Rada
Unii Europejskiej

Bruksela, 24 czerwca 2020 r.
(OR. en)

Międzyinstytucjonalny numer referencyjny:
2020/0123(NLE)

9068/20
ADD 1

ENV 373
CLIMA 123
ENER 213
IND 83
COMPET 289
MI 196
ECOFIN 532
TRANS 276
AELE 5
CH 11

WNIOSEK

Od:	Sekretarz generalna Komisji Europejskiej (podpisał dyrektor Jordi AYET PUIGARNAU)
Data otrzymania:	23 czerwca 2020 r.
Do:	Jeppe TRANHOLM-MIKKELSEN, Sekretarz Generalny Rady Unii Europejskiej
Nr dok. Kom.:	COM(2020) 255 final - Annex
Dotyczy:	ZAŁĄCZNIK do wniosku dotyczącego decyzji Rady w sprawie stanowiska, jakie ma zostać zajęte w imieniu Unii Europejskiej w ramach Wspólnego Komitetu ustanowionego Umową między Unią Europejską a Konfederacją Szwajcarską w sprawie powiązania ich systemów handlu uprawnieniami do emisji gazów cieplarnianych, w odniesieniu do przyjęcia wspólnych procedur operacyjnych

Delegacje otrzymują w załączeniu dokument COM(2020) 255 final - Annex.

Zał.: COM(2020) 255 final - Annex

KOMISJA
EUROPEJSKA

Bruksela, dnia 23.6.2020 r.
COM(2020) 255 final

ANNEX

ZAŁĄCZNIK

do

wniosku dotyczącego decyzji Rady

w sprawie stanowiska, jakie ma zostać zajęte w imieniu Unii Europejskiej w ramach Wspólnego Komitetu ustanowionego Umową między Unią Europejską a Konfederacją Szwajcarską w sprawie powiązania ich systemów handlu uprawnieniami do emisji gazów cieplarnianych, w odniesieniu do przyjęcia wspólnych procedur operacyjnych

DECYZJA NR 1/2020 WSPÓLNEGO KOMITETU USTANOWIONEGO NA MOCY UMOWY MIĘDZY UNIĄ EUROPEJSKĄ A KONFEDERACJĄ SZWAJCARSKĄ W SPRAWIE POWIĄZANIA ICH SYSTEMÓW HANDLU UPRAWNIENIAMI DO EMISJI GAZÓW CIEPLARNIANYCH

z dnia [...] r.

dotycząca wspólnych procedur operacyjnych

WSPÓLNY KOMITET

uwzględniając Umowę między Unią Europejską a Konfederacją Szwajcarską w sprawie powiązania ich systemów handlu uprawnieniami do emisji gazów cieplarnianych[1] (zwaną dalej „umową"), w szczególności jej art. 3,

a także mając na uwadze, co następuje:

(1) W decyzji nr 2/2019 Wspólnego Komitetu z dnia 5 grudnia 2019 r. zmieniono załączniki I i II do umowy, tym samym spełniając warunki wymagane do ustanowienia powiązania, które określono w umowie.

(2) W następstwie przyjęcia decyzji nr 2/2019 Wspólnego Komitetu i na podstawie art. 21 ust. 3 umowy strony wymieniły się swoimi instrumentami ratyfikacji lub zatwierdzenia, ponieważ uznały, że spełnione zostały wszystkie warunki wymagane do ustanowienia powiązania, które określono w umowie.

(3) Zgodnie z art. 21 ust. 4 umowy weszła ona w życie dnia 1 stycznia 2020 r.

(4) Na podstawie art. 3 ust. 6 umowy administrator rejestru Szwajcarii i centralny administrator Unii powinni określić wspólne procedury operacyjne związane z kwestiami technicznymi lub innymi kwestiami, które są niezbędne dla funkcjonowania powiązania między dziennikiem transakcji Unii Europejskiej (EUTL) rejestru Unii a dodatkowym dziennikiem transakcji Szwajcarii (SSTL) rejestru Szwajcarii, uwzględniając priorytety zawarte w prawodawstwie krajowym. Wspólne procedury operacyjne powinny stać się skuteczne z chwilą ich przyjęcia w drodze decyzji Wspólnego Komitetu.

(5) Zgodnie z art. 13 ust. 1 umowy Wspólny Komitet powinien uzgodnić wytyczne techniczne celem zapewnienia prawidłowego wykonania umowy, w tym kwestie techniczne lub inne kwestie, które są niezbędne dla funkcjonowania powiązania, uwzględniając priorytety zawarte w prawodawstwie krajowym. Wytyczne techniczne można opracować w ramach grupy roboczej utworzonej na podstawie art. 12 ust. 5 umowy. Grupa robocza powinna składać się co najmniej z administratora rejestru Szwajcarii i centralnego administratora rejestru Unii i powinna wspierać Wspólny Komitet w wykonywaniu jego funkcji zgodnie z art. 13 umowy.

(6) Z uwagi na techniczny charakter wytycznych i konieczność dostosowania ich do bieżących zmian wytyczne techniczne przygotowane przez administratora rejestru Szwajcarii i centralnego administratora Unii powinny zostać przedłożone Wspólnemu Komitetowi w celach informacyjnych lub, w stosownych przypadkach, w celu zatwierdzenia,

[1] Dz.U. L 322 z 7.12.2017, s. 3.

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

Niniejszym przyjmuje się wspólne procedury operacyjne załączone do niniejszej decyzji.

Artykuł 2

Niniejszym tworzy się grupę roboczą na mocy art. 12 ust. 5 umowy. Grupa robocza wspiera Wspólny Komitet w zapewnieniu prawidłowego wykonania umowy, w tym w przygotowaniu wytycznych technicznych dotyczących wdrożenia wspólnych procedur operacyjnych.

Grupa robocza składa się co najmniej z administratora rejestru Szwajcarii i centralnego administratora rejestru Unii.

Artykuł 3

Niniejsza decyzja wchodzi w życie z dniem jej przyjęcia.

Sporządzono w Brukseli w języku angielskim dnia XX 2020 r.

W imieniu Wspólnego Komitetu

Sekretarz ze strony Unii Europejskiej *Przewodniczący* *Sekretarz ze strony Szwajcarii*

DODATEK

ZAŁĄCZNIK

WSPÓLNE PROCEDURY OPERACYJNE

na podstawie art. 3 ust. 6 Umowy między Unią Europejską a Konfederacją Szwajcarską w sprawie powiązania ich systemów handlu uprawnieniami do emisji gazów cieplarnianych

- Procedury dotyczące tymczasowego rozwiązania -

1. SŁOWNICZEK

Tabela 1–1 Akronimy i definicje

Akronim/termin	Definicja
Centrum certyfikacji	Podmiot, który wydaje certyfikaty elektroniczne
CH	Konfederacja Szwajcarska
ETS	System handlu emisjami
UE	Unia Europejska
IMT	Zespół ds. zarządzania incydentami
Zasób informacyjny	Informacja, która ma wartość dla przedsiębiorstwa lub organizacji
IT	Technologia informacyjna
ITIL	*Information Technology Infrastructure Library* – Biblioteka dokumentów dotyczących zarządzania infrastrukturą IT
ITSM	Zarządzanie usługami informatycznymi
LTS	Normy techniczne powiązania
Rejestr	System rejestracji uprawnień przyznanych na podstawie ETS służący do śledzenia własności uprawnień utrzymywanych na kontach elektronicznych
RFC	Wniosek o zmianę
SIL	Wykaz danych szczególnie chronionych
SR	Wniosek o usługę
Wiki	Strona internetowa umożliwiająca użytkownikom wymianę informacji i wiedzy w drodze dodawania lub dostosowywania treści bezpośrednio przez przeglądarkę internetową

2. WPROWADZENIE

Umowa między Unią Europejską a Konfederacją Szwajcarską w sprawie powiązania ich systemów handlu uprawnieniami do emisji gazów cieplarnianych z dnia 23 listopada 2017 r. („umowa") przewiduje wzajemne uznawanie uprawnień do emisji, które można wykorzystać na potrzeby dostosowania się do wymogów systemu handlu uprawnieniami do emisji Unii Europejskiej („EU ETS") lub systemu handlu uprawnieniami do emisji Szwajcarii („ETS Szwajcarii"). W celu uruchomienia powiązania między EU ETS a ETS Szwajcarii ustanowione zostanie bezpośrednie powiązanie między dziennikiem transakcji Unii Europejskiej (EUTL) rejestru Unii a dodatkowym dziennikiem transakcji Szwajcarii (SSTL) rejestru Szwajcarii, co umożliwi bezpośrednie przekazywanie między rejestrami uprawnień do emisji wydanych w ramach któregokolwiek z ETS (art. 3 ust. 2 umowy). W celu uruchomienia powiązania między EU ETS i ETS Szwajcarii do maja 2020 r. lub możliwie szybko po tej dacie zostanie wdrożone tymczasowe rozwiązanie. Strony współpracują w celu jak najszybszego zastąpienia tymczasowego rozwiązania stałym powiązaniem rejestrów (załącznik II do umowy).

Zgodnie z art. 3 ust. 6 umowy administrator rejestru Szwajcarii i centralny administrator Unii określają wspólne procedury operacyjne związane z kwestiami technicznymi lub innymi kwestiami, które są niezbędne dla funkcjonowania powiązania, uwzględniając priorytety zawarte w prawodawstwie krajowym. Wspólne procedury operacyjne opracowane przez administratorów stają się skuteczne z chwilą ich przyjęcia w drodze decyzji Wspólnego Komitetu.

Wspólne procedury operacyjne w formie przedstawionej w niniejszym dokumencie mają zostać przyjęte w przez Wspólny Komitet jego decyzją nr 1/2020. Zgodnie ze wspomnianą decyzją Wspólny Komitet zwraca się do administratora rejestru Szwajcarii i centralnego administratora Unii o opracowanie dalszych wytycznych technicznych celem uruchomienia powiązania oraz o zapewnienie, aby były one stale dostosowywane do postępu technicznego i nowych wymogów związanych z bezpieczeństwem i ochroną tego powiązania oraz jego skutecznym i sprawnym funkcjonowaniem.

2.1. Zakres

Niniejszy dokument odzwierciedla wspólne porozumienie stron umowy w kwestii ustanowienia podstaw proceduralnych powiązania między rejestrami EU ETS i ETS Szwajcarii. Chociaż nakreślono w nim ogólne wymogi proceduralne dotyczące operacji, do uruchomienia powiązania potrzebne będą dalsze wytyczne techniczne.

Jeżeli chodzi o prawidłowe funkcjonowanie, powiązanie będzie wymagało specyfikacji technicznych do dalszego uruchomienia powiązania. Zgodnie z art. 3 ust. 7 umowy kwestie te szczegółowo opisano w dokumencie dotyczącym norm technicznych powiązania przyjętym odrębną decyzją Wspólnego Komitetu.

Wspólne procedury operacyjne mają na celu zapewnienie, aby usługi informatyczne związane z funkcjonowaniem powiązania między rejestrami EU ETS i ETS Szwajcarii były świadczone skutecznie i sprawnie, szczególnie jeżeli chodzi o realizację wniosków o usługę, usuwanie awarii usług, naprawianie problemów, jak również realizację rutynowych zadań operacyjnych zgodnie z międzynarodowymi normami zarządzania usługami informatycznymi.

W przypadku uzgodnionego tymczasowego rozwiązania potrzebne będą jedynie następujące, przedstawione w niniejszym dokumencie wspólne procedury operacyjne:

- zarządzanie incydentami;

- zarządzanie problemami;
- realizacja wniosków;
- zarządzanie zmianą;
- zarządzanie wersjami;
- zarządzanie incydentami związanymi z bezpieczeństwem informacji;
- zarządzanie bezpieczeństwem informacji.

Po wdrożeniu stałego powiązania rejestrów w późniejszym terminie wspólne procedury operacyjne należy odpowiednio dostosować i uzupełnić.

2.2. Adresaci

Przedmiotowe wspólne procedury operacyjne są skierowane do zespołów wsparcia technicznego rejestrów UE i Szwajcarii.

3. PODEJŚCIE I NORMY

Poniższe zasady dotyczą wszystkich wspólnych procedur operacyjnych:

- UE i Szwajcaria zgadzają się, że wspólne procedury operacyjne określa się na podstawie ITIL (biblioteka dokumentów dotyczących zarządzania infrastrukturą (*Information Technology Infrastructure Library*), wersja 3). Praktyki wywodzące się z tej normy wykorzystuje się wielokrotnie i dostosowuje się je do szczególnych potrzeb tymczasowego rozwiązania;
- komunikacja i koordynacja niezbędne do realizacji wspólnych procedur operacyjnych między obiema stronami odbywają się za pośrednictwem centrów obsługi rejestrów Szwajcarii i UE. Zadanie zawsze przydziela się w ramach jeden ze stron;
- ewentualne spory dotyczące postępowania ze wspólnymi procedurami operacyjnymi wspólnie analizują i rozpatrują oba centra obsługi. Jeżeli nie uda się osiągnąć porozumienia, obowiązek ustalenia wspólnego rozwiązania przekazuje się na kolejny szczebel;

Kolejne szczeble	**UE**	**CH**
Pierwszy szczebel	Unijne centrum obsługi	Szwajcarskie centrum obsługi
Drugi szczebel	Unijny kierownik ds. operacji (*EU Operations Manager*)	Szwajcarski kierownik ds. aplikacji rejestru (*CH Registry Application Manager*)
Trzeci szczebel	Wspólny Komitet (może przekazać ten obowiązek zgodnie z art. 12 ust. 5 umowy)	
Czwarty szczebel	Wspólny Komitet, jeżeli na trzecim szczeblu przekazano ten obowiązek	

- każda ze stron może określić procedury dotyczące funkcjonowania własnego systemu rejestru, uwzględniając wymogi i interfejsy związane z przedmiotowym wspólnymi procedurami operacyjnymi;

- do obsługi wspólnych procedur operacyjnych wykorzystuje się narzędzie zarządzania usługami informatycznymi (*IT Service Management* – ITSM), w szczególności do zarządzania incydentami, zarządzania problemami i realizacji wniosków oraz do komunikacji między stronami;
- możliwa jest również wymiana informacji za pośrednictwem poczty elektronicznej;
- obie strony zapewniają spełnienie wymogów dotyczących bezpieczeństwa informacji zgodnie z instrukcjami postępowania z informacjami.

4. ZARZĄDZANIE INCYDENTAMI

Proces zarządzania incydentami ma na celu jak najszybsze przywrócenie usług informatycznych do normalnego poziomu usług przy jak najmniejszym zakłóceniu działalności.

W ramach zarządzania incydentami należy również zawsze rejestrować incydenty na potrzeby sprawozdawczości i współpracować z innymi procesami, aby stale dążyć do doskonałości.

- W ogólnej perspektywie zarządzanie incydentami składa się z następujących działań:
- wykrywania i rejestracji incydentów;
- klasyfikacji i wstępnego wsparcia;
- badania i diagnozy;
- rozwiązania i przywrócenia do stanu używalności;
- zamknięcia incydentu.

Na wszystkich etapach cyklu życia incydentu proces zarządzania incydentami odpowiada za ciągłe zarządzanie własnością, monitorowanie, śledzenie i komunikację.

4.1. Wykrywanie i rejestracja incydentów

Incydent może zostać wykryty przez zespół wsparcia, automatyczne narzędzia monitorujące lub personel techniczny wykonujący rutynowe działania kontrolne.

Po wykryciu incydent musi zostać zarejestrowany i opatrzony niepowtarzalnym identyfikatorem, który umożliwia odpowiednie śledzenie i monitorowanie incydentu. Niepowtarzalnym identyfikatorem incydentu jest identyfikator przydzielony w ramach wspólnego systemu zgłaszania przez centrum obsługi strony (albo UE, albo Szwajcarii), która poinformowała o incydencie, i należy go stosować w całej komunikacji związanej z tym incydentem.

W przypadku wszystkich incydentów punktem kontaktowym powinno być centrum obsługi strony, która zarejestrowała zgłoszenie.

4.2. Klasyfikacja i wstępne wsparcie

Klasyfikacja incydentu ma na celu zrozumienie, którego systemu lub której usługi on dotyczy i w jakim stopniu, oraz ich identyfikację. Jeżeli klasyfikacja ma być skuteczna, powinna już za pierwszym razem przydzielić incydent do właściwego zasobu, aby przyspieszyć jego rozwiązanie.

W ramach etapu klasyfikacji należy nadać incydentowi kategorię i priorytet, uwzględniając jego wpływ i pilność, aby został rozwiązany w terminie odpowiadającym temu priorytetowi.

Jeżeli incydent może mieć skutki dla poufności lub integralności danych szczególnie chronionych lub skutki dla dostępności systemu, incydent należy określić również jako

incydent związany z bezpieczeństwem informacji i zarządzać nim zgodnie z procesem określonym w rozdziale „Zarządzanie incydentami związanymi z bezpieczeństwem informacji" niniejszego dokumentu.

Jeżeli jest to możliwe, centrum obsługi, które zarejestrowało zgłoszenie, przeprowadza wstępną diagnozę. W tym celu centrum obsługi sprawdzi, czy incydent jest znanym błędem. Jeżeli tak, to sposób rozwiązania lub obejścia problemu jest już znany i udokumentowany.

Jeżeli centrum obsługi uda się rozwiązać incydent, to zamyka incydent na tym etapie, ponieważ główny cel zarządzania incydentami został spełniony (a mianowicie szybkie przywrócenie działania usługi u użytkownika końcowego). Jeżeli nie, to centrum obsługi przekaże incydent do odpowiedniego zespołu ds. rozwiązywania problemów celem dalszego zbadania i zdiagnozowania.

4.3. Badanie i diagnoza

Badanie i diagnozę incydentu przeprowadza się, jeżeli centrum obsługi nie było w stanie rozwiązać incydentu w ramach wstępnej diagnozy i zgodnie z procedurą przekazało problem na wyższy szczebel. Przekazanie incydentu jest pełnoprawną częścią procesu badania i diagnozy.

Częstą praktyką stosowaną na etapie badania i diagnozy jest próba odtworzenia incydentu w warunkach kontrolowanych. Istotnym elementem badania i diagnozy incydentu jest zrozumienie właściwej kolejności wydarzeń, które doprowadziły do incydentu.

Przekazanie oznacza przyznanie, że incydentu nie da się rozwiązać na obecnym szczeblu wsparcia technicznego i należy go przekazać do grupy wsparcia wyższego szczebla lub do drugiej strony. Przekazanie może się odbyć na dwa sposoby: poziomo (funkcjonalnie) lub pionowo (hierarchicznie).

Centrum obsługi, które zarejestrowało incydent i uruchomiło procedurę zarządzania nim, jest odpowiedzialne za przekazanie incydentu do odpowiedniego zasobu oraz za śledzenie ogólnego statusu incydentu i monitorowanie, do kogo jest przypisany.

Strona, której przypisano incydent, jest odpowiedzialna za zapewnienie, aby działania, o które wnioskowano, zostały przeprowadzone terminowo, oraz za przesłanie informacji zwrotnej do centrum obsługi swojej strony.

4.4. Rozwiązanie i przywrócenie do stanu używalności

Rozwiązanie incydentu i przywrócenie do stanu używalności przeprowadza się po pełnym zrozumieniu incydentu. Znalezienie rozwiązania incydentu oznacza, że zidentyfikowano sposób naprawienia problemu. Faktyczne zastosowanie rozwiązania to etap przywrócenia do stanu używalności.

Gdy odpowiednie zasoby usuną awarię usługi, incydent przekazuje się z powrotem do odpowiedniego centrum obsługi, które zarejestrowało incydent, aby potwierdziło użytkownikowi, który zgłosił incydent, że błąd został naprawiony i że incydent można zamknąć. Ustalenia z prac nad incydentem należy zarejestrować na przyszłe potrzeby.

Przywrócenia do stanu używalności może dokonać zespół wsparcia informatycznego lub użytkownik końcowy po otrzymaniu odpowiednich instrukcji.

4.5. Zamknięcie incydentu

Zamknięcie to ostatni etap procesu zarządzania incydentami i odbywa się wkrótce po rozwiązaniu incydentu.

Spośród działań, które należy przeprowadzić na etapie zamknięcia, najważniejsze są następujące:

- weryfikacja wstępnej kategorii przypisanej do incydentu;
- odpowiednie zgromadzenie wszystkich informacji związanych z incydentem;
- odpowiednie udokumentowanie incydentu i aktualizacja bazy wiedzy;
- odpowiednie powiadomienie wszystkich zainteresowanych stron bezpośrednio lub pośrednio dotkniętych incydentem.

Incydent jest oficjalnie zamknięty po przeprowadzeniu etapu zamknięcia incydentu przez centrum obsługi i poinformowaniu o tym drugiej strony.

Jeżeli incydent został zamknięty, już się go nie otwiera. Jeżeli niedługo później incydent powtórzy się, nie otwiera się ponownie pierwotnego incydentu, ale rejestruje się nowy.

Jeżeli zarówno unijne, jak i szwajcarskie centrum obsługi śledzi dany incydent, ostateczne zamknięcie jest obowiązkiem centrum obsługi, które zarejestrowało zgłoszenie.

5. ZARZĄDZANIE PROBLEMAMI

Niniejsza procedura dotyczy sytuacji, gdy zidentyfikowano problem, a tym samym uruchomiono proces zarządzania problemami. Zarządzanie problemami skupia się na poprawie jakości i ograniczeniu liczby zgłaszanych incydentów. Jeden problem może być przyczyną jednego incydentu lub większej ich liczby. Gdy incydent zostanie zgłoszony, celem zarządzania incydentami jest jak najszybsze przywrócenie działania usługi, co może obejmować zastosowanie obejść. Po zarejestrowaniu problemu należy zbadać jego podstawową przyczynę, aby wskazać zmiany, których wprowadzenie zagwarantuje, że problem i powiązane z nim incydenty nie będą więcej występowały.

5.1. Identyfikacja i rejestracja problemu

W zależności od strony, która utworzyła zgłoszenie, punktem kontaktowym w kwestiach dotyczących danego problemu będzie albo unijne, albo szwajcarskie centrum obsługi.

Niepowtarzalnym identyfikatorem problemu jest identyfikator przydzielony przez narzędzie zarządzania usługami informatycznymi (ITSM). Należy go stosować w całej komunikacji związanej z tym problemem.

Procedura zarządzania problemem może zostać uruchomiona w wyniku incydentu lub rozpoczęta z własnej inicjatywy celem naprawienia problemów wykrytych w systemie na dowolnym etapie.

5.2. Określanie priorytetu problemów

Tak samo jak w przypadku incydentów problemom można nadać kategorię odpowiednią dla ich wagi i priorytetu, aby ułatwić ich śledzenie, uwzględniając wpływ powiązanych incydentów i częstotliwość ich występowania.

5.3. Badanie i diagnoza problemu

Każda ze stron może zgłosić problem, a centrum obsługi strony, która rozpoczyna proces, będzie odpowiedzialne za zarejestrowanie problemu, przypisanie go do odpowiedniego zasobu i śledzenie jego ogólnego statusu.

Zespół ds. rozwiązywania problemów, któremu przekazano problem, ma obowiązek zająć się tym problemem w stosownym terminie i komunikować się z centrum obsługi.

Jeżeli zostaną do tego wezwane, obie strony odpowiadają za zapewnienie, aby przydzielone działania zostały przeprowadzone, oraz za przesłanie informacji zwrotnej do centrum obsługi swojej strony.

5.4. Rozwiązanie

Zespół ds. rozwiązywania problemów, któremu przydzielono problem, odpowiada za rozwiązanie tego problemu i za przesłanie stosownych informacji do centrum obsługi swojej strony.

Ustalenia z prac nad problemem należy zarejestrować na przyszłe potrzeby.

5.5. Zamknięcie problemu

Problem jest oficjalnie zamknięty, gdy zostanie naprawiony dzięki wprowadzeniu zmiany. Etap zamknięcia problemu przeprowadza centrum obsługi, które zarejestrowało problem i poinformowało centrum obsługi drugiej strony.

6. REALIZACJA WNIOSKÓW

Proces realizacji wniosków obejmuje kompleksowe zarządzanie wnioskiem dotyczącym nowej lub istniejącej usługi od momentu rejestracji i zatwierdzenia do zamknięcia. Wnioski o usługę to zazwyczaj niewielkie, określone wcześniej, powtarzalne, częste, uprzednio zatwierdzone wnioski o charakterze proceduralnym.

Poniżej przedstawiono najważniejsze działania, które należy przeprowadzić:

6.1. Wszczęcie procedury dotyczącej wniosku

Unijne lub szwajcarskie centrum obsługi otrzymuje informacje dotyczące wniosku o usługę pocztą elektroniczną, telefonicznie, za pośrednictwem narzędzia zarządzania usługami informatycznymi (ITSM) lub jakiegokolwiek innego uzgodnionego kanału komunikacji.

6.2. Rejestracja i analiza wniosku

W przypadku wszystkich wniosków o usługę punktem kontaktowym będzie albo unijne, albo szwajcarskie centrum obsługi w zależności od strony, która zgłosiła wniosek o usługę. Odpowiednie centrum obsługi będzie odpowiedzialne za rejestrację i analizę wniosku o usługę z dochowaniem należytej staranności.

6.3. Zatwierdzenie wniosku

Pracownik centrum obsługi strony, która zgłosiła wniosek o usługę, sprawdza, czy konieczne jest uzyskanie jakichkolwiek zgód od drugiej strony, a jeżeli tak, rozpoczyna proces ich uzyskania. Jeżeli wniosek o usługę nie zostanie zatwierdzony, centrum obsługi odpowiednio aktualizuje i zamyka zgłoszenie.

6.4. Realizacja wniosków

Niniejszy etap jest poświęcony skutecznemu i sprawnemu rozpatrywaniu wniosków o usługę. Należy rozróżnić następujące przypadki:

- realizacja wniosku o usługę wpływa wyłącznie na jedną stronę. W takim przypadku dana strona zleca odpowiednie prace i koordynuje ich wykonanie;
- wykonanie wniosku o usługę wpływa zarówno na UE, jak i Szwajcarię. W takim przypadku centra obsługi zlecają prace w obszarach, za które są odpowiedzialne. Centra obsługi koordynują między sobą proces realizacji

wniosku o usługę. Ogólna odpowiedzialność spoczywa na centrum obsługi, które otrzymało wniosek o usługę i wszczęło procedurę w jego sprawie.

Po rozpatrzeniu wniosku o usługę, należy nadać mu status wskazujący, że został rozpatrzony.

6.5. Przekazanie wniosku

W razie potrzeby centrum obsługi może przekazać nierozpatrzony wniosek o usługę do odpowiedniego zasobu (osoby trzeciej).

Wnioski przekazuje się do odpowiednich osób trzecich, tj. wnioski otrzymane przez unijne centrum obsługi muszą przejść przez szwajcarskie centrum obsługi, zanim zostaną przekazane do szwajcarskiej osoby trzeciej – i odwrotnie.

Osoba trzecia, której przekazano wniosek o usługę, ma obowiązek zająć się wnioskiem o usługę w stosownym terminie i komunikować się z centrum obsługi, które przekazało wniosek o usługę.

Centrum obsługi, które zarejestrowało wniosek o usługę, jest odpowiedzialne za śledzenie ogólnego statusu wniosku o usługę i monitorowanie, do kogo jest przypisany.

6.6. Przegląd realizacji wniosku

Właściwe centrum obsługi przedkłada zapis wniosku o usługę do ostatecznej kontroli jakości przed zamknięciem wniosku. Ma to na celu zagwarantowanie, że wniosek o usługę został faktycznie zrealizowany i że dostarczono w odpowiednim stopniu szczegółowości wszystkie informacje niezbędne do opisania cyklu życia wniosku. Ustalenia z prac nad wnioskiem należy ponadto zarejestrować na przyszłe potrzeby.

6.7. Zamknięcie wniosku

Jeżeli strony, którym przypisano wniosek, zgadzają się, że wniosek o usługę został zrealizowany i wnioskodawca uważa sprawę za rozwiązaną, należy nadać wnioskowi status „zamknięty”.

Wniosek o usługę jest formalnie zamknięty, gdy centrum obsługi, które zarejestrowało wniosek o usługę, przeprowadziło etap zamknięcia wniosku i poinformowało centrum obsługi drugiej strony.

7. ZARZĄDZANIE ZMIANĄ

Celem procesu jest zapewnienie stosowania standaryzowanych metod i procedur do sprawnego i szybkiego zarządzania wszystkimi zmianami dotyczącymi kontroli infrastruktury informatycznej, aby zminimalizować liczbę incydentów i ich wpływ na usługę. Zmiany w infrastrukturze informatycznej mogą powstać w reakcji na problemy lub na wymogi narzucone z zewnątrz, np. zmiany w przepisach, lub mogą zostać aktywnie wprowadzone w wyniku dążenia do osiągnięcia większej sprawności i skuteczności lub w celu umożliwienia bądź odzwierciedlenia inicjatyw dotyczących funkcjonowania.

Proces zarządzania zmianami obejmuje szereg różnych działań, w ramach których zbiera się wszystkie informacje szczegółowe na temat wniosku o zmianę na potrzeby przyszłego śledzenia. Procesy te gwarantują, że zmiana zostanie zatwierdzona i przetestowana przed przekazaniem jej do wdrożenia. Za skuteczne wdrożenie odpowiada proces zarządzania wersjami.

7.1. Wniosek o zmianę

Wniosek o zmianę przedkłada się zespołowi zarządzania zmianą do sprawdzenia i zatwierdzenia. W przypadku wszystkich wniosków o zmianę punktem kontaktowym będzie

albo unijne, albo szwajcarskie centrum obsługi w zależności od strony, która zgłosiła wniosek. Odpowiednie centrum obsługi będzie odpowiedzialne za rejestrację i analizę wniosku o zmianę z dochowaniem należytej staranności.

Wnioski o zmianę mogą powstać w wyniku:

- incydentu, który wywołuje zmianę;
- istniejącego problemu skutkującego zmianą;
- wniosku użytkownika końcowego o wprowadzenie nowej zmiany;
- zmian będących rezultatem bieżącej konserwacji;
- zmian ustawodawczych.

7.2. Ocena i planowanie zmiany

Niniejszy etap obejmuje działania dotyczące oceny i planowania zmiany. Uwzględnia on działania dotyczące określania priorytetów i planowania służące zminimalizowaniu ryzyka i wpływu.

Jeżeli wdrożenie wniosku o zmianę ma skutki zarówno dla UE, jak i Szwajcarii, strona, która zarejestrowała wniosek o zmianę, przedstawia ocenę i plan zmiany drugiej stronie do weryfikacji.

7.3. Zatwierdzanie zmiany

Każdy zarejestrowany wniosek o zmianę musi zostać zatwierdzony na odpowiednim szczeblu.

7.4. Wdrożenie zmiany

Zmiany wdraża się w ramach zarządzania wersjami. Zespoły ds. zarządzania wersjami obu stron stosują swoje własne procesy, które obejmują planowanie i testowanie. Przeglądu zmiany dokonuje się po zakończeniu wdrażania. Aby zagwarantować, że wszystko poszło zgodnie z planem, obowiązujący proces zarządzania zmianami jest stale poddawany przeglądowi i aktualizowany, gdy jest to konieczne.

8. ZARZĄDZANIE WERSJAMI

Wersja to jedna zmiana w usłudze informatycznej lub większa ich liczba zebrane w planie wersji, które muszą zostać zatwierdzone, przygotowane, stworzone, przetestowane i wdrożone jednocześnie. Jedna wersja może oznaczać poprawkę błędu, zmianę w sprzęcie lub w innych komponentach, zmiany w oprogramowaniu, aktualizacje aplikacji, zmiany w dokumentacji lub w procesach. Zawartość każdej wersji organizuje się, testuje i wdraża jako jedną całość.

Zarządzanie wersjami ma na celu planowanie, tworzenie, testowanie i sprawdzanie oraz zapewnianie zdolności do świadczenia zaprojektowanych usług, które spełnią wymagania zainteresowanych stron i pozwolą osiągnąć zamierzone cele. Kryteria akceptacji wszelkich zmian w usłudze zostaną określone i udokumentowane podczas etapu koordynacji projektu i przekazane do zespołów zarządzania wersjami.

Wersja zazwyczaj składa się z szeregu poprawek służących rozwiązaniu problemu i usprawnieniu usługi. Obejmuje nowe lub zmienione oprogramowanie oraz wszelki nowy lub zmieniony sprzęt niezbędne do wdrożenia zatwierdzonych zmian.

8.1. Planowanie wersji

Pierwszy etap procesu polega na przypisaniu zatwierdzonych zmian do pakietów wersji oraz określeniu zakresu i zawartości wersji. W oparciu o te informacje w podprocesie planowania wersji opracowuje się harmonogram tworzenia, testowania i wdrożenia wersji.

W planowaniu należy określić:

- zakres i zawartość wersji;
- ocenę ryzyka i profil ryzyka dotyczące danej wersji;
- klientów/użytkowników, na których dana wersja wpłynie;
- zespół odpowiedzialny za daną wersję;
- strategię dostarczenia i wdrożenia;
- zasoby na potrzeby danej wersji i wdrożenia.

Strony informują się nawzajem o swoich planach dotyczących wersji i planowych pracach konserwacyjnych. Jeżeli dana wersja dotyczy zarówno UE, jak i Szwajcarii, strony koordynują swoje plany i ustalają wspólny termin prac konserwacyjnych.

8.2. Tworzenie i testowanie pakietu wersji

Etap tworzenia i testowania w ramach procesu zarządzania wersjami polega na określeniu metody służącej do wykonania wersji lub pakietu wersji oraz do utrzymania środowisk kontrolowanych przed zmianą środowiska produkcyjnego, jak również testowania wszystkich zmian we wszystkich wdrożonych środowiskach.

Jeżeli dana wersja dotyczy zarówno UE, jak i Szwajcarii, strony koordynują swoje plany dostarczenia i testy. Obejmuje to następujące aspekty:

- sposób i czas dostarczenia składników wersji i komponentów usługi;
- typowy czas realizacji; procedurę na wypadek opóźnienia;
- sposób śledzenia postępów w dostarczaniu i uzyskiwaniu potwierdzenia;
- wskaźniki służące do monitorowania działań w zakresie dostarczenia wersji oraz do ustalenia, czy zakończyły się pomyślnie;
- wspólne przypadki testowe dotyczące istotnych funkcjonalności i zmian.

Po zakończeniu tego podprocesu wszystkie niezbędne elementy wersji są gotowe do przejścia do etapu wdrożenia do środowiska produkcyjnego.

8.3. Przygotowanie wdrożenia

Podproces przygotowania zapewnia, aby plany komunikacji zostały poprawnie określone, a powiadomienia przygotowane do wysłania do wszystkich zainteresowanych stron i użytkowników końcowych, na których zmiany będą miały wpływ, oraz aby wersja była zintegrowana z procesem zarządzania zmianami celem zagwarantowania, że wszystkich zmian dokonuje się w sposób kontrolowany i po zatwierdzeniu przez odpowiednie fora.

Jeżeli dana wersja dotyczy zarówno UE, jak i Szwajcarii, strony koordynują następujące działania:

- zapis wniosków o zmianę na potrzeby ustalenia harmonogramu i przygotowania wdrożenia do środowiska produkcyjnego;

- utworzenie planu wdrożenia;
- metodę cofnięcia zmian, aby w przypadku niepowodzenia wdrożenia można było przywrócić poprzedni stan;
- powiadomienia wysyłane do wszystkich niezbędnych stron;
- zobowiązanie do zatwierdzenia wdrożenia wersji na odpowiednim szczeblu.

8.4. Cofnięcie wersji

Jeżeli wdrożenie nie powiodło się lub podczas testów ustalono, że wdrożenie było nieskuteczne lub nie spełniło uzgodnionych kryteriów akceptacji/jakości, zespoły ds. zarządzania wersjami obu stron muszą cofnąć zmiany i przywrócić poprzedni stan. Należy poinformować wszystkie niezbędne zainteresowane strony, w tym użytkowników końcowych, na których zmiany wpłyną lub których dotyczyły. Z zastrzeżeniem zatwierdzenia proces można rozpocząć od nowa na którymkolwiek z poprzednich etapów.

8.5. Przegląd i zamknięcie wersji

Przegląd wdrożenia powinien obejmować następujące działania:

- zebranie informacji zwrotnych na temat zadowolenia klientów, użytkowników lub zadowolenia ze świadczenia usługi w związku z wdrożeniem (zgromadzenie informacji zwrotnych i ocena ich przydatności dla stałego ulepszania usługi);
- przegląd wszelkich kryteriów jakości, których nie spełniono;
- sprawdzenie kompletności działań, niezbędnych poprawek i zmian;
- upewnienie się, że na koniec wdrożenia nie ma żadnych problemów dotyczących zdolności, zasobów, możliwości lub funkcjonowania;
- sprawdzenie, czy wszystkie problemy, znane błędy i obejścia zostały udokumentowane i zaakceptowane przez klienta, użytkowników końcowych, dział wsparcia operacyjnego i inne strony, których dotyczą zmiany;
- monitorowanie incydentów i problemów wywołanych wdrożeniem (udzielenie wczesnego wsparcia powdrożeniowego zespołom operacyjnym, jeżeli dana wersja spowodowała wzrost ilości pracy);
- aktualizację dokumentacji wsparcia technicznego (tj. dokumentów zawierających informacje techniczne);
- oficjalne przekazanie wdrożenia wersji do działu obsługi usług;
- udokumentowanie wyciągniętych wniosków;
- zebranie podsumowań wersji od zespołów wdrożeniowych;
- oficjalne zamknięcie wersji po weryfikacji zapisu wniosków o zmianę.

9. ZARZĄDZANIE INCYDENTAMI ZWIĄZANYMI Z BEZPIECZEŃSTWEM INFORMACJI

Zarządzanie incydentami związanymi z bezpieczeństwem informacji to proces postępowania z incydentami związanymi z bezpieczeństwem informacji w celu umożliwienia przekazania informacji o incydencie zainteresowanym stronom, które mogły zostać nim dotknięte; oceny incydentu i ustalenia jego priorytetu; oraz reakcji na incydent służącej rozstrzygnięciu kwestii wszelkich faktycznych, podejrzewanych lub możliwych przypadków naruszenia poufności, dostępności lub integralności szczególnie chronionych zasobów informacyjnych.

9.1. Kategoryzacja incydentów związanych z bezpieczeństwem informacji

Wszystkie incydenty, które wpływają na powiązanie między rejestrem Unii i rejestrem Szwajcarii, analizuje się pod kątem ustalenia, czy nastąpiło naruszenie poufności, integralności lub dostępności jakichkolwiek danych szczególnie chronionych, które wpisano do wykazu danych szczególnie chronionych.

Jeżeli doszło do naruszenia, incydent określa się jako incydent związany z bezpieczeństwem informacji, natychmiast rejestruje się go w narzędziu zarządzania usługami informatycznymi (ITSM) i postępuje się z nim zgodnie z procedurą stosowaną w takim przypadku.

9.2. Postępowanie z incydentami związanymi z bezpieczeństwem informacji

Incydenty związane z bezpieczeństwem informacji należą do obowiązków trzeciego szczebla i ich rozwiązaniem zajmuje się specjalny zespół ds. zarządzania incydentami.

Zespół ds. zarządzania incydentami odpowiada za:

- przeprowadzenie pierwszej analizy, nadanie incydentowi kategorii i ocenę wagi incydentu;
- koordynację działań między wszystkimi zainteresowanymi stronami, uwzględniając pełną dokumentację analizy incydentu, decyzje podjęte w celu poradzenia sobie z incydentem i ewentualne rozpoznane słabe punkty;
- w zależności od wagi incydentu związanego z bezpieczeństwem informacji – terminowe przekazanie go na odpowiedni szczebel w celu uzyskania informacji lub decyzji.

W procesie zarządzania bezpieczeństwem informacji wszystkie informacje dotyczące incydentów klasyfikuje się jako dane o najwyższym poziomie wrażliwości, ale w żadnym wypadku nie niższym niż SZCZEGÓLNY POZIOM OCHRONY W ETS.

W przypadku trwającego postępowania lub słabego punktu, który można nieuczciwie wykorzystać, oraz do momentu jego naprawienia informacje klasyfikuje się jako KRYTYCZNY POZIOM OCHRONY W ETS.

9.3. Identyfikacja incydentów związanych z bezpieczeństwem informacji

W zależności od rodzaju zdarzenia związanego z bezpieczeństwem, osoba odpowiedzialna za bezpieczeństwo informacji określa odpowiednie organizacje w celu podjęcia z nimi współpracy i włączenia ich do zespołu ds. zarządzania incydentami.

9.4. Analiza incydentów związanych z bezpieczeństwem informacji

Zespół ds. zarządzania incydentami działa w porozumieniu ze wszystkimi zaangażowanymi organizacjami i odpowiednimi członkami ich zespołów, w stosownych przypadkach, w celu zbadania incydentu. Podczas analizy ustala się skalę utraty poufności, integralności lub dostępności zasobu i ocenia się skutki dla wszystkich organizacji, których dotyczy incydent. Następnie określa się działania wstępne i następcze mające na celu rozwiązanie incydentu i zarządzanie jego wpływem, w tym wpływ tych działań na zasoby.

9.5. Ocena wagi incydentu związanego z bezpieczeństwem informacji, przekazywanie go i związana z nim sprawozdawczość

Po określeniu charakteru każdego nowego incydentu związanego z bezpieczeństwem informacji zespół ds. zarządzania incydentami ocenia jego wagę i rozpoczyna najpilniejsze niezbędne działania zgodnie z wagą incydentu.

9.6. Sprawozdawczość dotycząca reakcji na incydent związany z bezpieczeństwem informacji

Zespół ds. zarządzania incydentami uwzględnia rezultaty działań służących ograniczeniu skutków incydentu i przywróceniu do stanu używalności w sprawozdaniu w sprawie reakcji na incydent związany z bezpieczeństwem informacji. Sprawozdanie przekazuje się na trzeci szczebel za pośrednictwem zabezpieczonej poczty elektronicznej lub innych wspólnie przyjętych metod bezpiecznej komunikacji.

Właściwa strona zapoznaje się z rezultatami działań służących ograniczeniu skutków incydentu i przywróceniu do stanu używalności oraz:

- przywraca połączenie z rejestrem, jeżeli zostało przerwane;
- przekazuje komunikaty dotyczące incydentu zespołom odpowiedzialnym za rejestr;
- zamyka incydent.

Zespół ds. zarządzania incydentami powinien uwzględnić w sprawozdaniu w sprawie incydentu związanego z bezpieczeństwem informacji – stosując bezpieczne metody – istotne dane szczegółowe, aby zapewnić spójną rejestrację i komunikację oraz umożliwić podjęcie szybkich i odpowiednich działań służących ograniczeniu skutków incydentu. Po zakończeniu prac nad sprawozdaniem zespół ds. zarządzania incydentami przedstawia w odpowiednim terminie sprawozdanie końcowe w sprawie incydentu związanego z bezpieczeństwem informacji.

9.7. Monitorowanie, budowanie zdolności i stałe dążenie do doskonałości

Zespół ds. zarządzania incydentami dostarczy sprawozdania w sprawie wszystkich incydentów związanych z bezpieczeństwem informacji na trzeci szczebel. Sprawozdania zostaną wykorzystane na tym szczeblu do ustalenia:

- słabych punktów w mechanizmach kontrolnych lub operacjach dotyczących bezpieczeństwa, które należy wzmocnić;
- ewentualnych potrzeb w kwestii ulepszenia niniejszej procedury, aby zwiększyć skuteczność reakcji na incydenty;
- możliwości dotyczących szkolenia i budowania zdolności w celu dodatkowego wzmocnienia odporności systemów rejestrów w zakresie bezpieczeństwa informacji, ograniczenia ryzyka zaistnienia przyszłych incydentów i zminimalizowania ich wpływu.

10. ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI

Zarządzanie bezpieczeństwem informacji ma na celu zapewnienie poufności, integralności i dostępności należących do danej organizacji niejawnych informacji, danych i usług informatycznych. Poza elementami technicznymi, w tym informacjami na temat ich budowy i testów (zob. normy techniczne powiązania), do spełnienia wymogów w zakresie bezpieczeństwa dotyczących tymczasowego rozwiązania konieczne są następujące wspólne procedury operacyjne:

10.1. Identyfikacja danych szczególnie chronionych

Wrażliwość danych ocenia się poprzez ustalenie, jaki wpływ na działalność (np. straty finansowe, utrata wizerunku, naruszenie przepisów...) miałoby naruszenie bezpieczeństwa związane z takimi danymi.

Szczególnie chronione zasoby informacyjne identyfikuje się na podstawie wpływu, jaki mają na powiązanie.

Poziom wrażliwości tych danych ocenia się zgodnie ze skalą wrażliwości obowiązującą w przypadku przedmiotowego powiązania i opisaną szczegółowo w sekcji niniejszego dokumentu zatytułowanej „Postępowanie z incydentami związanymi z bezpieczeństwem informacji".

10.2. Poziomy wrażliwości zasobów informacyjnych

Po identyfikacji zasobu informacyjnego klasyfikuje go się za pomocą następujących zasad:

- jeżeli określono, że co najmniej jeden z następujących aspektów – poufności, integralności lub dostępności – znajduje się na poziomie WYSOKIM, zasób klasyfikuje się do grupy KRYTYCZNY POZIOM OCHRONY W ETS;
- jeżeli określono, że co najmniej jeden z następujących aspektów – poufności, integralności lub dostępności – znajduje się na poziomie ŚREDNIM, zasób klasyfikuje się do grupy SZCZEGÓLNY POZIOM OCHRONY W ETS;
- jeżeli określono, że następujące aspekty – poufności, integralności lub dostępności – znajdują się wyłącznie na poziomie NISKIM, zasób klasyfikuje się do grupy OGRANICZONY POZIOM OCHRONY W ETS.

10.3. Przypisywanie zasobów informacyjnych do właściciela

Wszystkie zasoby informacyjne powinny być przypisane do określonego właściciela. Zasoby informacyjne ETS należące do powiązania między EUTL i SSTL lub z nim związane powinny zostać zawarte we wspólnym wykazie zasobów utrzymywanym przez obie strony. Zasoby informacyjne ETS poza powiązaniem między EUTL i SSTL powinny zostać zawarte w wykazie zasobów utrzymywanym przez odpowiednią stronę.

Strony uzgodnią, kto jest właścicielem każdego zasobu informacyjnego należącego do powiązania między EUTL i SSTL lub z nim związanego. Właściciel zasobu informacyjnego odpowiada za ocenę jego wrażliwości.

Właściciel powinien posiadać poziom uprzywilejowania stosowny do wartości przypisanego mu zasobu lub przypisanych mu zasobów. Należy uzgodnić i sformalizować odpowiedzialność właściciela za zasób lub zasoby oraz obowiązek utrzymywania wymaganego poziomu poufności, integralności i dostępności.

10.4. Rejestracja danych szczególnie chronionych

Wszystkie dane szczególnie chronione rejestruje się w wykazie danych szczególnie chronionych.

W stosownych przypadkach uwzględnia się i rejestruje w wykazie danych szczególnie chronionych agregację danych szczególnie chronionych, która mogłaby wywołać większy wpływ niż pojedynczy element danych (np. zbiór danych przechowywanych w bazie danych systemu).

Wykaz danych szczególnie chronionych nie jest niezmienny. Zagrożenia, luki w zabezpieczeniach, prawdopodobieństwo lub skutki incydentów związanych

z bezpieczeństwem informacji powiązane z tymi zasobami mogą się zmienić bez ostrzeżenia, a do działalności systemów rejestrów mogą zostać wprowadzone nowe zasoby.

W związku z tym należy dokonywać regularnego przeglądu wykazu danych szczególnie chronionych i natychmiast rejestrować w nim wszelkie nowe dane zidentyfikowane jako szczególnie chronione.

Każdy zapis w wykazie danych szczególnie chronionych obejmuje co najmniej następujące informacje:

- opis danych,
- właściciela danych,
- poziom wrażliwości,
- wskazanie, czy dane zawierają dane osobowe,
- dodatkowe informacje, jeżeli są wymagane.

10.5. Postępowanie z danymi szczególnie chronionymi

Podczas przetwarzania poza powiązaniem między rejestrem Unii i rejestrem Szwajcarii z danymi szczególnie chronionymi postępuje się zgodnie z instrukcjami postępowania z informacjami.

Z danymi szczególnie chronionymi przetwarzanymi w ramach powiązania między rejestrem Unii i rejestrem Szwajcarii postępuje się zgodnie z wymogami stron dotyczącymi bezpieczeństwa.

10.6. Zarządzanie dostępem

Celem zarządzania dostępem jest przyznawanie upoważnionym użytkownikom praw do korzystania z usługi oraz uniemożliwienie dostępu użytkownikom nieupoważnionym. Zarządzanie dostępem jest czasem jest nazywane „zarządzaniem prawami” lub „zarządzaniem tożsamością”.

W przypadku tymczasowego rozwiązania i jego działania obie strony muszą posiadać dostęp do następujących elementów:

- Wiki: środowiska współpracy służącego do wymiany wspólnych informacji, takich jak planowanie wersji;
- narzędzia zarządzania usługami informatycznymi (ITSM) służącego do zarządzania incydentami i problemami (zob. rozdział „Podejście i normy”);
- systemu wymiany wiadomości: każda ze stron zapewnia bezpieczny system przekazywania wymiany wiadomości na potrzeby przesyłania wiadomości zawierających dane dotyczące transakcji.

Administrator rejestru Szwajcarii i centralny administrator Unii zapewniają, aby prawa dostępu były aktualne, i pełnią rolę punktów kontaktowych dla swoich stron w odniesieniu do działań związanych z zarządzaniem dostępem. Wnioski o dostęp rozpatruje się zgodnie z procedurami realizacji wniosków.

10.7. Zarządzanie certyfikatami/kluczami

Każda ze stron odpowiada za zarządzanie własnymi certyfikatami/kluczami (generowanie, rejestracja, przechowywanie, instalacja, stosowanie, odnawianie, cofanie, tworzenie kopii

zapasowej i odzyskiwanie certyfikatów/kluczy). Jak określono w normach technicznych powiązania, stosuje się jedynie certyfikaty elektroniczne wydane przez centrum certyfikacji uznawane przez obie strony. Postępowanie z certyfikatami/kluczami i ich przechowywanie muszą być zgodnie z przepisami zawartymi w instrukcjach postępowania z informacjami.

Strony koordynują między sobą wszelkie cofnięcie lub odnowienie certyfikatów i kluczy. Odbywa się to zgodnie z procedurami realizacji wniosków.

Administrator rejestru Szwajcarii i centralny administrator Unii wymienią się certyfikatami/kluczami za pośrednictwem zabezpieczonych środków komunikacji zgodnie z przepisami określonymi w instrukcjach postępowania z informacjami.

Wszelka weryfikacja certyfikatów/kluczy dokonywana jakąkolwiek metodą pomiędzy stronami odbędzie się w sposób pozapasmowy.