistīto informāciju ES vai CH apkalpošanas dienestam iesniedz pa e-pastu, telefoniski, izmantojot IT pakalpojumu vadības (*ITSM*) rīku vai citu norunātu saziņas kanālu.

6.2. Pieprasījuma reģistrēšana un analīze

Attiecībā uz visiem pakalpojuma pieprasījumiem kontaktpunkts ir ES vai CH apkalpošanas dienests atkarībā no tā, kura puse izvirzījusi pakalpojuma pieprasījumu. Šis apkalpošanas dienests ir atbildīgs par pakalpojuma pieprasījuma reģistrēšanu un rūpīgu analīzi.

6.3. Pieprasījuma apstiprināšana

Pakalpojuma pieprasījumu izvirzījušās puses apkalpošanas dienesta darbinieks pārbauda, vai ir vajadzīgs kāds apstiprinājums no otras puses, un, ja jā, rīkojas, lai to saņemtu. Ja pakalpojuma pieprasījums netiek apstiprināts, apkalpošanas dienests atjaunina un noslēdz pretenziju.

6.4. Pieprasījuma izpilde

Šajā posmā tiek rezultatīvi un efektīvi apstrādāti pakalpojuma pieprasījumi. Jānošķir šādi gadījumi:

- pakalpojuma pieprasījuma izpilde skar tikai vienu pusi. Tādā gadījumā šī puse izdod darba rīkojumus un koordinē izpildi;
- pakalpojuma pieprasījuma realizācija skar gan ES, gan CH. Tādā gadījumā apkalpošanas dienesti izdod darba rīkojumus savā atbildības jomā. Pakalpojuma pieprasījuma izpildes norisi savstarpēji koordinē abi apkalpošanas dienesti. Vispārējā atbildība gulstas uz to apkalpošanas dienestu, kas pakalpojuma pieprasījumu saņēmis un iniciējis.

Kad pakalpojuma pieprasījums ir atrisināts, tam piešķir statusu "atrisināts".

6.5. Pieprasījuma eskalēšana

Vēl neizpildītu pakalpojuma pieprasījumu apkalpošanas dienests vajadzības gadījumā var eskalēt un novirzīt attiecīgajam resursam (trešām personām).

Eskalācijas gaitā pieprasījumus novirza attiecīgajām trešām personām, t. i., ES apkalpošanas dienests pieprasījumu CH trešai pusei var novirzīt tikai ar CH apkalpošanas dienesta starpniecību un otrādi.

Trešā puse, kurai pakalpojuma pieprasījums novirzīts, ir atbildīga par pakalpojuma pieprasījuma savlaicīgu risināšanu un saziņu ar to apkalpošanas dienestu, kas pakalpojuma pieprasījumu eskalējis.

Pakalpojuma pieprasījumu reģistrējušā apkalpošanas dienesta pienākums ir kopumā sekot līdzi pakalpojuma pieprasījuma statusam un piešķiršanai.

6.6. Pieprasījuma izpildes izskatīšana

Pirms pakalpojuma pieprasījuma noslēgšanas atbildīgais apkalpošanas dienests pakalpojuma pieprasījuma protokolu nodod galīgajai kvalitātes kontrolei. Mērķis ir pārliecināties, ka pakalpojuma pieprasījums ir patiešām apstrādāts un ka pietiekami detalizēti ir sniegta visa informācija, kas nepieciešama, lai aprakstītu pieprasījuma dzīves ciklu. Turklāt pieprasījuma apstrādes gaitā izdarītie konstatējumi ir jāfiksē, jo tie varētu noderēt turpmāk.

6.7. Pieprasījuma noslēgšana

Ja puses, kam pieprasījums piešķirts, vienojas, ka pakalpojuma pieprasījums ir izpildīts, un prasītājs uzskata, ka lieta ir atrisināta, nākamais pieprasījumam piešķiramais statuss ir "noslēgts".

Pakalpojuma pieprasījumu formāli noslēdz pēc tam, kad pakalpojuma pieprasījumu reģistrējušais apkalpošanas dienests ir izpildījis pieprasījuma noslēgšanas posmu un informējis otras puses apkalpošanas dienestu.

7. IZMAIŅU VADĪBA

Mērķis ir nodrošināt, ka tiek izmantotas standartizētas metodes un procedūras, kā efektīvi un nekavējoties pārņemt kontroli pār visām izmaiņām, kas skar IT infrastruktūru, lai līdz minimumam samazinātu jebkādu saistīto incidentu skaitu un ietekmi uz pakalpojumiem. Izmaiņas IT infrastruktūrā var rasties reaktīvi — kā atbildes reakcija uz problēmām vai ārēji uzliktām prasībām, piemēram, normatīvo aktu grozījumiem — vai proaktīvi — lai uzlabotu rezultativitāti un efektivitāti vai atspoguļotu komerciālas iniciatīvas.

Izmaiņu vadības process ietver dažādus posmus, kuru gaitā tiek fiksēta visa informācija par izmaiņas pieprasījumu, lai nākotnē būtu iespējams tam izsekot. Šie procesi nodrošina, ka izmaiņa pirms ieviešanas tiek validēta un testēta. Sekmīgu ieviešanu nodrošina laidumu vadības process.

7.1. Izmaiņas pieprasījums

Izmaiņas pieprasījumu (*RFC*) iesniedz izmaiņu vadības vienībai validēšanai un apstiprināšanai. Attiecībā uz visiem izmaiņas pieprasījumiem kontaktpunkts ir ES vai CH apkalpošanas dienests atkarībā no tā, kura puse izvirzījusi izmaiņas pieprasījumu. Šis apkalpošanas dienests ir atbildīgs par izmaiņu pieprasījuma reģistrēšanu un rūpīgu analīzi.

Izmaiņas pieprasījumu iemesls var būt:

- incidents, kas izraisa izmaiņu;
- esoša problēma, kuras rezultātā rodas izmaiņa;
- galalietotāja pieprasījums pēc jaunas izmaiņas;
- izmaiņa, kas rodas notiekošas uzturēšanas rezultātā;
- leģislatīva izmaiņa.

7.2. Izmaiņas izvērtēšana un plānošana

Šajā posmā notiek izmaiņas novērtēšana un darbību plānošana. Tas ietver prioritizēšanu un darbību plānošanu nolūkā līdz minimumam samazināt risku un ietekmi.

Ja *RFC* realizācija skar gan ES, gan CH, puse, kas reģistrējusi *RFC*, izmaiņas izvērtēšanu un plānošanu verificē ar otru pusi.

7.3. Izmaiņas apstiprināšana

Visi reģistrētie izmaiņas pieprasījumi ir jāapstiprina attiecīgajā eskalācijas līmenī.

7.4. Izmaiņas īstenošana

Izmaiņas īstenošana notiek laidumu vadības ietvaros. Abu pušu laidumu vadības vienības ievēro pašas savas procedūras, kas ietver gan plānošanu, gan testēšanu. Izmaiņas izskatīšana notiek, kad īstenošana ir pabeigta. Lai nodrošinātu, ka viss ir paveikts saskaņā ar plānu, esošo izmaiņu vadības procesu pastāvīgi izskata un vajadzības gadījumā atjaunina.

8. LAIDUMU VADĪBA

Laidums jeb izlaišana nozīmē vienu vai vairākas izmaiņas IT pakalpojumā, kas ir apkopotas laiduma plānā un kas ir jāautorizē, jāsagatavo, jākompilē, jātestē un jāievieš vienlaikus. Vienvienīgs laidums var būt kļūdas izlabošana, aparatūras vai citu komponentu maiņa, izmaiņas programmatūrā, lietojumprogrammu versiju atjauninājumi, izmaiņas dokumentācijā un/vai procesos. Katra laiduma saturu pārvalda, testē un ievieš kā vienvienīgu vienumu.

Laidumu vadības mērķis ir plānot, kompilēt, testēt, validēt un nodrošināt spēju sniegt plānotos pakalpojumus tā, lai tie atbilstu ieinteresēto personu prasībām un sasniegtu iecerētos mērķus. Visu pakalpojumā ieviesto izmaiņu akceptēšanas kritēriji tiks definēti un dokumentēti projektēšanas koordinācijas laikā un nodoti laidumu vadības vienībām.

Laidums parasti sastāv no vairākiem problēmu labojumiem un pakalpojuma uzlabojumiem. Tas satur nepieciešamo jauno vai izmanīto programmatūru un jebkādu jaunu vai izmainītu aparatūru, kas nepieciešama apstiprināto izmaiņu ieviešanai.

8.1. Laiduma plānošana

Pirmajā procesa posmā autorizētās izmaiņas tiek sakopotas laiduma paketēs, kā arī tiek definēts laidumu tvērums un saturs. Pamatojoties uz šo informāciju, laiduma plānošanas apakšprocesa ietvaros tiek sagatavots laiduma kompilēšanas, testēšanas un ieviešanas grafiks.

Plānošanas gaitā definē šādus elementus:

- laiduma tvērums un saturs;
- laiduma riska novērtējums un riska profils;
- laiduma skartie klienti/lietotāji;
- par laidumu atbildīgā vienība;
- nodošanas un ieviešanas stratēģija;
- izlaišanai un ieviešanai vajadzīgie resursi.

Puses viena otru informē par saviem laidumu plānošanas un uzturēšanas logiem. Ja laidums ietekmē gan ES, gan CH, tās koordinē plānošanu un definē kopīgu uzturēšanas logu.

8.2. Laiduma paketes kompilēšana un testēšana

Laidumu vadības procesa kompilēšanas un testēšanas posmā tiek noteikta pieeja, kā realizēt laidumu vai laiduma paketi un kā saglabāt kontroli pār vidi pirms ražošanas maiņas, un kā testēt visas izmaiņas visās laiduma vidēs.

Ja laidums ietekmē gan ES, gan CH, tās koordinē nodošanas plānus un testus. Tas ietver šādus aspektus:

- kā un kad tiks nodoti laiduma vienumi un pakalpojuma komponenti;
- kādi ir tipiskie izpildes laiki; kas notiek kavēšanās gadījumā;
- kā izsekot nodošanas progresam un saņemt apstiprinājumu;
- kādu metriku izmantot laiduma ieviešanas monitoringā un sekmīguma novērtēšanā;
- kādi ir izplatītākie testpiemēri, ko izmanto relevantajai funkcionalitātei un izmaiņām.

Šī apakšprocesa noslēgumā visi vajadzīgie laiduma komponenti ir gatavi faktiskajam ieviešanas posmam.

8.3. Ieviešanas sagatavošana

Sagatavošanas apakšprocess nodrošina, ka tiek pareizi definēti komunikācijas plāni un ka ir sagatavoti paziņojumi, kas izsūtāmi visām skartajām ieinteresētajām personām un galalietotājiem, un ka laidums tiek integrēts izmaiņu vadības procesā, lai nodrošinātu, ka visas izmaiņas tiek izdarītas kontrolēti un ir apstiprinātas attiecīgajos forumos.

Ja laidums skar gan ES, gan CH, tās koordinē šādas darbības:

- izmaiņas pieprasījuma protokola sagatavošana nolūkā ieplānot un sagatavot ieviešanu ražošanas vidē;
- īstenošanas plāna sagatavošana;
- atrites pieeja, lai gadījumā, ja ieviešana ir kļūmīga, var atjaunot iepriekšējo stāvokli;

- paziņojumu izsūtīšana visām attiecīgajām pusēm;
- laiduma īstenošanai vajadzīgā apstiprinājuma pieprasīšana attiecīgajā eskalācijas līmenī.

8.4. Laiduma atrite

Ja ieviešana ir kļūmīga vai testēšanā ir noskaidrojies, ka ieviešana nav bijusi sekmīga vai nav atbildusi norunātajiem akceptēšanas/kvalitātes kritērijiem, abu pušu laiduma vadības vienībām ir jānodrošina atrite iepriekšējā stāvoklī. Par to jāinformē visas attiecīgās ieinteresētās personas, toskait skartie/ aptvertie galalietotāji. Kamēr nav saņemts apstiprinājums, procesu var atsākt jebkurā no iepriekšējiem posmiem.

8.5. Laiduma izskatīšana un noslēgšana

Izskatot, kā izdevusies ieviešana, veic šādas darbības:

- noskaidro un nodod tālāk informāciju par klientu un lietotāju apmierinātību un pakalpojuma kvalitāti pēc ieviešanas (ievāc atsauksmes un apdomā, kā pastāvīgi uzlabot pakalpojumu);
- izskata visus neizpildītos kvalitātes kritērijus;
- pārbauda, vai ir pabeigtas visas darbības, nepieciešamie labojumi un izmaiņas;
- pārliecinās, ka ieviešanas beigās nav radušās problēmas ar spējām, resursiem, kapacitāti vai veiktspēju;
- pārbauda, vai visas problēmas, zināmās kļūdas un aprisinājumi ir dokumentēti un ka tos ir akceptējuši klienti, galalietotāji, operacionālā atbalsta sniedzēji un citas skartās puses;
- seko līdzi ieviešanas radītiem incidentiem un problēmām (savlaicīgi sniedz atbalstu operacionālajām vienībām gadījumos, kad laiduma dēļ ir palielinājies darba apjoms);
- atjaunināt atbalsta dokumentāciju (t. i., tehniskās informācijas dokumentus);
- formāli nodod laiduma ieviešanu pakalpojumu operācijām;
- dokumentē gūto pieredzi;
- ievāc laiduma kopsavilkuma dokumentu no īstenošanas vienībām;
- formāli noslēdz laidumu pēc tam, kad ir verificēts izmaiņas pieprasījuma protokols.

9. DROŠĪBAS INCIDENTU VADĪBA

Drošības incidentu vadība ir process, kas nodarbojas ar drošības incidentiem nolūkā nodrošināt, ka ir iespējams par incidentiem paziņot potenciāli skartajām ieinteresētajām personām; incidentus izvērtēt un prioritizēt; uz incidentiem reaģēt tā, lai novērstu sensitīvu informācijas aktīvu konfidencialitātes, pieejamības vai integritātes jebkādu faktisku, aizdomīgu vai potenciālu pārkāpumu.

9.1. Informācijas drošības incidentu kategorizācija

Visus incidentus, kas ietekmē Savienības reģistra un Šveices reģistra sasaisti, analizē, lai noskaidrotu, vai ir noticis sensitīvas informācijas sarakstā (*SIL*) jebkādas iekļautās informācijas konfidencialitātes, integritātes vai pieejamības iespējams pārkāpums.

Tādā gadījumā incidentu raksturo kā informācijas drošības incidentu, nekavējoties reģistrē IT pakalpojumu vadības rīkā un kā tādu arī pārvalda.

9.2. Rīkošanās informācijas drošības incidentu gadījumā

Drošības incidenti ir 3. eskalācijas līmeņa pārziņā, un ar šo incidentu atrisināšanu nodarbojas īpaša incidentu vadības vienība (*IMT*).

IMT pienākumi ir:

- veikt pirmo analīzi, kategorizēt un novērtēt incidenta smagumu;
- koordinēt darbības starp visām ieinteresētajām personām, tostarp pilnībā dokumentēt incidenta analīzi, incidenta novēršanai pieņemtos lēmumus un konstatētās iespējamās vājās vietas;
- atkarībā no drošības incidenta smaguma laikus eskalēt līdz pienācīgam līmenim informēšanas un/vai lēmumu pieņemšanas nolūkā.

Informācijas drošības vadības procesā visa informācija par incidentiem tiek klasificēta visaugstākajā informācijas sensitivitātes līmenī, un jebkurā gadījumā zemākais līmenis ir "ETS SENSITĪVA INFORMĀCIJA".

Kamēr notiek izmeklēšana un/vai pastāv nepilnība, ko varētu ļaunprātīgi izmantot un kas vēl nav izlabota, informāciju klasificē ar grifu " ETS KRITISKI SVARĪGA INFORMĀCIJA".

9.3. Drošības incidenta identificēšana

Atkarībā no drošības notikuma veida informācijas drošības speciālists nosaka, kādas organizācijas jāiesaista *IMT*.

9.4. Drošības incidenta analīze

IMT incidenta izskatīšanā sadarbojas ar visām iesaistītajām organizācijām un attiecīgajiem to vienību dalībniekiem. Analīzes gaitā noskaidro aktīva konfidencialitātes, integritātes vai pieejamības zuduma apmēru un novērtē, kā tas ietekmēs visas skartās organizācijas. Pēc tam tiek definētas sākotnējās un pēcākās darbības, kā atrisināt incidentu un pārvaldīt tā ietekmi, tostarp šo darbību ietekmi uz resursiem.

9.5. Drošības incidentu smaguma novērtējums, eskalēšana un ziņošana

Pēc incidenta raksturošanas *IMT* novērtē jebkura jauna drošības incidenta smagumu un nekavējoties sāk rīkoties atkarībā no smaguma pakāpes.

9.6. Ziņošana par drošības incidentu

Ziņojumā par reaģēšanu uz informācijas drošības incidentu *IMT* norāda, ar kādiem rezultātiem incidents ir iegrožots un pakalpojums ir atjaunots. Ziņojumu nosūta 3. eskalācijas līmenim, izmantojot drošu e-pastu vai citus savstarpēji akceptētus drošas saziņas līdzekļus.

Atbildīgā puse pārskata iegrožošanas un pakalpojuma atjaunošanas rezultātus un:

- ja reģistrs iepriekš ticis atslēgts, to atkal pieslēdz;
- informāciju par incidentu sniedz reģistru vienībām;
- noslēdz incidentu.

Ziņojumā par informācijas drošības incidentu *IMT* būtu jāiekļauj (drošā veidā) relevantās ziņas, lai varētu garantēt, ka incidenti tiek reģistrēti un par tiem tiek paziņots saskanīgā veidā,

un lai būtu iespējams nekavējoties un pienācīgi rīkoties, lai incidentu iegrožotu. Galīgo ziņojumu par informācijas drošības incidentu *IMT* iesniedz, tiklīdz tas ir pabeigts.

9.7. Monitorings, kapacitātes veidošana un pastāvīgi uzlabojumi

IMT sniegs ziņojumus par visiem drošības incidentiem 3. eskalācijas līmenim. Šajā eskalācijas līmenī ziņojumus izmantos, lai apzinātu:

- drošības kontroļu vājās vietas un/vai operācijas, kas jāstiprina;
- iespējamās vajadzības šo procedūru pilnveidot, lai reaģēšanu uz incidentiem padarītu efektīvāku;
- apmācības un kapacitātes veidošanas iespējas, lai pastiprinātu reģistru sistēmu noturību informācijas drošības aspektā, mazinātu turpmāku incidentu risku un minimizētu to ietekmi.

10. INFORMĀCIJAS DROŠĪBAS VADĪBA

Informācijas drošības vadības mērķis ir nodrošināt organizācijas klasificētās informācijas, datu un IT pakalpojumu konfidencialitāti, integritāti un pieejamību. Līdztekus tehniskajiem komponentiem, t. sk. projektēšanai un testēšanai (sk. STS), pagaidu risinājuma drošības prasību izpildei ir vajadzīgas šādas kopējas darbības procedūras.

10.1. Sensitīvas informācijas identificēšana

Informācijas sensitivitāti novērtē, nosakot, kādā mērā ar šo informāciju saistīts drošības pārkāpums ietekmēs darbību (piem., finansiālie zaudējumi, tēla pasliktināšanās, normatīvo aktu pārkāpums).

Sensitīvās informācijas aktīvus identificē, balstoties uz to ietekmi uz sasaisti.

Šīs informācijas sensitivitātes pakāpi novērtē saskaņā ar sensitivitātes skalu, kas piemērojama šai sasaistei un kas sīki izklāstīta šā dokumenta sadaļā "Rīkošanās informācijas drošības incidentu gadījumā".

10.2. Informācijas aktīvu sensitivitātes pakāpes

Identificējot informācijas aktīvus, tos klasificē pēc šādiem noteikumiem:

- ja identificēta vismaz viena AUGSTA konfidencialitātes, integritātes vai pieejamības pakāpe, aktīvs klasificējams kā "ETS KRITISKI SVARĪGS" aktīvs;
- ja identificēta vismaz viena VIDĒJA konfidencialitātes, integritātes vai pieejamības pakāpe, aktīvs klasificējams kā "ETS SENSITĪVS" aktīvs;
- ja identificēta tikai ZEMA konfidencialitātes, integritātes vai pieejamības pakāpe, aktīvs klasificējams kā "ETS IEROBEŽOTAS PIEEJAMĪBAS" aktīvs.

10.3. Informācijas aktīvu īpašnieka nozīmēšana

Visiem informācijas aktīviem nozīmē īpašnieku. ETS informācijas aktīvi, kas ir daļa no *EUTL* un *SSTL* sasaistes vai ir ar to saistīti, ir jāiekļauj kopējo aktīvu inventarizācijas sarakstā, ko uztur abas puses. ETS informācijas aktīvi, kas nav daļa no *EUTL* un *SSTL* sasaistes, ir jāiekļauj aktīvu inventarizācijas sarakstā, ko uztur attiecīgā puse.

Par to, kas ir īpašnieks katram informācijas aktīvam, kurš ir daļa no *EUTL* vai *SSTL* sasaistes vai ir ar to saistīts, puses vienojas savā starpā. Par informācijas aktīva sensitivitātes novērtēšanu atbild tā īpašnieks.

Īpašniekam jābūt senioritātei, kas atbilst piešķirto aktīvu vērtībai. Par īpašnieka atbildību par aktīvu(-iem) un pienākumu uzturēt vajadzīgo konfidencialitātes, integritātes un pieejamības līmeni ir jāvienojas un šie aspekti ir jāformalizē.

10.4. Sensitīvas informācijas reģistrēšana

Visu sensitīvo informāciju iekļauj sensitīvās informācijas sarakstā (*SIL*).

SIL ir jāņem vērā un jāreģistrē gadījumi, kad sensitīvas informācijas sakopojumam (piemēram, informācijas kopumam, kas glabājas sistēmas datubāzē) var būt lielāka ietekme nekā vienvienīgam informācijas aktīvam.

SIL nav statisks. Ar aktīviem saistītie draudi, ievainojamības, drošības incidentu iespējamība vai sekas var mainīties negaidīti; tāpat reģistru sistēmas darbībā var tikt ieviesti jauni aktīvi.

Tāpēc *SIL* regulāri pārskata, un jebkādu jaunu informāciju, kas identificēta kā sensitīva, nekavējoties reģistrē *SIL*.

Katrā *SIL* ierakstā norāda vismaz šādas ziņas:

- informācijas apraksts;
- informācijas īpašnieks;
- sensitivitātes pakāpe;
- norāde, vai informācija satur persondatus;
- papildu ziņas, ja vajadzīgs.

10.5. Rīkošanās ar sensitīvu informāciju

Ja sensitīvu informāciju apstrādā ārpus Savienības reģistra un Šveices reģistra sasaistes, ar to rīkojas saskaņā ar rīkošanās instrukcijām.

Ja sensitīvu informāciju apstrādā Savienības reģistra un Šveices reģistra sasaistes ietvaros, ar to rīkojas saskaņā ar pušu drošības prasībām.

10.6. Piekļuves vadība

Piekļuves vadības uzdevums ir autorizētiem lietotājiem piešķirt tiesības izmantot pakalpojumu un tajā pašā laikā novērst neautorizētu lietotāju piekļuvi. Piekļuves vadību reizēm dēvē par "Tiesību pārvaldību" vai "Identitātes pārvaldību".

Kas attiecas uz pagaidu risinājumu un tā darbību, abām pusēm ir vajadzīga piekļuve šādiem komponentiem:

- *Wiki* — kopdarbības vide, kurā apmainās ar kopējo informāciju, piemēram, plānojot laidumus;
- IT pakalpojumu vadības rīks (*ITSM*), ko izmanto incidentu un problēmu vadībā (sk. nodaļu "Pieeja un standarti");
- ziņojumapmaiņas sistēma — katra puse nodrošina drošu ziņojumapmaiņas sistēmu, kas domāta, lai nosūtītu darījumu datus saturošus ziņojumus.

Šveices reģistra administrators un Savienības centrālais administrators nodrošina, ka piekļuve ir aktualizēta, un darbojas kā pušu kontaktpunkti attiecībā uz piekļuves vadības darbībām. Piekļuves pieprasījumus apstrādā saskaņā ar pieprasījuma izpildes procedūrām.

10.7. Sertifikātu/atslēgu vadība

Katra puse ir atbildīga par savu sertifikātu/atslēgu vadību (sertifikātu/ atslēgu ģenerēšanu, reģistrēšanu, glabāšanu, instalēšanu, izmantošanu, atjaunošanu, atsaukšanu, dublēšanu un atkopšanu). Kā izklāstīts sasaistes tehniskajos standartos (STS), izmantojami ir tikai digitālie sertifikāti, ko izdevis sertificētājs (*CA*), kuram uzticas abas puses. Rīkojoties ar sertifikātiem/atslēgām un tos glabājot, ir jāievēro rīkošanās instrukcijās izklāstītie noteikumi.

Sertifikātu un atslēgu atsaukšanu un/vai atjaunošanu abas puses koordinē savā starpā. Tas notiek saskaņā ar pieprasījuma izpildes procedūrām.

Šveices reģistra administrators un Savienības centrālais administrators ar sertifikātiem/atslēgām apmainās, izmantojot drošus saziņas līdzekļus saskaņā ar rīkošanās instrukcijās izklāstītajiem noteikumiem.

Sertifikātu/atslēgu verifikācija jebkādā veidā starp pusēm notiek ārpus joslas.