Rada
Evropské unie

Brusel 6. října 2020
(OR. en)

10831/20

Interinstitucionální spis:
2020/0123 (NLE)

ENV 516
CLIMA 187
ENER 290
IND 135
COMPET 405
MI 333
ECOFIN 803
TRANS 397
AELE 52
CH 24

PRÁVNÍ PŘEDPISY A JINÉ AKTY

Předmět:	Návrh ROZHODNUTÍ SMÍŠENÉHO VÝBORU ZŘÍZENÉHO DOHODOU MEZI EVROPSKOU UNIÍ A ŠVÝCARSKOU KONFEDERACÍ O PROPOJENÍ JEJICH SYSTÉMŮ OBCHODOVÁNÍ S EMISEMI SKLENÍKOVÝCH PLYNŮ o přijetí společných provozních postupů

NÁVRH

ROZHODNUTÍ SMÍŠENÉHO VÝBORU
ZŘÍZENÉHO DOHODOU MEZI EVROPSKOU UNIÍ
A ŠVÝCARSKOU KONFEDERACÍ O PROPOJENÍ JEJICH SYSTÉMŮ OBCHODOVÁNÍ
S EMISEMI SKLENÍKOVÝCH PLYNŮ č. 1/2020

ze dne ...

o přijetí společných provozních postupů

SMÍŠENÝ VÝBOR,

s ohledem na Dohodu mezi Evropskou unií a Švýcarskou konfederací o propojení jejich systémů obchodování s emisemi skleníkových plynů[1] (dále jen „dohoda“), a zejména na čl. 3 odst. 6 této dohody,

[1] Úř. věst. L 322, 7.12.2017, s. 3.

vzhledem k těmto důvodům:

(1) Rozhodnutím smíšeného výboru č. 2/2019 ze dne 5. prosince 2019[1] byly změněny přílohy I a II dohody, čímž byly splněny podmínky pro propojení stanovené v dohodě.

(2) Po přijetí rozhodnutí smíšeného výboru č. 2/2019 a podle čl. 21 odst. 3 dohody si strany vyměnily své listiny o ratifikaci nebo schválení, neboť došly k závěru, že jsou splněny veškeré podmínky pro propojení stanovené v dohodě.

(3) V souladu s čl. 21 odst. 4 dohody vstoupila dohoda v platnost dne 1. ledna 2020.

[1] Rozhodnutí č. 2/2019 smíšeného výboru zřízeného podle Dohody mezi Evropskou unií a Švýcarskou konfederací o propojení jejich systémů obchodování s emisemi skleníkových plynů ze dne 5. prosince 2019, kterým se mění přílohy I a II Dohody mezi Evropskou unií a Švýcarskou konfederací o propojení jejich systémů obchodování s emisemi skleníkových plynů (Úř. věst. L 314, 29.9.2020, s. 68).

(4) Podle čl. 3 odst. 6 dohody by správce švýcarského registru a ústřední správce Unie měli určit společné provozní postupy týkající se technických nebo jiných záležitostí nezbytných pro fungování propojení mezi protokolem transakcí Evropské unie (EUTL) registru Unie a švýcarským doplňkovým protokolem transakcí (SSTL) švýcarského registru a zohlednit priority vnitrostátních právních předpisů. Společné provozní postupy by měly nabýt účinnosti poté, co byly přijaty rozhodnutím smíšeného výboru.

(5) V souladu s čl. 13 odst. 1 dohody by se smíšený výbor měl dohodnout na technických pokynech k zajištění řádného provádění dohody, včetně technických či jiných záležitostí nezbytných pro fungování propojení, přičemž zohlední priority vnitrostátních právních předpisů. Technické pokyny mohou být vypracovány pracovní skupinou zřízenou podle čl. 12 odst. 5 dohody. Pracovní skupina by měla zahrnovat alespoň správce švýcarského registru a ústředního správce Unie a měla by smíšenému výboru pomáhat ve výkonu jeho funkcí podle článku 13 dohody.

(6) S ohledem na technickou povahu pokynů a nutnost přizpůsobit je dalšímu vývoji by technické pokyny vypracované správcem švýcarského registru a ústředním správcem Unie měly být předloženy smíšenému výboru pro informaci, nebo v příslušných případech ke schválení,

PŘIJAL TOTO ROZHODNUTÍ:

Článek 1

Přijímají se společné provozní postupy, které tvoří přílohu tohoto rozhodnutí.

Článek 2

Zřizuje se pracovní skupina podle čl. 12 odst. 5 dohody. Pracovní skupina pomáhá smíšenému výboru při zajišťování řádného provádění dohody včetně vypracování technických pokynů pro zavedení společných provozních postupů.

Pracovní skupina zahrnuje alespoň správce švýcarského registru a ústředního správce Unie.

Článek 3

Toto rozhodnutí vstupuje v platnost dnem přijetí.

V Bruselu dne … 2020.

Za smíšený výbor

tajemník pro Evropskou unii *předseda* *tajemník pro Švýcarsko*

PŘÍLOHA

SPOLEČNÉ PROVOZNÍ POSTUPY
PODLE ČL. 3 ODST. 6 DOHODY MEZI EVROPSKOU UNIÍ
A ŠVÝCARSKOU KONFEDERACÍ O PROPOJENÍ JEJICH SYSTÉMŮ
OBCHODOVÁNÍ S EMISEMI SKLENÍKOVÝCH PLYNŮ

Postupy pro prozatímní řešení -

1. Glosář

Tabulka 1-1 Zkratky a definice

Zkratka/výraz	Definice
Certifikační orgán	Subjekt, který vydává digitální certifikáty.
CH	Švýcarská konfederace
ETS	Systém obchodování s emisemi
EU	Evropská unie
IMT	Tým pro řízení incidentů
Informační položka	Informace, která je cenná pro společnost nebo organizaci.

Zkratka/výraz	Definice
IT	Informační technologie
ITIL	Knihovna infrastruktury informačních technologií (Information Technology Infrastructure Library)
ITSM	Řízení IT služeb
LTS	Technické normy pro propojování
Registr	Účetní systém pro povolenky vydané v rámci systému obchodování s emisemi, který sleduje vlastnictví povolenek vedených na elektronických účtech.
RFC	Žádost o změnu
SIL	Seznam citlivých informací
SR	Žádost o službu
Wiki	Webová stránka, která umožňuje uživatelům vyměňovat si informace a znalosti přidáváním nebo úpravou obsahu přímo přes webový prohlížeč.

2. Úvod

Dohoda mezi Evropskou unií a Švýcarskou konfederací o propojení jejich systémů obchodování s emisemi skleníkových plynů ze dne 23. listopadu 2017 (dále jen „dohoda“) stanoví vzájemné uznávání povolenek na emise, které mohou být použity k zajištění souladu v rámci systému obchodování s emisemi Evropské unie („unijní ETS“) nebo v rámci systému obchodování s emisemi Švýcarska („švýcarský ETS“). Za účelem operacionalizace propojení mezi unijním ETS a švýcarským ETS se zřídí přímé propojení mezi protokolem transakcí Evropské unie (EUTL) registru Unie a švýcarským doplňkovým protokolem transakcí (SSTL) švýcarského registru, které umožní převádět mezi registry povolenky na emise vydané v rámci obou ETS (čl. 3 odst. 2 dohody). Aby bylo možné zprovoznit propojení mezi unijním ETS a švýcarským ETS, zavede se do května 2020, nebo co nejdříve po tomto datu, prozatímní řešení. Strany spolupracují na tom, aby prozatímní řešení co nejdříve nahradily trvalým propojením registrů (příloha II dohody).

Podle čl. 3 odst. 6 dohody správce švýcarského registru a ústřední správce Unie určí společné provozní postupy týkající se technických nebo jiných záležitostí nezbytných pro fungování propojení a zohlední priority vnitrostátních právních předpisů. Společné provozní postupy vypracované správci nabývají účinnosti poté, co byly přijaty rozhodnutím smíšeného výboru.

Společné provozní postupy zaznamenané v tomto dokumentu přijme smíšený výbor svým rozhodnutím č. 1/2020. V souladu s tímto rozhodnutím požádá smíšený výbor správce švýcarského registru a ústředního správce Unie, aby vypracovali další technické pokyny k operacionalizaci propojení a aby zajistili jejich průběžné přizpůsobování technickému pokroku a novým požadavkům týkajícím se bezpečnosti a zabezpečení propojení a jeho účelného a efektivního fungování.

2.1. Oblast působnosti

Tento dokument vyjadřuje společné ujednání stran dohody, pokud jde o vytvoření procedurálních základů propojení mezi registry unijního ETS a švýcarského ETS. Přestože nastiňuje celkové procedurální náležitosti z hlediska fungování, budou nutné i některé další technické pokyny, aby bylo možné propojení zprovoznit.

Ke správnému fungování bude propojení vyžadovat technické specifikace, aby bylo možné propojení dále provozovat. Podle čl. 3 odst. 7 dohody jsou tyto záležitosti podrobně popsány v dokumentu obsahujícím technické normy pro propojování, který má být přijat samostatným rozhodnutím smíšeného výboru.

Cílem společných provozních postupů je zajistit, aby byly IT služby související s provozem propojení mezi registry unijního ETS a švýcarského ETS poskytovány účelně a efektivně, zejména při plnění žádostí o službu, řešení selhání služby, odstraňování problémů, jakož i při provádění rutinních provozních úkolů podle mezinárodních standardů pro řízení IT služeb.

Pro dohodnuté prozatímní řešení budou potřebné pouze tyto společné provozní postupy, které jsou součástí tohoto dokumentu:

– řízení incidentů;

– řízení problémů;

– plnění žádostí;

– řízení změn;

– řízení vydání;

– řízení bezpečnostních incidentů;

– řízení bezpečnosti informací.

Při pozdějším zprovoznění trvalého propojení registrů musí být společné provozní postupy v případě potřeby upraveny a doplněny.

2.2. Určení

Tyto společné provozní postupy jsou určeny pro podpůrné týmy unijního a švýcarského registru.

3. Přístup a standardy

Pro všechny společné provozní postupy platí tato zásada:

– EU a Švýcarsko se dohodly na definici společných provozních postupů podle ITIL (Knihovna infrastruktury informačních technologií, verze 3). Použity jsou postupy podle tohoto standardu, které jsou upraveny podle konkrétních potřeb souvisejících s prozatímním řešením.

– Komunikace a koordinace potřebná pro zpracování společných provozních postupů mezi stranami probíhá přes centra podpory registrů Švýcarska a EU. Úkoly se přidělují vždy v rámci jedné strany.

– Jestliže nedojde k dohodě, jak mají být společné provozní postupy zpracovány, bude to analyzováno a řešeno oběma centry podpory. Není-li možné dosáhnout dohody, nalezení společného řešení bude předáno na vyšší úroveň.

Úrovně eskalace	EU	Švýcarsko
1. úroveň	Unijní centrum podpory	Švýcarské centrum podpory
2. úroveň	Unijní provozní manažer	Švýcarský manažer pro aplikace registru
3. úroveň	Smíšený výbor (který může tuto odpovědnost delegovat podle čl. 12 odst. 5 dohody)	
4. úroveň	Smíšený výbor, pokud je delegováno na 3. úrovni	

– Každá strana může určit postupy pro provoz svého vlastního registračního systému, přičemž zohlední požadavky a rozhraní související s těmito společnými provozními postupy.

– Na podporu společných provozních postupů se používá nástroj pro řízení IT služeb (ITSM), zejména řízení incidentů, řízení problémů a plnění žádostí, a komunikace mezi oběma stranami.

– Kromě toho je přípustná výměna informací prostřednictvím elektronické pošty.

– Obě strany

– zajistí, aby byly splněny požadavky na bezpečnost informací v souladu s pokyny pro nakládání s informacemi.

4. Řízení incidentů

Cílem procesu řízení incidentů je vrátit IT služby po incidentu na běžnou úroveň služeb co možná nejrychleji a s minimálním narušením provozu.

Při řízení incidentů je také třeba vést záznam o incidentech pro účely vykazování a tento proces by měl být integrován s jinými procesy, aby bylo možné jej průběžně zdokonalovat.

– Z celkového pohledu zahrnuje řízení incidentů tyto činnosti:

– zjištění a záznam incidentu;

– klasifikace a počáteční podpora;

– šetření a diagnostika;

– vyřešení a obnova;

– uzavření incidentu.

Po celou dobu trvání incidentu je proces řízení incidentu odpovědný za trvalé zapojení odpovědných osob, monitorování, sledování a komunikaci.

4.1. Zjištění a záznam incidentu

Incident může zjistit podpůrná skupina, automatizované monitorovací nástroje nebo techničtí pracovníci vykonávající rutinní dozor.

Incident musí být po zjištění zaznamenán a musí mu být přiřazen jedinečný identifikátor umožňující jeho správné sledování a monitorování. Jedinečný identifikátor incidentu je identifikátor, který mu ve společném tiketovacím systému přiřadí centrum podpory té strany (EU nebo Švýcarsko), která incident zjistila, přičemž tento identifikátor musí být použit při každé komunikaci související s tímto incidentem.

U všech incidentů by kontaktním místem mělo být centrum podpory té strany, která tiket zaregistrovala.

4.2. Klasifikace a počáteční podpora

Cílem klasifikace incidentu je zjistit a určit, jaký systém a/nebo služba jsou postiženy incidentem a v jakém rozsahu. Aby byla klasifikace účinná, měla by vysledovat incident ke správnému zdroji hned napoprvé, aby se urychlilo jeho vyřešení.

Ve fázi klasifikace je třeba incident kategorizovat a určit jeho prioritu podle jeho dopadu a naléhavosti, aby mohl být řešen podle příslušného časového rámce pro danou prioritu.

Pokud má incident potenciální dopad na důvěrnost nebo integritu citlivých údajů a/nebo má dopad na dostupnost systému, je třeba tento incident označit také za bezpečnostní incident a poté jej řídit podle procesu uvedeného v kapitole „Řízení bezpečnostních incidentů“ tohoto dokumentu.

Centrum podpory, které tiket zaregistrovalo, by mělo pokud možno provést první diagnostiku. Centrum podpory přitom zjistí, zda je incident známou chybou. V kladném případě je již způsob řešení nebo dočasná oprava známá a zadokumentovaná.

Jestliže centrum podpory incident úspěšně vyřeší, potom jej v tomto okamžiku uzavře, neboť primární účel řízení incidentů byl splněn (a to rychlá obnova služby pro konečného uživatele). V opačném případě centrum podpory předá incident na vyšší úroveň příslušné řešitelské skupině k dalšímu šetření a diagnostice.

4.3. Šetření a diagnostika

Šetření a diagnostika incidentů se používá, když incident nedokáže vyřešit centrum podpory v rámci první diagnostiky, a proto jej předá na vyšší úroveň. Eskalace incidentů je součástí procesu šetření a diagnostiky.

Běžnou praxí ve fázi šetření a diagnostiky je pokus o zopakování incidentu za řízených podmínek. Při šetření a diagnostice incidentů je důležité zjistit správné pořadí událostí, které k incidentu vedly.

Eskalace je uznání toho, že incident nemůže být vyřešen na aktuální úrovni podpory a musí být předán podpůrné skupině vyšší úrovně nebo druhé straně. Eskalace může probíhat dvěma způsoby: horizontálně (funkčně) nebo vertikálně (hierarchicky).

Centrum podpory, které incident zaznamenalo a spustilo jeho řešení, je odpovědné za předání incidentu příslušnému zdroji a za sledování celkového stavu a přiřazení incidentu.

Strana, jíž byl incident přiřazen, je odpovědná za zajištění včasného provedení požadovaných opatření a za poskytnutí zpětné vazby svému vlastnímu centru podpory.

4.4. Vyřešení a obnova

Jakmile je incident zcela prozkoumán, dochází k jeho vyřešení a obnově. Nalezení řešení incidentu znamená, že byl zjištěn způsob nápravy problému. Provedení řešení je obnovovací fáze.

Jakmile příslušné zdroje selhání služby vyřeší, je incident předán zpět do příslušného centra podpory, které jej zaregistrovalo, a toto centrum podpory u iniciátora incidentu potvrdí, že chyba byla opravena a že incident lze uzavřít. Zjištění ze zpracování incidentu je třeba zaznamenat pro budoucí použití.

Obnovu mohou provést pracovníci IT podpory nebo je možné předat konečnému uživateli pokyny, jak má postupovat.

4.5. Uzavření incidentu

Uzavření je posledním krokem v procesu řízení incidentů a probíhá krátce po vyřešení incidentu.

Ze seznamu činností, které musí být v průběhu fáze uzavření incidentu provedeny, je třeba zdůraznit:

– ověření počáteční kategorizace, která byla incidentu přiřazena;

– správné zachycení všech informací souvisejících s incidentem;

– řádná dokumentace incidentu a aktualizace znalostní báze;

– adekvátní komunikace s každým účastníkem, který byl incidentem přímo nebo nepřímo postižen.

Incident je formálně uzavřen, jakmile centrum podpory provede fázi uzavření a oznámí to druhé straně.

Jakmile je incident uzavřen, znovu se neotevírá. Jestliže se incident v krátké době vyskytne znovu, původní incident se znovu neotevírá, ale je třeba zaregistrovat nový incident.

Jestliže incident sledují centra podpory EU i Švýcarska, je konečné uzavření povinností toho centra podpory, které tiket zaregistrovalo.

5. Řízení problémů

Tento postup je třeba použít při každém zjištění problému, a spouští se jím proces řízení problémů. Řízení problémů se zaměřuje na zvýšení kvality a snížení množství vzniklých incidentů. Problém může být příčinou jednoho nebo několika incidentů. Při ohlášení incidentu je cílem řízení incidentů obnovit službu co možná nejrychleji, což může zahrnovat dočasnou opravu. Když vznikne problém, je cílem prošetřit základní příčinu tohoto problému, aby bylo možné určit, jaká změna zajistí, aby se tento problém a s ním spojené incidenty již nevyskytly.

5.1. Identifikace a záznam problému

Podle toho, která strana iniciovala tiket, bude kontaktním místem pro záležitosti spojené s problémem buď unijní centrum podpory, nebo švýcarské centrum podpory.

Jedinečný identifikátor problému je identifikátor, který mu přiřadí řízení IT služeb (ITSM). Musí být používán při každé komunikaci týkající se tohoto problému.

Problém může být spuštěn incidentem nebo může být otevřen samostatně za účelem odstranění nedostatků zjištěných v jakékoli chvíli v systému.

5.2. Stanovení priority problému

Problémy mohou být kategorizovány podle své závažnosti a priority stejně jako incidenty, aby bylo usnadněno jejich sledování, přičemž se zohlední dopad s nimi souvisejících incidentů a četnost jejich výskytu.

5.3. Šetření a diagnostika problémů

Problém může nadnést každá strana, přičemž centrum podpory iniciující strany je odpovědné za zaregistrování problému, jeho přiřazení příslušnému zdroji a sledování jeho celkového stavu.

Řešitelská skupina, jíž byl problém předán, je odpovědná za včasné řešení problému a komunikaci s centrem podpory.

Obě strany jsou na požádání odpovědné za zajištění provedení přiřazených činností a poskytnutí zpětné vazby svému vlastnímu centru podpory.

5.4. Vyřešení

Řešitelská skupina, jíž byl problém přiřazen, je odpovědná za vyřešení problému a poskytnutí příslušných informací svému vlastnímu centru podpory.

Zjištění ze zpracování problému je třeba zaznamenat pro budoucí použití.

5.5. Uzavření problému

Problém je formálně uzavřen, jakmile je vyřešen provedením změny. Fázi uzavření problému provede centrum podpory, které tento problém zaregistrovalo a informovalo centrum podpory druhé strany.

6. Plnění žádostí

Proces plnění žádosti je komplexní řízení žádosti o novou nebo stávající službu od okamžiku jejího zaregistrování a schválení až do uzavření. Žádosti o službu jsou obvyklé drobné, předem definované, opakovatelné, časté, předem schválené a procedurální požadavky.

Níže jsou načrtnuty hlavní kroky, podle nichž je třeba postupovat:

6.1. Iniciování žádosti

Informace o žádosti o službu se předá unijnímu centru podpory nebo švýcarskému centru podpory e-mailem, telefonicky nebo prostřednictvím nástroje pro řízení IT služeb (ITSM) nebo jakéhokoli jiného komunikačního kanálu.

6.2. Registrování a analýza žádosti

Kontaktním místem pro všechny žádosti o službu by mělo být unijní nebo švýcarské centrum podpory podle toho, která strana žádost o službu podala. Toto centrum podpory bude odpovědné za řádné zaregistrování a analýzu žádosti o službu.

6.3. Schválení žádosti

Agent centra podpory strany, která žádost o službu podala, zkontroluje, zda je potřebné schválení druhé strany, a v kladném případě si je vyžádá. Jestliže žádost o službu není schválena, centrum podpory tiket aktualizuje a uzavře jej.

6.4. Plnění žádosti

Tento krok má na starosti účelné a efektivní zpracování žádostí o službu. Je třeba rozlišovat mezi těmito případy:

– Plnění žádosti o službu se týká pouze jedné strany. V tomto případě vydá tato strana pracovní příkazy a koordinuje provedení.

– Provedení žádosti o službu se týká EU i Švýcarska. V tomto případě centra podpory vydávají pracovní příkazy ve své oblasti odpovědnosti. Zpracování plnění žádosti o službu je koordinováno mezi oběma centry podpory. Celkovou odpovědnost nese centrum podpory, které žádost o službu obdrželo a iniciovalo.

Když je žádost o službu vyřešena, musí být nastavena do stavu Vyřešeno.

6.5. Eskalace žádosti

Centrum podpory může v případě potřeby předat nevyřízenou žádost o službu příslušnému zdroji (třetí straně).

Předává se příslušným třetím stranám, tj. unijní centrum podpory bude muset postupovat přes švýcarské centrum podpory, pokud má být žádost předána švýcarské třetí straně, a naopak.

Třetí strana, jíž byla žádost o službu předána, je odpovědná za včasné vyřízení žádosti o službu a komunikaci s centrem podpory, které žádost o službu předalo.

Centrum podpory, které žádost o službu zaregistrovalo, je odpovědné za sledování celkového stavu a přiřazení žádosti o službu.

6.6. Kontrola splnění žádosti

Odpovědné centrum podpory předloží záznam o žádosti o službu před uzavřením k závěrečné kontrole kvality. Cílem je zajistit, aby byla žádost o službu opravdu zpracována a aby byly dodány všechny informace potřebné k popisu životního cyklu žádosti s dostatečnými podrobnostmi. Kromě toho je třeba zaznamenat zjištění ze zpracování žádosti pro budoucí použití.

6.7. Uzavření žádosti

Jestliže se strany, jimž byla žádost o službu přiřazena, dohodnou, že žádost byla splněna, a žadatel považuje případ za vyřešený, nastaví se stav „Uzavřeno“.

Žádost o službu je formálně uzavřena, jakmile centrum podpory, které tuto žádost o službu zaregistrovalo, provede uzavírací fázi žádosti a informuje centrum podpory druhé strany.

7. Řízení změn

Cílem je zajistit, aby byly používány standardizované metody a postupy za účelem efektivního a rychlého zpracování všech změn v řízení IT infrastruktury, aby se tak minimalizoval počet případných souvisejících incidentů a jejich dopad na službu. Změny IT infrastruktury mohou vznikat v reakci na problémy nebo externě vznesené požadavky, např. legislativní změny, případně aktivně za účelem zlepšení efektivity a účelnosti nebo za účelem umožnění obchodních iniciativ či jejich zohlednění.

Proces řízení změn zahrnuje různé kroky, které zachycují každou podrobnost o žádosti o změnu pro účely budoucího dohledání. Tyto procesy zajišťují, aby byla změna před provedením validována a otestována. Úspěšné provedení má na starosti proces řízení vydání.

7.1. Žádost o změnu

Žádost o změnu (RFC) se předá týmu pro řízení změn k validaci a schválení. Kontaktním místem pro všechny žádosti o změnu by mělo být unijní nebo švýcarské centrum podpory podle toho, která strana žádost podala. Toto centrum podpory bude odpovědné za řádné zaregistrování a analýzu žádosti.

Žádosti o změnu mohou vznikat z důvodu:

– incidentu, který změnu způsobí;

– stávajícího problému, v jehož důsledku ke změně dojde;

– požadavku na novou změnu vzneseného konečným uživatelem;

– změny v důsledku probíhající údržby;

– změny právních předpisů.

7.2. Hodnocení a plánování změn

V této fázi se provádí hodnocení změn a činností plánování. Zahrnuje stanovení priorit a plánování činností za účelem minimalizace rizik a dopadu.

Jestliže se provádění žádosti o změnu týká EU i Švýcarska, strana, která žádost o změnu zaregistrovala, ověří hodnocení a plánování změny u druhé strany.

7.3. Schválení změny

Každou zaregistrovanou žádost o změnu je třeba schválit na příslušné úrovni eskalace.

7.4. Provedení změny

K provedení změny dochází formou řízení vydání. Týmy obou stran pro řízení vydání postupují podle svých vlastních procesů, které zahrnují plánování a testování. Po dokončení provedení dochází ke kontrole změny. Aby bylo zajištěno, že vše proběhlo podle plánu, je stávající proces řízení změn průběžně kontrolován a v případě potřeby aktualizován.

8. Řízení vydání

Vydání představuje jednu nebo několik změn IT služby shromážděných v plánu vydání, které musí být povoleny, připraveny, vytvořeny, otestovány a zavedeny společně. Vydání může představovat opravu chyby, změnu hardwaru nebo jiných komponentů, změny softwaru, upgrady verzí aplikací, změny dokumentace a/nebo procesů. Obsah každého vydání se řídí, testuje a zavádí jako jedna entita.

Cílem řízení vydání je naplánovat, vytvořit, otestovat, validovat a zajistit možnost poskytování navržených služeb, které budou plnit požadavky účastníků a uskutečňovat zamýšlené cíle. V průběhu koordinace návrhu budou definována a zadokumentována kritéria přijatelnosti pro všechny změny služby, která budou předána týmům pro řízení vydání.

Vydání obvykle sestává z několika oprav problémů a vylepšení služby. Obsahuje požadovaný nový nebo změněný software a veškerý nový nebo změněný hardware potřebný k provedení schválených změn.

8.1. Plánování vydání

Prvním krokem procesu je přiřazení schválených změn do balíčků vydání a definování rozsahu a obsahu vydání. Na základě těchto informací se v dílčím procesu plánování vydání vypracuje harmonogram vytvoření, otestování a zavedení vydání.

Při plánování je třeba definovat:

– rozsah a obsah vydání;

– posouzení rizika a rizikový profil vydání;

– zákazníka/uživatele, jichž se vydání dotkne;

– tým odpovědný za vydání;

– strategii dodání a zavedení;

– zdroje pro dodání a zavedení.

Obě strany se vzájemně informují o plánování svých vydání a oknech pro údržbu. Jestliže se vydání týká EU i Švýcarska, obě strany koordinují plánování a určují společné okno pro údržbu.

8.2. Vytvoření a otestování balíčku vydání

V kroku vytváření a testování v procesu řízení vydání se stanoví způsob provedení vydání nebo balíčku vydání a údržby řízených prostředí před změnou produkce a dále proběhne otestování všech změn ve všech vydaných prostředích.

Jestliže se vydání týká EU i Švýcarska, obě strany koordinují plány dodání a testování. Zahrnuje to tyto aspekty:

– jak a kdy budou dodány jednotky vydání a komponenty služby;

– jaké jsou obvyklé doby realizace; co se stane, pokud dojde ke zpoždění;

– jak sledovat postup dodání a získat konfirmaci;

– měřítka monitorování a stanovení úspěšného zavedení vydání;

– společné testovací případy pro příslušné funkce a změny.

Na konci tohoto dílčího procesu jsou všechny potřebné komponenty vydání připraveny pro vstup do fáze skutečného provozu.

8.3. Příprava na zprovoznění

Přípravný dílčí proces zajišťuje, aby byly správně definovány komunikační plány a aby byla připravena oznámení pro rozeslání všem dotčeným účastníkům a konečným uživatelům a dále aby bylo vydání integrováno do procesu řízení změn, aby bylo zajištěno, že všechny změny budou provedeny kontrolovaně a budou schváleny potřebnými fóry.

Jestliže se vydání týká EU i Švýcarska, obě strany koordinují tyto činnosti:

– záznam žádosti o změnu pro účely naplánování a přípravy zavedení do produkčního prostředí;

– vytvoření prováděcího plánu;

– způsob návratu, aby v případě, že zavedení selže, mohl být navrácen předchozí stav;

– sdělení zaslaná všem potřebným stranám;

– žádost o schválení implementace vydání z příslušné úrovně eskalace.

8.4. Návrat do původního stavu

V případě, že zprovoznění selže nebo se při testování ukáže, že zprovoznění nebylo úspěšné nebo nesplnilo dohodnutá kritéria přijatelnosti/kvality, týmy obou stran pro řízení vydání musí vrátit systém do předchozího stavu. Bude třeba informovat všechny potřebné účastníky, včetně dotčených/cílových konečných uživatelů. Až do schválení může být proces znovu spuštěn v kterékoli z předchozích fází.

8.5. Kontrola a uzavření vydání

Při kontrole zprovoznění je třeba provést tyto činnosti:

– získat zpětnou vazbu o spokojenosti zákazníka/uživatele s dodáním a zprovozněním služby (shromáždit zpětnou vazbu a zohlednit ji při průběžném zdokonalování služby);

– zrevidovat všechna kritéria kvality, která nebyla splněna;

– zkontrolovat, zda jsou kompletní všechny úkony, potřebné opravy a změny;

– zajistit, že po dokončení zavádění nezůstaly nevyřešeny žádné problémy s funkčností, zdroji, kapacitou nebo výkonem;

– zkontrolovat, zda jsou zdokumentovány a akceptovány zákazníkem, konečnými uživateli, provozní podporou a dalšími dotčenými stranami všechny problémy, známé chyby a dočasné opravy;

– monitorovat incidenty a problémy způsobené zavedením (poskytnout podporu provozním týmům v rané fázi, pokud vydání způsobilo nárůst objemu práce);

– aktualizovat podkladovou dokumentaci (tj. technické informační dokumenty);

– formálně předat zavedené vydání do provozu;

– zdokumentovat získané poznatky;

– shromáždit od realizačních týmů souhrnnou dokumentaci vydání;

– formálně uzavřít vydání po ověření záznamu o žádosti o změnu.

9. Řízení bezpečnostních incidentů

Řízení bezpečnostních incidentů je proces řešení bezpečnostních incidentů, aby mohli být potenciálně dotčení účastníci informováni o incidentu; hodnocení incidentu a stanovení jeho priority a reakce na incident za účelem vyřešení skutečného nebo potenciálního narušení důvěrnosti, dostupnosti či integrity citlivých informací či podezření na takové narušení důvěrnosti, dostupnosti či integrity.

9.1. Kategorizace incidentů v oblasti bezpečnosti informací

Všechny incidenty s dopadem na propojení mezi unijním registrem a švýcarským registrem se analyzují za účelem zjištění, zda nedošlo k narušení důvěrnosti, integrity nebo dostupnosti jakýchkoli citlivých informací zaznamenaných v seznamu citlivých informací (SIL).

V kladném případě se incident charakterizuje jako incident v oblasti bezpečnosti informací, neprodleně se zaregistruje do nástroje řízení IT služeb (ITSM) a jako takový se řídí.

9.2. Řešení incidentů v oblasti bezpečnosti informací

Za bezpečnostní incidenty je odpovědná 3. úroveň eskalace a řešením incidentů bude pověřen specializovaný tým pro řízení incidentů (IMT).

Tým IMT odpovídá za:

– provedení první analýzy, kategorizaci a stanovení závažnosti incidentu;

– koordinaci činností mezi všemi účastníky včetně úplné dokumentace analýzy incidentu, rozhodnutí přijatých za účelem vyřešení incidentu a možných zjištěných slabých stránek;

– v závislosti na závažnosti bezpečnostního incidentu včasné předání na příslušnou úroveň pro informaci a/nebo k rozhodnutí.

V procesu řízení bezpečnosti informací se všechny informace o incidentech klasifikují na nejvyšší úrovni citlivosti informací, v každém případě však nejméně jako ETS CITLIVÉ.

V případě probíhajícího šetření a/nebo výskytu slabé stránky, která by mohla být zneužita, se informace klasifikují jako ETS KRITICKÉ, dokud nebude zjednána náprava.

9.3. Identifikace bezpečnostních incidentů

Podle druhu bezpečnostní události určí pracovník pro bezpečnost informací příslušné organizace, které mají být zapojeny a budou zařazeny do týmu IMT.

9.4. Analýza bezpečnostních incidentů

Při zkoumání incidentu je tým IMT ve spojení se všemi zapojenými organizacemi a podle potřeby s příslušnými členy jejich týmů. V průběhu analýzy se určí rozsah ztráty důvěrnosti, integrity nebo dostupnosti položek a vyhodnotí se důsledky pro všechny postižené organizace. Dále se definují počáteční a následná opatření pro vyřešení incidentu a řízení jeho dopadu, včetně dopadu těchto opatření na zdroje.

9.5. Posouzení závažnosti bezpečnostního incidentu, eskalace a podávání zpráv

Tým IMT posoudí závažnost každého nového bezpečnostního incidentu po jeho charakterizaci za bezpečnostní incident a neprodleně zahájí potřebná opatření podle závažnosti incidentu.

9.6. Podávání zpráv o reakcích v oblasti bezpečnosti

Tým IMT uvede informace o omezení důsledků incidentu a výsledcích obnovy do zprávy o reakci na bezpečnostní incident. Tato zpráva se předává na 3. úroveň eskalace pomocí bezpečné elektronické pošty nebo jiných vzájemně akceptovaných prostředků bezpečné komunikace.

Odpovědná strana zkontroluje omezení důsledků incidentu a výsledky obnovy a:

– opět připojí registr v případě, že byl předtím odpojen;

– zajistí komunikaci o incidentu s týmy, které se starají o registr;

– uzavře incident.

Tým IMT by měl ve zprávě o incidentu v oblasti bezpečnosti informací zabezpečeným způsobem uvést příslušné podrobnosti, aby byl zajištěn konzistentní záznam a komunikace a aby bylo možné přijmout rychlá a vhodná opatření za účelem omezení důsledků incidentu. Po dokončení tým IMT předloží v příslušné lhůtě závěrečnou zprávou o incidentu v oblasti bezpečnosti informací.

9.7. Monitorování, budování kapacit a průběžné zdokonalování

Tým IMT předává zprávy o všech bezpečnostních incidentech na 3. úroveň eskalace. Zprávy budou na této úrovni eskalace použity k určení:

– slabých míst v kontrolách bezpečnosti anebo provozu, které je třeba posílit;

– případné potřeby zdokonalit tento postup, aby se zlepšila jeho účinnost při reagování na incidenty;

Možnosti školení a budování kapacit za účelem dalšího posílení odolnosti systémů registrů v oblasti bezpečnosti informací, snížení rizika budoucích incidentů a minimalizace jejich dopadu.

10. Řízení bezpečnosti informací

Cílem řízení bezpečnosti informací je zajistit důvěrnost, integritu a dostupnost utajovaných informací, dat a IT služeb organizace. Vedle technických složek včetně jejich návrhu a testování (viz technické normy pro propojování) jsou pro splnění bezpečnostních požadavků na prozatímní řešení potřebné následující společné provozní postupy.

10.1. Identifikace citlivých informací

Citlivost informace se posuzuje stanovením, jaký dopad na podnik by mohlo mít narušení bezpečnosti v případě této informace (například finanční ztráty, poškození pověsti, porušení právního předpisu...).

Citlivé informační položky se identifikují podle jejich dopadu na propojení.

Úroveň citlivosti těchto informací se posuzuje podle stupnice citlivosti platné pro toto propojení a uvedené v oddílu „Řešení incidentů v oblasti bezpečnosti informací“ tohoto dokumentu.

10.2. Úrovně citlivosti informačních položek

Po identifikaci se informační položka klasifikuje podle těchto pravidel:

– při identifikaci alespoň jedné VYSOKÉ úrovně u důvěrnosti, integrity nebo dostupnosti je položka klasifikována jako ETS KRITICKÁ;

– při identifikaci alespoň jedné STŘEDNÍ úrovně u důvěrnosti, integrity nebo dostupnosti je položka klasifikována jako ETS CITLIVÁ;

– při identifikaci alespoň jedné NÍZKÉ úrovně u důvěrnosti, integrity nebo dostupnosti je položka klasifikována jako ETS OMEZENÁ.

10.3. Přiřazení vlastníka informačních položek

Všechny informační položky by měly mít svého přiřazeného vlastníka. Informační položky ETS patřící k propojení mezi EUTL a SSTL nebo s ním spojené by měly být uvedeny ve společném inventurním soupisu položek vedeném oběma stranami. Informační položky ETS mimo propojení mezi EUTL a SSTL by měly být uvedeny v inventurním soupisu položek vedeném příslušnou stranou.

Strany se dohodnou na vlastnictví každé informační položky patřící k propojení mezi EUTL a SSTL nebo s ním spojené. Vlastník informační položky je odpovědný za posouzení její citlivosti.

Vlastník by měl mít vhodnou úroveň pracovní funkce podle hodnoty přiřazené položky (položek). Odpovědnost vlastníka za položku (položky) a povinnost zachovávání potřebné úrovně důvěrnosti, integrity a dostupnosti je třeba dohodnout a formalizovat.

10.4. Registrace citlivých informací

Všechny citlivé informace se registrují v seznamu citlivých informací (SIL).

V příslušných případech se zohlední a v seznamu citlivých informací zaregistruje agregace citlivých informací, která by mohla vést k vyššímu dopadu, než je dopad jednotlivé informace (např. soubor informací uložených v systémové databázi).

Seznam citlivých informací není statický. Hrozby, zranitelnost, pravděpodobnost nebo důsledky bezpečnostních incidentů souvisejících s informačními položkami se mohou měnit bez jakéhokoli varovného signálu a do provozu registrů mohou být zaváděny nové položky.

Proto je třeba seznam citlivých informací pravidelně kontrolovat a neprodleně do něj registrovat všechny nové informace identifikované jako citlivé.

Seznam citlivých informací obsahuje u každého zápisu alespoň tyto informace:

– popis informace

– vlastník informace

– úroveň citlivosti

– označení, zda informace zahrnuje osobní údaje

– další informace, jsou-li potřebné

10.5. Nakládání s citlivými informacemi

Pokud jsou citlivé informace zpracovávány mimo propojení mezi unijním registrem a švýcarským registrem, je třeba s nimi nakládat v souladu s pokyny pro nakládání.

S citlivými informacemi zpracovávanými v rámci propojení mezi unijním registrem a švýcarským registrem se nakládá v souladu s bezpečnostními požadavky stran.

10.6. Řízení přístupu

Cílem řízení přístupu je udělit oprávněným uživatelům právo používat službu a současně zabránit v přístupu neoprávněným uživatelům. Řízení přístupu se někdy také nazývá „správa práv“ nebo „správa identit“.

Pro prozatímní řešení a jeho provoz potřebují obě strany přístup k těmto komponentům:

– Wiki: prostředí pro spolupráci na výměnu společných informací, jako je plánování vydání;

– nástroj pro řízení IT služeb (ITSM) pro řízení incidentů a problémů (viz kapitola 3 „Přístup a standardy“);

– systém výměny zpráv: každá strana zajistí bezpečný přenosový systém výměny zpráv pro přenos zpráv obsahujících údaje o transakcích.

Správce švýcarského registru a ústřední správce Unie zajistí, aby byly přístupy aktuální, a budou fungovat jako kontaktní místa pro své strany pro činnosti v oblasti řízení přístupu. Žádosti o přístup se řeší podle postupů plnění žádostí.

10.7. Správa certifikátů/klíčů

Každá strana je odpovědná za správu svých vlastních certifikátů/klíčů (generování, registrace, ukládání, instalace, používání, prodloužení, zrušení, zálohování a obnova certifikátů/klíčů). Jak je uvedeno v technických normách pro propojování (LTS), používají se pouze digitální certifikáty vydané certifikačním orgánem (CA), kterému obě strany důvěřují. Nakládání s certifikáty/klíči a jejich ukládání musí být v souladu s ustanoveními uvedenými v pokynech pro nakládání.

Každé zrušení a/nebo prodloužení certifikátů a klíčů bude koordinováno oběma stranami. Probíhá to podle postupů plnění žádostí.

Správce švýcarského registru a ústřední správce Unie si vymění certifikáty/klíče prostřednictvím zabezpečených komunikačních prostředků podle ustanovení stanovených v pokynech pro nakládání.

Každé ověření certifikátů/klíčů jakýmikoli prostředky mezi stranami bude probíhat mimo IP síť.