



Rat der
Europäischen Union

047489/EU XXVI. GP
Eingelangt am 12/12/18

Brüssel, den 12. Dezember 2018
(OR. en)

**Interinstitutionelles Dossier:
2018/0422 (NLE)**

15503/18
ADD 1

FISC 558
N 67
ECOFIN 1197

ÜBERMITTLUNGSVERMERK

Absender: Herr Jordi AYET PUIGARNAU, Direktor, im Auftrag des Generalsekretärs der Europäischen Kommission

Eingangsdatum: 12. Dezember 2018

Empfänger: Herr Jeppe TRANHOLM-MIKKELSEN, Generalsekretär des Rates der Europäischen Union

Nr. Komm.dok.: ANNEXES 1 to 6 to COM(2018) 832 final

Betr.: ANHANG des Vorschlags für einen Beschluss des Rates über den Standpunkt, der im Namen der Europäischen Union in dem Gemischten Ausschuss zu vertreten ist, welcher gemäß Artikel 41 Absatz 1 der Übereinkunft zwischen der Europäischen Union und dem Königreich Norwegen über die Zusammenarbeit der Verwaltungsbehörden, die Betrugsbekämpfung und die Beitreibung von Forderungen auf dem Gebiet der Mehrwertsteuer eingerichtet wurde

Die Delegationen erhalten in der Anlage das Dokument ANNEXES 1 to 6 to COM(2018) 832 final.

Anl.: ANNEXES 1 to 6 to COM(2018) 832 final



Brüssel, den 12.12.2018
COM(2018) 832 final

ANNEXES 1 to 6

ANHANG

des Vorschlags für einen

Beschluss des Rates

über den Standpunkt, der im Namen der Europäischen Union in dem Gemischten Ausschuss zu vertreten ist, welcher gemäß Artikel 41 Absatz 1 der Übereinkunft zwischen der Europäischen Union und dem Königreich Norwegen über die Zusammenarbeit der Verwaltungsbehörden, die Betrugsbekämpfung und die Beitreibung von Forderungen auf dem Gebiet der Mehrwertsteuer eingerichtet wurde

ANLAGE 1

Entwurf

BESCHLUSS Nr. 1/[Datum] des Gemischten Ausschusses vom [Datum] über die Annahme der Geschäftsordnung des Gemischten Ausschusses

DER GEMISCHTE AUSSCHUSS –

gestützt auf die Übereinkunft zwischen der Europäischen Union und dem Königreich Norwegen über die Zusammenarbeit der Verwaltungsbehörden, die Betrugsbekämpfung und die Beitreibung von Forderungen auf dem Gebiet der Mehrwertsteuer (im Folgenden die „Übereinkunft“), insbesondere auf Artikel 41 Absatz 1,

in Erwägung nachstehender Gründe:

- (a) Es ist erforderlich, Vorschriften über Zusammensetzung und Vorsitz des Ausschusses, Beobachter und Sachverständige, die Einberufung von Sitzungen, Tagesordnungen, die Sekretariatsunterstützung, Entwurf und Annahme von Sitzungsprotokollen, die Annahme von Beschlüssen und Empfehlungen sowie über Ausgaben festzulegen.
- (b) Es ist erforderlich, praktische Modalitäten für die Durchführung von Artikel 41 Absatz 3 der Übereinkunft festzulegen –

GIBT SICH FOLGENDE GESCHÄFTSORDNUNG:

Artikel 1

Zusammensetzung und Vorsitz

- (1) Der Gemischte Ausschuss besteht aus Vertretern der Europäischen Union und des Königreichs Norwegen (im Folgenden „die Vertragsparteien“).
- (2) Die Europäische Union wird durch die Europäische Kommission vertreten. Das Königreich Norwegen wird durch [.....] vertreten.
- (3) Der Vorsitz des Gemischten Ausschusses wird von den Vertragsparteien abwechselnd für jeweils zwei Kalenderjahre geführt. Die Dauer des ersten Vorsitzes endet am 31. Dezember des Jahres nach dem Jahr des Inkrafttretens der Übereinkunft. Den ersten Vorsitz wird die Europäische Union führen.

Artikel 2

Beobachter und Sachverständige

- (1) Vertreter der Mitgliedstaaten der Europäischen Union können als Beobachter teilnehmen.
- (2) Der Gemischte Ausschuss kann auch andere Personen als Beobachter zu seinen Sitzungen zulassen.
- (3) Beobachter können vom Vorsitz zur Teilnahme an den Beratungen zugelassen werden und ihr Fachwissen einbringen. Sie haben jedoch keine Stimmrechte und beteiligen sich nicht an der Formulierung der Beschlüsse und Empfehlungen des Gemischten Ausschusses.

- (4) Sachverständige mit besonderem Fachwissen können auch zu bestimmten Tagesordnungspunkten eingeladen werden.

Artikel 3

Einberufung von Sitzungen

- (1) Sitzungen des Gemischten Ausschusses werden vom Vorsitz mindestens einmal alle zwei Jahre einberufen. Jede Vertragspartei kann die Einberufung einer Sitzung veranlassen.
- (2) Datum und Ort jeder Sitzung werden von den Vertragsparteien festgelegt und vereinbart.
- (3) Sitzungen können auch in Form von Telekonferenzen/Videokonferenzen abgehalten werden.
- (4) Der Vorsitz übermittelt die Einladung der anderen Vertragspartei, den in Artikel 2 Absatz 2 genannten Beobachtern und den Sachverständigen mindestens 15 Arbeitstage vor der Sitzung. Die Europäische Kommission lädt die in Artikel 2 Absatz 1 genannten Vertreter der Mitgliedstaaten der Europäischen Union ein.
- (5) Die Sitzungen sind nicht öffentlich, sofern nichts anderes vereinbart wird. Die Beratungen des Gemischten Ausschusses sind vertraulich.

Artikel 4

Tagesordnung

- (1) Der Vorsitz stellt für jede Sitzung eine vorläufige Tagesordnung auf und übermittelt sie den Vertragsparteien spätestens sechs Monate vor der Sitzung. Die endgültige Tagesordnung wird spätestens 15 Arbeitstage vor der Sitzung zwischen den Vertragsparteien vereinbart und vom Vorsitz verteilt.
- (2) Referenzunterlagen und Belegdokumente werden den Vertragsparteien spätestens am Tag des Versands der vorläufigen Tagesordnung übermittelt.
- (3) Zu Tagesordnungspunkten, die Beschlüsse des Gemischten Ausschusses betreffen, sind der Antrag auf Aufnahme in die Tagesordnung und alle etwaigen diesbezüglichen Unterlagen mindestens sieben Monate vor der Sitzung an den Gemischten Ausschuss zu übermitteln.

Artikel 5

Sekretariat

- (1) Die Aufgaben des Sekretariats des Gemischten Ausschusses übernimmt der Vorsitz. Jegliche Korrespondenz an den Gemischten Ausschuss, einschließlich Anträgen auf Aufnahme bzw. Streichung von Punkten in die bzw. aus der Tagesordnung, ist an den Vorsitz zu richten.
- (2) Ungeachtet der vorstehenden Ausführungen fungiert die Kommission als Sekretär für die Übermittlung der statistischen Daten gemäß den Artikeln 20 und 39 der Übereinkunft.

Artikel 6

Sitzungsprotokoll

- (1) Der Vorsitz erstellt für jede Sitzung einen Protokollentwurf. Der Vorsitz verteilt das Protokoll unverzüglich, spätestens aber einen Monat nach der Sitzung. Das Protokoll wird von den Vertragsparteien in beiderseitigem Einvernehmen angenommen.
- (2) Der Vorsitz übermittelt den Vertragsparteien das angenommene Protokoll.

Artikel 7

Annahme von Beschlüssen und Empfehlungen

- (1) Alle Beschlüsse und Empfehlungen des Gemischten Ausschusses werden vorab von den Vertragsparteien erörtert.
- (2) Die Beschlüsse und Empfehlungen des Gemischten Ausschusses werden in seinen Sitzungen einstimmig angenommen.
- (3) Beschlüsse oder Empfehlungen können im schriftlichen Verfahren angenommen werden, sofern beide Vertragsparteien zustimmen.
- (4) Im schriftlichen Verfahren übermittelt der Vorsitz die Entwürfe der Beschlüsse und Empfehlungen an die Vertragsparteien und legt eine Frist für deren Stellungnahme fest. Lehnt eine Vertragspartei den Entwurf eines Rechtsakts nicht vor Ablauf dieser Frist ab, so gilt dies als stillschweigende Zustimmung zum Entwurf des Rechtsakts.
- (5) Der Vorsitz unterrichtet die Vertragsparteien unverzüglich, spätestens aber 14 Kalendertage nach Fristende vom Ergebnis des schriftlichen Verfahrens.

Artikel 8

Ausgaben

Jede Vertragspartei und gegebenenfalls jeder Beobachter trägt die Kosten, die ihr/ihm aus der Teilnahme an den Sitzungen des Gemischten Ausschusses entstehen.

Datum

ANLAGE 2

Entwurf

BESCHLUSS Nr. 2/[Datum] des Gemischten Ausschusses vom [Datum] zur Festlegung der Standardformblätter, der Informationsübermittlung und der praktischen Modalitäten für die Organisation von Kontakten zwischen den zentralen Verbindungsbüros

DER GEMISCHTE AUSSCHUSS, der gemäß Artikel 41 Absatz 1 der Übereinkunft zwischen der Europäischen Union und dem Königreich Norwegen über die Zusammenarbeit der Verwaltungsbehörden, die Betrugsbekämpfung und die Beitreibung von Forderungen auf dem Gebiet der Mehrwertsteuer (im Folgenden die „Übereinkunft“) eingerichtet wurde,

in Erwägung nachstehender Gründe:

- (1) a) Instrumente für die Informationsübermittlung, zum Beispiel Standardformblätter und elektronische Kommunikationssysteme, wurden bereits im Rahmen der Verordnung (EU) Nr. 904/2010 des Rates über die Zusammenarbeit der Verwaltungsbehörden und die Betrugsbekämpfung auf dem Gebiet der Mehrwertsteuer¹ und der Richtlinie 2010/24/EU des Rates über die Amtshilfe bei der Beitreibung von Forderungen in Bezug auf bestimmte Steuern, Abgaben und sonstige Maßnahmen² eingeführt, und diese sind mit der Zusammenarbeit der Verwaltungsbehörden im Rahmen der Übereinkunft in vollem Umfang vereinbar.
- (2) b) Es ist erforderlich, praktische Modalitäten für die Durchführung von Artikel 41 Absatz 2 Buchstaben d, e, g und h der Übereinkunft festzulegen –

HAT FOLGENDEN BESCHLUSS ERLASSEN:

Artikel 1

Standardformblätter

Gemäß Artikel 21 Absatz 1 und Artikel 40 Absatz 1 der Übereinkunft verwenden die zuständigen Behörden zur Übermittlung von Informationen im Rahmen der Titel II und III der Übereinkunft die für die Durchführung der Verordnung (EU) Nr. 904/2010 des Rates und der Richtlinie 2010/24/EU des Rates festgelegten Standardformblätter.

Struktur und Layout der Standardformblätter können an etwaige neue Anforderungen und Funktionen der Systeme für den Kommunikations- und Informationsaustausch angepasst werden, sofern die darin enthaltenen Daten und Informationen nicht wesentlich geändert werden.

¹ Verordnung (EU) Nr. 904/2010 des Rates vom 7. Oktober 2010 über die Zusammenarbeit der Verwaltungsbehörden und die Betrugsbekämpfung auf dem Gebiet der Mehrwertsteuer (ABl. L 268 vom 12.10.2010, S. 1).

² Richtlinie 2010/24/EU des Rates vom 16. März 2010 über die Amtshilfe bei der Beitreibung von Forderungen in Bezug auf bestimmte Steuern, Abgaben und sonstige Maßnahmen (ABl. L 84 vom 31.3.2010, S. 1).

Artikel 2

Informationsübermittlung

Alle Informationen im Rahmen der Titel II und III der Übereinkunft werden ausschließlich auf elektronischem Wege über das CCN/CSI-Netz übermittelt, es sei denn, dies ist aus technischen Gründen nicht praktikabel.

Artikel 3

Organisation der Kontakte

- (1) Bei der Organisation der Kontakte zwischen den zentralen Verbindungsbüros und den Verbindungsstellen gemäß Artikel 4 Absatz 2 Buchstabe b und Artikel 4 Absatz 3 Buchstabe b der Übereinkunft stützen sich die zuständigen Behörden auf die für die Durchführung der Richtlinie 2010/24/EU des Rates angenommenen Regeln.
- (2) Die gemäß Artikel 4 Absatz 2 der Übereinkunft benannten zentralen Verbindungsbüros halten die Liste der gemäß Artikel 4 Absätze 3 und 4 benannten Verbindungsstellen und zuständigen Beamten auf dem aktuellen Stand und stellen sie den übrigen zentralen Verbindungsbüros elektronisch zur Verfügung.

Datum

ANLAGE 3

Entwurf

BESCHLUSS Nr. 3/[Datum] des Gemischten Ausschusses vom [Datum] zur Festlegung des Verfahrens für den Abschluss der Dienstgütevereinbarung

DER GEMISCHTE AUSSCHUSS, der gemäß Artikel 41 Absatz 1 der Übereinkunft zwischen der Europäischen Union und dem Königreich Norwegen über die Zusammenarbeit der Verwaltungsbehörden, die Betrugsbekämpfung und die Beitreibung von Forderungen auf dem Gebiet der Mehrwertsteuer (im Folgenden die „Übereinkunft“) eingerichtet wurde,

in Erwägung nachstehender Gründe:

- (3) a) Zur Sicherstellung der technischen Qualität und der Quantität der für das Funktionieren der Kommunikations- und Informationsaustauschsysteme vorgesehenen Dienste wird gemäß dem vom Gemischten Ausschuss festgelegten Verfahren eine Dienstgütevereinbarung geschlossen.
- (4) b) Es ist erforderlich, praktische Modalitäten für die Durchführung von Artikel 5 der Übereinkunft festzulegen –

HAT FOLGENDEN BESCHLUSS ERLASSEN:

Einziges Artikel

- (1) Die in Artikel 5 der Übereinkunft genannte Dienstgütevereinbarung wird vom Gemischten Ausschuss geschlossen und ist für die Vertragsparteien ab dem Tag nach ihrer Genehmigung durch den Gemischten Ausschuss bindend.
- (2) Jede Vertragspartei kann eine Überarbeitung der Dienstgütevereinbarung verlangen, indem sie dem Vorsitz des Gemischten Ausschusses einen entsprechenden Antrag übermittelt. Bis der Gemischte Ausschuss über die vorgeschlagenen Änderungen entscheidet, bleiben die Bestimmungen der zuletzt geschlossenen Dienstgütevereinbarung in Kraft.

Datum

ANLAGE 4

Entwurf

BESCHLUSS Nr. 4/[Datum] des Gemischten Ausschusses vom [Datum] über den Abschluss der Dienstgütevereinbarung für die Systeme und Anwendungen für die Zusammenarbeit der Verwaltungsbehörden und die Beitreibung von Forderungen auf dem Gebiet der Mehrwertsteuer

1. REFERENZDOKUMENTE UND ANWENDBARE DOKUMENTE

1.1. ANWENDBARE RECHTSAKTE

Diese Dienstgütevereinbarung („Service Level Agreement“, SLA) trägt den nachstehend aufgeführten Übereinkünften und anwendbaren Beschlüssen („Applicable Documents“, AD) Rechnung.

[AD.1.]	Übereinkunft zwischen der Europäischen Union und dem Königreich Norwegen über die Zusammenarbeit der Verwaltungsbehörden, die Betrugsbekämpfung und die Beitreibung von Forderungen auf dem Gebiet der Mehrwertsteuer (die „Übereinkunft“) (ABl. L 195 vom 1.8.2018, S. 3).
[AD.2.]	Beschluss XX des Gemischten Ausschusses vom [Datum] zur Durchführung von Artikel 41 Absatz 2 Buchstaben d, e, g und h der Übereinkunft in Bezug auf die Standardformblätter, die Kommunikation und die Organisation von Kontakten

Tabelle 1: Anwendbare Rechtsakte

1.2. REFERENZDOKUMENTE

Diese SLA trägt den Informationen Rechnung, die in den folgenden Referenzdokumenten (RD) enthalten sind. Die geltenden Fassungen der Dokumente werden auf CIRCABC oder dem ITSM-Webportal veröffentlicht.

[RD.1.]	CCN Mail III User Guide for NAs (<i>ITSM Web Portal</i>)
[RD.2.]	CCN Intranet – Local Network Administrator Guide (<i>ITSM Web Portal</i>)
[RD.3.]	Statistics – Guidelines and instructions (ANNEX rev1) to SCAC No 560
[RD.4.]	VAT e-Forms – Functional Specifications
[RD.5.]	VAT e-Forms – Technical Specifications
[RD.6.]	Recovery e-Forms – Functional Specifications
[RD.7.]	Recovery e-Forms – Technical Specifications
[RD.8.]	CCN/CSI General Security Policy (ITSM Web Portal)

[RD.9.]	CCN Gateway Management Procedures (ITSM Web Portal)
[RD.10.]	CCN/CSI Baseline Security Checklist (ITSM Web Portal)

Tabelle 2: Referenzdokumente

2. **TERMINOLOGIE**

2.1. **AKRONYME**

AKRONYM	DEFINITION
CCN/CSI	Common Communication Network/Common System Interface (Gemeinsames Kommunikationsnetz/Gemeinsame Systemschnittstelle)
CIRCABC	Communication and Information Resource Centre for Administrations, Businesses and Citizens
CLO	Central Liaison Office (Zentrales Verbindungsbüro)
CT	Conformance Testing (Konformitätsprüfung)
DG	Directorate General (Generaldirektion)
EoF	Exchange of Forms (Austausch von Formularen)
FAT	Factory Acceptance Tests (Betriebsabnahmeprüfung)
HTTP	Hypertext Transfer Protocol (Hypertext-Übertragungsprotokoll)
ITIL ³	Information Technology Infrastructure Library
ITSM	Information Technology Service Management
MEZ	Mitteuropäische Zeit
MwSt	Mehrwertsteuer
Partei	Im Rahmen dieser SLA bezeichnet der Ausdruck „Partei“ entweder Norwegen oder die Kommission.

Tabelle 3: Akronyme

2.2. **DEFINITIONEN**

AUSDRUCK	DEFINITION
Arbeitstage und -stunden (ITSM-Servicedesk)	7.00 bis 20.00 Uhr (MEZ), 5 Tage pro Woche (Montag bis Freitag einschließlich Feiertage)
MEZ	Mitteuropäische Zeit, GMT+ 1 Stunde und während der Sommerzeit GMT+ 2 Stunden

Tabelle 4: Definitionen

³

ITIL:

- <http://www.iti1-officialsite.com>
- http://www.best-management-practice.com/gempdf/itSMF_An_Introductory_Overview_of_ITIL_V3.pdf

3. EINLEITUNG

Dieses Dokument besteht aus einer SLA zwischen dem Königreich Norwegen (im Folgenden „Norwegen“) und der Europäischen Kommission (im Folgenden „Kommission“), die gemeinsam als „die Parteien der SLA“ bezeichnet werden.

3.1. UMFANG DER SLA

In Artikel 5 der Übereinkunft heißt es: „Zur Sicherstellung der technischen Qualität und der Quantität der für das Funktionieren der Mitteilungs- und Informationsaustauschsysteme vorgesehenen Dienste wird ... eine Dienstgütevereinbarung geschlossen.“

Die vorliegende SLA legt die Beziehungen zwischen dem Königreich Norwegen und der Kommission in Bezug auf die Nutzung der Systeme und Anwendungen für die Zusammenarbeit der Verwaltungsbehörden und die Beibehaltung von Forderungen im MwSt-Bereich sowie die Beziehungen zwischen dem Königreich Norwegen und den Mitgliedstaaten in Bezug auf den Austausch von Formularen fest.

Die folgenden Systeme sind operationell und unterliegen den Bestimmungen der SLA:

- EoF (Austausch von Formularen);
- Monitoring, Statistiken und Tests.

Die Kommission legt das Verfahren fest, mit dem eine Einigung über die IT-gestützte Verwaltungszusammenarbeit erzielt werden soll. Dies schließt die Punkte Normen, Verfahren, Werkzeuge, Technologie und Infrastruktur ein. Norwegen erhält Unterstützung, damit gewährleistet ist, dass Datenaustauschsysteme zur Verfügung stehen und ordnungsgemäß implementiert werden. Die Kommission übernimmt zudem das Monitoring, die Überwachung und die Bewertung des Gesamtsystems. Darüber hinaus stellt die Kommission Norwegen Leitlinien zur Verfügung, die im Zusammenhang mit diesem Informationsaustausch einzuhalten sind.

Alle in der SLA genannten Ziele gelten nur unter normalen Arbeitsbedingungen.

Im Falle von Ereignissen höherer Gewalt wird die Anwendbarkeit der SLA für Norwegen für die Dauer der betreffenden Situation ausgesetzt.

Bei einem Ereignis höherer Gewalt handelt sich um ein unvorhersehbares Ereignis, das sich der Kontrolle Norwegens oder der Kommission entzieht und das nicht auf eine Handlung oder Nichtdurchführung präventiver Maßnahmen der verantwortlichen Partei zurückzuführen ist. Solche Ereignisse beziehen sich auf Regierungsmaßnahmen, Krieg, Brand, Explosion, Überschwemmung, Einfuhr- oder Ausfuhrregelungen oder Embargos und Arbeitsstreitigkeiten.

Die Partei, die höhere Gewalt geltend macht, unterrichtet die andere Partei unverzüglich über die Tatsache, dass es aufgrund von Ereignissen höherer Gewalt nicht möglich ist, bestimmte Dienste zu erbringen oder die SLA-Ziele zu erreichen, und gibt die betroffenen Dienste und Ziele an. Ist der Zustand höherer Gewalt nicht mehr gegeben, so setzt die betroffene Partei die andere Partei ebenfalls unverzüglich davon in Kenntnis.

3.2. LAUFZEIT DER VEREINBARUNG

Die SLA bindet die Vertragsparteien ab dem Tag nach ihrer Genehmigung durch den mit Artikel 41 der Übereinkunft eingesetzten Gemischten Ausschuss (im Folgenden „Gemischter Ausschuss“).

4. ZUSTÄNDIGKEITEN

Zweck dieser SLA ist es, die Qualität und die Quantität der von der Kommission und Norwegen zu erbringenden Dienste zu gewährleisten, damit Norwegen und der Kommission die genannten Systeme und Anwendungen für die Verwaltungszusammenarbeit und die Beitreibung von Forderungen im MwSt-Bereich zur Verfügung gestellt werden können.

4.1. DIENSTE, DIE DIE KOMMISSION NORWEGEN ZUR VERFÜGUNG STELLT

Die **Kommission** stellt folgende Dienste zur Verfügung:

- Operationelle Dienste wie folgt:
 - Helpdesk und Betrieb:
 - (a) Helpdesk-Unterstützung;
 - (b) Vorfallmanagement;
 - (c) Monitoring und Überprüfung;
 - (d) Schulung;
 - (e) Sicherheitsmanagement;
 - (f) Berichterstattung und Statistiken;
 - (g) Beratung.
 - Referenzzentrum:
 - (a) Informationsmanagement;
 - (b) Dokumentationszentrum (CIRCABC);

Um diese Dienste anbieten zu können, unterhält die Kommission folgende Anwendungen:

- statistische Anwendungen;
- CIRCABC;
- Servicedesk-Tool.

4.2. DIENSTE, DIE NORWEGEN DER KOMMISSION ZUR VERFÜGUNG STELLT

Norwegen stellt folgende Dienste zur Verfügung:

- Norwegen übermittelt der Kommission sämtliche verfügbaren Informationen, die für die Anwendung der Übereinkunft sachdienlich sind.
- Norwegen setzt die Kommission über alle außergewöhnlichen Umstände in Kenntnis.

- Norwegen legt jährlich die Statistiken über die Übermittlung von Informationen gemäß Artikel 20 der Übereinkunft vor.

5. ÜBERSICHT ÜBER DIE DIENSTE IM RAHMEN DER SLA

Dieses Kapitel enthält eine ausführliche Beschreibung der quantitativen und qualitativen Aspekte der von der Kommission und von Norwegen zu erbringenden Dienste (siehe oben).

5.1. DIENSTE DER KOMMISSION

5.1.1. ServiceDesk

5.1.1.1. *Vereinbarung*

Die Kommission stellt einen ServiceDesk bereit, um Fragen zu beantworten und über Probleme Bericht zu erstatten, die Norwegen mit den Systemen und Anwendungen für die Zusammenarbeit der Verwaltungsbehörden und die Beibehaltung von Forderungen im MwSt-Bereich oder mit Teilkomponenten, die sich auf die Systeme und Anwendungen auswirken könnten, hat. Dieser ServiceDesk wird von ITSM betrieben; seine Arbeitszeiten entsprechen jenen von ITSM.

Die Verfügbarkeit des ITSM-ServiceDesks ist in mindestens 95 % der Arbeitszeit zu gewährleisten. Alle Fragen oder Probleme können dem ServiceDesk während der ITSM-Arbeitszeit per Telefon, Fax oder E-Mail und außerhalb dieser Zeit per E-Mail oder Fax mitgeteilt werden. Werden diese Fragen oder Probleme außerhalb der Arbeitszeiten von ITSM übermittelt, so wird automatisch davon ausgegangen, dass sie am darauffolgenden Arbeitstag um 8.00 Uhr MEZ eingegangen sind.

Der ServiceDesk registriert und klassifiziert die Serviceanfragen in einem Managementsystem (Service-Management-Tool) und informiert die betreffende Partei über jede Statusänderung in Bezug auf ihre Serviceanfragen.

ITSM fungiert als erste Anlaufstelle für die Nutzer und leitet Serviceanfragen innerhalb der angegebenen Frist weiter, für die eine andere Partei (z. B. das Entwicklerteam oder ITSM-Vertragspartner) zuständig ist. ITSM stellt sicher, dass in mindestens 95 % der Fälle in einem Berichtsmonat die Registrierungsfristen eingehalten werden.

ITSM überwacht die Abwicklung sämtlicher Serviceanfragen und leitet ein Eskalationsverfahren ein, indem es die Kommission informiert, wenn der Abwicklungszeitraum einen vorab festgelegten Schwellenwert, der von der Art des Problems abhängt, überschreitet.

Die Prioritätsebene ist ausschlaggebend für die Reaktions- und Abwicklungsfrist. ITSM legt die Priorität fest, jedoch können die Mitgliedstaaten oder die Kommission um Behandlung gemäß einer bestimmten Prioritätsebene ersuchen.

Die *Registrierungszeit* ist die maximale Zeitspanne, die zwischen dem Eingang der E-Mail und dem Versand der Bestätigungsmail vergehen darf.

Die *Abwicklungszeit* ist die Zeitspanne zwischen der Registrierung der Anfrage und der Übermittlung von Informationen betreffend die Abwicklung an die anfragende Partei. Dies schließt auch die Zeit ein, die mit dem Abschluss des betreffenden Vorgangs verbunden ist.

Bei diesen Fristen handelt es sich nicht um absolute Fristen, da hier nur die Zeitpunkte zugrunde gelegt werden, zu denen ITSM auf die Serviceanfragen reagiert.

Wird eine Serviceanfrage an Norwegen, die Kommission oder eine andere Partei (z. B. Entwicklerteam, ITSM-Vertragspartner) weitergeleitet, so wird die entsprechende Zeit für die Abwicklungszeit des ITSM nicht berücksichtigt.

ITSM stellt sicher, dass in mindestens 95 % der Fälle in einem Monatsmonat die Registrierungs- und Abwicklungsfristen eingehalten werden.

PRIORITÄT	REGISTRIERUNGSZEIT	ABWICKLUNGSZEIT
P1: Kritisch	0,5 Stunde	4 Stunden
P2: Hoch	0,5 Stunde	13 Stunden (1 Tag)
P3: Mittel	0,5 Stunde	39 Stunden (3 Tage)
P4: Niedrig	0,5 Stunde	65 Stunden (5 Tage)

Tabelle5: Registrierungs- und Abwicklungszeiten (Arbeitsstunden/Tage)

5.1.1.2. *Berichterstattung*

Die Kommission berichtet wie folgt über alle mit den Systemen und Anwendungen für die Verwaltungszusammenarbeit und die Beitreibung von Forderungen im MwSt-Bereich zusammenhängenden Serviceanfragen:

- in Bezug auf alle im Laufe des Monats abgeschlossenen Serviceanfragen für Norwegen;
- in Bezug auf alle im Laufe des Monats eingegangenen Serviceanfragen für Norwegen;
- in Bezug auf alle zum Berichtszeitpunkt anhängigen Serviceanfragen für Norwegen.

5.1.2. **Statistische Dienste**

5.1.2.1. *Vereinbarung*

Die Kommission erstellt Statistiken über die Anzahl der ausgetauschten Formulare in den Bereichen Mehrwertsteuer und Beitreibung unter Verwendung von CCN/Mail; die Statistiken sind auf dem ITSM-Webportal verfügbar.

5.1.2.2. *Berichterstattung*

Die Kommission erstellt gegebenenfalls einen Bericht über die Berichte über die Konformitätsprüfung und stellt sie Norwegen zur Verfügung.

5.1.3. **Exchange of Forms (Austausch von Formularen)**

5.1.3.1. *Vereinbarung*

Die folgende Tabelle zeigt die für den Austausch von Formularen vorgesehene maximale Übermittlungsfrist bzw. maximale Antwortzeit, wie in den einschlägigen Rechtsvorschriften festgelegt.

<i>CCN/Mail (Mailbox)</i>	<i>Formular</i>	<i>Frist</i>

<i>CCN/Mail (Mailbox)</i>	<i>Formular</i>	<i>Frist</i>
VIESCLO	Informationsaustausch gemäß den Artikeln 7, 10, 12 und 18 der Übereinkunft 0 Allgemeiner Austausch	Die Informationsübermittlung erfolgt möglichst rasch, spätestens jedoch <u>drei Monate nach dem Zeitpunkt des Eingangs des Ersuchens (Artikel 8 der Übereinkunft 0)</u> . Liegen der ersuchten Behörde die angeforderten Informationen bereits vor, so verkürzt sich die Frist auf höchstens <u>einen Monat (Artikel 8 der Übereinkunft 0)</u> .
VIESCLO	Informationsaustausch gemäß den Artikeln 7, 10, 12 und 18 der Übereinkunft 0 Zustellungsersuchen	Zustellungsersuchen mit unverzüglicher Antwort (<i>Artikel 12 0 der Übereinkunft</i>).
TAXFRAUD	Informationsaustausch gemäß den Artikeln 7, 10, 12 und 18 der Übereinkunft 0 Austausch zu Betrugsfällen	Informationen zu Missing-Trader-Fällen werden übermittelt, <u>sobald die Informationen vorliegen</u> .
TAXAUTO	Automatischer Austausch	Die Kategorien von Informationen, die gemäß Artikel 11 der Übereinkunft Gegenstand eines automatischen Austauschs sind, werden vom Gemischten Ausschuss festgelegt.
REC-A-CUST; REC-B-VAT; REC-C-EXCISE; REC-D-INCOME-CAP; REC-E-INSUR; REC-F-INHERIT-GIFT;	Auskunftsersuchen gemäß Artikel 22 der Übereinkunft 0 Zustellungsersuchen gemäß Artikel 25 der Übereinkunft 0 Beitreibungersuchen gemäß Artikel 27 der	Auskunftsersuchen: - Empfangsbestätigung innerhalb von 7 Kalendertagen; - Information über den aktuellen Stand nach 6 Monaten ab dem Datum der Bestätigung Zustellungsersuchen:

<i>CCN/Mail (Mailbox)</i>	<i>Formular</i>	<i>Frist</i>
REC-G-NAT-IMMOV; REC-H-NAT-TRANSP; REC-I-NAT-OTHER; REC-J-REGIONAL; REC-K-LOCAL; REC-L-OTHER; REC-M-AGRI	Übereinkunft 0 Ersuchen um Sicherungsmaßnahmen gemäß Artikel 33 der Übereinkunft 0	- Empfangsbestätigung innerhalb von 7 Kalendertagen; Beitreibungsersuchen und Ersuchen um Sicherungsmaßnahmen: - Empfangsbestätigung innerhalb von 7 Kalendertagen; - Information über den aktuellen Stand alle 6 Monate, gerechnet ab dem Datum der Bestätigung

Tabelle 6: Fristen für den Austausch von Formularen

5.1.3.2. *Berichterstattung*

Norwegen übermittelt der Kommission ebenfalls jährlich statistische Daten per E-Mail in Bezug auf die Übermittlung von Informationen gemäß den Artikeln 20 und 39 der Übereinkunft [RD.3.].

5.1.4. **Problemmanagement**

5.1.4.1. *Vereinbarung*

Norwegen sieht einen angemessenen Problemregistrierungs⁴- und Follow-up-Mechanismus für Probleme vor, die sich auf den Anwendungshost, die Systemsoftware, Daten und Anwendungssoftware des Landes auswirken.

Probleme mit jedwedem Teil des CCN-Netzes (Gateways und/oder Exchange-Mail-Server) sind ITSM unverzüglich zu melden.

5.1.4.2. *Berichterstattung*

Norwegen unterrichtet ITSM, wenn es ein internes Problem mit der technischen Infrastruktur in Bezug auf seine eigenen Systeme und Anwendungen für die Verwaltungszusammenarbeit und Beitreibung von Forderungen im MwSt-Bereich gibt.

Ist Norwegen der Auffassung, dass ein Problem, das ITSM gemeldet wurde, nicht zufriedenstellend bearbeitet oder gelöst wird bzw. wurde, teilt Norwegen dies der Kommission so bald wie möglich mit.

⁴ Verbunden mit den Problem- und Änderungsmanagementprozessen von ITIL.

5.1.5. Sicherheitsmanagement

5.1.5.1. *Vereinbarung*⁵

Norwegen schützt seine Systeme und Anwendungen für die Verwaltungszusammenarbeit und die Beitreibung von Forderungen im MwSt-Bereich vor Verstößen gegen die Sicherheitsvorschriften und erfasst alle betreffenden Verstöße und die vorgenommenen Sicherheitsverbesserungen.

Norwegen wendet die in den folgenden Dokumenten enthaltenen Sicherheitsempfehlungen und/oder -anforderungen an:

Titel	Version	Datum
https security recommendations of CCN /Mail III Webmail access – Ref. CCN /Mail III User Guide for NAs	3.0	15.6.2012
Security recommendations of CCN /Mail III Webmail access – Ref. CCN Intranet – Local Network Administrator Guide	4.0	11.9.2008

5.1.5.2. *Berichterstattung*

Norwegen erstattet der Kommission auf Ad-hoc-Basis Bericht über alle Verstöße gegen die Sicherheitsvorschriften und die ergriffenen Maßnahmen.

5.2. DIENSTE NORWEGENS

5.2.1. Alle Bereiche der Dienstverwaltung

5.2.1.1. *Vereinbarung*

Norwegen registriert alle Nichtverfügbarkeiten oder Änderungen⁶ der technischen, funktionellen und organisatorischen Aspekte der Systeme und Anwendungen Norwegens für die Zusammenarbeit der Verwaltungsbehörden und die Beitreibung von Forderungen im MwSt-Bereich.

5.2.1.2. *Berichterstattung*

Norwegen unterrichtet ITSM gegebenenfalls über Nichtverfügbarkeiten oder Änderungen in Bezug auf die technischen, funktionellen oder organisatorischen Aspekte seines Systems. ITSM ist stets über Änderungen in Bezug auf das Betriebspersonal (Operatoren, Systemadministratoren) zu unterrichten.

5.2.2. Servicedesk

5.2.2.1. *Vereinbarung*

Norwegen stellt einen Servicedesk zur Verfügung, um auf Vorfälle zu reagieren, die Norwegen zugewiesen wurden, um Hilfe zu leisten und Prüfungen durchzuführen. Die Arbeitszeiten des Servicedesks sollten mit jenen des ITSM-Servicedesk an den ITSM-Arbeitstagen übereinstimmen. Der Servicedesk Norwegens ist an Arbeitstagen mindestens zwischen 10.00 und 16.00 Uhr MEZ tätig. Ausgenommen ist Norwegens

⁵ Dies sind die Fassungen der Dokumente, die zum Zeitpunkt der Erstellung dieser SLA verfügbar sind. Die Leserinnen und Leser werden gebeten, etwaige Aktualisierungen auf dem CCN/CSI-Portal (<http://portal.ccntc.cncsi.int:8080/portal/DesktopDefault.aspx?tabid=1>) zu konsultieren.

⁶ Es wird empfohlen, die für das Vorfällemanagement in ITIL beschriebenen Grundsätze anzuwenden.

Nationalfeiertag. Es wird empfohlen, dass der Servicedesk Norwegens bei der Behandlung von Fragen und Vorfällen dem ITIL-Leitfaden (ITIL service support guidelines) folgt.

5.2.2.2. *Berichterstattung*

Norwegen unterrichtet ITSM gegebenenfalls über Verfügbarkeitsprobleme im Zusammenhang mit seinem Servicedesk.

6. **QUALITÄTSMESSUNG**

6.1. **VEREINBARUNG**

Die Kommission bewertet die Berichte (Tätigkeitsberichte von ITSM, Mitteilungen, Statistiken, sonstige Informationen), die sie von ITSM und Norwegen erhält, bestimmt den Grad, zu dem diese SLA eingehalten wurde, und kontaktiert bei Problemen Norwegen, um die Probleme zu lösen und sicherzustellen, dass die Qualität der Dienste im Einklang mit dieser Vereinbarung steht.

6.2. **BERICHTERSTATTUNG**

Die Kommission erstattet Norwegen monatlich Bericht über die Dienstgüte gemäß Abschnitt 5.1.2.

7. **GENEHMIGUNG DER SLA**

Die Dienstgütevereinbarung (SLA) muss vom Gemischten Ausschuss genehmigt werden, damit sie anwendbar ist.

8. **ÄNDERUNGEN DER SLA**

Die Dienstgütevereinbarung (SLA) wird auf schriftlichen Antrag der Kommission oder Norwegens an den Gemischten Ausschuss überprüft.

Bis der Gemischte Ausschuss über die vorgeschlagenen Änderungen entscheidet, bleiben die Bestimmungen der aktuellen SLA in Kraft. Der Gemischte Ausschuss fungiert als Entscheidungsgremium für die vorliegende Vereinbarung.

9. **KONTAKTSTELLE**

Für Fragen oder Anmerkungen zu diesem Dokument wenden Sie sich bitte an:

DIENSTEANBIETER – SERVICEDESK

support@itsmtaxud.europa.eu

Datum

ANLAGE 5

Entwurf

BESCHLUSS Nr. 5/[Datum] des Gemischten Ausschusses vom [Datum] zur Annahme der Dienstgütevereinbarung (Service Level Agreement, SLA) für das Common Communication Network/Common System Interface (CCN/CSI-SLA)

1. REFERENZDOKUMENTE UND ANWENDBARE UNTERLAGEN

1.1. ANWENDBARE RECHTSAKTE

Diese CCN/CSI-SLA trägt den nachstehend aufgeführten Übereinkünften und anwendbaren Beschlüssen Rechnung.

[AD.1.]	Übereinkunft zwischen der Europäischen Union und dem Königreich Norwegen über die Zusammenarbeit der Verwaltungsbehörden, die Betrugsbekämpfung und die Beitreibung von Forderungen auf dem Gebiet der Mehrwertsteuer (die „Übereinkunft“) (ABl. L 195 vom 1.8.2018, S. 3).
[AD.2.]	Beschluss XX des Gemischten Ausschusses vom [Datum] zur Durchführung von Artikel 41 Absatz 2 Buchstaben d, e, g und h der Übereinkunft in Bezug auf die Standardformblätter, die Kommunikation und die Organisation von Kontakten

Tabelle 7: Anwendbare Rechtsakte

1.2. REFERENZDOKUMENTE

In dieser CCN/CSI-SLA werden die in den folgenden Referenzdokumenten enthaltenen Informationen berücksichtigt. Die anwendbaren Fassungen (Versionen) der Dokumente sind die, die zum Zeitpunkt der Unterzeichnung dieser Vereinbarung verfügbar sind.

ID	REFERENZ	TITEL	VERSION
RD1	CCN-COVW-GEN	CCN/CSI & SPEED2 Systems Overview	EN18.01
RD2	CCN-CMPRW-GW	CCN Gateways Manage Procedures	EN19.20
RD3	CCN-CSEC-POL	CCN/CSI General Secu Policy	EN05.00
RD4	CCN-CSEC-BSCK	CCN/CSI Baseline Secu Checklist	EN03.00
RD5	CCN-CLIST-ROL	Description of CCN/CS	EN02.10
RD6	CCN-CNEX-031	External note 031 - Proc for the Move of a CCN/ Site	EN06.20
RD7	CCN-CNEX-060	External Note 060 - Inst new CCN Site	EN02.20
RD8	CCN/CSI-PRG-AP/C- 01-MARB	CCN/CSI-PRG-AP/C-0 MARB-Application Programming Guide (C	EN11.00

		Language)	
--	--	-----------	--

Tabelle 8: Referenzunterlagen

2. TERMINOLOGIE

2.1. AKRONYME

AKRONYME	DEFINITION
ACT	Application Configuration Tool (Tool für die Anwendungskonfiguration)
AIX	Unix-Betriebssystem von IBM
CBS	Central Backup Site
CCN	Common Communication Network (Gemeinsames Kommunikationsnetz)
CCN/CSI	Common Communication Network/Common System Interface (Gemeinsames Kommunikationsnetz/Gemeinsame Systemschnittstelle)
CCN/WAN	Rahmendienst für die Bereitstellung von Netzdiensten für das CCN
CI	Configuration Item (Konfigurationsobjekt)
CIRCABC	Communication and Information Resource Centre for Administrations, Businesses and Citizens
COTS	Common off-the-shelf (handelsüblich, gängig)
CPR	Customer Premises Router (Router beim Kunden)
CSA	CCN Security Administrator (CCN-Sicherheitsadministrator)
CSI	Common Systems Interface (gemeinsame Systemschnittstelle)
DG	Directorate General (Generaldirektion)
DMZ	De-Militarised Zone (entmilitarisierte Zone)
EC	European Commission (Europäische Kommission)
ESTAT	Eurostat
FW	Firewall
HPUX	Unix-Betriebssystem von Hewlett Packard
HTTP	Hyper Text Transfer Protocol (Hypertext-Übertragungsprotokoll)
HTTPS	Hyper Text Transfer Protocol - Secure (sicheres Hypertext-Übertragungsprotokoll)
HVAC	Heating, Ventilating, and Air-Conditioning (Heizung, Lüftung und Klimatisierung)
HW	Hardware
ICT	Information and Communication Technology (Informations- und Kommunikationstechnologie)
IMAP	Internet Message Access Protocol
IP	Internetprotokoll
ITCAM	IBM Tivoli Composite Application Manager
ITS	IT Services (IT-Dienste)
ITSM	IT Service Management (IT-Diensteverwaltung)
LAN	Local Area Network (lokales Netzwerk)
LSA	Lokaler Systemadministrator

MQ	IBM MQ Series Software
MVS	Multiple Virtual Storage
N/A	Not Applicable (nicht zutreffend/entfällt)
NA	National Administration (nationale Verwaltung)
NDI	Nationale Domain Interface (Schnittstelle für nationale Domain)
OBS	Orange Business Services
OLA	Operational Level Agreement
OLAF	Office de Lutte Anti-Fraude (Amt für Betrugsbekämpfung)
OS	Operating System (Betriebssystem)
OSP	Obligation of Service Provider (Pflicht des Diensteanbieters)
OSR	Obligation of Service Requester (Pflicht des Diensteanforderers)
POL	Policy
PoP	Point of Presence (Präsenzpunkt)
PRG	Programm
QA	Quality Assurance (Qualitätssicherung)
RAP	Remote API Proxy
RD	Referenzdokument
REV	Revision
RFA	Request For Action (Handlungsanforderung)
ROL	Role (Funktion/Aufgabe)
SFI	Submit For Information
SMTP	Simple Mail Transport Protocol
SQI	Service Quality Indicator (Dienstqualitätsindikator)
SSG	Secure Services Gateways (Juniper Encryption box) (Gateways für sichere Dienste (Juniper-Verschlüsselungsbox))
SW	Software
TAXUD	Steuern und Zollunion
TCP	Transmission Control Protocol
UPS	Uninterruptible Power Supply (unterbrechungsfreie Stromversorgung)
VM	Virtual Machine
VPN	Virtual Private Network (virtuelles privates Netz)
WAN	Wide Area Network

Tabelle 9: Akronyme

2.2. DEFINITIONEN VON AUSDRÜCKEN FÜR DIE ZWECKE DER CCN/CSI-SLA

AUSDRUCK	BESCHREIBUNG
Meldezeitraum	Der abgelaufene abgedeckte Zeitraum beträgt einen Monat.
Arbeitstag	Die Arbeitstage sind die Arbeitstage des Servicedesks (SD) des Diensteanbieters. Dies sind sieben Tage pro Woche, einschließlich Feiertagen.
Arbeitsstunde	Die Arbeitsstunden sind die Arbeitsstunden des SD des Diensteanbieters. Dies sind 24/24 während der Arbeitstage.
Dienstzeit	Die „Dienstzeit“ des Diensteanbieters ist der Zeitraum, in dem die SD-Funktion abgedeckt ist. Der Dienst wird vom

	<p>SD des Diensteanbieters rund um die Uhr (24/24) während sieben Tagen pro Woche, einschließlich Feiertagen, gewährleistet.</p> <p>Abhängig vom Servicefenster des CI wird sofort gehandelt (24*7), oder die Intervention wird für den nächsten Tag eingeplant. Briefe, Faxe, E-Mails und elektronische Anfragen (über das ITSM-Portal) werden jederzeit akzeptiert. Eingehende Anfragen werden im Servicedesk-Managementsystem des Diensteanbieters als „Serviceanfrage“ registriert.</p>
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Tabelle 10: Definitionen

3. EINLEITUNG

Dieses Dokument besteht aus einem Common Communication Network/Common System Interface Service Level Agreement (CCN/CSI-SLA) zwischen der Europäischen Kommission („Diensteanbieter“) und dem Königreich Norwegen („Diensteanforderer“), die kollektiv als „Parteien des SLA“ bezeichnet werden.

Der „Diensteanbieter“ umfasst die nachstehend aufgeführten Organisationseinheiten der Generaldirektion (DG) TAXUD:

- Referat B2 der DG TAXUD, das alle CCN/CSI-Tätigkeiten koordiniert;
- ITSM3 Operations, der operative Dienste erbringt;
- CCN2DEV, der CCN-Software bereitstellt (evolutionäre und korrigierende Wartungsdienste);
- Europaweiter Backbone-Netzbetreiber (CCN/WAN, derzeit OBS).

Je nach Art des angeforderten Dienstes wird einer der Diensteanbieter die Aufgabe erfüllen.

Der „Diensteanforderer“ ist die nationale Steuerverwaltung (NA) Norwegens. Bei den Organisationseinheiten innerhalb der NA handelt es sich um

- Das **nationale CCN Support-Zentrum**, das für den Support und die Verwaltung der CCN-Infrastrukturausrüstung der DG TAXUD in den Räumlichkeiten der NA zuständig ist, sowie für die nationale Infrastruktur, die die Anwendungen unterstützt, die über die CCN/CSI-Infrastruktur laufen;
- das **nationale Application-Support-Zentrum**, das für den nationalen Support der Anwendungen der Europäischen Kommission (EC) zuständig ist, die in der nationalen Domain laufen und die CCN/CSI-Infrastrukturdienste nutzen;
- die **nationalen Application-Development-Teams**, die für die Entwicklung von Anwendungen mithilfe der CCN/CSI-Infrastruktur zuständig sind, einschließlich ihrer Unterauftragnehmer.

3.1. UMFANG DER CCN/CSI-DIENSTGÜTEVEREINBARUNG

In Artikel 5 der Übereinkunft heißt es: „Zur Sicherstellung der technischen Qualität und der Quantität der für das Funktionieren der Mitteilungs- und Informationssysteme vorgesehenen Dienste wird ... eine Dienstgütevereinbarung geschlossen.“

Diese CCN/CSI-Dienstgütevereinbarung (CCN/CSI-SLA) regelt die Beziehungen zwischen der Kommission (Diensteanbieter) und dem Königreich Norwegen (Diensteanforderer) im Zusammenhang mit der operativen Phase des Common Communication Network/Common System Interface Systems (CCN/CSI-System).

Festgelegt wird die erforderliche Güte der dem Diensteanforderer zu erbringenden Dienste. Darüber hinaus sorgt sie für ein einheitliches Verständnis bezüglich der Erwartungen an die Dienstgüte und der Zuständigkeiten der beteiligten SLA-Parteien.

In diesem Dokument werden die Dienste und die Dienstgüte beschrieben, die derzeit vom Diensteanbieter erbracht werden.

Alle in der CCN/CSI-SLA genannten Ziele gelten nur unter normalen Arbeitsbedingungen.

Im Falle eines Ereignisses höherer Gewalt haftet keine Vertragspartei, wenn sie ihren Verpflichtungen wegen einer Naturkatastrophe (einschließlich Brand, Überschwemmung, Erdbeben, Sturm, Wirbelsturm oder einer sonstigen Naturkatastrophe) oder wegen Krieg, Invasion, Handlung ausländischer Feinde, Feindseligkeiten (mit oder ohne Kriegserklärung), Bürgerkrieg, Rebellion, Revolution, Aufstand, militärische oder widerrechtliche Machtübernahme oder Beschlagnahme, terroristische Handlungen, Verstaatlichung, staatliche Sanktion, Blockade, Embargo, Arbeitskampf, Streik, Aussperrung, Stromunterbrechung oder langfristiger Stromausfall des kommerziellen Stromnetzes nicht nachkommen konnte.

3.2. CCN/CSI-DIENSTE: DEFINITION UND MERKMALE

Das Common Communication Network/Common System Interface (CCN/CSI) ist ein Instrument für den Austausch von Steuerinformationen zwischen den nationalen Verwaltungen im Bereich Steuern und Betrugsbekämpfung. Die Hauptmerkmale der CCN/CSI-Systeminfrastruktur sind nachstehend aufgeführt:

EUROPAWEIT	Das CCN/CSI bietet Diensteanforderern über eine Reihe von Präsenzpunkten (PoP) in allen Mitgliedstaaten, beitretenden Ländern und Norwegen einen globalen WAN-Zugang. Das Backbone-Netz des CCN/CSI weist die erforderliche Kapazität und Resilienz auf, um den Diensteanforderern ein hohes Maß an Verfügbarkeit zu bieten.
MULTI-PLATTFORM	Ermöglicht die Interoperabilität zwischen heterogenen Plattformen (Windows, Linux, Solaris, AIX, HPUX, SVR4, IBM MVS usw.) durch einen hoch portablen Kommunikationsstack (CSI), der auf nationalen Standard-Anwendungsplattformen installiert ist.
MULTI-PROTOKOLL	Unterstützt verschiedene Protokolle und Austauschparadigmen: <ul style="list-style-type: none"> ▪ CSI-Protokoll zur Unterstützung asynchroner und synchroner (Request/Response) Kommunikationsparadigmen (CCN/CSI-Kanal); ▪ HTTP/S-Protokoll für den interaktiven Zugriff auf CCN-Intranetdienste (CCN-Intranetkanal);

	POP, IMAP, SMTP-Protokolle für den Austausch von E-Mails zwischen NA-Nutzern, aber auch zwischen den Anwendungen (CCN Mail III-Kanal).
GESICHERT	<p>Der Informationsaustausch über das CCN/CSI-Netz ist geschützt, um eine optimale Vertraulichkeit und Datenintegrität zu gewährleisten. Die Sicherheitsdienste umfassen:</p> <ul style="list-style-type: none"> ▪ Site-to-site-Verschlüsselung (IPSec 256 bits) und Schutz vor unbefugten Zugriffen mithilfe von Firewall/Verschlüsselungsgeräten an jedem CCN/CSI-Standort; ▪ Zugangskontrollverfahren (Authentifizierung, Autorisierung, Accounting) auf Standort-Ebene am CCN-Gateway und unterstützt durch lokale Verwaltungsinstrumente (ADM3G); <p>Sicherheit der einzelnen Sitzung mithilfe von Nachrichtenverschlüsselung (CSI secure), gegenseitige Authentifizierung und Verschlüsselung mittels SSLv3 (HTTPS), POP-S und IMAP-S (gesicherter E-Mail-Transport).</p>
MANAGED	<p>Die CCN/CSI-Infrastruktur bietet Diensteanforderern außerdem Managed Services an, u. a.:</p> <ul style="list-style-type: none"> ▪ zentrales Monitoring; ▪ Ereignisprotokollierung; ▪ Erstellung von Statistiken über CSI und CCN Mail III-Nachrichtenaustausche (Größe, Anzahl der Nachrichten, Matrix) sowie über CCN-Gateways und CCN Mail III; ▪ Nutzerverwaltung (ADM3G) und Verzeichnisdienste; ▪ CSI Stack-Validierung; ▪ Portaldienste: <ul style="list-style-type: none"> ○ CCN-Portal: Online-Zugriff auf Statistiken, Online-Remote-Verwaltung von API-Proxys (RAP); ○ ITSM-Portal: Online-Newsletter, Online-Dokumentation und CSI-Stackpakete, CCN Frequently Asked Questions (FAQ) ▪ ACT (Werkzeug für die Anwendungskonfiguration); <p>Nachverfolgung von Serviceanfragen und Online-Support.</p>

Tabelle 5: Merkmale der von CCN/CSI bereitgestellten Dienste

3.3. LAUFZEIT DER VEREINBARUNG

Die CCN/CSI-SLA bindet die Vertragsparteien ab dem Tag nach ihrer Genehmigung durch den mit Artikel 41 der Übereinkunft eingesetzten Gemischten Ausschuss (im Folgenden „Gemischter Ausschuss“).

4. ZUSTÄNDIGKEITEN

4.1 PFLICHTEN DES DIENSTEANBIETERS (obligations of the service provider – OSP)

Der Diensteanbieter

[OSP1]	betreibt die CCN/CSI-Netzinfrastruktur, um die in Abschnitt 8 beschriebene Dienstgüte zu erreichen.
[OSP2]	wählt die verschiedenen CCN/CSI-Infrastruktur- und Softwarekomponenten aus.
[OSP3]	sorgt für die Hardware- und Softwarewartung der CCN-Infrastrukturausrüstung der DG TAXUD (z. B. CCN-Gateways), die in den Räumlichkeiten der Diensteanforderer installiert ist, sowie der zentralen CCN-Mail-III-Server.
[OSP4]	übernimmt das Monitoring der CCN-Infrastrukturausrüstung der DG TAXUD, die in den Räumlichkeiten der Diensteanforderer installiert ist.
[OSP5]	verwaltet die CCN/CSI-Auditdateien.
[OSP6]	verwaltet den CCN/CSI-Adressierungsplan.
[OSP7]	hält sich an die Vorschriften und Empfehlungen in den „Sicherheitsdokumenten“: <ul style="list-style-type: none">▪ CCN/CSI General Security Policy RD3; CCN/CSI Baseline Security Checklist RD4 ;
[OSP8]	Von Zeit zu Zeit muss der Diensteanforderer sicherstellen, dass die Netzverfügbarkeit nicht durch Wartung oder eine sonstige absehbare Nichtverfügbarkeit eingeschränkt wird. In diesem Fall unterrichtet der Diensteanforderer den Diensteanbieter mindestens einen Monat im Voraus. Wenn der Diensteanforderer diese Frist nicht einhalten kann, klärt die DG TAXUD die Situation.
[OSP9]	Alle Softwarelizenzen, die auf den CCN-Gateways laufen, werden von der DG TAXUD bereitgestellt.
[OSP10]	respektiert die Backup-Vorgaben für die CCN/CSI-Site (vgl. RD2).
[OSP11]	auditert das System gemäß RD2 .
[OSP12]	nimmt regelmäßig die Sicherheitsüberprüfung des Systems gemäß RD2 vor.

Tabelle 6: PFLICHTEN DES DIENSTEANBIETERS (OSP)

4.2. PFLICHTEN DES DIENSTEANFORDERERS (obligations of the service requester – OSR)

Der Diensteanforderer

Technik und Infrastruktur	
[OSR1]	<p>beherbergt die von der DG TAXUD bereitgestellte CCN-Infrastrukturausrüstung und stellt in ausreichendem Umfang Folgendes bereit:</p> <ul style="list-style-type: none"> ▪ Ablage-/Lagerflächen; ▪ Stromversorgung; <p>Heizung, Lüftung und Klimatisierung (HVAC)</p>
[OSR2]	<p>stellt sicher, dass die CCN/CSI-Komponenten „elektrisch“ mit der unterbrechungsfreien Stromversorgung (UPS) verbunden sind. Spezifische Anpassungen an lokale Normen (z. B. Adapter) müssen vom Diensteanforderer vorgenommen bzw. bereitgestellt werden.</p>
Betrieb und Organisation	
[OSR3]	<p>betrachtet Mitarbeiter mit den in RDS aufgeführten Aufgaben.</p>
[OSR4]	<p>sorgt dafür, dass jemand auch außerhalb der normalen Arbeitszeiten anwesend ist, wann immer dies vom Diensteanbieter für notwendig erachtet und gefordert wird.</p> <p>Bei einigen Tätigkeiten, die vom Backbone-Carrier oder vom Diensteanbieter durchgeführt werden, kann vom Nutzer der Dienste die Koordinierung durch den LSA oder dessen Anwesenheit gefordert werden. Für die Planung dieser Aktivitäten ist eine Vorankündigung von mindestens einem Monat vorzusehen; eine umfassende Zusammenarbeit ist notwendig, um die komplexe Planung aufgrund der Zahl der Standorte Rechnung zu tragen.</p>
[OSR5]	<p>darf nichts von der CCN-Infrastrukturausrüstung der DG TAXUD ohne förmliche Genehmigung des Diensteanbieters abschalten.</p>
[OSR6]	<p>holt die förmliche Genehmigung des Diensteanbieters ein, bevor er in die CCN-Infrastrukturausrüstung der DG TAXUD zusätzliche Hardware- oder Softwarekomponenten installiert, die nicht zum Standardlieferumfang gehören.</p>
[OSR7]	<p>stellt eine aussagekräftige Beschreibung der wahrgenommenen/gemeldeten Vorfälle bereit, die vom Auftraggeber gemeldet werden.</p>

[OSR8]	arbeitet aktiv mit dem Diensteanbieter und/oder seinen Vertretern zusammen, wenn dies für die Erbringung der Dienste erforderlich ist.
Kommunikation	
[OSR9]	verwendet ausschließlich die Kontaktstellen des Diensteanbieters und innerhalb seiner eigenen Organisation.
[OSR10]	informiert den Diensteanbieter über jede Abwesenheit der Kontaktstellen während der Öffnungszeiten des Diensteanbieters oder bietet zumindest eine alternative Lösung an, um die Kontaktstellen zu ersetzen.
[OSR11]	informiert den Diensteanbieter mindestens fünf Arbeitstage, bevor eine Änderung bezüglich seiner eigenen Kontaktstellen wirksam wird.
[OSR12]	informiert den Diensteanbieter über jede geplante Infrastrukturwartung, die die CCN-Infrastrukturausrüstung der DG TAXUD, die sich in den Räumlichkeiten des Nutzers der Dienste befindet, potenziell betreffen könnte (mindestens eine Woche im Voraus für die gesamte Ausrüstung). z. B.: geplante Strom-/Netzinfrastukturausfälle, Umzug des Rechenzentrums, IP-Adressen-Änderungen.
[OSR13]	informiert den Diensteanbieter über jedes externe Problem, etwa den Ausfall der Stromversorgung, das den ordnungsgemäßen Betrieb der CCN-Gateways und Anwendungsplattformen beeinträchtigt.
[OSR14]	informiert den Diensteanbieter mittels eines förmlichen Antrags mindestens sechs Monate im Voraus, wenn ein Umzug von CCN-Infrastrukturausrüstung der DG TAXUD erfolgen soll. Die Umzugskosten trägt der Diensteanforderer. Für weitere Einzelheiten zum Verfahren siehe RD6 .
[OSR15]	informiert den Diensteanbieter über jeden Ausfall der gesicherten Verbindungen zwischen der CCN-Infrastruktur der DGTAXUD und dem Diensteanforderer (NA oder „peer DG“).
[OSR16]	informiert den Diensteanbieter über etwaige Ausfälle der Anwendungsplattformen.
[OSR28]	Der Diensteanforderer wird gebeten, alle geplanten Ausfallzeiten des lokalen Rechenzentrums/Computerraums (einschließlich WAN)

	eine Woche im Voraus anzukündigen. Dies soll es der DG TAXUD ermöglichen, die notwendigen Vorkehrungen für die Unterrichtung anderer Beteiligter zu treffen.
Sicherheit und Nutzerverwaltung	
[OSR17]	verwaltet die lokalen Nutzerkonten auf dem CCN-Gateway (vgl. RD2).
[OSR18]	gewährt den vom Diensteanbieter beauftragten Mitarbeitern bei Bedarf physischen Zugang zur Ausrüstung.
[OSR19]	genehmigt die geeigneten TCP-Ports im Netz des Nutzers der Dienste (nationale Domain) (vgl. RD2).
[OSR20]	stellt sicher, dass sich die Netzwerkverschlüsselungsgeräte (derzeit Juniper SSG) am Standort des Diensteanforderers in einem Bereich mit Zugangskontrolle befinden.
[OSR21]	beschränkt den Zugang zu allen Geräten der CCN-Infrastruktur der DG TAXUD auf befugte Mitarbeiter. Der Zugang wird nur auf Anforderung des CSA gewährt. Der unbefugte Zugang zu diesen Geräten kann die Sicherheit gefährden oder zumindest Netzausfälle verursachen.
[OSR22]	hält sich an die Vorschriften und Empfehlungen in den „Sicherheitsdokumenten“: <ul style="list-style-type: none"> ▪ CCN/CSI General Security Policy RD5; ▪ CCN/CSI Baseline Security Checklist RD6;
Verwaltung und Entwicklung der Anwendungen	
[OSR27]	Der Diensteanforderer ist allein verantwortlich für die Entwicklung, den Support und die Verwaltung seiner Anwendungen. Sie müssen den Regeln von RD8 entsprechen.

Tabelle 7: PFLICHTEN DES DIENSTEANFORDERERS (OSR)

4.3. VOM DIENSTEANBIETER ZU ERBRINGENDE DIENSTE

4.3.1. IT-Servicedesk

Der Diensteanbieter hält einen konsolidierten IT-Servicedesk mit Vorfall- und Problemmanagement vor. Der IT-Servicedesk bietet neben den klassischen Helpdesk-Diensten einen stärker global ausgerichteten Ansatz, der es ermöglicht, Businessabläufe in das CCN/CSI-Servicemanagement zu integrieren.

Der IT-Servicedesk kümmert sich nicht nur um Vorfälle, Probleme und Fragen, sondern fungiert auch als Schnittstelle für andere Tätigkeiten, etwa

Änderungsanträge, Wartungsverträge, Softwarelizenzen, Service-Level-Management, Konfigurationsmanagement, Verfügbarkeitsmanagement, Sicherheitsmanagement und das Management der IT-Betriebskontinuität.

Der IT-Servicedesk leitet dem Diensteanforderer auch unaufgefordert alle dringenden Informationen weiter und fungiert somit als Informationszentrale für den Diensteanforderer.

Eine „Meldung“ wird als eine Nachricht definiert, mit der der Diensteanbieter den Diensteanforderer vor einem Ereignis warnt, das Einfluss auf den CCN/CSI-Betrieb haben kann: Nichtverfügbarkeit des Gateways, Systemausfall, Funktionsstörungen, Wartung der Infrastruktur oder Aktualisierung der Software.

Die Schnittstelle IT-Servicedesk/Diensteanforderer wird über die Kontaktstelle des Diensteanbieters oder über das ITSM-Webportal erreicht, das für den Diensteanforderer Online-Dienste, etwa die Nachverfolgung von Serviceanfragen, erbringt, das ACT und das CCN-Webportal, das einen Downloadbereich für CSI-Pakete, Zugriff auf Statistiken, Monitoring-Informationen usw. bietet.

4.3.1.1. *Vorfall- und Problemmanagement*

Dieser Dienst befasst sich mit Vorfällen, die von Nutzern des Servicedesks ausgehen (einschließlich Systembetrieb). Ein Vorfall kann als einfaches Informations- oder Klärungersuchen definiert, aber auch als das Melden eines nicht ordnungsgemäßen Verhaltens einer bestimmten Komponente eingestuft werden.

Ein Vorfall wird als ein unerwartetes Ereignis definiert, das nicht Teil des Standardbetriebs der Infrastruktur ist, oder als ein Ausfall, der einen operativen CCN/CSI-Dienst beeinträchtigt. Der Vorfall ist behoben, wenn der Dienst wieder hergestellt ist.

Der Vorfall kann mit den folgenden Konfigurationsobjekten (CI) zusammenhängen:

- mit der Hardware, für die der Diensteanbieter zuständig ist: CCN-Gateways, Sicherheitsgeräte, Router beim Kunden (CPR) und andere Geräte für die Verbindung zum Eurodomain-LAN (CCN-Infrastruktur der DG TAXUD);
- mit der Software der Verschlüsselungsgeräte;
- mit der Systemsoftware der Gateways: Betriebssystem, grundlegende Kommunikationssoftware wie TCP/IP usw.;
- mit der Software von Dritten, die auf den Gateways betrieben wird, etwa Tuxedo, MQSeries, Sun ONE Directory Server, PostgreSQL, Apache usw.;
- mit CCN Mail III;
- mit der CCN/CSI-Software der Gateways;
- mit der CSI-Software der Anwendungsplattformen;
- mit SIAP (Secure Internet Access Point) – Unified Defence.

Ein Problem ergibt sich entweder aus einem einzelnen Vorfall, der äußerst nachteilige Auswirkungen auf den Nutzerdienst hat und dessen Ursache nicht bekannt ist, oder aus mehreren Vorfällen mit gemeinsamen Symptomen. Ein Problem ist gelöst, wenn der Auslöser ermittelt und beseitigt wurde.

Beim Auftreten eines Vorfalls wird die Situation untersucht, um (falls erforderlich) die operativen CCN/CSI-Dienste wiederherzustellen und die Ursache des Vorfalls zu

finden. Der Diensteanbieter hilft, Vorfälle in der Anwendungssoftware der NA zu beheben – auf der Ebene der Schnittstelle mit CCN/CSI –, sofern dies die anderen vom Diensteanbieter zu erbringenden Dienste nicht beeinträchtigt. Die Unterstützung des Diensteanbieters besteht in der Bereitstellung von Informationen über die ordnungsgemäße Nutzung des CCN/CSI. **Sie besteht nicht darin, sich an der Behebung von Fehlern bei der Anwendungssoftware der NA zu beteiligen.**

4.3.2. Tools für das Service Management

Das Monitoring der CCN-Gateway-Infrastruktur, der Anwendungen und der CCN-Warteschlangen wird von IBM® Tivoli Monitoring (Tivoli Monitoring) und von IBM Tivoli Composite Application Manager (ITCAM) unterstützt.

Der CCN Tivoli Monitoring and Reporting Service, der auf der IBM Tivoli Monitoring Suite beruht, bietet folgende Funktionen:

- Monitoring der Warteschlangen an den CCN-Gateways (WebSphere MQ);
- Monitoring des Systemstatus der CCN-Gateways;
- CPU-Nutzung, Speicherplatz, Speichernutzung, Netzwerklast, Prozesse;
- Monitoring von Out-of-Band-HW;
- Monitoring der laufenden Prozesse der CCN-Komponenten auf den CCN-Gateways;
- Monitoring der CCN Mail III-Infrastruktur;
- Bereitstellung einer Ansicht der zuvor überwachten Informationen für die CCN-Tivoli-Nutzer;
- Generierung vorab festgelegter Warnmeldungen zu den vorigen überwachten Komponenten;
- Bereitstellung von Berichten auf der Grundlage der gesammelten historischen Daten (CCN Tivoli Data Warehouse);
- Systematische und kohärente Bereitstellung von Informationen über die Verfügbarkeit und Leistung der CCN/CSI-Infrastruktur im Zeitverlauf und über wichtige Trends.

4.3.3. ICT-Infrastruktur-Management und Betrieb

Der Diensteanbieter hat die operative CCN/CSI-Infrastruktur zu installieren, zu betreiben und zu warten, um die vereinbarten Verfügbarkeitslevels zu gewährleisten.

Die operative CCN/CSI-Infrastruktur besteht aus den Eurodomain-Relaisgeräten (CCN-Gateways), den Sicherheitsgeräten, dem CPR und der Telekommunikation.

Dieser Dienst umfasst:

- Verfügbarkeitsmanagement;
- Notfallmanagement;
- Management der Anwendungskonfigurationsdaten;
- Sicherheitsmanagement.

Dazu gehören ferner:

- die Koordinierung der Umzüge von CCN/CSI-Ausrüstung;

- die Koordinierung der Bereitstellung neuer Standorte;
- die Kapazitätsplanung der CCN-Infrastruktur;
- Berichterstattung über die geforderten Tätigkeiten während der monatlichen Sitzung über den Arbeitsfortschritt. An dieser einer Qualitätssicherung unterliegenden Sitzung nehmen alle Vertragsparteien teil, die einen Beitrag zum CCN/CSI-Dienst leisten.
- Erleichterung von Anträgen auf „Einfrieren“. Diese können nur von ermächtigten Nutzern bei einem dafür bestimmten Beamten der DG TAXUD gestellt werden;
- Konzeption, Planung, Einführung, Betrieb, technischer Support und Deaktivierung von HW, OS und COTS;
- Netzdienste;
- HW-, OS- und COTS-Dienste;
- Backup und Restore;
- Auftragsverwaltungsmanagement-Dienst;
- Aufstellung und Pflege von Plänen im Zusammenhang mit dem IKT-Infrastrukturmanagement, d. h. IKT-Infrastrukturplan, Verfügbarkeitsplan, Kapazitätsplan, Kontinuitätsplan;
- Durchführbarkeitsstudien im Zusammenhang mit der Infrastruktur.

4.3.3.1. *Verfügbarkeitsmanagement*

Die Hauptaufgabe des Diensteanbieters besteht darin sicherzustellen, dass das CCN/CSI-System auf dem geforderten Verfügbarkeitslevel „funktioniert“.

Der Diensteanbieter stellt sicher, dass alle CCN/CSI-Standorte über ein Wide Area Network (WAN) miteinander verbunden sind, das die nötige Resilienz und Kapazität aufweist, um das ordnungsgemäße Funktionieren kritischer Businessanwendungen zu gewährleisten, die die CCN/CSI-Infrastruktur und -Dienste nutzen.

Das Verfügbarkeitsmanagement deckt folgende Punkte ab:

- globaler Zugang in allen angeschlossenen NA;
- Bereitstellung einer Teilnehmeranschlussleitung (+ einer Backup-Leitung) zwischen dem lokalen WAN-Zugangspunkt (PoP) und den Räumlichkeiten der NA;
- Installation, Konfiguration und Wartung des CPR;
- Installation und Wartung des Sicherheitsgeräts (SSG encryption-firewall box);
- Kommunikations-Gateways in der DMZ an jedem lokalen Standort (d. h. CCN-Gateways);
- das zentrale CCN Mail III-System.

Der Diensteanbieter stellt auch statistische Informationen über die Verfügbarkeit, die unter Betriebsbedingungen gesammelt wurden, und einen Monitoringdienst bereit, sowohl für das proaktive Aufspüren von Problemen als auch für statistische Zwecke.

4.3.3.2. *Notfallmanagement*

Der Diensteanbieter ist an jedem CCN/CSI-Standort für die CCN/CSI-Komponenten in der CCN-Infrastruktur der DG TAXUD zuständig.

Der Notfalldienst dient der Wiederherstellung der vereinbarten Dienstgüte innerhalb eines vereinbarten Zeitrahmens für den Fall einer teilweisen oder vollständigen Funktionsstörung oder der Zerstörung des CCN/CSI-Systems; hierzu wird dem Diensteanforderer Hilfe geleistet und zum Beispiel Folgendes bereitgestellt:

- Software-Backup von CCN-Gateways (an jedem Standort);
- CCN-CBS;
- redundante Verschlüsselungsgeräte;
- Umschaltmöglichkeiten zwischen Produktions- und Backup-Gateways;
- Ersatzeinheiten für Hardware-Geräte;
- doppelte Telekommunikationszugangsleitungen zum CCN-Backbone (an jedem Standort);
- Unterstützung bei der Installation und Konfiguration von CCN/CSI-Elementen in der CCN-Infrastruktur der DG TAXUD;
- Wiederherstellungsverfahren.

4.3.3.3. *Management der Anwendungskonfigurationsdaten*

Dieser Dienst betrifft die Verwaltung von Konfigurationsdaten, die von CCN/CSI-Anwendungen benötigt werden, durch den Diensteanbieter.

Diese Konfigurationsdaten sind im zentralen CCN/CSI-Verzeichnis gespeichert. Der Diensteanbieter und die nationalen Verwaltungen teilen sich die Verwaltung des zentralen CCN/CSI-Verzeichnisses. Jede nationale Verwaltung ist für die Verwaltung ihrer lokalen CCN/CSI-Nutzer zuständig. Der Rest wird vom Diensteanbieter verwaltet.

Beispiele für Konfigurationen, die einer Serviceanfrage der Verwaltung bedürfen:

- Festlegung des Profils eines lokalen Administrators;
- Registrierung eines Anwendungsdienstes;
- Registrierung einer Anwendungswarteschlange;
- Registrierung einer Nachrichtenart;
- Validierung von Anwendungskonfigurationsdaten;
- Registrierung von Administratorfunktionen;
- Verwaltung von Kontaktlisten.

4.3.4. **Sicherheitsmanagement**

Dieser Dienst betrifft das Management der Sicherheitsvorrichtungen, die von der CCN/CSI-Umgebung benötigt werden, durch den Diensteanbieter.

Die Sicherheit ist auch auf der Ebene der beteiligten Server-Ausrüstung (OS) und Netzausrüstung sowie auf der Betriebsebene zu managen.

- Der Informationsaustausch über das CCN/CSI-Netz ist geschützt, um eine optimale Vertraulichkeit und Datenintegrität zu gewährleisten.
- Die Sicherheitsdienste umfassen:
 - Site-to-site-Verschlüsselung und Schutz vor unbefugten Zugriffen mithilfe von Firewall/Verschlüsselungsgeräten;
 - Zugangskontrollverfahren (Authentifizierung, Autorisierung, Accounting) auf Standort-Ebene am CCN-Gateway und unterstützt durch lokale Verwaltungsinstrumente (ADM3G);
 - Sicherheit auf Sitzungsebene mithilfe von Nachrichtenverschlüsselung (CSI secure), gegenseitiger SSL-Authentifizierung und -Verschlüsselung (HTTPS & NJCSI), POP-S und IMAP-S (gesicherter E-Mail-Transport);
 - SIAP Unified Defence-Verfahren für den gesicherten Internetzugang zu CCN-Diensten.

4.3.5. Dokumentationsmanagement

Der Diensteanbieter hält die gesamte technische CCN/CSI-Dokumentation (technisches Dokument, Benutzerhandbücher, häufig gestellte Fragen, Newsletter, künftige Ereignisse usw.), die als Dokumentationszentrum fungiert, auf dem aktuellen Stand.

Dies umfasst die Dokumentation zur CCN/CSI-Infrastruktur: Oracle-Tuxedo, IBM-MQ, CCN Gateways, CCN Mail III, CSI-Software, Verfahren, Berichte, Historie der Kommunikation mit Partnern usw.

Der Diensteanbieter verwaltet eine Dokumentenliste, die mit dem CCN/CSI im Zusammenhang steht und dem Diensteanforderer übermittelt werden kann. Diese Dokumente sind über CIRCABC und das ITSM-Portal abrufbar.

Der Diensteanbieter aktualisiert die Liste automatisch mit den neuesten genehmigten Versionen der Dokumente.

4.3.6. Berichte und Statistiken

Der Diensteanbieter stellt dem Diensteanforderer über das CCN und das ITSM-Webportal Folgendes bereit:

- Zahlen zur Online-Verfügbarkeit für CCN-Gateways und CCN Mail III-Server;
- Online-Newsletter;
- Statistiken zum CCN/CSI-Austausch.

Darüber hinaus veranstaltet der Diensteanbieter regelmäßig IT-Tech & Infra-Meetings, in denen die Berichte und Statistiken präsentiert werden.

4.3.7. Schulungen

Der Diensteanbieter arbeitet Kurse über die technischen Aspekte des CCN/CSI-Systems aus und führt entsprechende Schulungen durch. Die Standardkurse werden in Schuleinheiten mit Modulen unterteilt. In der Regel werden jedes Jahr Schulungen organisiert. Die Standardschulungspakete werden zweimal jährlich über die DG TAXUD verbreitet und sind im ITSM-Portal online verfügbar.

5. MESSUNG DER QUALITÄT DER ERBRACHTEN DIENSTE

5.1. **DIENSTGÜTE (service level)**

Die Dienstgüte ist ein Maß für die Qualität der vom Diensteanbieter erbrachten Dienste. Sie wird mithilfe eines Qualitätsindikators (service quality indicator –SQI) berechnet.

Es wird erwartet, dass der Diensteanforderer seinen Verpflichtungen (siehe Abschnitt 0) nachkommt, um die vereinbarte Dienstgüte zu erreichen.

5.2. **ANWENDBARE SQI**

5.2.1. Individuelle Verfügbarkeit des CCN/CSI-Standorts

Dieser Qualitätsindikator gibt die geringste gemessene Verfügbarkeit eines einzelnen Standorts während des „Gesamtzeitraums“, d. h. 24 * 7, für einen bestimmten Monat an. Der CCN/CSI-SLA-Grenzwert wird wie folgt definiert:

GRENZWERT	≥ 97,0 % Verfügbarkeit
------------------	------------------------

5.2.2. Qualitätsindikator für die Dienstzeit

Die „Dienstzeit“ des Diensteanbieters ist der Zeitraum, in dem die SD-Funktion abgedeckt ist. Der Dienst wird vom Diensteanbieter rund um die Uhr (24/24) während sieben Tagen pro Woche, einschließlich Feiertagen, gewährleistet.

Abhängig vom Servicefenster für die CI wird sofort gehandelt (24*7), oder die Intervention wird für das nächste Servicefenster eingeplant. Briefe, Faxe, E-Mails und elektronische Anfragen (über das ITSM-Portal) werden jederzeit akzeptiert. Eingehende Anfragen werden im Servicedesk-Managementsystem des Diensteanbieters als „Serviceanfrage“ registriert.

Der SLA-Grenzwert wird wie folgt definiert:

GRENZWERT	Der Servicedesk darf während der Dienstzeit höchstens zweimal pro Monat nicht erreichbar sein.
------------------	------------------------------------------------------------------------------------------------

5.2.3. Qualitätsindikator für den Meldungsdienst

Der Diensteanbieter erbringt dem Diensteanforderer Meldungsdienste.

Es gibt zwei Arten von Meldungen, dringende und normale:

- **DRINGENDE MELDUNGEN** (wenn nicht genug Zeit bleibt, um die CCN/CSI-Gemeinschaft mindestens sieben Kalendertage im Voraus zu benachrichtigen): Die Meldungen werden spätestens zwei Stunden nach Eingang des entsprechenden Antrags an die relevanten Empfänger weitergeleitet.
- **NORMALE MELDUNGEN** (oder geplante Interventionen): Die Meldungen werden mindestens eine Woche (sieben Kalendertage) vor der Intervention an die relevanten Empfänger weitergeleitet, und spätestens 24 Stunden vor den Ereignissen wird eine Erinnerung verschickt.

Dieser Indikator misst die Einhaltung der Ankündigungsfrist (über Massenmails) für eine geplante Nichtverfügbarkeit.

5.3.4. Qualitätsindikator für das Notfallmanagement

Cold Standby (Umschaltverfahren, Backup& Restore oder CCN über Internet)

Um zu wissen, wie umgeschaltet werden soll, ist eine gründliche Analyse der spezifischen Gegebenheiten in der nationalen Verwaltung (NA) und des jeweiligen Problems nötig.

Wie lange ein Umschalten von einem Produktions-Gateway einer NA zu einem geeigneten CCN-Backup-Gateway höchstens dauern darf, wird wie folgt definiert:

GRENZWERT	Höchstens fünf Arbeitsstunden nach der Einigung mit dem Diensteanforderer über das Umschalten.
------------------	------------------------------------------------------------------------------------------------

5.3.5. Qualitätsindikator für das Management der Anwendungskonfigurationsdaten

Wie lange die Umsetzung einer Anforderung einer Anwendungskonfiguration über das Tool für das Anwendungskonfigurations-Tool (ACT) für einen einzelnen Standort höchstens dauern darf, wird wie folgt definiert:

GRENZWERT	Fünf Arbeitstage
------------------	------------------

5.3.6. Qualitätsindikator für die Zeit bis zur Übermittlung einer Empfangsbestätigung

Wie viel Zeit zwischen dem Eingang einer Anfrage beim Servicedesk und dem Zeitpunkt, zu dem dem Diensteanforderer eine Empfangsbestätigung (d. h. eine Nummer der Serviceanfrage) übermittelt wird, höchstens vergehen darf, wird wie folgt festgelegt:

GRENZWERT	30 Minuten
------------------	------------

Die Einstufung von Vorfällen erfolgt entsprechend ihrer **Dringlichkeit**.

Jeder **Dringlichkeitsstufe** entspricht eine Zahl zwischen 1 und 4:

1	KRITISCH
2	HOCH
3	MITTEL
4	NIEDRIG

5.3.7. Qualitätsindikator für die zur Vorfallbehebung benötigte Zeit

Die Zeit bis zur Behebung eines Vorfalls ist die Zeitspanne zwischen der Bestätigung des Vorfalls durch den Diensteanbieter und dem Zeitpunkt, zu dem der Diensteanbieter die Ursache des Vorfalls behoben oder eine Ausweidlösung implementiert hat.

Je nach Dringlichkeit gelten für die Vorfallbehebung folgende Fristen:

DRINGLICHKEITSSTUFE	FRIST FÜR DIE VORFALLBEHEBUNG
KRITISCH	5 Arbeitsstunden
HOCH	13 Arbeitsstunden

MITTEL	39 Arbeitsstunden
NIEDRIG	65 Arbeitsstunden

Tabelle 8: Fristen für die Vorfalbehebung

DRINGLICHKEITSSTUFE	GRENZWERT
KRITISCH	≥ 95,00 % der Vorfälle in der Stufe KRITISCH müssen innerhalb der vereinbarten Frist (5 Arbeitsstunden) behoben sein.
HOCH	≥ 95,00 % der Vorfälle in der Stufe HOCH müssen innerhalb der vereinbarten Frist (13 Arbeitsstunden) behoben sein.
MITTEL	≥ 95,00 % der Vorfälle in der Stufe MITTEL müssen innerhalb der vereinbarten Frist (39 Arbeitsstunden) behoben sein.

Tabelle 9: Prozentuale Grenzwerte für die Vorfalbehebung

6. GENEHMIGUNG DER SLA

Die Dienstgütevereinbarung (SLA) muss vom Gemischten Ausschuss genehmigt werden, damit sie anwendbar ist.

7. ÄNDERUNGEN DER SLA

Die CCN/CSI-SLA wird auf schriftlichen Antrag der Kommission oder Norwegens an den Gemischten Ausschuss überprüft.

Bis der Gemischte Ausschuss über die vorgeschlagenen Änderungen entscheidet, gelten die Bestimmungen der in Kraft befindlichen CCN/CSI-SLA. Der Gemischte Ausschuss fungiert als Entscheidungsgremium für die aktuelle Vereinbarung.

8. KONTAKTSTELLE

Für alle operativen Dienste fungiert ITSM3 Operations als zentrale Anlaufstelle. Kontaktinformation:

ITSM3 Operations - IBM

☎ Gebührenfrei: + 800 7777 4477

☎ Gebührenpflichtig: + 40 214 058 422

✉ support@itsmtaxud.europa.eu

🌐 <http://portal.ccntc.cncsi.int:8080/portal>
(CCN Web Portal - für registrierte CCN-Nutzer)

🌐 <https://itsmtaxud.europa.eu/smt/ess.do>
(ITSM Web Portal - für Serviceanfragen)

Datum

ANLAGE 6

Entwurf

BESCHLUSS Nr. 6/[Datum] des Gemischten Ausschusses vom [Datum] zur Festlegung der Höhe und der Modalitäten des finanziellen Beitrags Norwegens zum Gesamthaushalt der Europäischen Union aufgrund der durch die Teilnahme des Landes an den europäischen Informationssystemen entstehenden Kosten

DER GEMISCHTE AUSSCHUSS, der gemäß Artikel 41 Absatz 1 der Übereinkunft zwischen der Europäischen Union und dem Königreich Norwegen über die Zusammenarbeit der Verwaltungsbehörden, die Betrugsbekämpfung und die Beitreibung von Forderungen auf dem Gebiet der Mehrwertsteuer (im Folgenden „Übereinkunft“) eingerichtet wurde,

in Erwägung nachstehender Gründe:

- (a) Die Verordnung (EU) Nr. 1286/2013 des Europäischen Parlaments und des Rates vom 11. Dezember 2013 zur Festlegung eines Aktionsprogramms zur Verbesserung der Funktionsweise der Steuersysteme in der Europäischen Union für den Zeitraum 2014-2020 (Fiscalis 2020) regelt die Entwicklung, den Betrieb und die Pflege der europäischen Informationssysteme.
- (b) Das Gemeinsame Kommunikationsnetz/die Gemeinsame Systemschnittstelle und die nach Artikel 41 Absatz 2 Buchstabe d der Übereinkunft zu beschließenden elektronischen Formblätter sind Unionskomponenten der in Abschnitt A des Anhangs der Verordnung (EU) Nr. 1286/2013 genannten europäischen Informationssysteme.
- (c) Gemäß Artikel 9 Absatz 3 der Verordnung (EU) Nr. 1286/2013 wird die Nutzung der Unionselemente der europäischen Informationssysteme gemäß Teil A des Anhangs durch nicht teilnehmende Länder in Abkommen mit diesen Ländern geregelt, die gemäß Artikel 218 des Vertrags über die Arbeitsweise der Europäischen Union geschlossen werden.
- (d) Es ist erforderlich, praktische Modalitäten für die Durchführung von Artikel 41 Absatz 2 Buchstabe f der Übereinkunft festzulegen –

HAT FOLGENDEN BESCHLUSS ERLASSEN:

Artikel 1

Installationskosten

Die vom Königreich Norwegen für die Einrichtung des Zugangs zum Virtual Private Network (VPN) zu zahlenden anfänglichen Kosten belaufen sich auf 20 000 EUR.

Der Betrag wird innerhalb von 60 Tagen nach dem Erlass dieses Beschlusses gezahlt.

Artikel 2

Jährlicher Finanzbeitrag

Der jährliche Finanzbeitrag des Königreichs Norwegen zum Gesamthaushalt der Union beläuft sich auf 20 000 EUR. Dieser Betrag wird bis zum 1. September eines jeden Jahres gezahlt.

Der Beitrag deckt die Ausgaben im Zusammenhang mit der Entwicklung, Wartung und Modernisierung von IT-Lösungen (Gemeinsames Kommunikationsnetz/Gemeinsame Systemschnittstelle, E-Formulare).

Artikel 3

Zahlungsart

Die Beiträge gemäß den Artikeln 1 und 2 werden in Euro auf das auf Euro lautende Bankkonto der Kommission überwiesen, das in der Zahlungsaufforderung angegeben ist.

Datum