EUROPEISKA
KOMMISSIONEN

Bryssel den 23.6.2020
COM(2020) 255 final

ANNEX

BILAGA

till

förslag till rådets beslut

om den ståndpunkt som ska intas på Europeiska unionens vägnar i den gemensamma kommitté som inrättats genom avtalet mellan Europeiska unionen och Schweiziska edsförbundet om sammankoppling av deras utsläppshandelssystem för växthusgaser avseende antagandet av gemensamma driftsförfaranden

BESLUT NR 1/2020 AV DEN GEMENSAMMA KOMMITTÉ SOM INRÄTTATS GENOM AVTALET MELLAN EUROPEISKA UNIONEN OCH SCHWEIZISKA EDSFÖRBUNDET OM SAMMANKOPPLING AV DERAS UTSLÄPPSHANDELSSYSTEM FÖR VÄXTHUSGASER
av den ...
om gemensamma driftsförfaranden

DEN GEMENSAMMA KOMMITTÉN HAR ANTAGIT DETTA BESLUT

med beaktande av avtalet mellan Europeiska unionen och Schweiziska edsförbundet om sammankoppling av deras utsläppshandelssystem för växthusgaser[1] (nedan kallat *avtalet*), särskilt artikel 3, och

av följande skäl:

(1) Genom den gemensamma kommitténs beslut nr 2/2019 av den 5 december 2019 ändrades bilagorna I och II till avtalet, vilket innebär att de villkor för sammankoppling som anges i avtalet därmed är uppfyllda.

(2) Efter antagandet av beslut nr 2/2019 av den gemensamma kommittén och i enlighet med artikel 21.3 i avtalet har parterna utväxlat sina ratifikations- eller godkännandeinstrument, eftersom de anser att samtliga villkor för sammankoppling som anges i avtalet är uppfyllda.

(3) I enlighet med artikel 21.4 i avtalet trädde avtalet i kraft den 1 januari 2020.

(4) Enligt artikel 3.6 i avtalet ska den schweiziska registerförvaltaren och unionens centrala förvaltare fastställa gemensamma driftsförfaranden för tekniska angelägenheter eller angelägenheter som är nödvändiga för driften av kopplingen mellan EU:s transaktionsförteckning (EUTL) i unionsregistret och den schweiziska kompletterande transaktionsförteckningen (SSTL) i det schweiziska registret, och beakta prioriterade områden i nationell lagstiftning. De gemensamma driftsförfarandena ska träda i kraft när de har antagits genom beslut av den gemensamma kommittén.

(5) I enlighet med artikel 13.1 i avtalet ska den gemensamma kommittén enas om tekniska riktlinjer för att säkerställa att avtalet genomförs på ett korrekt sätt, inbegripet sådana som avser tekniska angelägenheter eller angelägenheter som är nödvändiga för driften av kopplingen och med beaktande av prioriterade områden i nationell lagstiftning. Tekniska riktlinjer får utarbetas av en arbetsgrupp som är inrättad i enlighet med artikel 12.5 i avtalet. Arbetsgruppen bör minst omfatta förvaltaren av det schweiziska registret och unionens centrala förvaltare och bistå den gemensamma kommittén i dess uppgifter enligt artikel 13 i avtalet.

(6) Mot bakgrund av riktlinjernas tekniska karaktär och behovet att anpassa dem till utvecklingen bör de tekniska riktlinjer som utarbetas av den schweiziska registerförvaltaren och unionens centrala förvaltare läggas fram inför den gemensamma kommittén för kännedom eller, vid behov, godkännande.

[1] EUT L 322, 7.12.2017, s. 3.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Härmed antas de gemensamma driftsförfaranden som bifogas detta beslut.

Artikel 2

Härmed ska en arbetsgrupp inrättas i enlighet med artikel 12.5 i avtalet. Den ska bistå den gemensamma kommittén i att säkerställa att avtalet genomförs på ett korrekt sätt, och med att utarbeta tekniska riktlinjer för genomförandet av de gemensamma driftsförfarandena.

Arbetsgruppen ska minst omfatta den schweiziska registerförvaltaren och unionens centrala förvaltare.

Artikel 3

Detta beslut träder i kraft samma dag som det antas.

Utfärdat på engelska i Bryssel den XX 2020.

På gemensamma kommitténs vägnar

Sekreterare för Europeiska unionen	*Ordförande*	*Sekreterare för Schweiz*

TILLÄGG

BILAGA

Gemensamma driftsförfaranden

i enlighet med artikel 3.6 i avtalet mellan Europeiska unionen och Schweiziska edsförbundet om sammankoppling av deras utsläppshandelssystem för växthusgaser – Förfaranden för en provisorisk lösning –

1. ORDLISTA

Tabell 1-1: Förkortningar och definitioner

Förkortning/Term	Definition
Certifikatutfärdare	Enhet som utfärdar digitala certifikat
Schweiz	Schweiziska edsförbundet
Utsläppshandelssystem	System för handel med utsläppsrätter
EU	Europeiska unionen
IMT	Incidenthanteringsgrupp
Informationstillgång	Information som är värdefull för ett företag eller en organisation
IT	Informationsteknik
ITIL	Information Technology Infrastructure Library (internationellt erkänd uppsättning bästa praxis och normer som stöder förvaltning av it-tjänster)
ITSM	Hantering av IT-tjänster
LTS	Tekniska standarder för sammankoppling
Register	Ett redovisningssystem för utsläppsrätter som utfärdats inom ramen för utsläppshandelssystemet för att hålla reda på innehavaren av utsläppsrätter på elektroniska konton.
RFC	Förändringsförfrågan
SIL	Förteckning över känsliga uppgifter
SR	Tjänsteförfrågan
Wiki	Webbplats som ger användarna möjlighet att utbyta information och kunskaper genom att lägga till eller anpassa innehåll direkt via en webbläsare.

2. INLEDNING

Avtalet mellan Europeiska unionen och Schweiziska edsförbundet om sammankoppling av deras utsläppshandelssystem för växthusgaser av den 23 november 2017 (nedan kallat *avtalet*) innehåller bestämmelser om ett ömsesidigt erkännande av utsläppsrätter som kan användas för fullgörande i Europeiska unionens utsläppshandelssystem eller i Schweiz utsläppshandelssystem. För att praktiskt genomföra sammankopplingen av unionens utsläppshandelssystem och Schweiz utsläppshandelssystem ska en direkt koppling mellan unionens transaktionsförteckning (EUTL) i unionsregistret och den schweiziska kompletterande transaktionsförteckningen (SSTL) i det schweiziska registret upprättas, vilket kommer att möjliggöra överföring mellan registren av utsläppsrätter som har utfärdats i något av utsläppshandelssystemen (artikel 3.2 i avtalet). För att praktiskt genomföra sammankopplingen av EU:s utsläppshandelssystem och Schweiz utsläppshandelssystem ska en provisorisk lösning vara införd i maj 2020, eller så snart som möjligt därefter. Parterna ska samarbeta för att så snart som möjligt ersätta den provisoriska lösningen med en permanent registerkoppling (bilaga II till avtalet).

Enligt artikel 3.6 i avtalet ska den schweiziska registerförvaltaren och unionens centrala förvaltare fastställa gemensamma driftsförfaranden för tekniska angelägenheter eller angelägenheter som är nödvändiga för driften av kopplingen, och beakta prioriterade områden i nationell lagstiftning. De gemensamma driftsförfaranden som förvaltarna utarbetar ska träda i kraft när de antagits genom beslut av den gemensamma kommittén.

De gemensamma driftsförfaranden som anges i detta dokument ska antas av den gemensamma kommittén genom dess beslut nr 1/2020. I enlighet med detta beslut ska den gemensamma kommittén be den schweiziska registerförvaltaren och unionens centrala förvaltare att fastställa ytterligare tekniska riktlinjer för att praktiskt genomföra sammankopplingen och säkerställa att dessa kontinuerligt anpassas till den tekniska utvecklingen och nya krav på kopplingens säkerhet och skydd samt till en ändamålsenlig och effektiv drift av kopplingen.

2.1. Tillämpningsområde

Detta dokument utgör en gemensam överenskommelse mellan parterna till avtalet avseende fastställandet av en förfarandemässig grund för kopplingen mellan registren i unionens utsläppshandelssystem och Schweiz utsläppshandelssystem. I dokumentet anges de övergripande kraven på driftsförfaranden, men vissa ytterligare tekniska riktlinjer kommer att krävas för att praktiskt genomföra sammankopplingen.

För att kopplingen ska fungera korrekt krävs tekniska specifikationer för att praktiskt genomföra sammankopplingen. I enlighet med artikel 3.7 i avtalet ska de närmare detaljerna i dessa beskrivas i det dokument om tekniska standarder för sammankoppling som ska antas separat genom beslut av den gemensamma kommittén.

Syftet med de gemensamma driftsförfarandena är att säkerställa att IT-tjänster som rör driften av kopplingen mellan registren i unionens utsläppshandelssystem och Schweiz utsläppshandelssystem tillhandahålls på ett ändamålsenligt och effektivt sätt, i synnerhet när det gäller tjänsteförfrågningar, lösning av tjänsteavbrott, åtgärdande av problem samt utförande av rutinmässiga driftsuppgifter i enlighet med internationella standarder för hantering av IT-tjänster.

För den överenskomna provisoriska lösningen krävs endast följande gemensamma driftsförfaranden, som ingår i detta dokument:

- Incidenthantering

- Problemhantering
- Tillgodoseende av begäran
- Förändringshantering
- Releasehantering
- Hantering av säkerhetsincidenter
- Informationssäkerhetshantering

I samband med produktionssättningen av en permanent registerkoppling vid en senare tidpunkt måste de gemensamma driftsförfarandena vid behov anpassas och kompletteras.

2.2. Målgrupper

Målgrupperna för dessa gemensamma driftsförfaranden är supportgrupperna för unionsregistret och det schweiziska registret.

3. TILLVÄGAGÅNGSSÄTT OCH STANDARDER

Följande principer gäller för samtliga gemensamma driftsförfaranden:

- EU och Schweiz har enats om att definiera de gemensamma driftsförfarandena baserat på ITIL (Information Technology Infrastructure Library, version 3). Metoderna i denna standard används för och anpassas till de särskilda behoven i samband med den provisoriska lösningen.
- Den kommunikation och samordning mellan de båda parterna som behövs för utförandet av de gemensamma driftsförfarandena sker via servicedeskarna för det schweiziska registret och unionsregistret. Uppgifter tilldelas alltid inom en av parterna.
- Om det råder olika uppfattningar om hur en uppgift i de gemensamma driftsförfarandena ska utföras ska frågan analyseras och lösas av båda servicedeskarna. Om ingen överenskommelse kan nås ska frågan om en gemensam lösning hänskjutas till nästa eskaleringsnivå.

Eskaleringsnivåer	**EU**	**Schweiz**
Nivå 1	EU:s servicedesk	Schweiz servicedesk
Nivå 2	EU:s driftsansvarige	Schweiz applikationsansvarige för registret
Nivå 3	Den gemensamma kommittén (som kan delegera detta ansvar i enlighet med artikel 12.5 i avtalet)	
Nivå 4	en gemensamma kommittén (om nivå 3 har delegerats)	

- Varje part kan fastställa förfaranden för driften av sitt eget registersystem, med beaktande av de krav och gränssnitt som berörs av dessa gemensamma driftsförfaranden.
- Ett verktyg för hantering av IT-tjänster ska användas till stöd för de gemensamma driftsförfarandena, i synnerhet för incidenthantering, problemhantering och tillgodoseende av begäranden samt för kommunikation mellan de båda parterna.

- Även utbyte av information via e-post är tillåten.
- Båda parterna ska säkerställa att informationssäkerhetskraven uppfylls i enlighet med hanteringsanvisningarna.

4. INCIDENTHANTERING

Syftet med incidenthanteringsprocessen är att säkerställa att IT-tjänster återställs till en normal nivå för tjänsten så snabbt som möjligt och med minimal påverkan på verksamheten.

Vid incidenthantering bör incidenter även registreras för rapporteringsändamål, och incidenthanteringen bör integreras med andra processer som underlag för kontinuerliga förbättringar.

- På en övergripande nivå omfattar incidenthantering följande aktiviteter:
- Upptäckt och registrering
- Klassificering och inledande support
- Utredning och diagnostisering
- Åtgärd och återställning
- Stängning av incidenten

Under incidentens hela livscykel ansvarar incidenthanteringsprocessen för att kontinuerligt hantera ägarskap, övervakning, uppföljning och kommunikation.

4.1. Upptäckt och registrering av incidenter

En incident kan upptäckas av en supportgrupp, med hjälp av verktyg för automatiserad övervakning eller av teknisk personal i samband med rutinmässig övervakning.

När en incident upptäcks ska den registreras och tilldelas en unik identifikationskod så att den kan följas upp och övervakas på lämpligt sätt. Den unika identifieringskoden för en incident är den identifieringskod som den tilldelats i det gemensamma ärendesystem som används av partens servicedesk (antingen EU:s eller Schweiz) och där incidenten har registrerats, och identifieringskoden ska användas i all kommunikation om incidenten.

För alla incidenter bör kontaktpunkten vara den parts servicedesk som har registrerat incidenten.

4.2. Klassificering och inledande support

Syftet med att klassificera incidenter är att förstå och fastställa vilket system och/eller vilka tjänster som påverkas och i vilken omfattning. För att klassificeringen ska vara ändamålsenlig bör den redan från början dirigera incidenten till rätt resurs så att den snabbt kan åtgärdas.

I klassificeringsfasen bör incidenten kategoriseras och prioriteras i enlighet med vilken påverkan den har och hur snabbt den måste lösas så att den kan behandlas inom den tidsram som gäller för prioriteringsnivån.

Om incidenten potentiellt kan påverka känsliga uppgifters sekretess och integritet och/eller påverkar systemets tillgänglighet ska incidenten betecknas som en säkerhetsincident och hanteras enligt den process som fastställs i avsnittet ”Hantering av säkerhetsincidenter” i detta dokument.

Om möjligt ska den servicedesk som registrerade ärendet genomföra den inledande diagnostiseringen. För att göra detta kontrollerar servicedesken om incidenten härrör från ett

känt fel. I så fall är åtgärden för att lösa eller kringgå problemet redan känd och dokumenterad.

Om servicedesken lyckas lösa incidenten stänger den incidenten i detta skede, eftersom huvudsyftet med incidenthanteringen har uppnåtts (dvs. att snabbt återställa tjänsten för slutanvändaren). Om servicedesken inte lyckas lösa incidenten eskalerar servicedesken incidenten till lämplig lösningsgrupp för vidare utredning och diagnostisering.

4.3. Utredning och diagnostisering

Utredning och diagnostisering av incidenter görs om en incident inte kan lösas av servicedesken under den inledande diagnostiseringen och därför har eskalerats på lämpligt sätt. Eskalering av incidenter ingår som en integrerad del i utrednings- och diagnostiseringsprocessen.

En vanlig metod i utrednings- och diagnostiseringsfasen är att försöka återskapa incidenten under kontrollerade förhållanden. Vid utredning och diagnostisering av incidenter är det viktigt att man förstår vilken följd av händelser som ledde fram till incidenten.

Eskalering innebär en insikt om att incidenten inte kan lösas på den aktuella supportnivån utan måste skickas vidare till en supportgrupp på högre nivå eller till den andra parten. Eskaleringen kan följa två vägar: horisontell (funktionell) eskalering eller vertikal (hierarkisk) eskalering.

Den servicedesk som registrerade och initierade incidentärendet ansvarar för att incidenten eskaleras till lämplig resurs och för att följa upp den övergripande statusen för incidenten och vem den tilldelats.

Den av parterna som tilldelats incidenten ansvarar för att se till att de åtgärder som begärs utförs inom lämplig tid och för att återkoppla till sin egen servicedesk.

4.4. Åtgärd och återställning

Åtgärder och återställning i samband med incidenter utförs när man har en full förståelse av incidenten. Att hitta en åtgärd för en incident innebär att man har identifierat ett sätt att korrigera felet. Tillämpningen av åtgärden sker i återställningsfasen.

När lämpliga resurser har åtgärdat felet i tjänsten skickas incidenten tillbaka till den servicedesk som registrerade den, som kontrollerar med den som rapporterade incidenten att felet är löst och att incidenten kan stängas. Kunskaperna från hanteringen av incidenten ska dokumenteras för framtida bruk.

Återställningen kan göras av IT-supportpersonal eller genom att ge slutanvändaren instruktioner som han eller hon kan följa.

4.5. Stängning av incidenter

Stängning av incidenter är det sista steget i incidenthanteringsprocessen och görs kort efter det att incidenten har åtgärdats.

Checklistan med åtgärder som behöver göras i stängningsfasen för en incident omfattar i synnerhet följande:

- Kontrollera att den ursprungliga kategoriseringen av incidenten var korrekt.
- På lämpligt sätt samla in all information om omständigheterna kring incidenten.
- På lämpligt sätt dokumentera incidenten och uppdatera kunskapsdatabasen.

- På lämpligt sätt informera alla intressenter som direkt eller indirekt påverkades av incidenten.

En incident stängs formellt när servicedesken har genomfört stängningsfasen för incidenten och informerat den andra parten.

När en incident har stängts kan den inte öppnas på nytt. Om en incident uppstår på nytt inom kort tid öppnas inte den ursprungliga incidenten på nytt utan en ny incident registreras.

Om en incident följs upp av både EU:s och Schweiz servicedeskar ansvarar den servicedesk som registrerade ärendet för att slutgiltigt stänga incidenten.

5. PROBLEMHANTERING

Detta förfarande bör följas om ett problem har identifierats, vilket utgör startpunkten för problemhanteringsprocessen. Problemhantering fokuserar på att förbättra kvaliteten och minska volymen av incidenter. Ett problem kan vara orsaken till en eller flera incidenter. När en incident rapporteras är målet för incidenthanteringen att så snabbt som möjligt återställa tjänsten, eventuellt genom tillfälliga lösningar. Syftet med att registrera ett problem är att utreda grundorsaken till felet för att fastställa en förändring som kan genomföras för att hindra att problemet och de incidenter som kan kopplas till det uppstår på nytt.

5.1. Identifiering och registrering av problem

Kontaktpunkt för problemrelaterade frågor är antingen EU:s eller Schweiz servicedesk, beroende på vilken av parterna som registrerade ärendet.

Den unika identifieringskoden för ett problem är den identifieringskod som det tilldelades inom ramen för hanteringen av IT-tjänster. Den måste användas i all kommunikation som rör det aktuella problemet.

Ett problem kan initieras genom en incident eller öppnas på eget initiativ för att lösa fel som i något skede upptäckts i systemet.

5.2. Prioritering av problem

För att underlätta uppföljningen kan problem, på samma sätt som incidenter, kategoriseras enligt hur allvarliga och prioriterade de är, med hänsyn till vilken påverkan de incidenter som kan knytas till problemet har och hur ofta de uppstår.

5.3. Utredning och diagnostisering av problem

Varje part kan initiera ett problem, och det är den initierande partens servicedesk som ansvarar för att registrera problemet, skicka det vidare till lämplig resurs och följa upp den övergripande statusen för det.

Den lösningsgrupp som problemet har eskalerats till ansvarar för att hantera problemet inom lämplig tid och kommunicera med servicedesken.

På begäran ansvarar båda parterna för att de åtgärder som fastställts utförs och för att återkoppla till den egna partens servicedesk.

5.4. Åtgärd

Den lösningsgrupp som tilldelats problemet ansvarar för att åtgärda det och lämna relevant information till den egna partens servicedesk.

Kunskaperna från hanteringen av problemet ska dokumenteras för framtida bruk.

5.5. Stängning av problem

Ett problem stängs formellt när problemet har lösts genom att en förändring har genomförts. Stängningsfasen för ett problem genomförs av den servicedesk som registrerade problemet och informerade den andra partens servicedesk.

6. TILLGODOSEENDE AV BEGÄRAN

Processen för tillgodoseende av begäran är hanteringen av en tjänsteförfrågan avseende en ny eller befintlig tjänst under hela dess livscykel, från registrering och godkännande av tjänsteförfrågan till stängningen av den. Tjänsteförfrågningar är vanligtvis förfrågningar om mindre, fördefinierade, återkommande, förhandsgodkända tjänster och förfaranden.

De viktigaste steg som ska följas anges nedan:

6.1. Initiering av tjänsteförfrågningar

Uppgifterna om en tjänsteförfrågan skickas till EU:s eller Schweiz servicedesk via e-post eller telefon, eller via verktyget för hantering av IT-tjänster eller någon annan överenskommen kommunikationskanal.

6.2. Registrering och analys av tjänsteförfrågningar

För alla tjänsteförfrågningar bör kontaktpunkten vara EU:s eller Schweiz servicedesk, beroende på vilken av parterna som initierade tjänsteförfrågan. Denna servicedesk ansvarar för att registrera och analysera tjänsteförfrågan med erforderlig noggrannhet.

6.3. Godkännande av tjänsteförfrågningar

Servicedesken hos den av parterna som initierade tjänsteförfrågan kontrollerar om godkännande från den andra parten krävs och vänder sig i så fall till den för att erhålla godkännande. Om tjänsteförfrågan inte godkänns uppdaterar servicedesken ärendet och stänger det.

6.4. Tillgodoseende av begäran

I detta steg ombesörjs en ändamålsenlig och effektiv hantering av tjänsteförfrågningar. Åtskillnad måste göras mellan följande fall:

- Tillgodoseende av en tjänsteförfrågan som bara påverkar en av parterna. I så fall utfärdar den parten arbetsorder och samordnar utförandet.
- Genomförandet av tjänsteförfrågan påverkar både EU och Schweiz. I så fall utfärdar servicedeskarna arbetsorder inom sina respektive ansvarsområden. Processen för att tillgodose tjänsteförfrågan samordnas av båda servicedeskarna. Det övergripande ansvaret ligger hos den servicedesk som mottog och initierade tjänsteförfrågan.

När tjänsteförfrågan har åtgärdats måste den tilldelas statusen åtgärdad.

6.5. Eskalering av tjänsteförfrågningar

Servicedesken kan vid behov eskalera ej åtgärdade tjänsteförfrågningar till lämplig resurs (tredje part).

Eskalering görs till respektive tredje part, dvs. EU:s servicedesk måste vända sig till Schweiz servicedesk för eskalering till Schweiz tredje part och omvänt.

Den tredje part som tjänsteförfrågan eskalerats till ansvarar för att hantera den inom lämplig tid och kommunicera med den servicedesk som eskalerade tjänsteförfrågan.

Den servicedesk som registrerade tjänsteförfrågan ansvarar för att följa upp den övergripande statusen för den och vem den tilldelats.

6.6. Granskning av tillgodoseende av begäran

Den ansvariga servicedesken gör en slutlig kvalitetskontroll av de uppgifter som registrerats i tjänsteförfrågan innan den stängs. Syftet är att kontrollera att tjänsteförfrågan verkligen har behandlats och att alla uppgifter som krävs för att beskriva livscykeln för den anges i tillräcklig detalj. Kunskaperna från hanteringen av tjänsteförfrågan ska också dokumenteras för framtida bruk.

6.7. Stängning av förfrågningar

Om de parter som tilldelats tjänsteförfrågan är överens om att den har tillgodosetts och den som gjorde förfrågan betraktar ärendet som åtgärdat, ska tjänsteförfrågan tilldelas nästa status, ”Stängd”.

En tjänsteförfrågan stängs formellt när den servicedesk som registrerade den har genomfört stängningsfasen för tjänsteförfrågan och informerat den andra partens servicedesk.

7. FÖRÄNDRINGSHANTERING

Syftet med förändringshantering är att tillse att standardiserade metoder och förfaranden används för en effektiv och snabb hantering av alla förändringar för att kontrollera IT-infrastrukturen, så att antalet relaterade incidenter och deras påverkan på tjänsten minimeras. Förändringar av IT-infrastrukturen kan genomföras reaktivt för att lösa problem eller tillgodose externa krav, t.ex. förändrad lagstiftning, eller proaktivt för att förbättra effektivitet och ändamålsenlighet eller för att möjliggöra eller ta hänsyn till verksamhetsinitiativ.

Förändringshanteringsprocessen omfattar olika steg för att samla in alla detaljer om en förändringsbegäran för framtida spårning. Genom processerna säkerställs att förändringen valideras och testas innan den produktionssätts. Ansvaret för en framgångsrik produktionssättning ligger i releasehanteringsprocessen.

7.1. Förändringsförfrågningar

En förändringsförfrågan skickas till förändringshanteringsgruppen för validering och godkännande. För alla förändringsförfrågningar bör kontaktpunkten vara EU:s eller Schweiz servicedesk, beroende på vilken av parterna som initierade förfrågan. Denna servicedesk ansvarar för att registrera och analysera förfrågan med lämplig omsorg.

En förändringsförfrågan kan ha sitt ursprung i

- en incident som ger upphov till en förändring,
- ett befintligt problem som leder till en förändring,
- en begäran om en ny förändring från en slutanvändare,
- en förändring till följd av pågående underhåll,
- ändrad lagstiftning.

7.2. Utvärdering och planering av förändringar

I denna fas hanteras bedömningen och planeringen av förändringar. Här ingår prioriterings- och planeringsaktiviteter för att minimera risker och påverkan.

Om genomförandet av en förändringsförfrågan påverkar både EU och Schweiz kontrollerar den part som registrerade förändringsförfrågan utvärderingen och planeringen av förändringen med den andra parten.

7.3. Godkännande av förändringar

Alla registrerade förändringsförfrågningar måste godkännas på relevant eskaleringsnivå.

7.4. Implementering av förändringar

Implementering av förändringar hanteras inom releasehanteringen. Båda parternas releasehanteringsgrupper följer sina egna processer som omfattar planering och testning. När implementeringen slutförts granskas förändringen. För att säkerställa att allt går planenligt ses förändringshanteringsprocessen över kontinuerligt och uppdateras vid behov.

8. RELEASEHANTERING

En release är en eller flera förändringar inom en IT-tjänst som ingår i en releaseplan och måste godkännas, förberedas, byggas, testas och produktionssättas tillsammans. En enda release kan innehålla en felrättning, en förändring av hårdvara eller andra komponenter, programändringar, uppgradering av programversioner och ändringar av dokumentation och/eller processer. Innehållet i varje release hanteras, testas och produktionssätts som en enhet.

Syftet med releasehantering är att planera, bygga, testa, validera och leverera förmågan att tillhandahålla den tjänst som tagits fram för att uppfylla intressentens krav och uppfylla de avsedda målen. Kriterierna för godkännande av alla förändringar av tjänsten fastställs och dokumenteras under designkoordineringen och lämnas till releasehanteringsgrupperna.

En release består oftast av ett antal problemrättningar och förbättringar av tjänsten. Den innehåller den nya eller ändrade programvara som krävs och ny eller ändrad hårdvara som behövs för att implementera de godkända förändringarna.

8.1. Planering av releaser

Det första steget i processen är att gruppera godkända förändringar i releasepaket och att fastställa omfattningen och innehållet i releaserna. Baserat på denna information utarbetas inom ramen för delprocessen releaseplanering ett tidsschema för att bygga, testa och produktionssätta releasen.

I releaseplaneringen bör följande information ingå:

- Releasens omfattning och innehåll.
- Riskbedömning av releasen och releasens riskprofil.
- Kunder/användare som påverkas av releasen.
- Vilken grupp som ansvarar för releasen.
- Strategi för leverans och produktionssättning.
- Resurser som krävs för releasen och produktionssättning av den.

Båda parterna ska informera varandra om sin releaseplanering och sina underhållsperioder. Om en release påverkar både EU och Schweiz ska parterna samordna sin planering och fastställa en gemensam underhållsperiod.

8.2. Byggande och testning av releasepaket

I bygg- och testningsstegen i releasehanteringsprocessen fastställs tillvägagångssättet för att genomföra releasen eller releasepaketet och för att upprätthålla en kontrollerad miljö före förändringen av produktionsmiljön, samt för testning av alla förändringar i alla miljöer där de driftsätts.

Om en release påverkar både EU och Schweiz ska parterna samordna sin leveransplanering och testning. Detta omfattar följande aspekter:

- Hur och när releaseenheter och tjänstekomponenter levereras.
- De typiska ledtiderna och vad som händer vid förseningar.
- Hur arbetets fortskridande ska följas upp och bekräftas.
- Mätmetoder för att övervaka och fastställa i vilken utsträckning produktionssättningen av releasen har varit framgångsrik.
- Gemensamma testfall för relevanta funktioner och förändringar.

Vid slutet av denna delprocess är alla releasekomponenter klara för driftsättning i produktionsmiljön.

8.3. Förberedelse av produktionssättningar

Genom denna delprocess säkerställs att korrekta kommunikationsplaner tagits fram och att meddelanden är klara att skickas till alla intressenter och slutanvändare som påverkas, samt att releasen har integrerats med förändringshanteringsprocessen så att alla förändringar genomförs på ett kontrollerat sätt och har godkänts i de forum som krävs.

Om en release påverkar både EU och Schweiz ska parterna samordna följande:

- Uppgifterna i förändringsförfrågan för schemaläggning och förberedelse av driftsättning i produktionsmiljön.
- Utarbetandet av en övergripande implementeringsplan.
- En strategi för återställning så att en återgång till tillståndet före produktionssättningen kan göras om produktionssättningen misslyckas.
- Meddelanden till alla nödvändiga parter.
- Begäran om godkännande att genomföra releasen från relevant eskaleringsnivå.

8.4. Återställning av tillståndet före releasen

Om produktionssättningen misslyckas eller testning visar att produktionssättningen inte var framgångsrik eller inte uppfyller de överenskomna kriterierna för godkännande/kvalitetskriterierna måste båda parternas releasehanteringsgrupper återställa produktionsmiljön till tillståndet före produktionssättningen. Alla nödvändiga intressenter måste informeras, inbegripet de slutanvändare som påverkas eller utgjorde målgruppen för releasen. I avvaktan på godkännande kan processen återstartas vid något av de tidigare stegen.

8.5. Granskning och stängning av releasen

Vid granskningen av produktionssättningen bör följande aktiviteter ingå:

- Samla in synpunkter från kunden och användarna om deras tillfredsställelse med produktionssättningen och leveransen av tjänsten (samla in synpunkter och använda som underlag för kontinuerlig förbättring).

- Granska eventuella kvalitetskriterier som inte uppfylldes.
- Kontrollera att alla åtgärder, nödvändiga rättningar och förändringar är kompletta.
- Säkerställa att inga problem i fråga om funktionalitet, resurser, kapacitet eller prestanda förekommer efter produktionssättningen.
- Kontrollera att eventuella problem, kända fel eller tillfälliga lösningar har dokumenterats och godtas av kunden, slutanvändare, driftsupport och andra berörda parter.
- Övervaka incidenter och problem som orsakas av produktionssättningen (tillhandahålla tidig support till driftspersonal om releasen har medfört ökad arbetsbelastning).
- Uppdatera supportdokumentationen.
- Formellt överlämna den produktionssatta releasen till tjänstedriften.
- Dokumentera de erfarenheter som gjorts.
- Ta emot den sammanfattande rapporten om releasen från implementeringsgrupperna.
- Formellt stänga releasen efter verifiering mot uppgifterna i förändringsförfrågan.

9. HANTERING AV SÄKERHETSINCIDENTER

Hantering av säkerhetsincidenter är en process med syftet att möjliggöra kommunikation av incidentinformation till potentiellt berörda intressenter, incidentbedömning och incidentprioritering samt incidentåtgärder i fråga om alla faktiska, misstänkta eller potentiella överträdelser som påverkar känsliga informationstillgångars sekretess, tillgänglighet eller integritet.

9.1. Kategorisering av informationssäkerhetsincidenter

Alla incidenter som påverkar kopplingen mellan unionsregistret och det schweiziska registret ska analyseras för att fastställa eventuell påverkan på sekretessen, integriteten eller tillgängligheten för uppgifter i förteckningen över känsliga uppgifter.

Om en sådan påverkan kan fastställas ska incidenten betecknas som en informationssäkerhetsincident, omedelbart registreras i verktyget för hantering av IT-tjänster och behandlas som en informationssäkerhetsincident.

9.2. Hantering av informationssäkerhetsincidenter

Ansvaret för säkerhetsincidenter ligger hos eskaleringsnivå 3 och lösningen av incidenterna ska hanteras av en särskild incidenthanteringsgrupp.

Incidenthanteringsgruppen ansvarar för att

- göra en inledande analys och kategorisera och bedöma incidentens allvarlighetsgrad,
- samordna insatserna från alla intressenter, inbegripet en fullständig dokumentation av incidentanalysen, de beslut som fattats för att åtgärda incidenten och eventuella svagheter som har identifierats,

- beroende på säkerhetsincidentens allvarlighetsgrad, inom lämplig tid eskalera incidenten till lämplig nivå för kännedom och/eller beslut.

I processen för informationssäkerhetshantering klassificeras all information om incidenter enligt den högsta känslighetsnivån hos de uppgifter som berörs, dock aldrig lägre än ETS KÄNSLIG.

Under en pågående utredning och/eller i samband med svagheter och tills dessa har avhjälpts klassificeras informationen som ETS KRITISK.

9.3. Identifiering av säkerhetsincidenter

Beroende på typen av säkerhetshändelse fastställer den informationssäkerhetsansvarige vilka organisationer som bör involveras och ingå i incidenthanteringsgruppen.

9.4. Analys av säkerhetsincidenter

Incidenthanteringsgruppen samverkar med alla involverade organisationer och relevanta medlemmar i deras grupper för att bedöma incidenten. Vid analysen fastställs i vilken utsträckning sekretessen, integriteten eller tillgängligheten för en tillgång har förlorats, och följderna för alla berörda organisationer bedöms. Därefter fastställs vilka inledande åtgärder och uppföljningsåtgärder som ska vidtas för att åtgärda incidenten och hantera dess påverkan, inbegripet vilka resurser som krävs för åtgärderna.

9.5. Allvarlighetsbedömning, eskalering och rapportering för säkerhetsincidenter

Incidenthanteringsgruppen ska bedöma alla nya säkerhetsincidenter efter att de betecknats som sådana och omedelbart inleda de åtgärder som krävs i enlighet med incidentens allvarlighetsgrad.

9.6. Rapportering av säkerhetsåtgärder

I åtgärdsrapporten för informationssäkerhetsincidenten anger incidenthanteringsgruppen vidtagna åtgärder för incidentbegränsning och resultatet av återställningsåtgärderna. Rapporten lämnas till eskaleringsnivå 3 via säker e-post eller annan ömsesidigt godtagbar metod för säker kommunikation.

Den ansvariga parten granskar begränsningsåtgärderna och resultatet av återställningsåtgärderna, och

- återstartar registerkopplingen, om den tidigare stängts av,
- kommunicerar incidentinformationen till registergrupperna,
- stänger incidenten.

Incidenthanteringsgruppen bör, på ett säkert sätt, ange relevanta uppgifter i åtgärdsrapporten för informationssäkerhetsincidenten för att säkerställa en enhetlig dokumentation och kommunikation och möjliggöra snabba och lämpliga åtgärder för att begränsa incidenten. När rapporten har färdigställts lämnar incidenthanteringsgruppen slutversionen av åtgärdsrapporten för informationssäkerhetsincidenten inom lämplig tid.

9.7. Övervakning, kapacitetsuppbyggnad och kontinuerlig förbättring

Incidenthanteringsgruppen lämnar rapporter om alla säkerhetsincidenter till eskaleringsnivå 3. Denna eskaleringsnivå använder rapporterna för att fastställa

- svagheter i säkerhetskontroller eller driften som behöver avhjälpas,

- eventuella behov att förbättra förfarandet för att effektivisera hanteringen av incidenter,

- möjligheter till utbildning och kapacitetsuppbyggnad för att ytterligare förstärka registersystemens motståndskraft mot informationssäkerhetshot, minska risken för framtida incidenter och minimera incidenternas påverkan.

10. INFORMATIONSSÄKERHETSHANTERING

Informationssäkerhetshanteringens syfte är att säkerställa sekretessen, integriteten och tillgängligheten för en organisations säkerhetsskyddsklassificerade uppgifter, data och IT-tjänster. Utöver tekniska komponenter såsom utformning och testning (se de tekniska standarderna för sammankoppling) krävs följande gemensamma driftsförfaranden för att uppfylla säkerhetskraven för den provisoriska lösningen:

10.1. Identifiering av känsliga uppgifter

En uppgifts känslighet bedöms genom att fastställa i vilken omfattning en säkerhetsöverträdelse som rör uppgiften kan påverka verksamheten (t.ex. i form av ekonomiska förluster, försämrad uppfattning om verksamheten, lagöverträdelser osv.).

Känsliga informationstillgångar ska identifieras på grundval av deras påverkan på sammankopplingen.

Känslighetsnivån för dessa uppgifter ska bedömas enligt en känslighetsskala som kan tillämpas på sammankopplingen och som beskrivs i avsnittet ”Hantering av informationssäkerhetsincidenter” i detta dokument.

10.2. Känslighetsnivåer för informationstillgångar

Informationstillgångar som identifierats som känsliga ska klassificeras med hjälp av följande regler:

- Tillgångar som omfattar minst en uppgift för vilken känslighetsnivån i fråga om sekretess, integritet eller tillgänglighet har angetts som HÖG ska klassificeras som ETS KRITISK.

- Tillgångar som omfattar minst en uppgift för vilken känslighetsnivån i fråga om sekretess, integritet eller tillgänglighet har angetts som MEDELHÖG ska klassificeras som ETS KÄNSLIG.

- Tillgångar som endast omfattar uppgifter för vilka känslighetsnivån i fråga om sekretess, integritet eller tillgänglighet har angetts som LÅG ska klassificeras som ETS BEGRÄNSAD.

10.3. Tilldelning av ägarskap för informationstillgångar

Alla informationstillgångar ska tilldelas en ägare. Informationstillgångar i utsläppshandelssystemet som ingår i eller används för kopplingen mellan EUTL och SSTL bör föras upp på en gemensam förteckning över informationstillgångar som underhålls av båda parterna. Informationstillgångar i utsläppshandelssystemet som ligger utanför kopplingen mellan EUTL och SSTL bör föras upp på en förteckning över informationstillgångar som underhålls av respektive part.

Ägarskapet för varje informationstillgång som ingår i eller används för kopplingen mellan EUTL och SSTL ska överenskommas av parterna. Ägaren till en informationstillgång ansvarar för att bedöma dess känslighet.

Ägaren bör ha en tjänstegrad som är lämplig med hänsyn till värdet på den eller de tilldelade tillgångarna. Ägarens ansvar för tillgången eller tillgångarna och skyldigheten att upprätthålla den nödvändiga sekretess-, integritets- och tillgänglighetsnivån bör godkännas och formaliseras.

10.4. Registrering av känsliga uppgifter

Alla känsliga uppgifter ska registreras i förteckningen över känsliga uppgifter.

Om en aggregering av känsliga uppgifter skulle kunna leda till en större påverkan än påverkan av en enda uppgift, ska detta beaktas och registreras i förteckningen över känsliga uppgifter (t.ex. en uppsättning uppgifter i systemets databas).

Förteckningen över känsliga uppgifter är inte statisk. Hot, sårbarheter, sannolikheten för eller konsekvenserna av säkerhetsincidenter som rör tillgångarna kan förändras utan förvarning, och nya tillgångar kan tillkomma i samband med driften av registersystemen.

En översyn av förteckningen över känsliga uppgifter ska därför göras regelbundet, och nya uppgifter som identifieras som känsliga ska omedelbart föras upp på förteckningen.

Förteckningen över känsliga uppgifter ska innehålla minst följande information om varje post:

- Beskrivning av uppgiften
- Uppgiftsägare
- Känslighetsnivå
- Information om huruvida uppgiften omfattar personuppgifter
- Ytterligare information om så krävs.

10.5. Registrering av känsliga uppgifter

När känsliga uppgifter behandlas utanför kopplingen mellan unionsregistret och det schweiziska registret ska de hanteras i enlighet med hanteringsanvisningarna.

Känsliga uppgifter som behandlas genom kopplingen mellan unionsregistret och det schweiziska registret ska hanteras i enlighet med parternas säkerhetskrav.

10.6. Behörighetshantering

Syftet med behörighetshantering är att ge auktoriserade användare rätt att använda en tjänst och samtidigt förhindra tillgången för icke auktoriserade användare. Behörighetshantering kallas ibland även ”rättighetshantering” eller ”identitetshantering”.

När det gäller den provisoriska lösningen och driften av denna behöver båda parterna behörighet till följande komponenter:

- Wiki: en samarbetsmiljö för utbyte av gemensam information, exempelvis releaseplanering.
- Verktyg för hantering av IT-tjänster, för incident- och problemhantering (se avsnittet ”Tillvägagångssätt och standarder”).

- System för meddelandeutbyte: varje part ska tillhandahålla ett säkert överföringssystem för utbyte av meddelanden för överföring av de meddelanden som innehåller transaktionsuppgifter.

Den schweiziska registerförvaltaren och unionens centrala förvaltare säkerställer att behörigheterna hålls aktuella och fungerar som respektive parts kontaktpunkt för aktiviteter som rör behörighetshantering. Behörighetsförfrågningar hanteras i enlighet med förfarandena för tillgodoseende av begäran.

10.7. Hantering av certifikat/nycklar

Varje part ansvarar för sin egen hantering av certifikat/nycklar (skapande, registrering, lagring, installation, användning, förnyelse, återkallande, säkerhetskopiering och återställning av certifikat/nycklar). Som anges i de tekniska standarderna för sammankoppling ska bara digitala certifikat som utfärdats av en certifikatutfärdare som är betrodd av båda parterna användas. Hanteringen och lagringen av certifikat/nycklar måste följa bestämmelserna i hanteringsanvisningarna.

Återkallande och/eller förnyelse av certifikat och nycklar ska samordnas av båda parterna. Detta görs i enlighet med förfarandena för tillgodoseende av begäran.

Den schweiziska registerförvaltaren och unionens centrala förvaltare utbyter certifikat/nycklar via en säker kommunikationsmetod i enlighet med bestämmelserna i hanteringsanvisningarna.

All verifiering av certifikat/nycklar som på något sätt görs av parterna ska ske via en separat kanal.