ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 23.6.2020 г.
COM(2020) 255 final

ANNEX

ПРИЛОЖЕНИЕ

към

предложение за Решение на Съвета

относно позицията, която трябва да се заеме от името на Европейския съюз в рамките на Съвместния комитет, създаден по силата на Споразумението между Европейския съюз и Конфедерация Швейцария за свързване на техните системи за търговия с емисии на парникови газове, във връзка с приемането на Общи работни процедури

РЕШЕНИЕ № 1/2020 НА СЪВМЕСТНИЯ КОМИТЕТ, СЪЗДАДЕН СЪГЛАСНО СПОРАЗУМЕНИЕТО МЕЖДУ ЕВРОПЕЙСКИЯ СЪЮЗ И КОНФЕДЕРАЦИЯ ШВЕЙЦАРИЯ ЗА СВЪРЗВАНЕ НА ТЕХНИТЕ СИСТЕМИ ЗА ТЪРГОВИЯ С ЕМИСИИ НА ПАРНИКОВИ ГАЗОВЕ

от … година

относно Общи работни процедури (ОРП)

СЪВМЕСТНИЯТ КОМИТЕТ,

като взе предвид Споразумението между Европейския съюз и Конфедерация Швейцария за свързване на техните системи за търговия с емисии на парникови газове[1] (наричано по-нататък „споразумението“), и по-специално член 3 от него,

като има предвид, че:

(1) С Решение № 2/2019 на Съвместния комитет от 5 декември 2019 г. бяха изменени приложения I и II към споразумението и по този начин бяха удовлетворени условията за свързване, посочени в споразумението.

(2) След приемането на Решение № 2/2019 на Съвместния комитет и в съответствие с член 21, параграф 3 от споразумението страните размениха своите инструменти за ратифициране или одобрение, тъй като считат, че всички условия за свързване, предвидени в споразумението, са изпълнени.

(3) В съответствие с член 21, параграф 4 от споразумението то влезе в сила на 1 януари 2020 г.

(4) Съгласно член 3, параграф 6 от споразумението администраторът на Швейцарския регистър и централният администратор за Съюза определят Общи работни процедури (ОРП) във връзка с технически или други въпроси, необходими за функционирането на връзката между Дневника на ЕС за трансакциите (EUTL) към Регистъра на Съюза и Швейцарския допълнителен дневник на трансакциите (SSTL) към Швейцарския регистър, с отчитане на приоритетите на вътрешното законодателство. Общите работни процедури следва да пораждат действие след приемането им с решение на Съвместния комитет.

(5) В съответствие с член 13, параграф 1 от споразумението Съвместният комитет следва да постигне съгласие по технически насоки, за да осигури правилното изпълнение на споразумението, включително технически или други въпроси, необходими за функционирането на връзката, и като се отчитат приоритетите на вътрешното законодателство. Техническите насоки може да бъдат разработени от работна група, учредена съгласно член 12, параграф 5 от споразумението. Работната група следва да включва най-малко администратора на Швейцарския регистър и централния администратор за Регистъра на Съюза и следва да подпомага Съвместния комитет във функциите му съгласно член 13 от споразумението.

(6) С оглед на техническия характер на насоките и необходимостта от адаптирането им към текущите новости, техническите насоки, разработени от администратора

[1] ОВ L 322, 7.12.2017 г., стр. 3.

на Швейцарския регистър и централния администратор за Съюза, следва да се предоставят на Съвместния комитет за информация или, когато това е необходимо — за одобрение,

ПРИЕ НАСТОЯЩОТО РЕШЕНИЕ:

Член 1

Приемат се Общите работни процедури (ОПР), приложени към настоящото решение.

Член 2

С настоящото се учредява работна група съгласно член 12, параграф 5 от споразумението. Тя подпомага Съвместния комитет, за да се гарантира правилното изпълнение на споразумението, включително при разработването на технически насоки за изпълнение на Общите работни процедури.

Работната група включва най-малко администратора на Швейцарския регистър и централния администратор за Регистъра на Съюза.

Член 3

Настоящото решение влиза в сила в деня на приемането му.

Съставено на английски език в Брюксел на XX 2020 г.

За Съвместния комитет

Секретар за Европейския съюз	*Председател*	*Секретар за Швейцария*

ДОПЪЛНЕНИЕ

ПРИЛОЖЕНИЕ

ОБЩИ РАБОТНИ ПРОЦЕДУРИ (ОРП)

съгласно член 3, параграф 6 от Споразумението между Европейския съюз и Конфедерация Швейцария за свързване на техните системи за търговия с емисии на парникови газове

— Процедури за временно решение —

1. ТЕРМИНИ

Таблица 1-1 Съкращения и определения

Съкращение/Термин	Определение
Сертифициращ орган (СО)	Субект, който издава електронни сертификати
CH	Конфедерация Швейцария
СТЕ	Система за търговия с емисии
ЕС	Европейски съюз
ЕУИ	Екип за управление на инциденти
Информационен актив	Информация, която е ценна за дружество или организация
ИТ	Информационна технология
ITIL	Библиотека за инфраструктурата на информационните технологии
ITSM	Управление на услугите в областта на информационните технологии
LTS	Технически стандарти за свързването
Регистър	Система за отчитане на квотите, издадени в рамките на СТЕ, с която собствеността на квотите се проследява по електронен път.
ЗП	Заявка за промяна
СЧИ	Списък с чувствителна информация
ЗУ	Заявка за услуга
Уики	Уебсайт, който позволява на потребителите да обменят информация и знания чрез добавяне или адаптиране на

	съдържание директно чрез уеб браузър.

2. ВЪВЕДЕНИЕ

В Споразумението между Европейския съюз и Конфедерация Швейцария за свързване на техните системи за търговия с емисии на парникови газове от 23 ноември 2017 г. (наричано по-долу „споразумението“) се предвижда взаимно признаване на квотите за емисии, които могат да бъдат използвани за спазване на изискванията по Системата за търговия с емисии на Европейския съюз („СТЕ на ЕС“) със Системата за търговия с емисии на Швейцария („СТЕ на Швейцария“). За да може да функционира връзката между СТЕ на ЕС и СТЕ на Швейцария, се създава директна връзка между Дневника на ЕС за трансакциите (EUTL) към Регистъра на Съюза и Швейцарския допълнителен дневник на трансакциите (SSTL) към Швейцарския регистър, която ще позволи прехвърлянето от регистър до регистър на квоти за емисии, издадени в рамките на всяка от двете СТЕ (член 3, параграф 2 от споразумението). С цел привеждане в действие на свързването на СТЕ на ЕС и СТЕ на Швейцария през май 2020 г. или възможно най-скоро след това се въвежда временно решение. Страните си сътрудничат, за да заменят възможно най-скоро временното решение с постоянна връзка между регистрите (приложение II към споразумението).

В съответствие с член 3, параграф 6 от споразумението администраторът на Швейцарския регистър и централният администратор за Съюза определят Общи работни процедури във връзка с технически или други въпроси, необходими за функционирането на връзката, с отчитане на приоритетите на вътрешното законодателство. Изготвените от администраторите Общи работни процедури пораждат действие след приемането им с решение на Съвместния комитет.

Посочените в настоящия документ Общи работни процедури следва да бъдат приети от Съвместния комитет с Решение № 1/2020 на Съвместния комитет. В съответствие с настоящото решение Съвместният комитет отправя искане до администратора на Швейцарския регистър и централния администратор за Съюза да разработят допълнителни технически насоки за привеждане в действие на връзката и да гарантират, че те постоянно се адаптират към техническия прогрес и новите изисквания, свързани с безопасността и сигурността на връзката и нейното ефективно и ефикасно функциониране.

2.1. Област на приложение

В настоящия документ е изложена общата договореност между страните по споразумението във връзка с установяването на процедурните основи за връзката между регистъра на СТЕ на ЕС и регистъра на СТЕ на Швейцария. Макар в него да са очертани общите процедурни изисквания по отношение на операциите, за привеждане в действие на връзката ще бъдат необходими някои допълнителни технически насоки.

За правилното функциониране ще бъдат необходими технически спецификации за връзката за по-нататъшното ѝ привеждане в действие. Съгласно член 3, параграф 7 от споразумението тези въпроси са описани подробно в документа за Технически стандарти за свързването (LTS), който трябва да бъде приет отделно с решение на Съвместния комитет.

Целта на Общите работни процедури е да се гарантира, че услугите в областта на информационните технологии, свързани с функционирането на връзката между регистъра на СТЕ на ЕС и регистъра на СТЕ на Швейцария, се предоставят ефективно и ефикасно, особено за целите на изпълнението на заявки за услуги, отстраняването на

неизправности на услугите, разрешаването на проблеми, както и за изпълнението на рутинни оперативни задачи в съответствие с международните стандарти за управление на услугите в областта на информационните технологии.

За договореното временно решение ще бъдат необходими само следните Общи работни процедури, които са част от настоящия документ:

- Управление на инциденти
- Управление на проблеми
- Изпълнение на заявки
- Управление на промени
- Управление на версии
- Управление на инциденти, свързани със сигурността
- Управление на информационната сигурност

С въвеждането на по-късен етап на постоянна връзка между регистрите, при необходимост Общите работни процедури трябва да бъдат адаптирани и допълвани.

2.2. Адресати

Целевата аудитория на настоящите Общи работни процедури са екипите за поддръжка на регистъра на ЕС и Швейцарския регистър.

3. ПОДХОД И СТАНДАРТИ

Следният принцип се прилага за всички ОРП:

- ЕС и Швейцария се договарят да определят ОРП въз основа на ITIL (Библиотека за инфраструктурата на информационните технологии, версия 3). Практиките от този стандарт се използват повторно и се адаптират към специфичните нужди, свързани с временното решение.
- Комуникацията и координацията между двете страни, необходими за обработката на ОРП, се осъществяват чрез бюрата за обслужване на регистрите на Швейцария и ЕС. Задачите винаги се възлагат на една от страните.
- Ако има несъгласие относно боравенето с ОРП, то ще бъде анализирано и разрешено между двете бюра за обслужване. Ако не може да се постигне съгласие, намирането на съвместно решение се пренасочва на следващото равнище.

Равнища на пренасочване	**ЕС**	**Швейцария**
1-во равнище	Бюро за обслужване на ЕС	Бюро за обслужване на Швейцария
2-ро равнище	Ръководител операции за ЕС	Ръководител по прилагането за Швейцарския регистър
3-то равнище	Съвместен комитет (който може да делегира тази отговорност предвид член 12, параграф 5 от споразумението)	
4-то равнище	Съвместният комитет, ако 3-то равнище е делегирано	

- Всяка от страните може да определя процедурите за функционирането на системата на своя регистър, като взема предвид изискванията и интерфейсите, свързани с настоящите ОРП.
- За поддръжката на ОРП, по-специално управление на инциденти, управление на проблеми и изпълнение на заявки, както и за комуникацията между двете страни, се използва инструмент за управление на услугите в областта на информационните технологии (ITSM).
- Освен това се разрешава обмен на информация по електронна поща.
- Двете страни гарантират, че изискванията за информационна сигурност се изпълняват в съответствие с указанията за боравене с чувствителна информация.

4. УПРАВЛЕНИЕ НА ИНЦИДЕНТИ

Целта на процеса на управление на инциденти е възможно най-бързо връщане на ИТ услугите към нормално ниво на обслужване и при минимално прекъсване на стопанската дейност.

Управлението на инциденти следва да включва също така воденето на регистър на инцидентите за целите на докладването и то следва да се интегрира с други процеси, за да води към непрекъснато подобрение.

- В по-общ план управлението на инциденти включва следните дейности:
- засичане и записване на инциденти;
- класифициране и дейности по първоначална поддръжка;
- проучване и диагностика;
- разрешаване на инциденти и възстановяване на услугата;
- приключване на инцидента.

През целия жизнен цикъл на инцидента от процеса на управление на инциденти зависи постоянното разглеждане на въпросите, свързани със собствеността, наблюдението, проследяването и комуникацията.

4.1. Засичане и записване на инциденти

Един инцидент може да бъде засечен от група за поддръжка, от инструменти за автоматизирано наблюдение или от техническия персонал, който извършва рутинен надзор.

След като бъде засечен, инцидентът трябва да бъде записан и да му се зададе уникален идентификатор, който дава възможност за правилно проследяване и наблюдение на инцидента. Уникалният идентификатор на инцидента е идентификаторът, зададен в общата система за записване от бюрото за обслужване на съответната страна (ЕС или Швейцария), което е отчело инцидента, и трябва да се използва при всяка комуникация, свързана с този инцидент.

По отношение на всички инциденти звеното за контакт следва да бъде бюрото за обслужване на съответната страна, която е регистрирала записа.

4.2. Класифициране и дейности по първоначална поддръжка

Класифицирането на инциденти има за цел да се разбере и определи коя система и/или услуга е засегната и доколко. За да бъде ефективно класифицирането, инцидентът следва да бъде насочен към правилния екип още от първия път, за да се ускори разрешаването му.

В етапа на класифициране инцидентът следва да се категоризира и приоритизира според неговото въздействие и спешност, за да бъде третиран съгласно сроковете за съответното ниво на приоритет.

Ако инцидентът има потенциално въздействие върху поверителността или интегритета на чувствителни данни и/или въздействие върху работата на системата, той се обявява и като инцидент, свързан със сигурността, и след това се управлява в съответствие с процеса, определен в глава „Управление на инциденти, свързани със сигурността“, от настоящия документ.

Ако е възможно, бюрото за обслужване, което е регистрирало записа, извършва първоначална диагностика. За целта бюрото за обслужване ще прецени дали инцидентът представлява известна грешка. Ако това е така, тогава начинът на разрешаване или временното решение вече са известни и документирани.

Ако бюрото за обслужване успее да разреши инцидента, тогава то всъщност ще приключи инцидента още на този етап, тъй като основната цел на управлението на инциденти би била изпълнена (т.е. бързото възстановяване на услугата за крайния ползвател). Ако това не е така, бюрото за обслужване ще пренасочи инцидента към правилната група по разрешаване, за да бъде допълнително проучен и диагностициран.

4.3. Проучване и диагностика

Проучване и диагностика на инциденти се прилагат, когато бюрото за обслужване не може да разреши даден инцидент като част от първоначалната диагностика и поради това го пренасочва към подходящото равнище. Пренасочването на инцидента е самостойна част от процеса на проучване и диагностика.

Обща практика на етапа на проучване и диагностика е опитът инцидентът да се пресъздаде при контролирани условия. Важно е при проучването и диагностиката на инциденти да се разбере правилният ред на събитията, довели до инцидента.

Пренасочване означава да се признае, че даден инцидент не може да бъде разрешен на настоящото равнище на поддръжка и трябва да бъде прехвърлен на група за поддръжка на по-високо равнище или на другата страна. Пренасочването може да следва две направления: хоризонтално (функционално) или вертикално (йерархично).

Бюрото за обслужване, което е записало и завело инцидента, е отговорно за неговото пренасочване към правилния екип и за проследяването на цялостния статус и възлагане на инцидента.

Страната, на която е възложен инцидентът, отговаря за това поисканите действия да се извършват своевременно и нейното бюро за обслужване да получи обратна информация.

4.4. Разрешаване на инциденти и възстановяване на услугата

Разрешаването на инциденти и възстановяването на услугата се извършва, след като се добие пълна представа за инцидента. Намирането на разрешение на даден инцидент

означава, че е установен начин за отстраняване на проблема. Прилагането на разрешението представлява етапа на възстановяване на услугата.

След като проблемът с услугата бъде разрешен от подходящия екип, инцидентът се насочва обратно към съответното бюро за обслужване, което е регистрирало инцидента, и то потвърждава заедно с инициатора на инцидента, че грешката е отстранена и инцидентът може да бъде приключен. Констатациите от обработката на инцидента трябва да се записват с цел бъдеща употреба.

Възстановяването на услугата може да се извършва от ИТ персонал по поддръжка или чрез предоставяне на набор от инструкции на крайния ползвател, които той да следва.

4.5. Приключване на инциденти

Приключването е последната стъпка в процеса на управление на инциденти и се извършва малко след разрешаването на инцидента.

В контролните списъци на дейностите, които трябва да бъдат извършвани по време на етапа на приключване, е подчертано следното:

- проверка на първоначалната категоризация на инцидента;
- правилно отразяване на цялата информация, свързана с инцидента;
- правилно документиране на инцидента и актуализиране на базата от знания;
- подходящо информиране на всички заинтересовани страни, които са засегнати пряко или косвено от инцидента.

Инцидентът е официално приключен, след като бюрото за обслужване изпълни етапа на приключване на инцидента и го съобщи на другата страна.

След като инцидентът бъде приключен, той не се въвежда отново. Ако той се появи отново в рамките на кратък период от време, първоначалният инцидент не се въвежда отново, а вместо това трябва да се регистрира нов инцидент.

Ако инцидентът се проследява както от бюрото за обслужване на ЕС, така и от бюрото за обслужване на Швейцария, окончателното приключване е отговорност на бюрото за обслужване, което е регистрирало записа.

5. Управление на проблеми

Тази процедура следва да се прилага всеки път, когато се открие проблем и съответно процесът на управление на проблеми се задейства. Управлението на проблеми е насочено към повишаване на качеството и намаляване на броя на възникналите инциденти. Даден проблем може да бъде причината за един или повече инциденти. Когато се докладва инцидент, целта на управлението на инциденти е услугата да се възстанови възможно най-бързо, евентуално с помощта на временни решения. Когато възникне проблем, целта е да се проучи основната причина за него, за да се установи промяна, която да гарантира, че проблемът и свързаните с него инциденти няма да се повторят.

5.1. Установяване и записване на проблеми

В зависимост от това коя страна е извършила записа, бюрото за обслужване на ЕС или бюрото за обслужване на Швейцария ще бъде звеното за контакт по въпроси, свързани с проблема.

Уникалният идентификатор на даден проблем е идентификаторът, който му е зададен от инструмента за управление на услугите в областта на информационните технологии (ITSM). Той трябва да се използва при всяка комуникация, свързана с този проблем.

Даден проблем може да бъде въведен заради инцидент или по собствена инициатива за разрешаване на въпроси, открити в системата на който и да е от етапите.

5.2. Приоритизиране на проблеми

Проблемите могат да бъдат категоризирани според тяхната сериозност и приоритет по същия начин като инцидентите с цел да се улесни проследяването им, като се вземе предвид въздействието на свързаните с тях инциденти и честотата им на възникване.

5.3. Проучване и диагностика на проблеми

Всяка от страните може да съобщи за проблем и бюрото за обслужване на инициращата страна ще бъде отговорно за регистрирането на проблема, възлагането му на съответния екип и проследяването на цялостния му статус.

Групата за разрешаване, към която е пренасочен проблемът, е отговорна за своевременното разглеждане на проблема и за комуникацията с бюрото за обслужване.

При поискване всяка от двете страни е отговорна да гарантира изпълнението на възложените действия и да предостави обратна информация на своето бюро за обслужване.

5.4. Разрешаване

Групата по разрешаване, на която е възложен проблемът, отговаря за разрешаването му и за предоставянето на съответната информация на бюрото за обслужване на своята страна.

Констатациите от обработката на проблема трябва да се записват за бъдеща употреба.

5.5. Приключване на проблеми

Даден проблем е официално приключен, след като бъде разрешен чрез внасяне на промяна. Етапът на приключване на проблема ще се изпълнява от бюрото за обслужване, което е регистрирало проблема и е уведомило бюрото за обслужване на другата страна.

6. ИЗПЪЛНЕНИЕ НА ЗАЯВКИ

Процесът на изпълнение на заявка представлява управление от край до край на заявка за нова или съществуваща услуга от момента, в който тя е регистрирана и е одобрена, до момента на приключване. Заявките за услуги обикновено представляват кратки, предварително определени, възпроизводими, чести, предварително одобрени и процедурни искания.

По-долу са изложени основните стъпки, които трябва да бъдат следвани.

6.1. Внасяне на заявка

Информацията, свързана със заявка за услуга, се подава до бюрото за обслужване на ЕС или бюрото за обслужване на Швейцария по електронна поща, по телефона или чрез инструмента за управление на услугите в областта на информационните технологии (ITSM) или всеки друг договорен канал за комуникация.

6.2. Регистриране и анализ на заявки

За всички заявки за услуги звеното за контакт следва да бъде бюрото за обслужване на ЕС или бюрото за обслужване на Швейцария, в зависимост от това коя страна е подала заявката за услуга. Това бюро за обслужване ще отговаря за регистрирането и анализирането на заявката за услуга с надлежното внимание.

6.3. Одобряване на заявка

Представителят на бюрото за обслужване на страната, която е подала заявката за услуга, проверява дали са необходими някакви одобрения от другата страна, и ако това е така, пристъпва към получаването им. Ако заявката за услуга не бъде одобрена, бюрото за обслужване актуализира и приключва записа.

6.4. Изпълнение на заявки

Тази стъпка е предназначена за ефективно и ефикасно обработване на заявките за услуги. Трябва да се прави разлика между следните случаи:

- изпълнението на заявката за услуга засяга само една от страните. В този случай съответната страна издава указанията за работа и координира изпълнението им;
- изпълнението на заявката за услуга засяга както ЕС, така и Швейцария. В този случай бюрата за обслужване издават указанията за работа в областта, за която носят отговорност. Процесът на изпълнение на заявката за услуга се координира между двете бюра за обслужване. Цялостната отговорност се носи от бюрото за обслужване, което е получило и внесло заявката за услуга.

Когато заявката за услуга бъде изпълнена, трябва да ѝ се зададе статус „изпълнена“.

6.5. Пренасочване на заявка

Бюрото за обслужване може, ако е необходимо, да пренасочи неизпълнената заявка за услуга към съответния екип (трета страна).

Пренасочването се извършва към съответните трети страни, т.е. бюрото за обслужване на ЕС ще трябва да изпрати заявката първо на бюрото за обслужване на Швейцария, за да я пренасочи към трета страна от Швейцария, и обратно.

Третата страна, към която е пренасочена заявката за услуга, е отговорна за своевременното ѝ обработване и за комуникацията с бюрото за обслужване, което я е пренасочило.

Бюрото за обслужване, което е регистрирало заявката за услуга, е отговорно за проследяването на цялостния ѝ статус и за възлагането ѝ.

6.6. Преглед на изпълнението на заявка

Отговорното бюро за обслужване представя записа на заявката за услуга на орган по краен контрол на качеството, преди тя да бъде приключена. Целта е да се гарантира, че заявката за услуга действително е обработена и че цялата необходима информация за описване на жизнения цикъл на заявката е предоставена достатъчно подробно. В допълнение към това, констатациите от обработката на заявката трябва да се записват за бъдеща употреба.

6.7. Приключване на заявка

Ако страните, на които е възложена заявката за услуга, са съгласни, че тя е изпълнена и вносителят счита случая за разрешен, следващият статус, който трябва да ѝ се определи, е „приключена“.

Заявката за услуга е официално приключена, след като бюрото за обслужване, което я е регистрирало, е изпълнило етапа на приключване на заявката и е уведомило бюрото за обслужване на другата страна.

7. УПРАВЛЕНИЕ НА ПРОМЕНИ

Целта е да се гарантира, че при управлението на ИТ инфраструктурата се използват стандартизирани методи и процедури за ефикасно и бързо разглеждане на всички промени, за да се сведе до минимум броят на всички свързани инциденти и тяхното отражение върху услугата. Промените в ИТ инфраструктурата могат да възникнат в отговор на проблеми или наложени външни изисквания, например законодателни промени, или да бъдат предприети активно с цел подобряване на ефикасността и ефективността или с цел разкриване на възможности или реагиране на бизнес инициативи.

Процесът на управление на промените включва различни стъпки, които отчитат всички подробности относно заявката за промяна с цел бъдещо проследяване. Тези процеси гарантират, че преди да се премине към внедряването ѝ, промяната е валидирана и изпитана. Успешното внедряване се осъществява чрез процеса на управление на версиите.

7.1. Заявка за промяна

Заявката за промяна (ЗП) се подава до екипа за управление на промените, за да бъде валидирана и одобрена. За всички заявки за промяна звеното за контакт следва да бъде бюрото за обслужване на ЕС или бюрото за обслужване на Швейцария, в зависимост от това коя страна е подала заявката. Това бюро за обслужване ще отговаря за регистрирането и анализирането на заявката с надлежното внимание.

Заявките за промяна могат да произтичат:

- от инцидент, който води до промяна;
- от съществуващ проблем, който води до промяна;
- от краен ползвател, който подава заявка за нова промяна;
- от промяна в резултат на текуща поддръжка;
- от законодателна промяна.

7.2. Оценяване и планиране на промени

Този етап е свързан с дейностите по оценяване и планиране на промените. Той включва дейности по определяне на приоритет и планиране с цел свеждане до минимум на риска и въздействието.

Ако изпълнението на ЗП засяга както ЕС, така и Швейцария, страната, която е регистрирала ЗП, проверява оценката и планирането на промяната с помощта на другата страна.

7.3. Одобряване на промени

Всяка регистрирана заявка за промяна трябва да бъде одобрена от съответното равнище на пренасочване.

7.4. Изпълнение на промени

Изпълнението на промяната се осъществява в рамките на управлението на версии. Екипите за управление на версии и на двете страни следват своите собствени процеси, които включват планиране и изпитване. След като приключи изпълнението, се извършва преглед на промяната. За да се гарантира, че всичко е преминало в съответствие с плана, съществуващият процес на управление на промените се преразглежда постоянно и се актуализира при необходимост.

8. УПРАВЛЕНИЕ НА ВЕРСИИ

Версията представлява една или повече промени в ИТ услуга, събрани в план за версия, които трябва да бъдат разрешени, подготвени, компилирани, изпитани и внедрени заедно. Версията може да представлява отстраняване на бъг, промяна на хардуер или други компоненти, промени на софтуер, надстройка на версии на приложения, промени в документацията и/или процесите. Съдържанието на всяка версия се управлява, изпитва и внедрява като едно цяло.

Управлението на версиите има за цел планиране, компилиране, изпитване и валидиране и осигуряване на способност за предоставяне на проектираните услуги, които ще удовлетворят изискванията на заинтересованите страни и ще реализират поставените цели. Критериите за приемане на всички промени в услугата ще бъдат определени и документирани по време на координирането на проекта и ще бъдат предоставени на екипите за управление на версии.

Версията обикновено се състои от редица решения на проблеми и подобрения на услугата. Тя съдържа необходимия нов или променен софтуер и всеки нов или променен хардуер, необходим за изпълнение на одобрените промени.

8.1. Планиране на версии

На първия етап от процеса се възлагат разрешените промени на пакетите от версии и се определят обхватът и съдържанието на версиите. Въз основа на тази информация чрез подпроцеса на планиране на версията се изготвя график за компилиране, изпитване и внедряване на версията.

При планирането следва да се определят:

- обхватът и съдържанието на версията;
- оценката на риска и рисковият профил на версията;
- клиентите/ползвателите, засегнати от версията;
- екипът, който отговаря за версията;
- стратегията за изпълнение и внедряване;
- ресурсите за версията и нейното внедряване.

Двете страни се уведомяват взаимно относно своите периоди на планиране и поддръжка. Ако дадена версия засяга както ЕС, така и Швейцария, те координират планирането и определят общ период на поддръжка.

8.2. Изготвяне и изпитване на пакети от версии

На етапа на компилиране и изпитване от процеса на управление на версиите се установява подходът за изпълнение на версията или пакета от версии и за поддържане на контролираните среди преди промяната на производствената среда, както и за изпитване на всички промени във всички вече пуснати в експлоатация среди.

Ако версията засяга както ЕС, така и Швейцария, те координират плановете за изпълнение и изпитванията. Това включва следните аспекти:

- как и кога ще се изпълняват елементи от версията и компоненти от услугата;
- какви са типичните необходими периоди за въвеждане; какво се случва, ако има забавяне;
- как да се проследи напредъкът по изпълнението и да се получи потвърждение;
- показателите за наблюдение и установяване на успеха на усилията за внедряване на версията;
- общите случаи на изпитване на съответните функции и промени.

В края на този подпроцес всички необходими компоненти на версията са готови за влизане в етапа на реална експлоатация.

8.3. Подготвяне за внедряване

Подготвителният подпроцес гарантира, че плановете за комуникация са определени правилно и уведомленията са готови за изпращане до всички засегнати заинтересовани страни и крайни ползватели и че версията е включена в процеса на управление на промените, за да се гарантира, че всички промени се извършват контролирано и се одобряват от съответните субекти.

Ако версията засяга както ЕС, така и Швейцария, те координират следните дейности:

- записване на заявките за промяна с цел изготвяне на график и подготвяне на внедряването в работна среда;
- създаване на план за изпълнение;
- приемане на подход за връщане в предишно стабилно състояние, така че в случай на неуспешно внедряване да е възможно връщане към предишното състояние;
- изпращане на уведомления до всички необходими страни;
- изискване на одобрение за изпълнението на версията на съответното равнище на пренасочване.

8.4. Връщане на версия в предишно стабилно състояние

В случай че внедряването е било неуспешно или при изпитването се установи, че внедряването е било неуспешно или не отговаря на договорените критерии за приемане/качество, екипите за управление на версиите и на двете страни ще трябва да възстановят предишното състояние. Всички необходими заинтересовани страни трябва да бъдат уведомени, включително засегнатите/целевите крайни ползватели. До получаване на одобрение процесът може да бъде пуснат отново на всеки от предходните етапи.

8.5. Преглед и приключване на версии

При прегледа на внедряването на версията следва да бъдат включени дейностите, изброени по-долу:

- събиране на обратна информация от клиентите, ползвателите и звената, предоставящи услугата, относно удовлетвореността им от внедряването на версията (събиране и разглеждане на обратната информация с цел постоянно подобряване на услугата);
- преглед на всички критерии за качество, които не са изпълнени;
- проверка на това дали всички действия, необходими корекции и промени са завършени;
- гарантиране, че в края на внедряването няма проблеми, свързани със способностите, ресурсите, капацитета или изпълнението;
- гарантиране, че всички проблеми, известни грешки и временни решения са документирани и приети от клиента, крайните ползватели, звената за оперативна поддръжка и други засегнати страни;
- наблюдаване на инцидентите и проблемите, причинени от внедряването на версията (оказване на навременна подкрепа на оперативните екипи, в случай че версията води до увеличаване на обема на работа);
- актуализиране на документацията за поддръжката (т.е. технически информационни документи);
- официално предаване на версията за внедряване в експлоатационна среда;
- документиране на извлечените поуки;
- получаване на резюме за версията от екипите за изпълнение;
- официално приключване на версията след проверка на записа на заявката за промяна.

9. УПРАВЛЕНИЕ НА ИНЦИДЕНТИ, СВЪРЗАНИ СЪС СИГУРНОСТТА

Управлението на инциденти, свързани със сигурността, е процес за разглеждане на свързани със сигурността инциденти, за да се даде възможност за съобщаване на инциденти на потенциално засегнати заинтересовани страни; оценяване и приоритизиране на инцидентите; и реагиране при инциденти с цел уреждане на действителни, предполагаеми или потенциални нарушения на поверителността, наличието или интегритета на чувствителни информационни активи.

9.1. Категоризация на инциденти, свързани с информационната сигурност

Всички инциденти, които оказват въздействие върху връзката между Регистъра на Съюза и Швейцарския регистър, се анализират, за да се установи евентуално нарушаване на поверителността, интегритета или наличността на чувствителна информация, записана в списъка с чувствителна информация (СЧИ).

Ако е налице такова нарушение, инцидентът се характеризира като инцидент, свързан със сигурността на информацията, незабавно се регистрира в инструмента за управление на услугите в областта на информационните технологии (ITSM) и се управлява като такъв.

9.2. Разглеждане на инциденти, свързани с информационната сигурност

Инцидентите, свързани със сигурността, са поставени под отговорността на 3-тото равнище на пренасочване и с разрешаването на инцидентите ще се занимава специализиран екип за управление на инциденти (ЕУИ).

ЕУИ отговаря:

- за извършването на първоначален анализ, категоризиране и оценяване на сериозността на инцидента;
- за координирането на действията между всички заинтересовани страни, включително цялата документация от анализа на инцидента, взетите решения за справяне с инцидента и евентуалните установени слабости;
- в зависимост от сериозността на инцидента, свързан със сигурността, за своевременното пренасочване към съответното равнище с цел получаване на информация и/или вземане на решение.

По време на процеса на управление на информационната сигурност цялата информация относно инциденти се класифицира с най-високата степен на чувствителност на информацията, но при всички случаи не по-ниска от „чувствителна информация за СТЕ“ (ETS SENSITIVE).

За целите на текущо разследване и/или слабост, която би могла да бъде проучена и до отстраняването ѝ, информацията се класифицира като „информация за СТЕ с критично значение“ (ETS CRITICAL).

9.3. Установяване на инциденти, свързани със сигурността

Въз основа на вида на случая, свързан със сигурността, служителят по информационната сигурност определя съответните организации, които да се ангажират и да участват в ЕУИ.

9.4. Анализ на инциденти, свързани със сигурността

ЕУИ поддържа връзка с всички ангажирани организации и съответните членове на техните екипи, както е целесъобразно, за да направи преглед на инцидента. По време на анализа се установява до каква степен са изгубени поверителността, интегритетът или наличността на актива и се оценяват последиците за всички засегнати организации. След това се определят първоначалните и последващите действия за разрешаване на инцидента и за управление на неговото въздействие, включително въздействието на тези действия върху ресурсите.

9.5. Оценка на сериозността, пренасочване и докладване на свързани със сигурността инциденти

ЕУИ оценява сериозността на всеки нов свързан със сигурността инцидент след характеризирането му и започва незабавни необходими действия в зависимост от сериозността на инцидента.

9.6. Докладване на реакции във връзка със сигурността

ЕУИ включва резултатите от ограничаването на инцидента и възстановяването от него в доклада за реакция при инциденти, свързани с информационната сигурност. Докладът се представя на 3-тото равнище на пренасочване чрез защитена електронна поща или по друг договорен начин на комуникация.

Страната, която носи отговорност, прави преглед на резултатите от ограничаването и възстановяването и:

- отново свързва регистъра, в случай че връзката е била прекъсната;
- осигурява комуникация относно инцидентите с екипите за регистрация;
- приключва инцидента.

ЕУИ следва да включва — по сигурен начин — съответни подробни данни в доклада за инцидента, свързан с информационната сигурност, за да се гарантира последователно записване и комуникация и да се даде възможност за предприемане на бързи и подходящи действия за ограничаване на инцидента. След като приключи инцидента, вързан с информационната сигурност, ЕУИ представя своевременно окончателния доклад за него.

9.7. Наблюдение, изграждане на капацитет и непрекъснато подобрение

ЕУИ ще представя доклади за всички свързани със сигурността инциденти на 3-тото равнище на пренасочване. Докладите ще се използват от това равнище на пренасочване, за да се определи следното:

- слабостите при проверките за сигурност и/или операцията, която трябва да бъде подсилена;
- евентуалната необходимост от подобряване на тази процедура, за да се повиши ефективността ѝ по отношение на реакцията при инциденти;

- възможностите за обучение и изграждане на капацитет за по-нататъшно укрепване на устойчивостта на системите на регистъра по отношение на информационната сигурност, намаляване на риска от бъдещи инциденти и свеждане до минимум на тяхното въздействие.

10. УПРАВЛЕНИЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ

Управлението на информационната сигурност има за цел да гарантира поверителността, интегритета и наличността на класифицираната информация, данни и ИТ услуги на дадена организация. В допълнение към техническите компоненти, включително тяхното проектиране и изпитване (вж. LTS), са необходими следните Общи работни процедури, за да бъдат изпълнени изискванията за сигурност за временното решение.

10.1. Разпознаване на чувствителната информация

Доколко е чувствителна дадена информация се преценява по отражението върху стопанската дейност (например финансови загуби, накърняване на репутацията, законови нарушения...), което би имало евентуалното нарушение на сигурността, свързано с тази информация.

Чувствителните информационни активи се обозначават като такива въз основа на отражението им върху свързването.

Степента на чувствителност на тази информация се оценява по скалата на чувствителност, приложима за въпросното свързване и описана подробно в раздел „Разглеждане на инциденти, свързани с информационната сигурност“ от настоящия документ.

10.2. Степени на чувствителност на информационните активи

Веднъж обозначен, информационният актив се класифицира по следните правила:

- при определянето на най-малко един висок („HIGH“) клас на поверителност, на интегритет или на достъпност активът се класифицира като ETS CRITICAL;
- при определянето на най-малко един среден („MEDIUM“) клас на поверителност, на интегритет или на достъпност активът се класифицира като ETS SENSITIVE;
- при определянето само на нисък („LOW“) клас на поверителност, на интегритет или на достъпност активът се класифицира като ETS LIMITED.

10.3. Определяне на собственик на информационните активи

Всички информационни активи следва да имат определен собственик. Информационните активи на CTE, които принадлежат към връзката между EUTL и SSTL или са свързани с нея, следва да бъдат включени в съвместен инвентарен списък на активите, поддържан от двете страни. Информационните активи на CTE извън връзката между EUTL и SSTL следва да бъдат включени в инвентарен списък на активите, поддържан от съответната страна.

Страните се договарят за собствеността върху всеки информационен актив, принадлежащ към връзката между EUTL и SSTL или свързан с нея. Собственикът на даден информационен актив е отговорен за оценката на неговата чувствителност.

Собственикът следва да има опит, съответстващ на стойността на записани(те) му актив(и). Отговорността на собственика за актива(ите) и задължението му за поддържане на изискваната поверителност, интегритет и наличност следва да бъдат договорени и формализирани.

10.4. Регистриране на чувствителна информация

Цялата чувствителна информация се регистрира в списъка с чувствителна информация (СЧИ).

Когато е целесъобразно, се взема предвид и се регистрира в СЧИ съвкупността от чувствителна информация, която би могла да доведе до по-голямо въздействие от въздействието на само едно сведение (например съвкупност от информация, съхранявана в базата данни на системата).

Списъкът с чувствителна информация не е статичен. Заплахи, слаби места, вероятност за настъпване на засягащи активи инциденти, свързани със сигурността, или последствия от такива инциденти могат да бъдат променяни, без това да се указва по какъвто и да е начин и в работата на регистрационните системи могат да бъдат въвеждани нови активи.

Поради това СЧИ се преразглежда редовно и всяка нова информация, определена като чувствителна, незабавно се регистрира в него.

Списъкът включва най-малко следните сведения за всяко вписване:

- описание на информацията
- собственик на информацията

- степен на чувствителност
- указание дали информацията включва лични данни
- допълнителна информация при необходимост

10.5. Боравене с чувствителна информация

Когато чувствителна информация се обработва извън връзката между Регистъра на Съюза и Швейцарския регистър, тя се третира в съответствие с указанията за боравене с чувствителна информация.

Чувствителната информация, обработвана чрез връзката между Регистъра на Съюза и Швейцарския регистър, се третира от страните в съответствие с изискванията за сигурност.

10.6. Управление на достъпа

Целта на управлението на достъпа е на упълномощените ползватели да се предостави правото да използват дадена услуга, като същевременно се предотврати достъпът на неупълномощени ползватели. Управлението на достъпа понякога се нарича също „управление на правата“ или „управление на идентичността“.

За временното решение и неговото функциониране двете страни се нуждаят от достъп до следните елементи:

- Уики: среда за сътрудничество за обмен на обща информация, като например планирането на версии;
- инструмента за управление на услугите в областта на информационните технологии (ITSM) за управление на инциденти и проблеми (вж. глава „Подход и стандарти“);
- системата за обмен на съобщения: всяка от страните предоставя защитена система за обмен на съобщения за предаване на съобщенията, съдържащи данните за трансакции.

Администраторът на Швейцарския регистър и централният администратор за Съюза гарантират, че достъпът до тях е актуален и изпълняват ролята на звена за контакт за своите страни по отношение на дейностите по управление на достъпа. Заявките за достъп се обработват в съответствие с процедурите за изпълнение на заявки.

10.7. Управление на сертификати/ключове

Всяка от страните е отговорна за управлението на своите сертификати/ключове (генериране, регистриране, съхранение, инсталиране, използване, подновяване, анулиране, създаване на резервни копия и възстановяване на сертификати/ключове). Както е посочено в Техническите стандарти за свързването (LTS), се използват само електронни сертификати, издадени от сертифициращия орган (CO), на които се доверяват и двете страни. Боравенето със сертификати/ключове и съхранението им трябва да се извършват в съответствие с разпоредбите, определени в указанията за боравене с чувствителна информация.

Всяко анулиране и/или подновяване на сертификати и ключове се координира от двете страни. Това се извършва в съответствие с процедурите за изпълнение на заявки.

Администраторът на Швейцарския регистър и централният администратор за Съюза ще обменят сертификати/ключове чрез сигурни средства за комуникация в съответствие с разпоредбите, предвидени в указанията за боравене с чувствителна информация.

Всяка проверка на сертификати/ключове между страните по какъвто и да е начин ще се извършва по различен от обичайния канал за връзка (out-of-band).