EUROPA-
KOMMISSIONEN

Bruxelles, den 23.6.2020
COM(2020) 255 final

ANNEX

BILAG

til

Forslag til Rådets afgørelse

om den holdning, som på Den Europæiske Unions vegne skal indtages i det fælles udvalg, der er nedsat i henhold til aftalen mellem Den Europæiske Union og Det Schweiziske Forbund om sammenkobling af deres systemer for handel med drivhusgasemissioner, for så vidt angår vedtagelsen af fælles driftsprocedurer

AFGØRELSE NR. 1/2020 TRUFFET AF DET FÆLLES UDVALG, DER ER OPRETTET VED SAMARBEJDSAFTALEN MELLEM DEN EUROPÆISKE UNION OG DET SCHWEIZISKE FORBUND OM SAMMENKOBLING AF DERES SYSTEMER FOR HANDEL MED DRIVHUSGASEMISSIONER

af ...

om fælles driftsprocedurer

DET FÆLLES UDVALG HAR —

under henvisning til aftalen mellem Den Europæiske Union og Det Schweiziske Forbund om sammenkobling af deres systemer for handel med drivhusgasemissioner[1] (herefter "aftalen"), særlig artikel 3, og

ud fra følgende betragtninger:

(1) Ved afgørelse nr. 2/2019 truffet af det fælles udvalg den 5. december 2019 blev bilag I og II til aftalen ændret således, at de betingelser for sammenkoblingen, der er fastsat i aftalen, opfyldes.

(2) Efter vedtagelsen af det fælles udvalgs afgørelse nr. 2/2019 og i overensstemmelse med aftalens artikel 21, stk. 3, har parterne udvekslet deres ratifikations- eller godkendelsesinstrumenter, da de finder, at alle betingelser for sammenkobling er opfyldt.

(3) I overensstemmelse med aftalens artikel 21, stk. 4, trådte aftalen i kraft den 1. januar 2020.

(4) Ifølge aftalens artikel 3, stk. 6, skal administratoren af det schweiziske register og Unionens centrale administrator fastlægge fælles driftsprocedurer for tekniske og andre forhold, som er nødvendige for driften af sammenkoblingen mellem EU-registrets EU-transaktionsjournal (EUTL) og det schweiziske registers supplerende transaktionsjournal (SSTL), under hensyntagen til prioriteter i den nationale lovgivning. De fælles driftsprocedurer bør træde i kraft, når de er vedtaget ved afgørelse i det fælles udvalg.

(5) I overensstemmelse med aftalens artikel 13, stk. 1, bør det fælles udvalg aftale tekniske retningslinjer for at sikre en korrekt gennemførelse af aftalen, herunder for tekniske og andre forhold, som er nødvendige for driften af forbindelsen, under hensyntagen til prioriteter i den nationale lovgivning. Tekniske retningslinjer kan udarbejdes af en arbejdsgruppe nedsat i henhold til aftalens artikel 12, stk. 5. Arbejdsgruppen bør som minimum omfatte administratoren af det schweiziske register og den centrale administrator for EU-registret og bør bistå det fælles udvalg i dets funktioner i henhold til aftalens artikel 13.

(6) I betragtning af retningslinjernes tekniske karakter og behovet for at tilpasse dem til den løbende udvikling bør de tekniske retningslinjer, som er udarbejdet af administratoren af det schweiziske register og Unionens centrale administrator, forelægges det fælles udvalg til orientering eller i givet fald godkendelse —

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

VEDTAGET DENNE AFGØRELSE:

Artikel 1

De fælles driftsprocedurer, der er knyttet som bilag til denne afgørelse, vedtages hermed.

Artikel 2

Hermed nedsættes der en arbejdsgruppe i henhold til aftalens artikel 12, stk. 5. Den bistår det fælles udvalg med at sikre en korrekt gennemførelse af aftalen, herunder udarbejdelse af tekniske retningslinjer for gennemførelsen af de fælles driftsprocedurer.

Arbejdsgruppen skal som minimum omfatte administratoren af det schweiziske register og den centrale administrator for EU-registret.

Artikel 3

Denne afgørelse træder i kraft på dagen for vedtagelsen.

Udfærdiget på engelsk i Bruxelles den XX 2020.

På det fælles udvalgs vegne

Sekretær for Den Europæiske Union	*Formanden*	*Sekretær for Schweiz*

TILLÆG

BILAG

FÆLLES DRIFTSPROCEDURER

i henhold til artikel 3, stk. 6, i aftalen mellem Den Europæiske Union og Det Schweiziske Forbund om sammenkobling af deres systemer for handel med drivhusgasemissioner
- Procedurer for en foreløbig løsning -

1. ORDLISTE

Tabel 1-1 Akronymer og definitioner

Akronym/ord	Definition
Certificeringsmyndighed	Enhed, der udsteder digitale certifikater
CH	Det Schweiziske Forbund
ETS	Emissionshandelssystemet
EU	Den Europæiske Union
IMT	Hændelsesstyringsteam
Informationsaktiv	En oplysning, der er værdifuld for en virksomhed eller organisation
IT	Informationsteknologi
ITIL	IT-infrastrukturbibliotek
ITSM	IT-servicemanagement
LTS	Tekniske standarder for sammenkobling
Register	Et regnskabssystem for kvoter udstedt under emissionshandelssystemet, som holder styr på ejerskabet af kvoter, der opbevares på elektroniske konti.
RFC	Ændringsanmodning
SIL	Liste over følsomme oplysninger
SR	Serviceanmodning
Wiki	Websted, hvor brugerne kan udveksle information og viden ved at tilføje eller tilpasse indhold direkte via en webbrowser.

2. INDLEDNING

Aftalen mellem Den Europæiske Union og Det Schweiziske Forbund om sammenkobling af deres systemer for handel med drivhusgasemissioner af 23. november 2017 ("aftalen")

indeholder bestemmelser om gensidig anerkendelse af emissionskvoter, der kan anvendes til at opfylde kravene i Den Europæiske Unions emissionshandelssystem ("EU's emissionshandelssystem") eller Schweiz' emissionshandelssystem ("Schweiz' emissionshandelssystem"). Med henblik på at gennemføre sammenkoblingen af EU's emissionshandelssystem og Schweiz' emissionshandelssystem etableres der en direkte forbindelse mellem EU-registrets EU-transaktionsjournal (EUTL) og det schweiziske registers supplerende transaktionsjournal (SSTL), som vil muliggøre overdragelse af emissionskvoter udstedt i et af emissionshandelssystemerne mellem registrene (aftalens artikel 3, stk. 2). For at gennemføre sammenkoblingen mellem EU's emissionshandelssystem og Schweiz' emissionshandelssystem skal en foreløbig løsning være på plads senest i maj 2020 eller så hurtigt som muligt derefter. Parterne samarbejder om at erstatte den foreløbige løsning med en permanent registerforbindelse hurtigst muligt (bilag II til aftalen).

I henhold til aftalens artikel 3, stk. 6, fastlægger administratoren af det schweiziske register og Unionens centrale administrator fælles driftsprocedurer for tekniske og andre forhold, som er nødvendige for driften af forbindelsen, under hensyntagen til prioriteter i den nationale lovgivning. De fælles driftsprocedurer, der udvikles af administratorerne, træder i kraft, når de er vedtaget ved afgørelse i det fælles udvalg.

De fælles driftsprocedurer, der fremgår af dette dokument, skal vedtages af det fælles udvalg ved afgørelse nr. 1/2020. I overensstemmelse med denne afgørelse anmoder det fælles udvalg administratoren af det schweiziske register og Unionens centrale administrator om at udarbejde yderligere tekniske retningslinjer for at gennemføre forbindelsen og sikre, at disse løbende tilpasses til den tekniske udvikling, og at der stilles nye krav til forbindelsens sikkerhed samt dens virkningsfulde og effektive funktion.

2.1. Anvendelsesområde

Dette dokument repræsenterer den fælles forståelse mellem aftalens parter om oprettelse af det proceduremæssige grundlag for forbindelsen mellem registrene i EU's emissionshandelssystem og Schweiz' emissionshandelssystem. Det skitserer de overordnede proceduremæssige krav med hensyn til driften, men der vil være behov for yderligere tekniske retningslinjer for at gennemføre sammenkoblingen.

For at sikre, at forbindelsen fungerer korrekt, vil det kræve tekniske specifikationer for yderligere at gennemføre sammenkoblingen. I henhold til aftalens artikel 3, stk. 7, er disse spørgsmål beskrevet i de tekniske standarder for sammenkobling, der skal vedtages separat ved afgørelse i det fælles udvalg.

Formålet med de fælles driftsprocedurer er at sikre, at de IT-tjenester, der er knyttet til driften af forbindelsen mellem registrene i EU's emissionshandelssystem og Schweiz' emissionshandelssystem, leveres effektivt, navnlig for at kunne imødekomme serviceanmodninger, løse servicefejl, løse problemer og udføre rutinemæssige operationelle opgaver i overensstemmelse med internationale standarder for IT-servicemanagement.

For den aftalte foreløbige løsning vil der kun være behov for følgende fælles driftsprocedurer, som indgår i dette dokument:

- Hændelsesstyring
- Problemstyring
- Opfyldelse af anmodninger
- Ændringsstyring

- Releasestyring
- Styring af sikkerhedshændelser
- Informationssikkerhedsstyring

Når den permanente registerforbindelse senere tages i anvendelse, skal de fælles driftsprocedurer tilpasses og suppleres, hvor det er nødvendigt.

2.2. Adressater

Målgrupperne for disse fælles driftsprocedurer er EU's og de schweiziske supportteams for registrene.

3. FREMGANGSMÅDE OG STANDARDER

Følgende princip gælder for alle fælles driftsprocedurer:

- EU og CH er enige om at definere de fælles driftsprocedurer på grundlag af ITIL (IT-infrastrukturbibliotek, version 3). Praksis fra denne standard genbruges og tilpasses de særlige behov for den foreløbige løsning.
- Den kommunikation og koordinering, der er nødvendig for behandlingen af de fælles driftsprocedurer mellem de to parter, foregår via servicedeskene under CH's og EU's registre. Opgaverne tildeles altid inden for den ene part.
- Hvis der er uenighed om håndteringen af en fælles driftsprocedure, vil dette blive analyseret og løst mellem de to servicedeske. Hvis det ikke er muligt at nå til enighed, eskaleres problemstillingen til det næste niveau.

Eskaleringsniveauer	**EU**	**CH**
1. niveau	EU's servicedesk	CH's servicedesk
2. niveau	EU's driftsleder	Den ansvarlige for CH's registerapplikation
3. niveau	Det fælles udvalg (som kan uddelegere dette ansvar under hensyntagen til aftalens artikel 12, stk. 5)	
4. niveau	Det fælles udvalg, hvis 3. niveau uddelegeres	

- Hver part kan fastsætte procedurer for driften af sit eget registersystem under hensyntagen til krav og grænseflader i forbindelse med disse fælles driftsprocedurer.
- Der anvendes et ITSM-værktøj (IT-servicemanagement) til støtte for de fælles driftsprocedurer, herunder navnlig hændelsesstyring, problemstyring og opfyldelse af anmodninger, samt kommunikation mellem partere.
- Desuden tillades udveksling af oplysninger via e-mail.
- Begge parter sikrer, at kravene til informationssikkerhed opfyldes i overensstemmelse med håndteringsinstrukserne.

4. HÆNDELSESSTYRING

Formålet med hændelsesstyringsprocessen er at sikre, at IT-tjenester kan vende tilbage til det normale serviceniveau så hurtigt som muligt og med minimale afbrydelser af driften.

Hændelsesstyringen bør også omfatte et register over hændelser med henblik på indberetning og integration med andre processer for at sikre løbende forbedringer.

- Fra et overordnet perspektiv omfatter hændelsesstyring følgende aktiviteter:
- Opdagelse og registrering af hændelser
- Klassificering og indledende support
- Undersøgelse og diagnosticering
- Løsning og genopretning
- Lukning af hændelser

I løbet af en hændelses livscyklus sikrer hændelsesstyringsprocessen den løbende håndtering af ejerskab, overvågning, sporing og kommunikation.

4.1. Opdagelse og registrering af hændelser

En hændelse kan opdages af en supportgruppe, af automatiserede overvågningsværktøjer eller af teknisk personale, der udfører rutinemæssig overvågning.

Når en hændelse opdages, skal den registreres og tildeles en entydig identifikator, der muliggør korrekt sporing og overvågning. Den entydige identifikator for en hændelse er den identifikator, der er tildelt i det fælles sagsstyringssystem i servicedesken for den part (enten EU eller CH), der konstaterede hændelsen, og den skal anvendes i alle meddelelser vedrørende denne hændelse.

For alle hændelser bør kontaktpunktet være servicedesken for den part, der har åbnet sagen.

4.2. Klassificering og indledende support

Klassificeringen af hændelser har til formål at forstå og identificere, hvilket system og/eller hvilke tjenester, der er berørt, og i hvilket omfang. For at være effektiv bør klassificeringen sikre, at hændelsen henvises til den korrekte ressource i første forsøg for at fremskynde løsningen af hændelsen.

I klassificeringsfasen kategoriseres og prioriteres hændelsen afhængigt af, hvilken virkning den har, og hvor meget den haster, så den kan behandles inden for den tidshorisont, der er relevant i forhold til prioriteringen.

Hvis hændelsen har en potentiel indvirkning på følsomme datas fortrolighed eller integritet og/eller på systemets tilgængelighed, skal hændelsen også angives som en sikkerhedshændelse og derefter håndteres i henhold til den proces, der er defineret i kapitlet "Styring af sikkerhedshændelser" i dette dokument.

Om muligt udfører den servicedesk, der åbnede sagen, en indledende diagnose. Her vil servicedesken undersøge, om hændelsen er en kendt fejl. Hvis dette er tilfældet, er det allerede kendt og dokumenteret, hvordan man løser problemet eller laver en workaround.

Hvis servicedesken løser hændelsen, vil den rent faktisk lukke hændelsen på dette tidspunkt, da det primære formål med hændelsesstyring er blevet opfyldt (dvs. hurtig genoptagelse af service for slutbrugeren). Hvis dette ikke er tilfældet, vil servicedesken eskalere hændelsen til et relevant team, der kan undersøge og diagnosticere problemet nærmere.

4.3. Undersøgelse og diagnosticering

Undersøgelse og diagnosticering af hændelser bruges, når en hændelse ikke kan afhjælpes af servicedesken som en del af den indledende diagnose og derfor er blevet eskaleret. Eskalering af hændelser er en del af undersøgelses- og diagnosticeringsprocessen.

En almindelig praksis i undersøgelses- og diagnosticeringsfasen er at forsøge at genskabe hændelsen under kontrollerede forhold. Det er i forbindelse med undersøgelse og diagnosticering af hændelser vigtigt, at man forstår rækkefølgen af de handlinger, der førte til hændelsen.

Eskalering er en anerkendelse af, at en hændelse ikke kan afhjælpes på det nuværende supportniveau og skal overdrages til en supportgruppe på et højere plan eller til den anden part. Eskaleringen kan følge to veje: horisontalt (funktionelt) eller vertikalt (hierarkisk).

Den servicedesk, der registrerede og udløste hændelsen, er ansvarlig for at eskalere hændelsen til den relevante ressource og for at følge den overordnede status for og placering af hændelsen.

Den part, som har fået tildelt hændelsen, er ansvarlig for at sikre, at de ønskede handlinger udføres rettidigt, samt for at give feedback til sin egen parts servicedesk.

4.4. Løsning og genopretning

Løsning af hændelser og genopretning foretages, når man ved, hvad der forårsagede hændelsen. At finde en løsning på en hændelse betyder, at man har fundet en metode til afhjælpning af problemet. Det at gennemføre løsningen er genopretningsfasen.

Når de passende ressourcer har løst problemet, henvises hændelsen tilbage til den relevante servicedesk, som har registreret hændelsen, og det bekræftes over for den, der konstaterede hændelsen, at fejlen er rettet, og at hændelsen kan lukkes. Resultaterne af behandlingen af hændelsen skal registreres til fremtidig brug.

Genopretning kan foretages af IT-supportere eller ved at give slutbrugeren en række instrukser, der skal følges.

4.5. Lukning af hændelser

Lukning er det sidste trin i hændelsesstyringsprocessen lige efter, at der er fundet en løsning.

Tjeklisten over handlinger, der skal foretages i denne fase, omfatter bl.a.:

- Kontrol af den oprindelige kategorisering, der blev tildelt hændelsen
- Korrekt indsamling af alle oplysninger om hændelsen
- Behørig dokumentation af hændelsen og opdatering af videnbasen
- Passende kommunikation til alle interessenter, der er direkte eller indirekte berørt af hændelsen.

En hændelse lukkes formelt, når servicedesken har afsluttet lukningen af hændelsen og meddelt det til den anden part.

Når en hændelse er lukket, genåbnes den ikke. Hvis en hændelse sker igen inden for kort tid, skal den oprindelige hændelse ikke genåbnes, men der skal åbnes en ny hændelse.

Hvis hændelsen behandles af både EU's og CH's servicedesk, ligger ansvaret for lukning af sagen hos den servicedesk, der åbnede sagen.

5. PROBLEMSTYRING

Denne procedure bør følges, hver gang der konstateres et problem, som udløser problemstyringsprocessen. Problemstyring fokuserer på at forbedre kvaliteten og reducere antallet af hændelser, der rettes til servicedesken. Et problem kan være årsagen til en eller flere hændelser. Når en hændelse rapporteres, er formålet med hændelsesstyringen at genoprette tjenesten så hurtigt som muligt, eventuelt gennem en workaround. Når et problem oprettes, er formålet at undersøge den grundlæggende årsag til problemet for at finde frem til en ændring, der vil sikre, at problemet og de dermed forbundne hændelser ikke vil ske igen.

5.1. Problemidentifikation og -løsning

Afhængigt af hvilken part, der har åbnet sagen, vil enten EU's eller CH's servicedesk være kontaktpunkt for spørgsmål vedrørende problemet.

Den entydige identifikator for et problem er den identifikator, der er tildelt af IT-servicemanagement (ITSM). Den skal fremgå af alle meddelelser vedrørende dette problem.

Et problem kan udløses af en hændelse eller kan åbnes på eget initiativ for at løse problemer, der opdages i systemet i en hvilken som helst fase.

5.2. Prioritering af problemer

Problemer kan ligesom hændelser kategoriseres efter alvorsgrad og prioritering for at gøre det nemmere at spore dem, hvor konsekvenserne af de tilknyttede hændelser og deres hyppighed tages i betragtning.

5.3. Undersøgelse og diagnosticering af problemer

Hver part kan gøre opmærksom på et problem, og den pågældende parts servicedesk vil være ansvarlig for at registrere problemet, tildele passende ressourcer og følge den overordnede status.

Den gruppe, som problemet blev eskaleret til, er ansvarlig for at løse problemet hurtigt og kommunikere med servicedesken.

Efter anmodning er begge parter ansvarlige for at sikre, at de anviste foranstaltninger gennemføres, og for at give feedback til sin egen parts servicedesk.

5.4. Løsning

Den gruppe, som problemet er blevet henvist til, er ansvarlig for at løse problemet og give relevante oplysninger til sin egen parts servicedesk.

Resultaterne af behandlingen af problemet skal registreres til fremtidig brug.

5.5. Lukning af problemer

Et problem lukkes formelt, når problemet er blevet løst ved at gennemføre ændringen. Denne fase gennemføres af den servicedesk, der registrerede problemet og informerede den anden parts servicedesk.

6. OPFYLDELSE AF ANMODNINGER

Opfyldelse af anmodninger er håndtering fra start til slut af en anmodning om en ny eller eksisterende tjeneste fra det øjeblik, hvor den registreres og godkendes, og indtil den lukkes. Serviceanmodninger er normalt små, foruddefinerede, repeterbare, hyppige, forhåndsgodkendte og proceduremæssige anmodninger.

De vigtigste trin, der skal følges, er beskrevet nedenfor:

6.1. Oprettelse af anmodning

Oplysningerne vedrørende en serviceanmodning gives til EU's eller CH's servicedesk pr. e-mail, telefon eller via ITSM-værktøjet eller en anden aftalt kommunikationskanal.

6.2. Registrering og analyse af anmodning

For alle serviceanmodninger bør kontaktpunktet være EU's eller CH's servicedesk, afhængigt af hvilken part serviceanmodningen kommer fra. Denne servicedesk vil være ansvarlig for at registrere og analysere serviceanmodningen med den fornødne omhu.

6.3. Godkendelse af anmodning

Medarbejderen i servicedesken for den part, serviceanmodningen kom fra, kontrollerer, om der kræves godkendelse fra den anden part, og indhenter den i så fald. Hvis serviceanmodningen ikke godkendes, ajourfører og lukker servicedesken sagen.

6.4. Opfyldelse af anmodninger

I dette trin sikres effektiv og virkningsfuld behandling af serviceanmodningerne. Der skal skelnes mellem følgende tilfælde:

- Opfyldelsen af serviceanmodningen berører kun den ene part. I dette tilfælde udsteder denne part arbejdsordrerne og koordinerer udførelsen.
- Gennemførelsen af serviceanmodningen berører både EU og CH. I dette tilfælde udsteder begge servicedeske arbejdsordrerne inden for deres ansvarsområde. Behandlingen af serviceanmodningen koordineres mellem de to servicedeske. Det overordnede ansvar ligger hos den servicedesk, som modtog og igangsatte serviceanmodningen.

Når serviceanmodningen er blevet løst, skal den have status som "løst" ("Resolved").

6.5. Eskalering af anmodning

Servicedesken kan om nødvendigt eskalere den udestående serviceanmodning til den relevante ressource (tredjepart).

Eskalering sker til de respektive tredjeparter, dvs. at EU's servicedesk skal gå gennem CH's servicedesk for at eskalere til en tredjepart i CH og omvendt.

Den tredjepart, som serviceanmodningen blev eskaleret til, er ansvarlig for at behandle serviceanmodningen rettidigt og kommunikere med den servicedesk, der har eskaleret anmodningen.

Den servicedesk, der registrerede serviceanmodningen, er ansvarlig for at følge den overordnede status og placering af en serviceanmodning.

6.6. Gennemgang af opfyldelsen af anmodning

Den ansvarlige servicedesk fremsender serviceanmodningen til en endelig kvalitetskontrol, inden den lukkes. Formålet er at sikre, at serviceanmodningen faktisk behandles, og at alle de oplysninger, der er nødvendige for at beskrive anmodningens livscyklus, leveres med tilstrækkelige detaljer. Derudover skal resultaterne af behandlingen af anmodningen registreres til fremtidig brug.

6.7. Lukning af anmodning

Hvis de deltagende parter er enige om, at serviceanmodningen er blevet opfyldt, og rekvirenten mener, at sagen er løst, er den næste status, der skal angives, "lukket" ("Closed").

En serviceanmodning lukkes formelt, når den servicedesk, der registrerede serviceanmodningen, har gennemført lukningen og underrettet den anden parts servicedesk.

7. ÆNDRINGSSTYRING

Formålet er at sikre, at der anvendes standardiserede metoder og procedurer til effektiv og hurtig håndtering af alle ændringer i kontrolinfrastrukturen for at minimere antallet og virkningen af relaterede hændelser ved service. Ændringer i IT-infrastrukturen kan ske som reaktion på problemer eller krav udefra, f.eks. lovgivningsmæssige ændringer, eller som et proaktivt forsøg på at opnå større effektivitet eller virkningsfuldhed eller for at kunne gennemføre eller afspejle forretningsmæssige initiativer.

Ændringsstyringsprocessen omfatter forskellige trin, der omfatter alle detaljer af en ændringsanmodning med henblik på fremtidig sporing. Disse processer sikrer, at ændringen valideres og testes, før den gennemføres. Gennemførelsen af ændringen sker i forbindelse med releasestyringen.

7.1. Ændringsanmodning

En ændringsanmodning indgives til ændringsstyringsteamet med henblik på validering og godkendelse. For alle ændringsanmodninger bør kontaktpunktet være EU's eller CH's servicedesk, afhængigt af hvilken part der har fremsat anmodningen. Denne servicedesk vil være ansvarlig for at registrere og analysere anmodningen med den fornødne omhu.

Ændringsanmodninger kan stamme fra:

- En hændelse, der medfører en ændring
- Et eksisterende problem, der medfører en ændring
- En slutbruger, der anmoder om en ny ændring
- Ændring som følge af løbende vedligeholdelse
- Lovgivningsmæssig ændring.

7.2. Evaluering og planlægning af ændring

På dette trin sker vurderingen og planlægningen af ændringer. Det omfatter prioritering og planlægning af aktiviteter med henblik på at minimere risici og virkninger.

Hvis gennemførelsen af ændringsanmodningen berører både EU og CH, verificerer den part, der har registreret ændringsanmodningen, evalueringen og planlægningen med den anden part.

7.3. Godkendelse af ændring

Alle registrerede ændringsanmodninger skal godkendes af det relevante eskaleringsniveau.

7.4. Gennemførelse af ændring

Gennemførelsen af ændringer sker i forbindelse med releasestyringen. Parternes teams følger deres egne processer, der omfatter planlægning og test. Ændringen vurderes derefter, når den er gennemført. For at sikre, at alt er forløbet efter planen, gennemgås den eksisterende ændringsstyringsproces hele tiden og ajourføres, hvis det er nødvendigt.

8. RELEASESTYRING

En release er en eller flere ændringer i en IT-tjeneste, der er samlet i en releaseplan, og som skal godkendes, forberedes, udvikles, testes og anvendes sammen. En enkelt release kan f.eks. være en fejlrettelse, en ændring af hardware eller andre komponenter, ændringer i software,

opgradering af applikationsversioner, ændringer af dokumentation og/eller processer. Indholdet af hver enkelt release styres, testes og anvendes som én enkelt enhed.

Releasestyring har til formål at planlægge, udvikle, teste og validere og levere kapacitet til at udføre den ønskede service, som vil opfylde de berørte parters behov samt de tilsigtede mål. Acceptkriterier for alle serviceændringer vil blive fastlagt og dokumenteret i forbindelse med designkoordinering og leveres til de relevante teams.

Releasen vil typisk bestå af en række problemrettelser og forbedringer af en service. Den indeholder det nye eller ændrede software, der kræves, og det nye eller ændrede hardware, der er nødvendigt for at gennemføre de godkendte ændringer.

8.1. Planlægning af release

I det første trin i processen fordeles godkendte ændringer på releasepakker, og releasens omfang og indhold bestemmes. På grundlag af disse oplysninger vil der i planlægningen af releasen blive udarbejdet en tidsplan for udvikling, test og ibrugtagning af releasen.

Planlægningen bør omfatte:

- Releasens omfang og indhold
- Risikovurdering og risikoprofil for releasen
- Kunder/brugere, der berøres af releasen
- Det team, der er ansvarligt for releasen
- Strategi for levering og ibrugtagning
- Ressourcer til release og ibrugtagning.

Begge parter informerer hinanden om deres vinduer for planlægning og vedligeholdelse af releases. Hvis en release berører både EU og CH, koordinerer de planlægningen og definerer et fælles vindue for vedligeholdelse.

8.2. Udvikling og test af releasepakke

I udviklings- og testfasen fastlægges det, hvordan releasen eller pakken skal behandles, og hvordan de kontrollerede miljøer, inden produktionen ændres, kan opretholdes, samt test af alle ændringer i alle miljøer.

Hvis en release berører både EU og CH, koordinerer de leveringsplaner og test. Dette omfatter følgende aspekter:

- Hvordan og hvornår de enkelte dele af en release og servicekomponenter vil blive leveret
- Hvad produktionstiden normalt er, og hvad der sker i tilfælde af en forsinkelse
- Hvordan man kan følge med i, hvordan leveringen skrider frem, og få det bekræftet
- Parametre for overvågning og bestemmelse af, om ibrugtagningen af releasen sker korrekt
- Fælles testcases for relevante funktioner og ændringer.

Ved afslutningen af denne delproces er alle de krævede releasekomponenter klar til ibrugtagning.

8.3. Forberedelse af ibrugtagning

Forberedelsesprocessen sikrer, at kommunikationsplanerne defineres korrekt, at meddelelser er klar til at blive sendt til alle berørte interessenter og slutbrugere, og at releasen integreres i ændringsstyringsprocessen for at sikre, at alle ændringer udføres på en kontrolleret måde og godkendes i de krævede fora.

Hvis en release berører både EU og CH, skal de koordinere følgende aktiviteter:

- Registrering af ændringsanmodning og forberedelse af ibrugtagning i produktionsmiljø
- Udarbejdelse af en gennemførelsesplan
- Rollback-metode, så det er muligt at vende tilbage til den tidligere tilstand, hvis ibrugtagning af releasen mislykkes
- Meddelelser til alle de nødvendige parter
- Krav om godkendelse af gennemførelsen af releasen fra det relevante eskaleringsniveau.

8.4. Rollback af releasen

Hvis der har været fejl i ibrugtagningen, eller det viste sig i testen, at ibrugtagningen ikke lykkedes, eller ikke opfyldte de aftalte godkendelses-/kvalitetskriterier, vil begge parters teams skulle rulle tilbage til den tidligere tilstand. Alle berørte interessenter skal informeres, herunder berørte og tilsigtede slutbrugere. Mens der afventes godkendelse, kan processen genoptages på ethvert af de foregående trin.

8.5. Gennemgang og lukning af releasen

Ved gennemgangen af en release bør følgende aktiviteter være omfattet:

- Indhente feedback om kundens, brugerens og de pågældende medarbejderes tilfredshed med udsendelsen (indsamle feedback og overveje løbende at forbedre servicen)
- Gennemgå alle kvalitetskriterier, der ikke er opfyldt
- Kontrollere, at eventuelle handlinger, nødvendige rettelser og ændringer er fuldstændige
- Sikre, at der ikke er nogen problemer med hensyn til funktioner, ressourcer, kapacitet eller resultater efter idriftsættelse af releasen
- Kontrollere, at eventuelle problemer, kendte fejl og workarounds er dokumenteret og accepteret af kunden, slutbrugerne, driftssupport og andre berørte parter
- Overvåge hændelser og problemer som følge af idriftsættelsen (yde tidlig support til driftsteams, hvis releasen har medført en forøgelse af arbejdsmængden)
- Ajourføre supportdokumentationen (dvs. tekniske dokumenter)
- Formelt overdrage releasen til driften
- Dokumentere de indhøstede erfaringer
- Indhente en oversigt over releasen fra de teams, der har gennemført den

- Formelt lukke releasen efter kontrol af ændringsanmodninger.

9. STYRING AF SIKKERHEDSHÆNDELSER

Styring af sikkerhedshændelser er en proces for håndtering af sikkerhedshændelser med henblik på at muliggøre kommunikation om hændelser til potentielt berørte interessenter, evaluering og prioritering af hændelser samt håndtering af hændelser med henblik på at løse eventuelle faktiske, formodede eller potentielle brud på fortroligheden, tilgængeligheden eller integriteten af følsomme informationsaktiver.

9.1. Kategorisering af informationssikkerhedshændelser

Alle hændelser, der påvirker forbindelsen mellem EU-registret og det schweiziske register, analyseres for at fastslå eventuelle brud på fortroligheden, integriteten eller tilgængeligheden af følsomme oplysninger, der er registreret på listen over følsomme oplysninger (SIL).

Hvis dette er tilfældet, skal hændelsen kategoriseres som en informationssikkerhedshændelse, straks registreres i ITSM-værktøjet og behandles som sådan.

9.2. Håndtering af informationssikkerhedshændelser

Sikkerhedshændelser placeres under det 3. eskaleringsniveau, og løsningen af hændelser vil blive varetaget af et særligt team til styring af hændelser (Incident Management Team (IMT)).

Teamet er ansvarligt for:

- Den første analyse, kategorisering og vurdering af hændelsens alvor
- Koordinering af foranstaltninger mellem alle interessenter, herunder den fulde dokumentation af analysen af hændelsen, de beslutninger, der træffes for at håndtere hændelsen, og de mulige identificerede svagheder
- Afhængigt af, hvor alvorlig sikkerhedshændelsen er, eskalering af den til det rette niveau til orientering og/eller afgørelse.

I informationsstyringsprocessen klassificeres alle oplysninger vedrørende hændelser på det højeste følsomhedsniveau, men under ingen omstændigheder lavere end ETS SENSITIVE.

I forbindelse med en igangværende undersøgelse og/eller en svaghed, der kan udnyttes, og indtil den afhjælpes, klassificeres oplysningerne som ETS CRITICAL.

9.3. Identifikation af sikkerhedshændelser

Afhængigt af typen af sikkerhedshændelse fastsætter den informationssikkerhedsansvarlige de relevante organisationer, der skal inddrages, og som skal indgå i IMT.

9.4. Analyse af sikkerhedshændelser

IMT samarbejder med alle involverede organisationer og de relevante medlemmer af deres teams, alt efter hvad der er relevant, for at gennemgå hændelsen. Under analysen afdækkes det, i hvilket omfang et aktivs fortrolighed, integritet eller tilgængelighed er berørt, og konsekvenserne for alle berørte organisationer vurderes. Dernæst defineres indledende og opfølgende foranstaltninger til at afhjælpe hændelsen og styre dens virkninger, herunder de ressourcemæssige konsekvenser af disse foranstaltninger.

9.5. Vurdering, eskalering og rapportering af sikkerhedshændelser

IMT vurderer, hvor alvorlig en ny sikkerhedshændelse er, efter at den er blevet konstateret, og begynder omgående at træffe de nødvendige foranstaltninger afhængigt af hændelsens alvor.

9.6. Rapportering om håndteringen af sikkerhedshændelsen

IMT udarbejder en rapport om håndteringen af sikkerhedshændelsen med oplysninger om, hvordan den er blevet inddæmmet, og den efterfølgende genopretning. Rapporten sendes til det 3. eskaleringsniveau pr. sikker e-mail eller andre gensidigt accepterede sikre kommunikationsmidler.

Den ansvarlige part gennemgår resultaterne af inddæmningen og genopretningen og:

- Tilkobler registret igen, hvis det er blevet afkoblet
- Oplyser registerteams om hændelsen
- Lukker hændelsen.

IMT bør — på en sikker måde — medtage relevante oplysninger i rapporten om sikkerhedshændelsen for at sikre konsekvent registrering og kommunikation og gøre det muligt at træffe hurtige og hensigtsmæssige foranstaltninger til at inddæmme hændelsen. Efter færdiggørelsen forelægger IMT den endelige rapport om sikkerhedshændelsen inden for rimelig tid.

9.7. Overvågning, kapacitetsopbygning og løbende forbedringer

IMT leverer rapporter om alle sikkerhedshændelser til det 3. eskaleringsniveau. Rapporterne vil blive anvendt af dette eskaleringsniveau til at fastslå følgende:

- Svage punkter i sikkerhedskontrollen og/eller driften, der skal styrkes
- Eventuelle behov for at forbedre denne procedure for at forbedre effektiviteten af reaktionen på hændelser

- Uddannelses- og kapacitetsopbygningsmuligheder for yderligere at styrke registersystemers modstandsdygtighed over for informationssikkerhedshændelser, mindske risikoen for fremtidige hændelser og minimere deres virkning.

10. INFORMATIONSSIKKERHEDSSTYRING

Informationssikkerhedsstyring har til formål at sikre fortrolighed, integritet og tilgængelighed af en organisations fortrolige oplysninger, data og IT-tjenester. Ud over de tekniske komponenter, herunder design og test (se de tekniske standarder for sammenkobling), er følgende fælles driftsprocedurer nødvendige for at opfylde sikkerhedskravene til den foreløbige løsning.

10.1. Identifikation af følsomme oplysninger

Oplysningernes følsomhed vurderes ved at bestemme virkningerne for virksomheden (f.eks. økonomiske tab, skade på image, overtrædelse af lovgivningen osv.) af et brud på sikkerheden i forbindelse med disse oplysninger.

De følsomme informationsaktiver skal identificeres på grundlag af deres indvirkning på forbindelsen.

Disses følsomhed vurderes i henhold til den følsomhedsskala, der gælder for denne forbindelse, og som er beskrevet i afsnittet "Håndtering af informationssikkerhedshændelser" i dette dokument.

10.2. Følsomhedsniveauer for informationsaktiver

Når et informationsaktiv er identificeret, klassificeres det efter følgende regler:

- Ved mindst ét højt niveau med hensyn til fortrolighed, integritet eller tilgængelighed klassificeres aktivet som ETS CRITICAL.
- Ved mindst ét mellemhøjt niveau med hensyn til fortrolighed, integritet eller tilgængelighed klassificeres aktivet som ETS SENSITIVE.
- Ved kun lave niveauer med hensyn til fortrolighed, integritet eller tilgængelighed klassificeres aktivet som ETS LIMITED.

10.3. Tildeling af ejer af informationsaktiver

Alle informationsaktiver bør få tildelt en ejer. Informationsaktiver i ETS, som tilhører eller er forbundet med forbindelsen mellem EUTL og SSTL, bør medtages i en fælles liste over aktiver, der føres af begge parter. Informationsaktiver i ETS, som er uden for forbindelsen mellem EUTL og SSTL, bør medtages i en fælles liste over aktiver, der føres af den respektive part.

Parterne skal aftale, hvem der ejer hvert enkelt informationsaktiv, der tilhører eller er forbundet med forbindelsen mellem EUTL og SSTL. Ejeren af et informationsaktiv er ansvarlig for at vurdere dets følsomhed.

Ejeren bør have de beføjelser, der passer til værdien af de tildelte aktiver. Ejerens ansvar for aktivet/aktiverne og forpligtelsen til at opretholde den nødvendige fortrolighed, integritet og tilgængelighed bør aftales og formaliseres.

10.4. Registrering af følsomme oplysninger

Alle følsomme oplysninger registreres i listen over følsomme oplysninger (SIL).

Hvis det er relevant, skal der tages højde for, at flere følsomme oplysninger tilsammen kan have en større virkning end virkningen af én enkelt oplysning, og dette skal registreres i listen (f.eks. oplysninger lagret i systemdatabasen).

Listen er ikke statisk. Trusler, sårbarheder, sandsynlighed eller konsekvenser af sikkerhedshændelser i forbindelse med aktiverne kan ændre sig uden forvarsel, og der kan indføres nye aktiver i driften af registersystemerne.

Derfor skal listen regelmæssigt tages op til revision, og nye oplysninger, der kategoriseres som følsomme, skal straks registreres i listen.

Listen skal mindst indeholde følgende oplysninger:

- Beskrivelse af oplysningerne
- Oplysningens ejer
- Følsomhedsniveau
- Angivelse af, om oplysningerne omfatter personoplysninger
- Eventuelle yderligere oplysninger.

10.5. Håndtering af følsomme oplysninger

Når følsomme oplysninger behandles uden for forbindelsen mellem EU-registret og det schweiziske register, skal de behandles i overensstemmelse med håndteringsinstrukserne.

Følsomme oplysninger, der behandles via en forbindelse mellem EU-registret og det schweiziske register, behandles i overensstemmelse med parternes sikkerhedskrav.

10.6. Adgangsstyring

Formålet med adgangsstyring er at give autoriserede brugere ret til at benytte en service og samtidig forhindre adgang for uautoriserede brugere. Adgangsstyring omtales undertiden også som "rettighedsstyring" eller "identitetsstyring".

I forbindelse med den foreløbige løsning og anvendelsen af den har begge parter behov for adgang til følgende komponenter:

- Wiki: Et samarbejdsmiljø for udveksling af fælles oplysninger som f.eks. planlægning af releases
- ITSM-værktøj til styring af hændelser og problemer (se kapitlet "Fremgangsmåde og standarder")
- System til udveksling af meddelelser: Hver part skal have et sikkert system til udveksling af meddelelser, der indeholder transaktionsdata.

Administratoren af det schweiziske register og Unionens centrale administrator sørger for, at adgangsrettighederne er ajourført, og fungerer som kontaktpunkter for parternes adgangsstyringsaktiviteter. Anmodninger om adgang behandles i henhold til procedurerne for opfyldelse af anmodninger.

10.7. Certifikat-/nøglestyring

Hver part er ansvarlig for sin egen certifikat-/nøglestyring (generering, registrering, lagring, installation, anvendelse, fornyelse, tilbagekaldelse, sikkerhedskopiering og tilbagelevering af certifikater/nøgler). Som beskrevet i de tekniske standarder for sammenkobling må der kun bruges digitale certifikater udstedt af en certificeringsmyndighed, som begge parter har tillid til. Håndtering og opbevaring af certifikater/nøgler skal følge de bestemmelser, der er fastsat i håndteringsinstrukserne.

Tilbagekaldelse og/eller fornyelse af certifikater og nøgler koordineres af begge parter. Dette sker i overensstemmelse med procedurerne for opfyldelse af anmodninger.

Administratoren af det schweiziske register og Unionens centrale administrator udveksler certifikater/nøgler via sikre kommunikationsmidler i overensstemmelse med de bestemmelser, der er fastlagt i håndteringsinstrukserne.

Enhver verifikation af certifikater/nøgler på en hvilken som helst måde mellem parterne sker via en anden kanal.