Rat der
Europäischen Union

Brüssel, den 24. Juni 2020
(OR. en)

9068/20
ADD 1

Interinstitutionelles Dossier:
2020/0123 (NLE)

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

VORSCHLAG

Absender:	Herr Jordi AYET PUIGARNAU, Direktor, im Auftrag der Generalsekretärin der Europäischen Kommission
Eingangsdatum:	23. Juni 2020
Empfänger:	Herr Jeppe TRANHOLM-MIKKELSEN, Generalsekretär des Rates der Europäischen Union
Nr. Komm.dok.:	COM(2020) 255 final - Annex
Betr.:	ANHANG des Vorschlags für einen Beschluss des Rates über den im Namen der Europäischen Union in dem durch das Abkommen zwischen der Europäischen Union und der Schweizerischen Eidgenossenschaft zur Verknüpfung ihrer jeweiligen Systeme für den Handel mit Treibhausgasemissionen eingesetzten Gemeinsamen Ausschuss im Hinblick auf die Annahme gemeinsamer Verfahrensvorschriften zu vertretenden Standpunkt

Die Delegationen erhalten in der Anlage das Dokument COM(2020) 255 final - Annex.

Anl.: COM(2020) 255 final - Annex

EUROPÄISCHE
KOMMISSION

Brüssel, den 23.6.2020
COM(2020) 255 final

ANNEX

ANHANG

des

Vorschlags für einen Beschluss des Rates

über den im Namen der Europäischen Union in dem durch das Abkommen zwischen der Europäischen Union und der Schweizerischen Eidgenossenschaft zur Verknüpfung ihrer jeweiligen Systeme für den Handel mit Treibhausgasemissionen eingesetzten Gemeinsamen Ausschuss im Hinblick auf die Annahme gemeinsamer Verfahrensvorschriften zu vertretenden Standpunkt

BESCHLUSS NR. 1/2020 DES MIT DEM ABKOMMEN ZWISCHEN DER EUROPÄISCHEN UNION UND DER SCHWEIZERISCHEN EIDGENOSSENSCHAFT ZUR VERKNÜPFUNG IHRER JEWEILIGEN SYSTEME FÜR DEN HANDEL MIT TREIBHAUSGASEMISSIONEN EINGESETZTEN GEMEINSAMEN AUSSCHUSSES

vom ...

über gemeinsame Verfahrensvorschriften

DER GEMEINSAME AUSSCHUSS —

gestützt auf das Abkommen zwischen der Europäischen Union und der Schweizerischen Eidgenossenschaft zur Verknüpfung ihrer jeweiligen Systeme für den Handel mit Treibhausgasemissionen[1] (im Folgenden das „Abkommen"), insbesondere auf Artikel 3,

in Erwägung nachstehender Gründe:

(1) Mit dem Beschluss Nr. 2/2019 des Gemeinsamen Ausschusses vom 5. Dezember 2019 wurden die Anhänge I und II des Abkommens geändert, sodass die im Abkommen festgelegten Bedingungen für die Verknüpfung erfüllt sind.

(2) Nach Annahme des Beschlusses Nr. 2/2019 des Gemeinsamen Ausschusses tauschten die Vertragsparteien im Einklang mit Artikel 21 Absatz 3 des Abkommens ihre Ratifizierungs- oder Genehmigungsurkunden aus, da sie alle Bedingungen für eine Verknüpfung im Sinne des Abkommens erfüllt sehen.

(3) Im Einklang mit Artikel 21 Absatz 4 des Abkommens ist das Abkommen am 1. Januar 2020 in Kraft getreten.

(4) Gemäß Artikel 3 Absatz 6 des Abkommens sollten der Schweizer Registerverwalter und der Zentralverwalter der Union gemeinsame Verfahrensvorschriften für technische oder andere Fragen festlegen, die für das Funktionieren der Verknüpfung zwischen dem Transaktionsprotokoll der Europäischen Union (EUTL) des Unionsregisters und dem Schweizer Zusatztransaktionsprotokoll (Swiss Supplementary Transaction Log, SSTL) des Schweizer Registers erforderlich sind, und dabei den Prioritäten der innerstaatlichen Rechtsvorschriften Rechnung tragen. Die gemeinsamen Verfahrensvorschriften sollten wirksam werden, sobald sie durch Beschluss des Gemeinsamen Ausschusses angenommen wurden.

(5) Im Einklang mit Artikel 13 Absatz 1 des Abkommens sollte sich der Gemeinsame Ausschuss auf technische Leitlinien zur Gewährleistung der ordnungsgemäßen Umsetzung des Abkommen einigen, die auch technische oder andere Fragen, die für das Funktionieren der Verknüpfung erforderlich sind, betreffen und dabei den Prioritäten der innerstaatlichen Rechtsvorschriften Rechnung tragen. Die technischen Leitlinien können von einer gemäß Artikel 12 Absatz 5 des Abkommens eingesetzten Arbeitsgruppe erarbeitet werden. Die Arbeitsgruppe sollte mindestens den Schweizer Registerverwalter und den Zentralverwalter des Unionsregisters umfassen und den Gemeinsamen Ausschuss bei seinen Aufgaben gemäß Artikel 13 des Abkommens unterstützen.

(6) Wegen des technischen Inhalts der Leitlinien und der Notwendigkeit, sie an laufende Entwicklungen anzupassen, sollten die vom Schweizer Registerverwalter und vom

[1] ABl. L 322 vom 7.12.2017, S. 3.

Zentralverwalter des Unionsregisters erarbeiteten Leitlinien dem Gemeinsamen Ausschuss zur Information und gegebenenfalls zur Genehmigung vorgelegt werden —

HAT FOLGENDEN BESCHLUSS ERLASSEN:

Artikel 1

Die gemeinsamen Verfahrensvorschriften im Anhang werden angenommen.

Artikel 2

Im Einklang mit Artikel 12 Absatz 5 des Abkommens wird eine Arbeitsgruppe eingesetzt. Sie unterstützt den Gemeinsamen Ausschuss, um die ordnungsgemäße Umsetzung des Abkommens, einschließlich der Erarbeitung von technischen Leitlinien für die Umsetzung der gemeinsamen Verfahrensvorschriften, zu gewährleisten.

Die Arbeitsgruppe umfasst mindestens den Schweizer Registerverwalter und den Zentralverwalter des Unionsregisters.

Artikel 3

Dieser Beschluss tritt am Tag seiner Annahme in Kraft.

Ausgefertigt in englischer Sprache in Brüssel, am XX.2020.

Im Namen des Gemeinsamen Ausschusses

Sekretariat für die Europäische Union	*Der Vorsitz*	*Sekretariat für die Schweiz*

ANLAGE

ANHANG

GEMEINSAME VERFAHRENSVORSCHRIFTEN

gemäß Artikel 3 Absatz 6 des Abkommens zwischen der Europäischen Union und der Schweizerischen Eidgenossenschaft zur Verknüpfung ihrer jeweiligen Systeme für den Handel mit Treibhausgasemissionen
- Verfahren für eine vorläufige Lösung

1. GLOSSAR

Tabelle 1-1 Abkürzungen und Begriffsbestimmungen

Abkürzung/Begriff	Begriffsbestimmung
Zertifizierungsstelle	Stelle, die digitale Zertifikate ausstellt
CH	Schweizerische Eidgenossenschaft
EHS	Emissionshandelssystem
EU	Europäische Union
IMT	Incident Management Team (Vorfallmanagement-Team)
Informationswert	Eine Information, die für ein Unternehmen oder eine Organisation von Wert sind.
IT	Informationstechnologie
ITIL	Information Technology Infrastructure Library (Bibliothek für Informationstechnologie-Infrastruktur)
ITSM	IT-Servicemanagement
LTS	Linking Technical Standards (Technische Verknüpfungsstandards)
Register	Ein Verbuchungssystem für im Rahmen des EHS ausgestellte Zertifikate, das das Eigentum an in elektronischen Konten verbuchten Zertifikaten verfolgt.
RFC	Request for Change (Änderungsanfrage)
SIL	Sensitive Information List (Verzeichnis sensibler Informationen)
SR	Service Request (Dienstanfrage)
Wiki	Website, auf der Nutzer Informationen und Wissen austauschen können, indem sie über einen Webbrowser direkt

	Inhalte hinzufügen oder anpassen.

2. EINLEITUNG

Das Abkommen zwischen der Europäischen Union und der Schweizerischen Eidgenossenschaft zur Verknüpfung ihrer jeweiligen Systeme für den Handel mit Treibhausgasemissionen vom 23. November 2017 (im Folgenden das „Abkommen“) sieht die gegenseitige Anerkennung von Emissionszertifikaten vor, die für die Einhaltung der Vorschriften im Rahmen des Emissionshandelssystems der Europäischen Union (im Folgenden das „EU-EHS“) oder des Emissionshandelssystems der Schweiz (im Folgenden das „EHS der Schweiz“) genutzt werden können. Um die Verknüpfung zwischen dem EU-EHS und dem EHS der Schweiz zu operationalisieren, wird eine direkte Verknüpfung zwischen dem Transaktionsprotokoll der Europäischen Union (European Union Transaction Log, im Folgenden „EUTL“) des Unionsregisters und dem Schweizer Zusatztransaktionsprotokoll (Swiss Supplementary Transaction Log, im Folgenden „SSTL“) des Schweizer Registers eingerichtet, sodass im Rahmen eines der beiden EHS vergebene Emissionszertifikate von diesem Register in das andere übertragen werden können (Artikel 3 Absatz 2 des Abkommens). Für die Operationalisierung der Verknüpfung zwischen dem EU-EHS und dem EHS der Schweiz muss bis Mai 2020 oder so bald wie möglich danach eine vorläufige Lösung eingeführt werden. Die Vertragsparteien arbeiten zusammen, um so bald wie möglich die vorläufige Lösung durch eine dauerhafte Registerverknüpfung zu ersetzen (Anhang II des Abkommens).

Gemäß Artikel 3 Absatz 6 des Abkommens legen der Schweizer Registerverwalter und der Zentralverwalter der Union gemeinsame Verfahrensvorschriften für technische oder andere Fragen fest, die für das Funktionieren der Verknüpfung erforderlich sind; dabei tragen sie den Prioritäten der innerstaatlichen Rechtsvorschriften Rechnung. Die von den Verwaltern entwickelten gemeinsamen Verfahrensvorschriften treten in Kraft, sobald sie durch Beschluss des Gemeinsamen Ausschusses angenommen wurden.

Der Gemeinsame Ausschuss soll die in diesem Dokument festgehaltenen gemeinsamen Verfahrensvorschriften mit seinem Beschluss Nr. 1/2020 annehmen. Im Einklang mit diesem Beschluss ersucht der Gemeinsame Ausschuss den Schweizer Registerverwalter und den Zentralverwalter der Union, weitere technische Leitlinien zur Operationalisierung der Verknüpfung zu erarbeiten und sicherzustellen, dass diese laufend an den technischen Fortschritt und die neuen Anforderungen in Bezug auf die Sicherheit der Verknüpfung und ihr wirksames und effizientes Funktionieren angepasst werden.

2.1. Geltungsbereich

Dieses Dokument stellt den Konsens der Vertragsparteien über die Schaffung der verfahrenstechnischen Grundlagen der Verknüpfung zwischen den Registern des EU-EHS und des EHS der Schweiz dar. Es gibt zwar einen Überblick über die allgemeinen Verfahrensanforderungen für Funktionen, doch sind weitere technische Leitlinien erforderlich, um die Verknüpfung betriebsfähig zu machen.

Für das ordnungsgemäße Funktionieren der Verknüpfung sind weitere technische Spezifikationen erforderlich, um die Verknüpfung weiter zu operationalisieren. Gemäß Artikel 3 Absatz 7 des Abkommens werden diese Aspekte eingehend in dem Dokument mit technischen Verknüpfungsstandards (Linking Technical Standards, LTS) geregelt, das gesondert durch einen Beschluss des Gemeinsamen Ausschusses angenommen werden soll.

Die gemeinsamen Verfahrensvorschriften sollen sicherstellen, dass die IT-Dienste im Zusammenhang mit dem Funktionieren der Verknüpfung zwischen den Registern des EU-

EHS und des EHS der Schweiz wirksam und effizient ausgeführt werden, namentlich im Hinblick auf die Erledigung von Dienstanfragen, die Behebung von Dienstausfällen und von Problemen sowie auf die Durchführung von betrieblichen Routineaufgaben im Einklang mit internationalen Normen für das IT-Servicemanagement.

Für die vereinbarte vorläufige Lösung sind lediglich die folgenden gemeinsamen Verfahrensvorschriften erforderlich, die Teil des vorliegenden Dokuments sind:

- Vorfallmanagement
- Problemmanagement
- Anfrageerledigung
- Änderungsmanagement
- Releasemanagement
- Sicherheitsvorfall-Management
- Informationssicherheits-Management

Bei der Einrichtung der dauerhaften Registerverknüpfung zu einem späteren Zeitpunkt müssen die gemeinsamen Verfahrensvorschriften erforderlichenfalls angepasst und ergänzt werden.

2.2. Adressaten

Zielgruppe dieser gemeinsamen Verfahrensvorschriften sind die Supportteams des Registers der EU bzw. der Schweiz.

3. VORGEHEN UND STANDARDS

Der folgende Grundsatz gilt für alle gemeinsamen Verfahrensvorschriften:

- Die EU und die Schweiz vereinbaren, die gemeinsamen Verfahrensvorschriften auf der Grundlage der Version 3 der Bibliothek für Informationstechnologie-Infrastruktur (ITIL) festzulegen. Praktiken aus diesem Standard werden herangezogen und an den besonderen Bedarf im Zusammenhang mit der vorläufigen Lösung angepasst.
- Die für die Regelung der gemeinsamen Verfahrensvorschriften erforderliche Kommunikation und Abstimmung zwischen den beiden Vertragsparteien erfolgt über die Register-Servicedesks der Schweiz und der EU. Aufgaben werden stets innerhalb einer Vertragspartei zugewiesen.
- Besteht Uneinigkeit über die Handhabung einer gemeinsamen Verfahrensvorschrift, so wird diese von beiden Servicedesks gemeinsam untersucht und gelöst. Kann keine Einigung erzielt werden, wird die Suche nach einer gemeinsamen Lösung an die nächsthöhere Ebene eskaliert.

Eskalationsebenen	**EU**	**CH**
1. Ebene	Servicedesk der EU	Servicedesk der Schweiz
2. Ebene	EU-Operationsmanager	Anwendungsmanager des Schweizer Registers
3. Ebene	Gemeinsamer Ausschuss (der diese Zuständigkeit angesichts des Artikels 12 Absatz 5 des Abkommens	

	delegieren könnte)
4. Ebene	emeinsamer Ausschuss, falls auf der 3. Ebene delegiert wird.

- Jede Vertragspartei kann die Verfahren für den Betrieb ihres eigenen Registersystems unter Berücksichtigung der an diese gemeinsamen Verfahrensvorschriften gerichteten Anforderungen und die damit verbundenen Schnittstellen festlegen.
- Die gemeinsamen Verfahrensvorschriften werden durch ein IT-Servicemanagementtool unterstützt, insbesondere in Bezug auf Vorfallmanagement, Problemmanagement und Anfrageerledigung sowie die Kommunikation zwischen den beiden Vertragsparteien.
- Darüber hinaus ist der Informationsaustausch per E-Mail zulässig.
- Beide Vertragsparteien stellen sicher, dass die Anforderungen an die Informationssicherheit im Einklang mit den Handhabungsanweisungen erfüllt werden.

4. VORFALLMANAGEMENT

Ziel des Vorfallmanagement-Prozesses ist es, das normale Leistungsniveau von IT-Diensten so schnell wie möglich mit möglichst geringer Störung der Geschäftsabläufe wiederherzustellen.

Darüber hinaus sollte das Vorfallmanagement für Berichtszwecke Aufzeichnungen über Vorfälle führen und sich in andere Prozesse eingliedern, um ständige Verbesserungen zu erzielen.

- Allgemein betrachtet umfasst das Vorfallmanagement die folgenden Tätigkeiten:
- Ermittlung und Aufzeichnung von Vorfällen
- Einstufung und Erstsupport
- Untersuchung und Diagnose
- Lösung und Wiederherstellung
- Abschluss des Vorfalls

Während der gesamten Dauer eines Vorfalls muss die kontinuierliche Handhabung von Eigentumsrechten, Überwachung, Verfolgung und Kommunikation durch den Vorfallmanagement-Prozess gewährleistet sein.

4.1. Ermittlung und Aufzeichnung von Vorfällen

Ein Vorfall kann von einem Supportteam, durch automatisierte Überwachungstools oder durch technisches Personal im Zuge der Routineüberwachung ermittelt werden.

Ein ermittelter Vorfall muss aufgezeichnet werden; dabei ist ihm eine eindeutige Kennung zuzuweisen, die eine ordnungsgemäße Verfolgung und eine ordnungsgemäße Überwachung ermöglicht. Die eindeutige Kennung eines Vorfalls ist die Kennung, die ihm im gemeinsamen Ticketsystem des Servicedesks der Vertragspartei (EU oder Schweiz), die den Vorfall festgestellt hat, zugewiesen wird. Sie muss in jeder Mitteilung im Zusammenhang mit dem Vorfall angegeben werden.

Anlaufstelle für alle Vorfälle sollte der Servicedesk der Vertragspartei sein, der das Ticket erfasst hat.

4.2. Einstufung und Erstsupport

Durch die Einstufung eines Vorfalls soll verstanden und ermittelt werden, welches System und/oder welcher Dienst in welchem Umfang betroffen ist. Um wirksam zu sein, sollte der Vorfall bei der Einstufung im ersten Anlauf zur korrekten Ressource geroutet werden, sodass der Vorfall schneller gelöst werden kann.

In der Einstufungsphase sollte der Vorfall nach seiner Wirkung und Dringlichkeit kategorisiert und priorisiert werden, damit er innerhalb eines Zeitrahmen behandelt wird, der der Priorität gerecht wird.

Besteht die Möglichkeit, dass der Vorfall sich auf die Vertraulichkeit oder die Integrität sensibler Daten und/oder auf die Systemverfügbarkeit auswirkt, muss der Vorfall außerdem als Sicherheitsvorfall deklariert und nach dem Verfahren behandelt werden, das im Kapitel „Sicherheitsvorfallmanagement“ dieses Dokuments festgelegt ist.

Soweit möglich nimmt der Servicedesk, der das Ticket erfasst hat, eine erste Diagnose vor. Zu diesem Zweck stellt der Servicedesk fest, ob es sich bei dem Vorfall um einen bekannten Fehler handelt. Ist dies der Fall, so ist der Lösungsweg oder die Ausweichlösung bereits bekannt und dokumentiert.

Konnte der Servicedesk den Vorfall lösen, so wird er den Vorfall zu diesem Zeitpunkt abschließen, da der Primärzweck des Vorfallmanagements erfüllt wurde (nämlich die schnelle Wiederherstellung des Dienstes für den Endnutzer). Anderenfalls eskaliert der Servicedesk den Vorfall zur weiteren Untersuchung und Diagnose an die geeignete Resolvergruppe.

4.3. Untersuchung und Diagnose

Die Untersuchung und Diagnose von Vorfällen erfolgt, wenn der Servicedesk einen Vorfall nicht im Rahmen der Erstdiagnose lösen kann und dieser daher in geeigneter Weise eskaliert wird. Die Eskalation von Vorfällen ist Teil des Untersuchungs- und Diagnoseprozesses.

Eine gemeinsame Praxis in der Untersuchungs- und Diagnosephase ist der Versuch, den Vorfall unter kontrollierten Bedingungen nachzuvollziehen. Bei der Untersuchung und Diagnose eines Vorfalls ist wichtig, dass die richtige Abfolge der Ereignisse, die zu dem Vorfall geführt haben, deutlich wird.

Mit der Eskalation wird anerkannt, dass ein Vorfall auf der derzeitigen Supportebene nicht gelöst werden kann und an eine Supportgruppe auf höherer Ebene oder an die andere Vertragspartei weitergeleitet werden muss. Die Eskalation kann auf zwei Wegen erfolgen: horizontal (funktionsabhängig) oder vertikal (hierarchisch).

Der Servicedesk, der den Vorfall aufgezeichnet und ausgelöst hat, ist dafür verantwortlich, den Vorfall an die geeignete Ressource zu eskalieren und den Gesamtstatus und die Zuweisung des Vorfalls zu verfolgen.

Die Vertragspartei, der der Vorfall zugewiesen wurde, ist dafür verantwortlich, sicherzustellen, dass die angeforderten Maßnahmen zügig durchgeführt werden, und ihren eigenen Servicedesk auf dem Laufenden zu halten.

4.4. Lösung und Wiederherstellung

Die Vorfalllösung und die Wiederherstellung finden statt, sobald der Vorfall vollständig verstanden wird. Eine Lösung für einen Vorfall zu finden bedeutet, dass ein Weg gefunden

wurde, um Abhilfe zu schaffen. Der Akt der Anwendung der Lösung ist die Wiederherstellungsphase.

Wurde der Dienstausfall von den geeigneten Ressourcen behoben, so wird der Vorfall an den zuständigen Servicedesk zurückgeleitet, der den Vorfall erfasst hat. Dieser bestätigt dem Initiator des Vorfalls, dass der Fehler berichtigt wurde und der Vorfall abgeschlossen werden kann. Die Erkenntnisse aus der Bearbeitung des Vorfalls sind für die künftige Verwendung aufzuzeichnen.

Die Wiederherstellung kann von IT-Supportpersonal durchgeführt werden oder durch Übermittlung von zu beachtenden Anweisungen an den Endnutzer.

4.5. Abschluss des Vorfalls

Der Abschluss ist der letzte Schritt des Vorfallmanagement-Prozesses und erfolgt kurz nach der Lösung des Vorfalls.

Aus der Checkliste der Tätigkeiten, die in der Abschlussphase durchzuführen sind, werden die folgenden hervorgehoben:

- Überprüfung der Kategorie, in die der Vorfall ursprünglich eingeordnet wurde;
- ordnungsgemäße Erfassung aller Informationen zu dem Vorfall;
- ordnungsgemäße Dokumentation des Vorfalls und Aktualisierung der Wissensbasis;
- angemessene Kommunikation mit allen direkt oder indirekt von dem Vorfall betroffenen Beteiligten.

Ein Vorfall ist förmlich abgeschlossen, sobald der Servicedesk die Vorfallabschlussphase ausgeführt und die andere Vertragspartei darüber unterrichtet hat.

Ein einmal geschlossener Vorfall wird nicht wieder geöffnet. Tritt ein Vorfall innerhalb kurzer Zeit erneut auf, wird nicht der ursprüngliche Vorfall wieder geöffnet, sondern stattdessen muss ein neuer Vorfall erfasst werden.

Wird der Vorfall sowohl vom Servicedesk der EU als auch von dem der Schweiz verfolgt, so ist der Servicedesk, der das Ticket erfasst hat, für den endgültigen Abschluss zuständig.

5. PROBLEMMANAGEMENT

Dieses Verfahren sollte immer dann angewandt werden, wenn ein Problem ermittelt und dadurch der Problemmanagement-Prozess ausgelöst wird. Das Problemmanagement konzentriert sich auf Qualitätssteigerung und die Verringerung der Zahl der gemeldeten Vorfälle. Ein Problem kann einen oder mehrere Vorfälle verursachen. Wird ein Vorfall gemeldet, so besteht das Ziel des Vorfallmanagements darin, den Dienst so schnell wie möglich wiederherzustellen, was auch Ausweichlösungen umfassen kann. Wird ein Problem gestellt, so besteht das Ziel darin, den Ursprung des Problems zu untersuchen, um herauszufinden, welche Änderung gewährleistet, dass das Problem und die entsprechenden Vorfälle nicht mehr auftreten.

5.1. Ermittlung und Aufzeichnung eines Problems

Je nachdem, welche Vertragspartei das Ticket initiiert hat, ist entweder der Servicedesk der EU oder derjenige der Schweiz die Anlaufstelle für Fragen im Zusammenhang mit einem Problem.

Die einmalige Kennung eines Problems ist die vom IT-Servicemanagement zugewiesene Kennung. Sie muss in jeder Mitteilung im Zusammenhang mit dem Problem angegeben werden.

Ein Problem kann durch einen Vorfall ausgelöst oder auf Eigeninitiative mit dem Ziel geöffnet werden, im System ermittelte Mängel in einer beliebigen Phase zu beheben.

5.2. Problempriorisierung

Zwecks einfacherer Verfolgung können Probleme unter Berücksichtigung der Wirkung und Häufigkeit der damit zusammenhängenden Vorfälle genau wie Vorfälle nach ihrem Schweregrad und ihrer Priorität kategorisiert werden.

5.3. Untersuchung und Diagnose eines Problems

Jede Vertragspartei kann auf ein Problem hinweisen. Der Servicedesk der Vertragspartei, von der die Initiative ausgeht, ist dafür verantwortlich, das Problem zu erfassen, es der geeigneten Ressource zuzuweisen und den Gesamtstatus zu verfolgen.

Die Resolvergruppe, an die das Problem eskaliert wurde, ist für die zügige Behandlung des Problems und die Kommunikation mit dem Servicedesk verantwortlich.

Auf Anfrage sind beide Vertragsparteien dafür verantwortlich, sicherzustellen, dass die zugewiesenen Maßnahmen durchgeführt werden, und ihren eigenen Servicedesk auf dem Laufenden zu halten.

5.4. Problemlösung

Die Resolvergruppe, der das Problem zugewiesen wurde, ist verantwortlich dafür, das Problem zu lösen und dem Servicedesk ihrer eigenen Vertragspartei sachdienliche Informationen zu übermitteln.

Die Erkenntnisse aus der Bearbeitung des Problems sind für die künftige Verwendung aufzuzeichnen.

5.5. Abschluss eines Problems

Ein Problem ist förmlich geschlossen, sobald das Problem durch die Umsetzung der Änderung behoben wurde. Die Phase des Problemabschlusses wird von dem Servicedesk wahrgenommen, der das Problem erfasst und den Servicedesk der anderen Vertragspartei darüber informiert hat.

6. ANFRAGEERLEDIGUNG

Bei dem Prozess der Anfrageerledigung handelt es sich um das durchgehende Management einer Anfrage nach einem neuen oder bestehenden Dienst vom Zeitpunkt ihrer Registrierung und Genehmigung bis zum Abschluss. Bei Dienstanfragen handelt es sich in der Regel um kleine, vordefinierte, wiederholbare, häufige, vorabgenehmigte und verfahrenstechnische Anfragen.

Die wichtigsten Schritte werden nachstehend kurz beschrieben:

6.1. Einleitung einer Anfrage

Die Angaben zu einer Dienstanfrage werden dem Servicedesk der EU oder dem der Schweiz per E-Mail, Telefon oder über das ITSM-Tool oder jeden anderen vereinbarten Kommunikationskanal übermittelt.

6.2. Erfassung und Analyse von Anfragen

Anlaufstelle für alle Dienstanfragen sollte der Servicedesk der EU oder derjenige der Schweiz sein, je nachdem, welche Vertragspartei die Dienstanfrage eingeleitet hat. Der Servicedesk ist dafür verantwortlich, die Dienstanfrage mit der gebotenen Sorgfalt zu erfassen und zu analysieren.

6.3. Genehmigung der Anfrage

Der Sachbearbeiter des Servicedesks der Vertragspartei, die die Dienstanfrage eingeleitet hat, prüft, ob für die Anfrage etwaige Genehmigungen der anderen Vertragspartei erforderlich sind, und holt diese gegebenenfalls ein. Wird die Dienstanfrage nicht genehmigt, aktualisiert der Servicedesk das Ticket und schließt es.

6.4. Anfrageerledigung

Dieser Schritt dient der wirksamen und effizienten Bearbeitung von Dienstanfragen. Hierbei ist unter folgenden Fällen zu unterscheiden:

- Die Erledigung der Dienstanfrage betrifft nur eine Vertragspartei. In diesem Fall erteilt diese Vertragspartei die Arbeitsaufträge und koordiniert die Ausführung.
- Die Erledigung der Dienstanfrage betrifft sowohl die EU als auch die Schweiz. In diesem Fall erteilen die Servicedesks die Arbeitsaufträge in ihrem Zuständigkeitsbereich. Der Ablauf der Erledigung der Dienstanfrage wird von den beiden Servicedesks gemeinsam koordiniert. Die Gesamtverantwortung trägt der Servicedesk, der die Dienstanfrage erhalten und initiiert hat.

Sobald die Dienstanfrage erledigt wurde, muss sie den Status „Erledigt“ (Resolved) erhalten.

6.5. Anfrageeskalation

Der Servicedesk kann die offene Dienstanfrage erforderlichenfalls an die geeignete Ressource (Drittpartei) eskalieren.

Eskaliert wird an die jeweilige Drittpartei, d. h. der Servicedesk der EU muss den Servicedesk der Schweiz einschalten, um an eine Schweizer Drittpartei zu eskalieren und umgekehrt.

Die Drittpartei, an die die Dienstanfrage eskaliert wurde, ist für die zügige Behandlung der Dienstanfrage und die Kommunikation mit dem Servicedesk, der diese Anfrage eskaliert hat, verantwortlich.

Der Servicedesk, der die Dienstanfrage erfasst hat, ist für die Verfolgung des Gesamtstatus und der Zuweisung einer Dienstanfrage verantwortlich.

6.6. Überprüfung der Anfrageerledigung

Der zuständige Servicedesk unterzieht die Aufzeichnungen zu der Dienstanfrage vor dem Abschluss einer abschließenden Qualitätskontrolle. So soll sichergestellt werden, dass die Dienstanfrage tatsächlich bearbeitet wurde und dass alle zur Beschreibung des Lebenszyklus der Dienstanfrage erforderlichen Angaben mit hinreichenden Einzelheiten vorliegen. Darüber hinaus sind die Erkenntnisse aus der Bearbeitung der Anfrage für die künftige Verwendung aufzuzeichnen.

6.7. Abschluss der Anfrage

Sind sich die Vertragsparteien, denen die Anfrage zugewiesen wurde, einig, dass die Dienstanfrage erledigt wurde, und betrachtet der Urheber der Anfrage den Fall als gelöst, so wird als Nächstes der Status „Abgeschlossen“ (Closed) erteilt.

Eine Dienstanfrage wird förmlich abgeschlossen, sobald der Servicedesk, der die Anfrage erfasst hat, die Anfrageabschlussphase abgewickelt und den Servicedesk der anderen Vertragspartei unterrichtet hat.

7. ÄNDERUNGSMANAGEMENT

Das Änderungsmanagement soll sicherstellen, dass alle Änderungen zur Kontrolle von IT-Infrastruktur effizient und zeitnah nach standardisierten Methoden und Verfahren durchgeführt werden, damit die Zahl und die Auswirkungen etwaiger Vorfälle in diesem Zusammenhang auf den Dienst möglichst gering gehalten werden. Änderungen der IT-Infrastruktur können sich reaktiv infolge von Problemen oder von außen auferlegten Anforderungen, z. B Änderungen der Rechtsvorschriften, oder proaktiv ergeben, indem eine Verbesserung von Effizienz und Wirksamkeit angestrebt wird oder um unternehmerische Initiativen zu ermöglichen oder zu reflektieren.

Der Änderungsmanagement-Prozess umfasst verschiedene Schritte, bei denen jede Einzelheit einer Änderungsanfrage für die künftige Nachverfolgung erfasst wird. Diese Prozesse gewährleisten, dass die Änderung vor ihrer Einführung validiert und getestet wird. Ein Releasemanagement-Prozess sorgt für eine erfolgreiche Einführung.

7.1. Änderungsanfrage

Eine Änderungsanfrage wird dem Änderungsmanagement-Team zur Validierung und Genehmigung vorgelegt. Anlaufstelle für alle Änderungsanfragen sollte der Servicedesk der EU oder derjenige der Schweiz sein, je nachdem, welche Vertragspartei die Anfrage eingeleitet hat. Der Servicedesk ist dafür verantwortlich, die Anfrage mit der gebotenen Sorgfalt zu erfassen und zu analysieren.

Änderungsanfragen können ausgelöst werden durch

- einen Vorfall, der eine Änderung verursacht;
- ein bestehendes Problem, das zu einer Änderung führt;
- einen Endnutzer, der eine neue Änderung anfragt;
- eine Änderung infolge laufender Wartungsarbeiten;
- Änderungen von Rechtsvorschriften.

7.2. Bewertung und Planung einer Änderung

Diese Phase umfasst die Bewertung von Änderungen und Planungstätigkeiten. Dazu gehören Priorisierung und Planungstätigkeiten zur Minimierung der Risiken und Auswirkungen.

Wenn die Durchführung der Änderungsanfrage sowohl die EU als auch die Schweiz betrifft, überprüft die Vertragspartei, die die Anfrage erfasst hat, die Änderungsbewertung und -planung mit der anderen Vertragspartei.

7.3. Genehmigung einer Änderung

Eine eingeloggte Änderungsanfrage muss von der zuständigen Eskalationsebene genehmigt werden.

7.4. Durchführung der Änderung

Die Durchführung der Änderung erfolgt im Rahmen des Releasemanagements. Die Releasemanagement-Teams beider Vertragsparteien folgen bei der Planung und dem Testen ihren eigenen Prozessen. Die Änderung wird überprüft, sobald die Durchführung abgeschlossen ist. Um sicherzustellen, dass alles planmäßig abgewickelt wurde, wird der bestehende Änderungsmanagement-Prozess laufend überprüft und bei Bedarf aktualisiert.

8. RELEASEMANAGEMENT

Ein Release entspricht einer oder mehreren Änderungen eines IT-Dienstes, die in einem Releaseplan zusammengefasst sind und zusammen genehmigt, vorbereitet, aufgebaut, getestet und eingeführt werden. Bei einem einzigen Release kann es sich um eine Fehlerbehebung, eine Änderung der Hardware oder anderer Komponenten, Softwareänderungen, Aktualisierungen von Anwendungsversionen und/oder Änderungen der Dokumentation bzw. von Prozessen handeln. Jedes Release wird inhaltlich als Einheit verwaltet, getestet und eingeführt.

Releasemanagement zielt auf die Planung, den Aufbau, das Testen und die Validierung sowie die Schaffung der Fähigkeit ab, die konzipierten Dienste bereitzustellen, mit denen die Anforderungen der Beteiligten erfüllt und die angestrebten Ziele erreicht werden. Bei der Designkoordinierung werden für alle Änderungen des Dienstes Akzeptanzkriterien festgelegt und dokumentiert, die den Releasemanagement-Teams zur Verfügung gestellt werden.

Das Release besteht in der Regel aus mehreren Problembehebungen und Verbesserungen für einen Dienst. Er umfasst die erforderliche neue oder geänderte Software oder jegliche neue oder geänderte Hardware, die zur Umsetzung der genehmigten Änderungen erforderlich ist.

8.1. Planung des Releases

Als erster Schritt in diesem Prozess werden genehmigte Änderungen Releasebündeln zugewiesen und der Umfang und Inhalt der Releases festgelegt. Auf der Grundlage dieser Informationen wird als Teilprozess der Releaseplanung ein Zeitplan für den Aufbau, das Testen und die Einführung des Releases aufgestellt.

Bei der Planung sollte Folgendes festgelegt werden:

- Umfang und Inhalt des Releases;
- Risikobewertung und Risikoprofil des Releases;
- von dem Release betroffene Kunden/Nutzer;
- für das Release zuständiges Team;
- Bereitstellungs- und Einführungsstrategie;
- Ressourcen für das Release und die Einführung.

Die beiden Vertragsparteien unterrichten einander über ihre Releaseplanung und ihre Wartungsfenster. Wenn ein Release sowohl die EU als auch die Schweiz betrifft, koordinieren diese die Planung und legen ein gemeinsames Wartungsfenster fest.

8.2. Aufbau und Testen des Releasebündels

In der Aufbau- und Testphase im Rahmen des Releasemanagement-Prozesses wird zum einen das Konzept für die Ausführung des Releases oder des Releasebündels und die Wartung der kontrollierten Umgebungen vor der Vornahme der Änderung und zum anderen das Konzept

für das Testen aller Änderungen in allen betroffenen Umgebungen nach dem Release festgelegt.

Wenn ein Release sowohl die EU als auch die Schweiz betrifft, koordinieren diese die Bereitstellungpläne und die Tests. Dies umfasst die folgenden Fragen:

- Wie und wann werden Releaseeinheiten und Dienstleistungskomponenten bereitgestellt?
- Was sind die typischen Vorlaufzeiten und was geschieht bei Verzögerungen?
- Wie kann der Fortschritt der Bereitstellung verfolgt und eine Bestätigung eingeholt werden?
- Was sind die Messgrößen für die Überwachung und Feststellung des Gelingens der Releasemaßnahme?
- Welches sind die gemeinsamen Testfälle für wichtige Funktionen und Änderungen?

Am Ende dieses Teilprozesses sind alle erforderlichen Releasekomponenten für den Schritt der realen Einführung bereit.

8.3. Vorbereitung der Einführung

Beim Teilprozess der Vorbereitung wird sichergestellt, dass Kommunikationspläne korrekt festgelegt werden und Mitteilungen bereitliegen, um an alle betroffenen Beteiligten und Endnutzer versandt zu werden, und dass das Release in den Änderungsmanagement-Prozess eingebunden wird, um zu gewährleisten, dass alle Änderungen kontrolliert durchgeführt und von den erforderlichen Gremien genehmigt werden.

Wenn ein Release sowohl die EU als auch die Schweiz betrifft, koordinieren diese die folgenden Tätigkeiten:

- Aufzeichnungen zur Änderungsanfrage für die Planung und Vorbereitung der Einführung in die Produktionsumgebung;
- Aufstellung des Durchführungsplans;
- Zurücksetzungskonzept, damit bei einer misslungenen Einführung der vorherige Stand wiederhergestellt werden kann;
- Mitteilungen an alle notwendigen Parteien;
- Einholung der Genehmigung für die Durchführung des Releases von der zuständigen Eskalationsebene.

8.4. Zurücksetzen des Releases

Ist eine Einführung misslungen oder haben Tests ergeben, dass die Einführung ein Fehlschlag war oder die vereinbarten Akzeptanz-/Qualitätskriterien nicht erreichte, müssen die Releasemanagement-Teams beider Vertragsparteien zum vorigen Stand zurückkehren. Alle notwendigen Beteiligten müssen darüber unterrichtet werden, einschließlich der betroffenen/anvisierten Endnutzer. Bei erteilter Genehmigung kann der Prozess in jeder der vorangegangenen Phasen wieder aufgenommen werden.

8.5. Überprüfung und Abschluss des Releases

Bei der Überprüfung einer Einführung sollten folgende Tätigkeiten durchgeführt werden:

- Einholen von Feedback zur Kunden-/Nutzerzufriedenheit mit der Einführung/zur Zufriedenheit mit der Dienstbereitstellung im Rahmen der Einführung (Sammeln des Feedbacks und dessen Auswertung für die kontinuierliche Verbesserung des Dienstes);
- Überprüfung etwa nicht erfüllter Qualitätskriterien;
- Kontrolle, dass alle Maßnahmen, notwendigen Korrekturen und Änderungen vollständig sind;
- Sicherstellen, dass am Ende der Einführung keine Probleme in Bezug auf Fähigkeiten, Ressourcen, Kapazität oder Leistung auftreten;
- Kontrolle, dass alle Probleme, bekannten Fehler und Ausweichlösungen dokumentiert und von Kunden, Endnutzern, dem betrieblichen Support und anderen betroffenen Parteien akzeptiert werden;
- Überwachung von Vorfällen und Problemen, die durch die Einführung ausgelöst wurden (Early Life Support für operative Teams, wenn das Release Mehrarbeit verursacht hat);
- Aktualisierung der Supportdokumentation (d. h. Unterlagen mit technischen Informationen);
- förmliche Übergabe des eingeführten Releases an den Servicebetrieb;
- Dokumentation der gewonnenen Erkenntnisse;
- Einholen der Release-Kurzbeschreibung bei den Durchführungsteams;
- förmlicher Abschluss des Releases nach Überprüfung der Aufzeichnungen zur Änderungsanfrage.

9. SICHERHEITSVORFALL-MANAGEMENT

Das Sicherheitsvorfall-Management ist ein Prozess für den Umgang mit Sicherheitsvorfällen, der es ermöglichen soll, potenziell betroffene Beteiligte über den Vorfall zu unterrichten sowie Vorfälle zu bewerten und zu priorisieren; es umfasst auch die Reaktion auf den Vorfall, um eine tatsächliche, mutmaßliche oder potenzielle Verletzung der Vertraulichkeit, Verfügbarkeit oder Integrität von sensiblen Informationswerten zu beheben.

9.1. Kategorisierung von Informationssicherheitsvorfällen

Alle Vorfälle, die die Verknüpfung zwischen dem Unionsregister und dem Register der Schweiz beeinflussen, werden analysiert, um zu ermitteln, ob möglicherweise die Vertraulichkeit, Integrität oder Verfügbarkeit von im Verzeichnis sensibler Informationen aufgeführten sensiblen Informationen verletzt wurde.

Ist dies der Fall, so wird der Vorfall als Informationssicherheitsvorfall kategorisiert, unverzüglich im IT-Servicemanagement-Tool (ITSM-Tool) registriert und als solcher bearbeitet.

9.2. Handhabung von Informationssicherheitsvorfällen

Sicherheitsvorfälle werden der Verantwortung der 3. Eskalationsebene zugeordnet; die Lösung der Vorfälle übernimmt ein spezielles Vorfallmanagement-Team (IMT).

Das Vorfallmanagement-Team ist verantwortlich für

- die Durchführung einer ersten Analyse, die Kategorisierung und die Schwereeinstufung des Vorfalls;
- die Koordinierung von Maßnahmen aller Beteiligten einschließlich der vollständigen Dokumentation der Vorfallanalyse, der zur Behebung des Vorfalls getroffenen Entscheidungen und der ermittelten möglichen Schwachstellen;
- je nach Schwere des Sicherheitsvorfalls die zügige Eskalation an die geeignete Ebene zur Information und/oder Entscheidung.

Bei dem Prozess des Informationssicherheits-Managements werden alle Informationen zu Vorfällen in die höchste Sensibilitätsstufe für Informationen, auf jeden Fall aber nicht niedriger als „ETS SENSITIVE“ eingestuft.

Im Falle einer laufenden Untersuchung und/oder einer Schwachstelle, die ausgenutzt werden könnte, wird die Information so lange als „ETS CRITICAL“ eingestuft, bis Abhilfe geschaffen wurde.

9.3. Identifizierung eines Sicherheitsvorfalls

Je nach Art des Sicherheitsvorfalls bestimmt der Informationssicherheitsbeauftragte, welche geeigneten Organisationen einzubinden und am Vorfallmanagement-Team zu beteiligen sind.

9.4. Analyse eines Sicherheitsvorfalls

Das Vorfallmanagement-Team steht mit allen beteiligten Organisationen und gegebenenfalls den relevanten Mitgliedern von deren Teams in Kontakt, um den Vorfall genauer zu betrachten. Bei der Analyse wird ermittelt, in welchem Umfang die Vertraulichkeit, Integrität oder Verfügbarkeit eines Werts verloren gegangen ist, und bewertet, wie sich dies auf alle betroffenen Organisationen auswirkt. Anschließend werden Erst- und Folgemaßnahmen zur Behebung des Vorfalls und zur Verwaltung seiner Auswirkungen bestimmt, einschließlich der Auswirkungen dieser Maßnahmen auf die Ressourcen.

9.5. Bewertung der Schwere eines Sicherheitsvorfalls, Eskalation und Berichterstattung

Das Vorfallmanagement-Team bewertet die Schwere jedes neuen Sicherheitsvorfalls nach dessen Kategorisierung und leitet abhängig von der Schwere des Vorfalls die erforderlichen Sofortmaßnahmen ein.

9.6. Berichterstattung über die Reaktion auf einen Sicherheitsvorfall

Das Vorfallmanagement-Team nimmt die Ergebnisse der Begrenzung des Vorfalls (Incident Containment) und der Wiederherstellung in den Bericht über die Reaktion auf den Informationssicherheitsvorfall auf. Der Bericht wird der 3. Eskalationsebene mit gesicherter E-Mail oder anderen gegenseitig akzeptierten gesicherten Kommunikationsmitteln übermittelt.

Die zuständige Vertragspartei überprüft die Ergebnisse der Begrenzung und Wiederherstellung und

- stellt die Verbindung des Registers wieder her, wenn dieses zuvor abgetrennt worden war;
- übernimmt die Vorfallkommunikation gegenüber den Registerteams;
- schließt den Vorfall ab.

Das Vorfallmanagement-Team sollte sachdienliche Einzelheiten in gesicherter Form in den Bericht über den Informationssicherheitsvorfall aufnehmen, um die kohärente Aufzeichnung und Kommunikation zu gewährleisten und zügige, angemessene Maßnahmen zur Begrenzung des Vorfalls zu ermöglichen. Nach der Fertigstellung übermittelt das Vorfallmanagement-Team zügig den endgültigen Bericht über den Informationssicherheitsvorfall.

9.7. Überwachung, Kapazitätsaufbau und kontinuierliche Verbesserung

Das Vorfallmanagement-Team erstattet über alle Sicherheitsvorfälle an die 3. Eskalationsebene Bericht. Die Berichte werden von dieser Eskalationsebene verwendet, um Folgendes zu ermitteln:

- Schwachstellen bei Sicherheitskontrollen oder beim Betrieb, die gestärkt werden müssen;
- mögliche Notwendigkeit, dieses Verfahren zu verbessern, sodass wirksamer auf Vorfälle reagiert werden kann;
- Möglichkeiten für Schulung und Kapazitätsaufbau zur weiteren Stärkung der Resilienz von Registersystemen in Bezug auf die Informationssicherheit, um das Risiko künftiger Vorfälle zu verringern und deren Auswirkungen zu minimieren.

10. INFORMATIONSSICHERHEITS-MANAGEMENT

Das Informationssicherheits-Management zielt darauf ab, die Vertraulichkeit, Integrität und Verfügbarkeit von vertraulichen Informationen, Daten und IT-Dienstleistungen einer Organisation sicherzustellen. Neben den technischen Komponenten, darunter deren Design und Erprobung (siehe technische Verknüpfungsstandards, LTS), sind die folgenden gemeinsamen Verfahrensvorschriften erforderlich, um die Sicherheitsanforderungen für die vorläufige Lösung zu erfüllen.

10.1. Identifizierung von sensiblen Informationen

Zur Bewertung der Sensibilität einer Information wird ermittelt, in welchem Umfang sich eine Sicherheitsverletzung im Zusammenhang mit dieser Information auf die Geschäftstätigkeit auswirken könnte (z. B. finanzielle Verluste, Imageschaden, Rechtsverletzung usw.).

Die sensiblen Informationswerte werden auf der Grundlage ihrer Auswirkungen auf die Verknüpfung ermittelt.

Die Sensibilitätsstufe dieser Information wird anhand der für diese Verknüpfung anwendbaren Sensibilitätsskala bewertet, die im Abschnitt „Behandlung von Informationssicherheitsvorfällen“ dieses Dokuments eingehender behandelt wird.

10.2. Sensibilitätsstufen von Informationswerten

Sobald dies ermittelt wurde, wird der Informationswert nach folgenden Regeln eingestuft:

- Wird die Vertraulichkeits-, die Integritäts- oder die Verfügbarkeitsstufe auch nur in einem Fall als HOCH erachtet, wird der Wert als „ETS CRITICAL“ eingestuft;
- wird die Vertraulichkeits-, die Integritäts- oder die Verfügbarkeitsstufe auch nur in einem Fall als MITTEL erachtet, wird der Wert als „ETS SENSITIVE“ eingestuft;

- werden die Vertraulichkeits-, die Integritäts- und die Verfügbarkeitsstufen durchweg als NIEDRIG erachtet, wird der Wert als „ETS LIMITED“ eingestuft.

10.3. Bezeichnung des Eigentümers von Informationswerten

Für alle Informationswerte sollte es einen bezeichneten Eigentümer geben. Informationswerte des EHS, die zu der Verknüpfung zwischen dem EUTL und dem SSTL gehören oder damit in Verbindung stehen, sollten in ein gemeinsames Inventarverzeichnis der Informationswerte aufgenommen werden, das von den beiden Vertragsparteien geführt wird. Informationswerte des EHS außerhalb der Verknüpfung zwischen dem EUTL und dem SSTL sollten in ein Inventarverzeichnis der Informationswerte aufgenommen werden, das von der jeweiligen Vertragspartei geführt wird.

Die Eigentumsrechte an jedem Informationswert, der zu der Verknüpfung zwischen dem EUTL und dem SSTL gehört oder damit in Verbindung steht, müssen von den beiden Vertragsparteien vereinbart werden. Die Bewertung der Sensibilität eines Informationswerts ist Aufgabe des Eigentümers.

Die Position des Eigentümers sollte dem Wert des ihm zugeordneten Informationswerts angemessen sein. Die Verantwortung des Eigentümers für den Wert und die Verpflichtung zur Wahrung der erforderlichen Vertraulichkeits-, Integritäts- und Verfügbarkeitsstufe sollten vereinbart und förmlich festgelegt werden.

10.4. Registrierung sensibler Informationen

Alle sensiblen Informationen werden im Verzeichnis sensibler Informationen registriert.

Wenn sich die Aggregation von sensiblen Informationen stärker auswirken könnte als eine einzelne Information, wird dies gegebenenfalls berücksichtigt und im Verzeichnis sensibler Informationen registriert (z. B. ein in der Systemdatenbank gespeicherter Datensatz).

Das Verzeichnis sensibler Informationen ist nicht statisch. Bedrohungen, Schwachstellen, die Wahrscheinlichkeit oder die Folgen von Sicherheitsvorfällen im Zusammenhang mit den Werten können sich ohne Vorankündigung ändern, und es ist möglich, dass neue Werte in den Betrieb der Registersysteme eingeführt werden.

Deswegen wird das Verzeichnis sensibler Informationen regelmäßig überprüft, und alle neuen als sensibel eingestuften Informationen werden unverzüglich im Verzeichnis sensibler Informationen registriert.

Das Verzeichnis sensibler Informationen muss für jeden Eintrag mindestens folgende Angaben enthalten:

- Beschreibung der Information
- Eigentümer der Information
- Sensibilitätsstufe
- Angabe, ob die Informationen personenbezogene Daten enthält
- weitere Angaben soweit erforderlich.

10.5. Behandlung von sensiblen Informationen

Sensible Informationen, die außerhalb der Verknüpfung zwischen dem Unionsregister und dem Schweizer Register verarbeitet werden, werden im Einklang mit den Handhabungsanweisungen behandelt.

Sensible Informationen, die über die Verknüpfung zwischen dem Unionsregister und dem Schweizer Register verarbeitet werden, werden im Einklang mit den Sicherheitsanforderungen der Vertragsparteien behandelt.

10.6. Zugangsmanagement

Ziel des Zugangsmanagements ist es, autorisierten Nutzern die Berechtigung zur Nutzung eines Dienstes zu erteilen und gleichzeitig den Zugang von nicht autorisierten Nutzern zu verhindern. Das Zugangsmanagement wird manchmal auch als „Berechtigungsmanagement“ oder „Identitätsmanagement“ bezeichnet.

Für die vorläufige Lösung und ihren Betrieb benötigen die beiden Vertragsparteien Zugang zu den folgenden Komponenten:

- Wiki: Ein kollaboratives Umfeld für den Austausch gemeinsamer Informationen wie Releaseplanung;
- IT-Servicemanagement-Tool (ITSM-Tool) für das Vorfall- und Problemmanagement (siehe Kapitel „Vorgehen und Standards“);
- Informationsaustauschsystem: Jede Vertragspartei stellt ein System für den sicheren Austausch von Meldungen bereit, über das Meldungen, die Transaktionsdaten enthalten, übermittelt werden.

Der Schweizer Registerverwalter und der Zentralverwalter der Union sorgen dafür, dass Zugänge auf dem neuesten Stand sind, und fungieren für ihre jeweilige Vertragspartei als Anlaufstelle für Tätigkeiten des Zugangsmanagements. Anträge auf Zugang werden im Einklang mit den Verfahren für die Anfrageerledigung behandelt.

10.7. Zertifikat-/Schlüsselmanagement

Jede Vertragspartei ist für ihr eigenes Zertifikat-/Schlüsselmanagement (Generierung, Registrierung, Speicherung, Installation, Verwendung, Erneuerung, Aufhebung, Backup und Wiedererlangung von Zertifikaten/Schlüsseln) verantwortlich. Wie in den technischen Verknüpfungsstandards beschrieben, werden nur digitale Zertifikate verwendet, die von einer Zertifizierungsstelle ausgestellt wurden, der beide Vertragsparteien vertrauen. Die Handhabung und Speicherung von Zertifikaten/Schlüsseln muss den Bestimmungen der Handhabungsanweisungen folgen.

Jede Aufhebung und/oder Erneuerung von Zertifikaten und Schlüsseln muss von beiden Vertragsparteien koordiniert werden. Dies geschieht im Einklang mit den Verfahren für die Anfrageerledigung.

Der Schweizer Registerverwalter und der Zentralverwalter der Union tauschen Zertifikate/Schlüssel über ein gesichertes Kommunikationsmittel im Einklang mit den Bestimmungen der Handhabungsanweisungen aus.

Jede Überprüfung von Zertifikaten/Schlüsseln in jedem Kommunikationsmittel zwischen den Parteien erfolgt auf einem zweiten Kanal („out of band“).