BESCHLUSS (EU, Euratom) 2019/1963 DER KOMMISSION

vom 17. Oktober 2019

zur Festlegung von Durchführungsbestimmungen über den Geheimschutz in der Wirtschaft in Bezug auf als Verschlusssache eingestufte öffentliche Aufträge

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 249,

gestützt auf den Vertrag zur Gründung der Europäischen Atomgemeinschaft, insbesondere auf Artikel 106,

gestützt auf den Beschluss (EU, Euratom) 2015/443 der Kommission vom 13. März 2015 über Sicherheit in der Kommission ([1]),

gestützt auf den Beschluss (EU, Euratom) 2015/444 der Kommission vom 13. März 2015 über die Sicherheitsvorschriften für den Schutz von EU-Verschlusssachen ([2]),

gestützt auf den Beschluss (EU, Euratom) 2017/46 der Kommission vom 10. Januar 2017 über die Sicherheit von Kommunikations- und Informationssystemen in der Europäischen Kommission ([3]),

nach Zurateziehung der Sicherheitsexpertengruppe der Kommission gemäß Artikel 41 Absatz 5 des Beschlusses (EU, Euratom) 2015/444,

in Erwägung nachstehender Gründe:

(1) Nach den Artikeln 41, 42, 47 und 48 des Beschlusses (EU, Euratom) 2015/444 sind ausführlichere Bestimmungen zur Ergänzung und Unterstützung von Kapitel 6 des besagten Beschlusses in Durchführungsbestimmungen für den Geheimschutz in der Wirtschaft festzulegen, in denen unter anderem Ausschreibungen, der Abschluss von als Verschlusssache eingestuften Verträgen, Sicherheitsbescheide von Einrichtungen, Sicherheitsüberprüfungen von Personal, Besuche sowie die Übermittlung und Beförderung von EU-Verschlusssachen (im Folgenden „EU-VS“) geregelt werden.

(2) Nach dem Beschluss (EU, Euratom) 2015/444 sollen als Verschlusssache eingestufte Verträge in enger Zusammenarbeit mit der nationalen Sicherheitsbehörde, der beauftragten Sicherheitsbehörde oder einer anderen zuständigen Behörde des betreffenden Mitgliedstaats durchgeführt werden; die Mitgliedstaaten haben in dem Übereinkommen zwischen den im Rat vereinigten Mitgliedstaaten der Europäischen Union über den Schutz von Verschlusssachen, die im Interesse der Europäischen Union ausgetauscht werden (2011/C 202/05) ([4]), vereinbart sicherzustellen, dass alle ihrer Hoheitsgewalt unterstehende Einrichtungen, die von der Kommission herausgegebene Verschlusssachen erhalten oder erstellen dürfen, einer entsprechenden Sicherheitsprüfung unterzogen wurden und einen angemessenen Schutz gewährleisten können, der demjenigen entspricht, der durch die Sicherheitsvorschriften des Rates der Europäischen Union für den Schutz von EU-Verschlusssachen mit einer entsprechenden Einstufungskennzeichnung gewährt wird.

(3) Wie aus den Erklärungen hervorgeht, die dem Protokoll der Ratstagung beigefügt waren, auf der der Beschluss 2013/488/EU des Rates ([5]) über die Sicherheitsvorschriften für den Schutz von EU-Verschlusssachen erlassen wurde, haben der Rat, die Kommission und die Hohe Vertreterin der Union für Außen- und Sicherheitspolitik vereinbart, größtmögliche Einheitlichkeit bei der Anwendung der Sicherheitsvorschriften bezüglich des Schutzes von EU-VS zu gewährleisten, wobei jedoch ihren jeweiligen spezifischen institutionellen und organisatorischen Bedürfnissen Rechnung getragen wird.

(4) Die Durchführungsbestimmungen der Kommission über den Geheimschutz in der Wirtschaft in Bezug auf als Verschlusssache eingestufte Verträge sollten daher auch größtmögliche Einheitlichkeit gewährleisten und den vom Sicherheitsausschuss des Rates am 13. Dezember 2016 gebilligten Leitlinien für den Geheimschutz in der Wirtschaft sowie den Artikeln 7 und 22 der Richtlinie 2009/81/EG des Europäischen Parlaments und des Rates ([6]) Rechnung tragen.

(5) Am 4. Mai 2016 erließ die Kommission einen Beschluss ([7]), mit dem das für Sicherheitsfragen zuständige Kommissionsmitglied ermächtigt wurde, im Namen der Kommission und unter ihrer Verantwortung die in Artikel 60 des Beschlusses (EU, Euratom) 2015/444 vorgesehenen Durchführungsbestimmungen zu erlassen —

([1]) ABl. L 72 vom 17.3.2015, S. 41.
([2]) ABl. L 72 vom 17.3.2015, S. 53.
([3]) ABl. L 6 vom 11.1.2017, S. 40.
([4]) ABl. C 202 vom 8.7.2011, S. 13.
([5]) Beschluss 2013/488/EU des Rates vom 23. September 2013 über die Sicherheitsvorschriften für den Schutz von EU-Verschlusssachen (ABl. L 274 vom 15.10.2013, S. 1).
([6]) Richtlinie 2009/81/EG des Europäischen Parlaments und des Rates vom 13. Juli 2009 über die Koordinierung der Verfahren zur Vergabe bestimmter Bau-, Liefer- und Dienstleistungsaufträge in den Bereichen Verteidigung und Sicherheit (ABl. L 216 vom 20.8.2009, S. 76).
([7]) Beschluss der Kommission vom 4. Mai 2016 über eine Ermächtigung im Bereich der Sicherheit, C(2016) 2797 final.

HAT FOLGENDEN BESCHLUSS ERLASSEN:

KAPITEL 1

ALLGEMEINE BESTIMMUNGEN

Artikel 1

Gegenstand und Anwendungsbereich

(1) Dieser Beschluss enthält Durchführungsbestimmungen über den Geheimschutz in der Wirtschaft in Bezug auf als Verschlusssache eingestufte öffentliche Aufträge zur Unterstützung der Durchführung des Beschlusses (EU, Euratom) 2015/444, insbesondere Kapitel 6 des genannten Beschlusses.

(2) In diesem Beschluss werden spezifische Anforderungen festgelegt, um den Schutz von EU-Verschlusssachen (EU-VS) durch die Wirtschaftsteilnehmer in der vorvertraglichen Phase, während des gesamten Lebenszyklus der von der Europäischen Kommission geschlossenen, als Verschlusssache eingestuften Verträge und in den von den Auftragnehmern der Kommission geschlossenen Unterverträgen zu gewährleisten.

(3) Dieser Beschluss betrifft Verschlusssachen folgender Ebenen:

a) RESTREINT UE/EU RESTRICTED;

b) CONFIDENTIEL UE/EU CONFIDENTIAL;

c) SECRET UE/EU SECRET.

Artikel 2

Verantwortung innerhalb der Kommission

(1) Im Rahmen der in der Haushaltsordnung ([8]) beschriebenen Aufgaben stellt jeder Anweisungsbefugte der Kommission in ihrer Eigenschaft als öffentlicher Auftraggeber sicher, dass in dem als Verschlusssache eingestuften Vertrag auf die in Kapitel 6 des Beschlusses (EU, Euratom) 2015/444 und in diesen Durchführungsbestimmungen sowie gegebenenfalls in der Auftragsbekanntmachung oder in der Aufforderung zur Angebotsabgabe festgelegten Mindestnormen für den Geheimschutz in der Wirtschaft verwiesen wird und dass diese Normen bei der Durchführung eingehalten werden.

(2) Zu diesem Zweck zieht der zuständige Anweisungsbefugte in allen Phasen die Sicherheitsstelle der Kommission zu Fragen im Zusammenhang mit den Sicherheitselementen eines als Verschlusssache eingestuften Auftrags, Programms oder Projekts zu Rate und unterrichtet den örtlichen Sicherheitsbeauftragten über die abgeschlossenen Verträge. Die Entscheidung über den Geheimhaltungsgrad bestimmter Aspekte liegt beim öffentlichen Auftraggeber und wird unter gebührender Berücksichtigung des Einstufungsleitfadens für Verschlusssachen getroffen.

(3) Unter Einhaltung der Anforderungen dieser Durchführungsbestimmungen arbeitet die Sicherheitsstelle der Kommission eng mit den nationalen Sicherheitsbehörden und den beauftragten Sicherheitsbehörden der betroffenen Mitgliedstaaten zusammen, insbesondere in Bezug auf Sicherheitsbescheide für Einrichtungen sowie Sicherheitsüberprüfungen von Personal, Besuchsverfahren und Beförderungspläne.

KAPITEL 2

BEARBEITUNG VON AUSSCHREIBUNGEN VON ALS VERSCHLUSSSACHE EINGESTUFTEN VERTRÄGEN

Artikel 3

Grundsätze

(1) Als Verschlusssache eingestufte Verträge werden nur an in einem Mitgliedstaat registrierte Wirtschaftsteilnehmer oder an in einem Drittstaat registrierte oder von einer internationalen Organisation gegründete Wirtschaftsteilnehmer vergeben, wenn der betreffende Drittstaat oder die betreffende internationale Organisation ein Geheimschutzabkommen mit der Europäischen Union oder eine Verwaltungsvereinbarung mit der Kommission geschlossen hat ([9]).

(2) Vor der Ausschreibung eines als Verschlusssache eingestuften Auftrags legt der öffentliche Auftraggeber den Geheimhaltungsgrad der Informationen fest, die den Bietern zur Verfügung gestellt werden könnten. Der öffentliche Auftraggeber legt zudem die maximale Sicherheitseinstufung von Informationen, die bei der Durchführung des Auftrags, Programms oder Projekts generiert werden, oder zumindest die voraussichtliche Menge und Art der zu produzierenden oder zu bearbeitenden Informationen sowie die Notwendigkeit eines Kommunikations- und Informationssystems für Verschlusssachen fest.

([8]) Verordnung (EU, Euratom) 2018/1046 des Europäischen Parlaments und des Rates vom 18. Juli 2018 über die Haushaltsordnung für den Gesamthaushaltsplan der Union, zur Änderung der Verordnungen (EU) Nr. 1296/2013, (EU) Nr. 1301/2013, (EU) Nr. 1303/2013, (EU) Nr. 1304/2013, (EU) Nr. 1309/2013, (EU) Nr. 1316/2013, (EU) Nr. 223/2014, (EU) Nr. 283/2014 und des Beschlusses Nr. 541/2014/EU sowie zur Aufhebung der Verordnung (EU, Euratom) Nr. 966/2012 (ABl. L 193 vom 30.7.2018, S. 1).

([9]) Die Liste der von der EU geschlossenen Abkommen und der von der Europäischen Kommission geschlossenen Verwaltungsvereinbarungen, in deren Rahmen EU-Verschlusssachen mit Drittstaaten und internationalen Organisationen ausgetauscht werden können, ist auf der Website der Kommission zu finden.

(3) Der öffentliche Auftraggeber stellt sicher, dass die Auftragsbekanntmachung für als Verschlusssache eingestufte Verträge Informationen über die besonderen Sicherheitsanforderungen für Verschlusssachen enthält. Anhang I enthält ein Muster für entsprechende Informationen in Auftragsbekanntmachungen.

(4) Der öffentliche Auftraggeber stellt sicher, dass Verschlusssachen des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“, „CONFIDENTIEL UE/EU CONFIDENTIAL“ und „SECRET UE/EU SECRET“ den Bietern erst offengelegt werden, nachdem sie eine Geheimhaltungsvereinbarung unterzeichnet haben, mit der sie verpflichtet werden, EU-VS gemäß dem Beschluss (EU, Euratom) 2015/444 und seinen Durchführungsbestimmungen zu bearbeiten und zu schützen.

(5) Alle Auftragnehmer, die gehalten sind, Informationen des Geheimhaltungsgrads „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“ innerhalb ihrer Räumlichkeiten zu bearbeiten oder aufzubewahren, sei es während der Erfüllung des als Verschlusssache eingestuften Vertrags selbst oder in der vorvertraglichen Phase, müssen in Besitz eines entsprechenden Sicherheitsbescheids für Einrichtungen sein. Im Folgenden werden die drei Szenarien beschrieben, die während der Ausschreibungsphase für einen als Verschlusssache eingestuften Vertrag, der EU-VS der Geheimhaltungsgrade „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“ umfasst, auftreten können:

a) Kein Zugang zu EU-VS des Geheimhaltungsgrads „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“ in der Ausschreibungsphase:

   Betrifft die Auftragsbekanntmachung oder die Aufforderung zur Angebotsabgabe einen Auftrag, der EU-VS des Geheimhaltungsgrads „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“ umfasst, ohne dass der Bieter die betreffenden Informationen in der Ausschreibungsphase bearbeiten muss, so wird ein Bieter nicht von der Ausschreibung ausgeschlossen, weil er nicht über einen Sicherheitsbescheid für Einrichtungen verfügt.

b) Zugang zu EU-VS des Geheimhaltungsgrads „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“ in den Räumlichkeiten des öffentlichen Auftraggebers während der Ausschreibungsphase:

   Der Zugang wird dem Personal des Bieters gewährt, das über eine entsprechende Erklärung über die Sicherheitsüberprüfung von Personal verfügt und Kenntnis von den betreffenden Verschlusssachen haben muss. Bevor ein entsprechender Zugang gewährt wird, prüft der öffentliche Auftraggeber über die Sicherheitsstelle der Kommission gemeinsam mit der jeweiligen nationalen Sicherheitsbehörde/beauftragten Sicherheitsbehörde, ob in dieser Phase nach den nationalen Rechtsvorschriften auch ein Sicherheitsbescheid für Einrichtungen erforderlich ist.

c) Bearbeitung oder Speicherung bzw. Aufbewahrung von EU-VS des Geheimhaltungsgrads „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“ in den Räumlichkeiten des Bieters während der Ausschreibungsphase:

   Ist es gemäß der Auftragsbekanntmachung oder der Aufforderung zur Angebotsabgabe erforderlich, dass Bieter EU-VS in ihren Räumlichkeiten bearbeiten oder aufbewahren, so muss der Bieter über einen entsprechenden Sicherheitsbescheid für Einrichtungen verfügen. In diesem Fall vergewissert sich der öffentliche Auftraggeber über die Sicherheitsstelle der Kommission bei der zuständigen nationalen Sicherheitsbehörde/beauftragten Sicherheitsbehörde, dass dem Bieter ein entsprechender Sicherheitsbescheid für Einrichtungen erteilt wurde. Der Zugang wird dem Personal des Bieters gewährt, das über eine entsprechende Erklärung über die Sicherheitsüberprüfung von Personal verfügt und Kenntnis von den betreffenden Verschlusssachen haben muss.

(6) Grundsätzlich ist für den Zugang zu als „RESTREINT UE/EU RESTRICTED“ eingestuften Verschlusssachen weder in der Ausschreibungsphase noch bei der Ausführung des Auftrags ein Sicherheitsbescheid für Einrichtungen erforderlich. Verlangen Mitgliedstaaten — wie in Anhang IV aufgelistet — nach Maßgabe ihrer nationalen Rechtsvorschriften für Aufträge oder Unteraufträge des Geheimhaltungsgrads RESTREINT UE/EU RESTRICTED einen Sicherheitsbescheid für Einrichtungen, so dürfen diese nationalen Anforderungen anderen Mitgliedstaaten keine zusätzlichen Verpflichtungen auferlegen oder Bieter, Auftragnehmer oder Unterauftragnehmer aus Mitgliedstaaten, die für den Zugang zu Informationen des Geheimhaltungsgrads RESTREINT UE/EU RESTRICTED keinen Sicherheitsbescheid für Einrichtungen verlangen, nicht von entsprechenden Aufträgen/Unteraufträgen oder von diese betreffenden Vergabeverfahren ausgeschlossen werden. Diese Aufträge werden in den Mitgliedstaaten im Einklang mit ihren nationalen Rechtsvorschriften ausgeführt.

(7) Ist für die Ausführung eines als Verschlusssache eingestuften Vertrags ein Sicherheitsbescheid für Einrichtungen erforderlich, so richtet der öffentliche Auftraggeber über die Sicherheitsstelle der Kommission unter Verwendung eines Auskunftsformulars betreffend einen Sicherheitsbescheid für Einrichtungen ein Ersuchen an die nationale Sicherheitsbehörde/beauftragte Sicherheitsbehörde des Auftragnehmers. Anhang III Unteranhang D enthält ein Muster eines entsprechenden Auskunftsformulars ([10]). Der als Verschlusssache eingestufte Auftrag wird erst erteilt, wenn die nationale Sicherheitsbehörde/beauftragte Sicherheitsbehörde des Auftragnehmers bestätigt hat, dass der Bieter über einen Sicherheitsbescheid für Einrichtungen verfügt. Die Antwort auf ein entsprechendes Ersuchen erfolgt nach Möglichkeit innerhalb von zehn Arbeitstagen ab dem Datum der Übermittlung des Ersuchens.

([10]) Werden andere Formulare verwendet, so können sie in ihrer Aufmachung von dem in diesen Durchführungsbestimmungen enthaltenen Muster abweichen.

Artikel 4

Unterauftragsvergabe bei als Verschlusssache eingestuften Aufträgen

(1) Die Bedingungen, unter denen ein Auftragnehmer, der den Zuschlag für einen als Verschlusssache eingestuften Auftrag der Kommission erhalten hat, Unteraufträge vergeben kann, sind in der Aufforderung zur Angebotsabgabe und in den Ausschreibungsunterlagen festzulegen. Ist gemäß dem als Verschlusssache eingestuften Vertrag die Vergabe von Unteraufträgen für Teile des Auftrags zulässig, so unterliegt diese Unterauftragsvergabe der vorherigen schriftlichen Zustimmung des öffentlichen Auftraggebers. Bevor der öffentliche Auftraggeber seine Zustimmung erteilt, zieht er die Sicherheitsstelle der Kommission zurate.

(2) Unteraufträge im Rahmen von als Verschlusssache eingestuften Verträgen werden nur an in einem Mitgliedstaat registrierte Wirtschaftsteilnehmer oder an in einem Drittstaat registrierte oder von einer internationalen Organisation gegründete Wirtschaftsteilnehmer vergeben, wenn der betreffende Drittstaat oder die betreffende internationale Organisation ein Geheimschutzabkommen mit der EU oder eine Verwaltungsvereinbarung mit der Kommission geschlossen hat ([11]).

KAPITEL 3

VERGABE VON ALS VERSCHLUSSSACHE EINGESTUFTEN VERTRÄGEN DER KOMMISSION

Artikel 5

Grundsätze

(1) Bei der Vergabe eines als Verschlusssache eingestuften Vertrags stellt der öffentliche Auftraggeber zusammen mit der Sicherheitsstelle der Kommission sicher, dass die Pflichten des Auftragnehmers in Bezug auf den Schutz von EU-VS, die dem Auftragnehmer bereitgestellt oder die bei der Ausführung des Auftrags generiert werden, fester Bestandteil des Auftrags sind. Die auftragsspezifischen Sicherheitsanforderungen werden in Form einer Geheimschutzklausel festgelegt. Ein Muster einer Geheimschutzklausel ist in Anhang III enthalten.

(2) Vor der Unterzeichnung eines als Verschlusssache eingestuften Vertrags verfasst der öffentliche Auftraggeber nach Rücksprache mit der Sicherheitsstelle der Kommission einen Einstufungsleitfaden für Verschlusssachen für die wahrzunehmenden Aufgaben und die Informationen, die bei der Durchführung des Vertrags, des Programms oder des Projekts generiert werden. Dieser Leitfaden ist Teil der Geheimschutzklausel.

(3) Programm- oder projektspezifische Sicherheitsanforderungen werden in Form von Programm- oder Projektsicherheitsanweisungen festgelegt. Die Programm- oder Projektsicherheitsanweisungen können unter Nutzung des Musters einer Geheimschutzklausel in Anhang III abgefasst werden. Sie werden von der für die Verwaltung des Programms oder Projekts zuständigen Kommissionsdienststelle in enger Zusammenarbeit mit der Sicherheitsstelle der Kommission entwickelt und der Sicherheitsexpertengruppe der Kommission zur Stellungnahme vorgelegt. Ist ein Vertrag Teil eines Programms oder Projekts mit eigenen Programm- oder Projektsicherheitsanweisungen, so erhält die Geheimschutzklausel eine vereinfachte Form und enthält einen Verweis auf die Sicherheitsbestimmungen der betreffenden Programm- oder Projektsicherheitsanweisungen.

(4) Der öffentliche Auftraggeber gilt als Herausgeber von Verschlusssachen, die für die Ausführung des Auftrags erstellt und bearbeitet wurden.

(5) Der öffentliche Auftraggeber unterrichtet über die Sicherheitsstelle der Kommission die nationalen Sicherheitsbehörden/beauftragten Sicherheitsbehörden aller Auftragnehmer und Unterauftragnehmer über den Abschluss von als Verschlusssache eingestuften Verträgen oder Unterverträgen sowie über eine etwaige Verlängerung oder vorzeitige Kündigung derartiger Verträge oder Unterverträge. Anhang IV enthält eine Liste der länderspezifischen Anforderungen.

(6) Verträge, die Verschlusssachen des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“ umfassen, enthalten eine Sicherheitsklausel, mit der die Bestimmungen von Anhang III Unteranhang E für den Auftragnehmer verbindlich werden. Diese Verträge umfassen eine Geheimschutzklausel, in der Mindestanforderungen für die Bearbeitung von Verschlusssachen des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“, die auch auf Aspekte der Informationssicherung eingehen, sowie besondere Anforderungen festgelegt werden, die der vom öffentlichen Auftraggeber beauftragte Auftragnehmer zur Akkreditierung seines Kommunikations- und Informationssystems, mit dem Verschlusssachen des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“ bearbeitet werden, erfüllen muss.

([11]) Die Liste der von der EU geschlossenen Abkommen und der von der Europäischen Kommission geschlossenen Verwaltungsvereinbarungen, in deren Rahmen EU-Verschlusssachen mit Drittstaaten und internationalen Organisationen ausgetauscht werden können, ist auf der Website der Kommission zu finden.

(7) Erhalten Bieter oder potenzielle Auftragnehmer Informationen des Geheimhaltungsgrads RESTREINT UE/EU RESTRICTED, so werden die in Absatz 6 genannten Mindestanforderungen in Angebote oder Geheimhaltungsvereinbarungen aufgenommen, die in der Ausschreibungsphase geschlossen werden.

(8) Soweit dies aufgrund der nationalen Rechtsvorschriften der Mitgliedstaaten erforderlich ist, stellen die nationalen Sicherheitsbehörden/beauftragten Sicherheitsbehörden sicher, dass die ihrer Hoheitsgewalt unterstehenden Auftragnehmer oder Unterauftragnehmer die geltenden Sicherheitsbestimmungen für den Schutz von als „RESTREINT UE/EU RESTRICTED“ eingestuften Verschlusssachen einhalten, und führen Kontrollen bei in ihrem Hoheitsgebiet gelegenen Einrichtungen von Auftragnehmern durch. Besteht für die nationale Sicherheitsbehörde/beauftragte Sicherheitsbehörde keine derartige Verpflichtung, stellt der öffentliche Auftraggeber sicher, dass der Auftragnehmer die in Anhang III festgelegten Sicherheitsbestimmungen umsetzt.

Artikel 6

Zugang von Mitarbeitern der Auftragnehmer und Unterauftragnehmer zu EU-VS

(1) Die Kommissionsdienststelle in ihrer Eigenschaft als öffentlicher Auftraggeber stellt sicher, dass als Verschlusssache eingestufte Verträge Bestimmungen enthalten, die vorsehen, dass Mitarbeitern von Auftragnehmern oder Unterauftragnehmern, die für die Ausführung des als Verschlusssache eingestuften Auftrags oder Unterauftrags Zugang zu EU-VS benötigen, ein entsprechender Zugang nur dann gewährt werden kann, wenn

a) sie nachweislich Kenntnis von den Verschlusssachen haben müssen,

b) sie für Verschlusssachen des Geheimhaltungsgrads „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“ von der jeweiligen nationalen Sicherheitsbehörde/beauftragten Sicherheitsbehörde oder einer anderen zuständigen Sicherheitsbehörde eine entsprechende Erklärung über die Sicherheitsüberprüfung von Personal erhalten haben,

c) sie über die geltenden Sicherheitsvorschriften für den Schutz von EU-VS belehrt wurden und ihre Verantwortlichkeiten hinsichtlich des Schutzes solcher Verschlusssachen anerkannt haben.

(2) Will ein Auftragnehmer oder Unterauftragnehmer einen Drittstaatsangehörigen in einer Position beschäftigen, die den Zugang zu Verschlusssachen des Geheimhaltungsgrads „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“ erfordert, so liegt es in der Verantwortung des Auftragnehmers oder Unterauftragnehmers, gemäß den Rechtsvorschriften, die an dem Ort gelten. an dem der Zugang zu den EU-VS gewährt werden soll, das Verfahren zur Sicherheitsüberprüfung der betreffenden Person einzuleiten.

KAPITEL 4

BESUCHE IM ZUSAMMENHANG MIT ALS VERSCHLUSSSACHE EINGESTUFTEN VERTRÄGEN

Artikel 7

Grundsätze

(1) Benötigen die Kommission, die Auftragnehmer oder die Unterauftragnehmer zur Ausführung eines als Verschlusssache eingestuften Vertrags Zugang zu Informationen des Geheimhaltungsgrads „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“ in den Räumlichkeiten des jeweils anderen, werden im Benehmen mit der jeweiligen nationalen Sicherheitsbehörde/beauftragten Sicherheitsbehörde oder einer anderen zuständigen Sicherheitsbehörde Besuche vereinbart.

(2) Für die in Absatz 1 genannten Besuche gelten folgende Anforderungen:

a) Der Besuch hat einen offiziellen Zweck, der mit einem von der Kommission geschlossenen, als Verschlusssache eingestuften Vertrag zusammenhängt.

b) Jeder Besucher muss in Besitz einer entsprechenden Erklärung über die Sicherheitsüberprüfung von Personal sein und nachweislich Einsicht in die betreffenden Verschlusssachen benötigen, um Zugang zu EU-VS zu erhalten, die bei der Ausführung eines von der Kommission geschlossenen, als Verschlusssache eingestuften Vertrags bereitgestellt oder generiert werden.

Artikel 8

Besuchsanträge

(1) Besuche von Auftragnehmern in Einrichtungen anderer Auftragnehmer oder in Räumlichkeiten der Kommission, bei denen Zugang zu Verschlusssachen des Geheimhaltungsgrads „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“ gewährt werden soll, werden nach folgendem Verfahren vereinbart:

a) Der Sicherheitsbeauftragte der Einrichtung, die den Besucher entsendet, füllt alle relevanten Teile des Besuchsantrags aus und übermittelt den Antrag an deren nationale Sicherheitsbehörde/beauftragte Sicherheitsbehörde. Anhang III Unteranhang C enthält ein Muster des Besuchsantrags.

b) Die nationale Sicherheitsbehörde/beauftragte Sicherheitsbehörde der entsendenden Einrichtung muss die Sicherheitsüberprüfung des Besuchers bestätigen, bevor sie den Besuchsantrag an die nationale Sicherheitsbehörde/beauftragte Sicherheitsbehörde der empfangenden Einrichtung (oder an die Sicherheitsstelle der Kommission, wenn der Besuch in Räumlichkeiten der Kommission erfolgen soll) übermittelt.

c) Der Sicherheitsbeauftragte der entsendenden Einrichtung erhält daraufhin von seiner nationalen Sicherheitsbehörde/beauftragten Sicherheitsbehörde die Antwort der nationalen Sicherheitsbehörde/beauftragten Sicherheitsbehörde der empfangenden Einrichtung (oder der Sicherheitsstelle der Kommission), mit der dem Besuchsantrag stattgegeben oder der Antrag abgelehnt wird.

d) Ein Besuchsantrag gilt als genehmigt, wenn bis fünf Arbeitstage vor dem Datum des Besuchs keine Einwände erhoben werden.

(2) Besuche von Beamten der Kommission in Einrichtungen des Auftragnehmers, die einen Zugang zu Verschlusssachen des Geheimhaltungsgrads „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“ umfassen, werden nach folgendem Verfahren vereinbart:

a) Der Besucher füllt alle relevanten Teile des Besuchsantragsformulars aus und übermittelt den Antrag an die Sicherheitsstelle der Kommission.

b) Die Sicherheitsstelle der Kommission bestätigt die Sicherheitsüberprüfung des Besuchers, bevor sie den Besuchsantrag an die nationale Sicherheitsbehörde/beauftragte Sicherheitsbehörde der empfangenden Einrichtung übermittelt.

c) Die Sicherheitsstelle der Kommission erhält von der nationalen Sicherheitsbehörde/beauftragten Sicherheitsbehörde der empfangenden Einrichtung eine Antwort, mit der dem Besuchsantrag stattgegeben oder der Antrag abgelehnt wird.

d) Ein Besuchsantrag gilt als genehmigt, wenn bis fünf Arbeitstage vor dem Datum des Besuchs keine Einwände erhoben werden.

(3) Ein Besuchsantrag kann sich auf einen einmaligen Besuch oder auf wiederholte Besuche erstrecken. Bei wiederholten Besuchen kann der Besuchsantrag eine Gültigkeit von bis zu einem Jahr ab dem im Antrag angegebenen Datum haben.

(4) Die Gültigkeit eines Besuchsantrags darf die Gültigkeit der Sicherheitsüberprüfung des Besuchers nicht überschreiten.

(5) Grundsätzlich sollte ein Besuchsantrag spätestens 15 Arbeitstage vor dem Datum des Besuchs an die zuständige Sicherheitsbehörde der empfangenden Einrichtung übermittelt werden.

Artikel 9

Besuchsverfahren

(1) Bevor Besuchern Zugang zu EU-VS gewährt wird, hält der Sicherheitsbeauftragte der empfangenden Einrichtung alle von der nationalen Sicherheitsbehörde/beauftragten Sicherheitsbehörde festgelegten besuchsbezogenen Sicherheitsverfahren und -vorschriften ein.

(2) Besucher weisen ihre Identität bei der Ankunft in der empfangenden Einrichtung nach, indem sie einen gültigen Personalausweis oder Reisepass vorlegen. Diese Identitätsangaben müssen den Angaben im Besuchsantrag entsprechen.

(3) Die empfangende Einrichtung stellt sicher, dass von allen Besuchern insbesondere ihre Namen, die von ihnen vertretene Organisation, das Ablaufdatum ihrer Sicherheitsüberprüfung, das Datum des Besuchs und die Namen der besuchten Personen aufgezeichnet werden. Diese Aufzeichnungen werden für einen Zeitraum von mindestens fünf Jahren oder länger aufbewahrt, wenn die nationalen Rechtsvorschriften des Landes, in dem sich die empfangende Einrichtung befindet, dies vorschreiben.

Artikel 10

Unmittelbar verabredete Besuche

(1) Im Zusammenhang mit spezifischen Projekten können die jeweiligen nationalen Sicherheitsbehörden/beauftragten Sicherheitsbehörden und die Sicherheitsstelle der Kommission ein Verfahren vereinbaren, nach dem Besuche im Rahmen eines bestimmten, als Verschlusssache eingestuften Vertrags unmittelbar zwischen dem Sicherheitsbeauftragten des Besuchers und dem Sicherheitsbeauftragten der zu besuchenden Einrichtung verabredet werden können. Ein Muster des zu diesem Zweck zu verwendenden Formulars ist in Anhang III Unteranhang C enthalten. In diesen Fällen finden die Verfahren nach Artikel 8 und Artikel 9 Absatz 1 keine Anwendung.

(2) Besuche, die mit einem Zugang zu Verschlusssachen des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“ einhergehen, werden unmittelbar zwischen der entsendenden und der empfangenden Einrichtung vereinbart, ohne dass die Verfahren nach Artikel 8 und Artikel 9 Absatz 1 befolgt werden müssen.

KAPITEL 5

ÜBERMITTLUNG UND BEFÖRDERUNG VON EU-VS BEI DER AUSFÜHRUNG VON ALS VERSCHLUSSSACHE EINGESTUFTEN VERTRÄGEN

Artikel 11

Grundsätze

Der öffentliche Auftraggeber stellt sicher, dass alle Beschlüsse im Zusammenhang mit der Übermittlung und Beförderung von EU-VS dem Beschluss (EU, Euratom) 2015/444 und seinen Durchführungsbestimmungen sowie den Bedingungen des als Verschlusssache eingestuften Vertrags entsprechen und die Zustimmung des Herausgebers vorliegt.

Artikel 12

Elektronische Bearbeitung

(1) Die elektronische Bearbeitung und Übermittlung von EU-VS erfolgt gemäß den Kapiteln 5 und 6 des Beschlusses (EU, Euratom) 2015/444 und seinen Durchführungsbestimmungen.

Die Kommunikations- und Informationssysteme, die sich im Besitz eines Auftragnehmers befinden und bei der Ausführung des Auftrags zur Bearbeitung von EU-VS genutzt werden, unterliegen der Akkreditierung durch die zuständige Sicherheitsakkreditierungsstelle. Jedwede elektronische Übermittlung von EU-VS wird durch kryptografische Produkte geschützt, die nach Artikel 36 Absatz 4 des Beschlusses (EU, Euratom) 2015/444 zugelassen wurden. TEMPEST-Maßnahmen werden nach Artikel 36 Absatz 6 des genannten Beschlusses durchgeführt.

(2) Die Sicherheitsakkreditierung des Kommunikations- und Informationssystems des Auftragnehmers, mit dem EU-VS des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“ bearbeitet werden sollen, und jeder Zusammenschaltung dieses Systems mit anderen Systemen kann dem Sicherheitsbeauftragten des Auftragnehmers übertragen werden, wenn dies nach den nationalen Rechtsvorschriften zulässig ist. Im Fall einer Übertragung dieser Aufgabe ist der Auftragnehmer verantwortlich für die Umsetzung der in der Geheimschutzklausel beschriebenen Mindestsicherheitsanforderungen, wenn er als „RESTREINT UE/EU RESTRICTED“ eingestufte Verschlusssachen in seinem Kommunikations- und Informationssystem bearbeitet. Die betreffenden nationalen Sicherheitsbehörden/beauftragten Sicherheitsbehörden und Sicherheitsakkreditierungsstellen behalten jedoch die Zuständigkeit für den Schutz von Verschlusssachen des Geheimhaltungsgrads RESTREINT UE/EU RESTRICTED, die vom Auftragnehmer bearbeitet werden, sowie das Recht, die von den Auftragnehmern ergriffenen Sicherheitsmaßnahmen zu kontrollieren. Darüber hinaus legt der Auftragnehmer dem öffentlichen Auftraggeber und, sofern dies aufgrund der nationalen Rechtsvorschriften vorgeschrieben ist, der zuständigen nationalen Sicherheitsakkreditierungsstelle eine Konformitätserklärung vor, mit der bescheinigt wird, dass das Kommunikations- und Informationssystem sowie damit verbundene Zusammenschaltungen des Auftragnehmers für die Bearbeitung von EU-VS des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“ ([12]) akkreditiert wurden.

Artikel 13

Beförderung durch kommerzielle Kurierdienste

Die Beförderung von EU-VS durch kommerzielle Kurierdienste richtet sich nach den einschlägigen Bestimmungen der Beschlüsse der Kommission über Durchführungsbestimmungen für die Bearbeitung von Verschlusssachen der Geheimhaltungsgrade „RESTREINT UE/EU RESTRICTED“ und CONFIDENTIEL UE/EU CONFIDENTIAL.

Artikel 14

Beförderung als Handgepäck

(1) Für die Beförderung von Verschlusssachen als Handgepäck gelten strenge Sicherheitsanforderungen.

(2) Als RESTREINT UE/EU RESTRICTED eingestufte Verschlusssachen dürfen von Mitarbeitern des Auftragnehmers in der EU als Handgepäck mitgeführt werden, sofern die folgenden Anforderungen erfüllt sind:

a) Der verwendete Umschlag bzw. die verwendete Verpackung ist undurchsichtig und enthält keinerlei Hinweis auf die Einstufung seines bzw. ihres Inhalts.

([12]) Die Mindestanforderungen für Kommunikations- und Informationssysteme, mit denen EU-VS des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“ bearbeitet werden, sind in Anhang III Unteranhang E festgelegt.

b) Die Verschlusssache verbleibt ununterbrochen im Besitz des Überbringers.

c) Der Umschlag bzw. die Verpackung wird während der Beförderung nicht geöffnet.

(3) Bei als „CONFIDENTIEL UE/EU CONFIDENTIAL“ und „SECRET UE/EU SECRET“ eingestuften Verschlusssachen wird die Beförderung durch Mitarbeiter des Auftragnehmers in einem EU-Mitgliedstaat im Voraus zwischen der Ausgangs- und der Eingangsstelle vereinbart. Die Ausgangsstelle unterrichtet die Eingangsstelle über die Einzelheiten der Sendung, darunter das Aktenzeichen, die Einstufung, die voraussichtliche Ankunftszeit und den Namen des Kurierdienstes. Die Beförderung als Handgepäck ist zulässig, sofern die folgenden Anforderungen erfüllt sind:

a) Die Verschlusssachen werden in einem doppelten Umschlag bzw. in einer doppelten Verpackung befördert.

b) Der äußere Umschlag bzw. die äußere Verpackung ist gesichert und enthält keine Hinweise auf die Einstufung seines bzw. ihres Inhalts, und auf dem inneren Umschlag ist der Geheimhaltungsgrad angegeben.

c) Die Verschlusssache verbleibt ununterbrochen im Besitz des Überbringers.

d) Der Umschlag bzw. die Verpackung wird während der Beförderung nicht geöffnet.

e) Der Umschlag bzw. die Verpackung wird in einer verschließbaren Aktentasche oder einem ähnlichen zugelassenen Behältnis befördert, dessen Größe und Gewicht es ermöglichen, dass die Verschlusssache jederzeit im persönlichen Besitz des Überbringers verbleibt und nicht als aufgegebenes Gepäck befördert wird.

f) Der Kurierdienst führt einen von seiner zuständigen Sicherheitsbehörde ausgestellten Kurierausweis mit sich, mit dem er ermächtigt wird, die angegebene Verschlusssache zu befördern.

(4) Für die manuelle Beförderung von Verschlusssachen der Geheimhaltungsgrade „CONFIDENTIEL UE/EU CONFIDENTIAL“ und „SECRET UE/EU SECRET“ durch den Auftragnehmer von einem EU-Mitgliedstaat in einen anderen gelten die folgenden zusätzlichen Regeln:

a) Der Kurierdienst ist bis zur Übergabe an den Empfänger für die sichere Verwahrung der beförderten Verschlusssache verantwortlich.

b) Im Falle einer Verletzung der Sicherheit kann die nationale Sicherheitsbehörde/beauftragte Sicherheitsbehörde des Senders beantragen, dass die Behörden des Landes, in dem die Verletzung erfolgte, eine Untersuchung durchführen, ihre Ergebnisse melden und gegebenenfalls rechtliche oder sonstige Maßnahmen ergreifen.

c) Der Kurierdienst muss über alle während der Beförderung einzuhaltenden sicherheitsrelevanten Verpflichtungen belehrt worden sein und eine entsprechende Bestätigung unterzeichnet haben.

d) Die Anweisungen für den Kurierdienst werden dem Kurierausweis beigefügt.

e) Der Kurierdienst muss eine Beschreibung der Sendung und der Route erhalten haben.

f) Die Dokumente werden der ausstellenden nationalen Sicherheitsbehörde/beauftragten Sicherheitsbehörde nach Abschluss der Reise(n) zurückgeschickt oder vom Empfänger zu Kontrollzwecken aufbewahrt.

g) Wollen Zoll, Einwanderungsbehörden oder Grenzpolizei die Sendung prüfen und kontrollieren, so ist es ihnen gestattet, so viele Teile der Sendung zu öffnen und in Augenschein zu nehmen, wie erforderlich ist, um feststellen zu können, dass sie kein anderes als das angegebene Material enthält.

h) Der Zoll sollte aufgefordert werden, den amtlichen Charakter der Versandpapiere und der vom Kurierdienst mitgeführten Ermächtigungsunterlagen zu achten.

Wird eine Sendung durch den Zoll geöffnet, so sollte dies unter Ausschluss unbefugter Personen und nach Möglichkeit in Anwesenheit des Kurierdienstes erfolgen. Der Kurierdienst veranlasst die Neuverpackung der Sendung und fordert die für die Kontrolle zuständigen Behörden auf, die Sendung neu zu versiegeln und schriftlich zu bestätigen, dass die Sendung durch sie geöffnet wurde.

(5) Die manuelle Beförderung von Verschlusssachen des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“, „CONFIDENTIEL UE/EU CONFIDENTIAL“ und „SECRET UE/EU SECRET“ durch Mitarbeiter des Auftragnehmers in einen Drittstaat oder zu einer internationalen Organisation unterliegt den Bestimmungen des Geheimschutzabkommens zwischen der Europäischen Union und dem betreffenden Drittstaat oder der betreffenden internationalen Organisation bzw. den Bestimmungen der Verwaltungsvereinbarung zwischen der Kommission und dem Drittstaat oder der internationalen Organisation.

KAPITEL 6

BETRIEBSKONTINUITÄTSPLANUNG

Artikel 15

Notfallpläne und Wiederherstellungsmaßnahmen

Die Kommissionsdienststelle in ihrer Eigenschaft als öffentlicher Auftraggeber stellt sicher, dass der Auftragnehmer nach dem als Verschlusssache eingestuften Vertrag verpflichtet ist, Notfallpläne für den Schutz von EU-VS, die in Verbindung mit der Erfüllung des als Verschlusssache eingestuften Vertrags in Notsituationen bearbeitet werden, zu erstellen und im Rahmen der Betriebskontinuitätsplanung Präventiv- und Wiederherstellungsmaßnahmen durchzuführen, um die Auswirkungen von Zwischenfällen im Zusammenhang mit der Bearbeitung und Speicherung bzw. Aufbewahrung von EU-VS so gering wie möglich zu halten. Der Auftragnehmer unterrichtet den öffentlichen Auftraggeber über seine Betriebskontinuitätsplanung.

Artikel 16

Inkrafttreten

Dieser Beschluss tritt am zwanzigsten Tag nach seiner Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Brüssel, den 17. Oktober 2019

Für die Kommission,

im Namen des Präsidenten,

Günther OETTINGER

Mitglied der Kommission

ANHANG I

STANDARDINFORMATIONEN IN AUFTRAGSBEKANNTMACHUNGEN

(an die verwendeten Auftragsbekanntmachungen anzupassen)

Für Verträge, die Verschlusssachen des Geheimhaltungsgrads „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“ umfassen

Sonstige besondere Bedingungen (*falls zutreffend*)

Die Erfüllung des Vertrags unterliegt besonderen Bedingungen: ● ja ○ nein

(*wenn ja*) Darlegung der besonderen Bedingungen:

Im Vertrag ist ein Zugang zu als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“ eingestuften Verschlusssachen und deren Bearbeitung und/oder Aufbewahrung bzw. Speicherung, worauf der Beschluss (EU, Euratom) 2015/444 und dessen Durchführungsbestimmungen [1] Anwendung finden, vorgesehen.

Erforderlich sind ein Sicherheitsbescheid für Einrichtungen sowie Erklärungen über die Sicherheitsüberprüfung von Personal für Mitarbeiter des Auftragnehmers, die Verschlusssachen bearbeiten.

Besondere Sicherheitsanforderungen sind Bestandteil des Vertrags (Geheimschutzklausel im Anhang des Vertrags). Die Vergabe von Unteraufträgen unterliegt der schriftlichen vorherigen Genehmigung durch den öffentlichen Auftraggeber und der Einhaltung aller Sicherheitsvorschriften durch den Unterauftragnehmer und dessen Mitarbeiter.

Für Verträge, die Verschlusssachen des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“ umfassen

Sonstige besondere Bedingungen (*falls zutreffend*)

Die Erfüllung des Vertrags unterliegt besonderen Bedingungen: ● ja ○ nein

(*wenn ja*) Darlegung der besonderen Bedingungen:

Der Vertrag umfasst den Zugang zu als „RESTREINT UE/EU RESTRICTED“ eingestuften Verschlusssachen und deren Bearbeitung und/oder Aufbewahrung bzw. Speicherung, worauf der Beschluss (EU, Euratom) 2015/444 und dessen Durchführungsbestimmungen [2] Anwendung finden.

Besondere Sicherheitsanforderungen sind Bestandteil des Vertrags (Geheimschutzklausel im Anhang des Vertrags). Die Vergabe von Unteraufträgen unterliegt der schriftlichen vorherigen Genehmigung durch den öffentlichen Auftraggeber und der Einhaltung aller Sicherheitsvorschriften durch den Unterauftragnehmer und dessen Mitarbeiter.

[1] Der öffentliche Auftraggeber sollte die Verweise einfügen, sobald die Durchführungsbestimmungen angenommen wurden.
[2] Der öffentliche Auftraggeber sollte die Verweise einfügen, sobald die Durchführungsbestimmungen angenommen wurden.

ANHANG II

STANDARDKLAUSELN FÜR ÖFFENTLICHE AUFTRÄGE

(an die verwendeten Verträge anzupassen)

ARTIKEL XX

SICHERHEITSPFLICHTEN

XX.1 EU-Verschlusssachen

Werden bei der Erfüllung des Vertrags EU-Verschlusssachen verwendet oder erstellt, müssen diese Verschlusssachen gemäß der Geheimschutzklausel und deren Einstufungsleitfaden für Verschlusssachen nach Anhang I sowie gemäß dem Beschluss (EU, Euratom) 2015/444 und dessen Durchführungsbestimmungen [1] behandelt werden, bis deren Geheimhaltungsgrad aufgehoben ist.

Leistungen, die Verschlusssachen enthalten, sind gemäß den mit dem öffentlichen Auftraggeber vereinbarten besonderen Verfahren vorzulegen.

Für Aufgaben, die Verschlusssachen umfassen, darf ohne vorherige ausdrückliche schriftliche Zustimmung des öffentlichen Auftraggebers keine Unterauftragsvergabe erfolgen.

EU-Verschlusssachen dürfen ohne vorherige ausdrückliche schriftliche Zustimmung des öffentlichen Auftraggebers nicht an Dritte (einschließlich Unterauftragnehmern) weitergegeben werden.

[1] Der öffentliche Auftraggeber sollte die Verweise einfügen, sobald die Durchführungsbestimmungen angenommen sind.

ANHANG III

[Anhang IV (des Rahmenvertrags)]

GEHEIMSCHUTZKLAUSEL

[Muster]

Unteranhang A

SICHERHEITSANFORDERUNGEN

Der öffentliche Auftraggeber muss die folgenden Sicherheitsanforderungen in die Geheimschutzklausel aufnehmen. Einige Klauseln sind möglicherweise nicht auf den Vertrag anwendbar. Diese sind in eckigen Klammern angegeben.

Die Liste der Klauseln ist nicht erschöpfend. Je nach Art des als Verschlusssache eingestuften Vertrags können weitere Klauseln hinzugefügt werden.

ALLGEMEINE BEDINGUNGEN

[*Hinweis: gelten für alle als Verschlusssache eingestuften Verträge*]

1. Diese Geheimschutzklausel ist fester Bestandteil des als Verschlusssache eingestuften Vertrags [oder Untervertrags] und beschreibt die vertragsspezifischen Sicherheitsanforderungen. Die Nichterfüllung dieser Anforderungen kann einen hinreichenden Grund zur Kündigung des Vertrags darstellen.

2. Auftragnehmer unterliegen allen Verpflichtungen gemäß dem Beschluss (EU, Euratom) 2015/444 und dessen Durchführungsbestimmungen ([1]).

3. Verschlusssachen, die bei der Erfüllung des Vertrags erstellt werden, müssen gemäß dem Einstufungsleitfaden für Verschlusssachen in Unteranhang B zu dieser Geheimschutzklausel als EU-Verschlusssache (EU-VS) eingestuft sein. Von dem im Einstufungsleitfaden für Verschlusssachen festgelegten Einstufungsgrad darf nur mit schriftlicher Genehmigung des öffentlichen Auftraggebers abgewichen werden.

4. Die Rechte des Herausgebers von EU-VS, die für die Erfüllung des als Verschlusssache eingestuften Vertrags erstellt und bearbeitet werden, werden von der Kommission in ihrer Eigenschaft als öffentlicher Auftraggeber ausgeübt.

5. Ohne die schriftliche Zustimmung des öffentlichen Auftraggebers dürfen der Auftragnehmer oder der Unterauftragnehmer Informationen oder Materialien, die vom öffentlichen Auftraggeber bereitgestellt oder in dessen Auftrag erstellt werden, nicht für andere Zwecke als die vertraglich festgelegten Zwecke verwenden.

6. Der Auftragnehmer muss alle Sicherheitsverstöße im Zusammenhang mit EU-VS untersuchen und dem öffentlichen Auftraggeber so schnell wie möglich melden. Der Auftragnehmer oder der Unterauftragnehmer müssen der zuständigen nationalen Sicherheitsbehörde oder der beauftragten Sicherheitsbehörde und, soweit die nationalen Rechtsvorschriften dies zulassen, der Sicherheitsstelle der Kommission unverzüglich alle Fälle melden, in denen bekannt ist oder Grund zu der Annahme besteht, dass vertragsgemäß bereitgestellte oder erstellte EU-VS verloren gegangen oder an Unbefugte weitergegeben worden sind.

7. Nach Ablauf des Vertrags müssen der Auftragnehmer oder der Unterauftragnehmer dem öffentlichen Auftraggeber schnellstmöglich alle in ihrem Besitz befindlichen EU-VS zurückgeben. Sofern dies durchführbar ist, können der Auftragnehmer oder der Unterauftragnehmer EU-VS vernichten, anstatt sie zurückzugeben. Die Vernichtung bedarf der vorherigen Zustimmung der Sicherheitsstelle der Kommission und hat im Einklang mit den nationalen Rechtsvorschriften des Landes, in dem der Auftragnehmer seinen Sitz hat, nach den Anweisungen der Sicherheitsstelle zu erfolgen. EU-VS sind so zu vernichten, dass eine vollständige oder teilweise Wiederherstellung ausgeschlossen ist.

8. Wird dem Auftragnehmer oder dem Unterauftragnehmer gestattet, EU-VS nach der Kündigung oder Erfüllung des Vertrags in seinem Besitz zu behalten, müssen die EU-VS weiterhin gemäß dem Beschluss (EU, Euratom) 2015/444 (im Folgenden „Kommissionsbeschluss" 2015/444) und dessen Durchführungsbestimmungen ([2]) geschützt bleiben.

9. Jedwede elektronische Bearbeitung, Verarbeitung und Übermittlung von EU-VS muss nach den Bestimmungen der Kapitel 5 und 6 des Kommissionsbeschlusses 2015/444 erfolgen. Dazu gehören unter anderem folgende Anforderungen: Ein Kommunikations- und Informationssystem (im Folgenden „KIS") des Auftragnehmers, das für die Bearbeitung von EU-VS für die Zwecke des Vertrags verwendet wird, muss akkreditiert werden ([3]), jedwede elektronische Übermittlung von EU-VS muss durch kryptografische Produkte geschützt werden, die nach Artikel 36 Absatz 4 des Kommissionsbeschlusses 2015/444 zugelassen wurden, und TEMPEST-Maßnahmen müssen nach Artikel 36 Absatz 6 des Kommissionsbeschlusses 2015/444 durchgeführt werden.

([1]) Der öffentliche Auftraggeber sollte die Verweise einfügen, sobald die Durchführungsbestimmungen angenommen sind.
([2]) Der öffentliche Auftraggeber sollte die Verweise einfügen, sobald die Durchführungsbestimmungen angenommen wurden.
([3]) Die Partei, die die Akkreditierung durchführt, muss dem öffentlichen Auftraggeber über die Sicherheitsstelle der Kommission und in Abstimmung mit der zuständigen nationalen Sicherheitsakkreditierungsstelle eine Konformitätserklärung vorlegen.

10. Der Auftragnehmer oder der Unterauftragnehmer müssen über Notfallpläne für den Schutz von EU-VS verfügen, die bei der Erfüllung des als Verschlusssache eingestuften Vertrags in Notsituationen bearbeitet werden, und Präventiv- und Wiederherstellungsmaßnahmen vorsehen, um die Auswirkungen von Zwischenfällen im Zusammenhang mit der Bearbeitung und Speicherung bzw. Aufbewahrung von EU-VS so gering wie möglich zu halten. Der Auftragnehmer oder der Unterauftragnehmer müssen den öffentlichen Auftraggeber über ihre Betriebskontinuitätsplanung unterrichten.

AUFTRÄGE, DIE DEN ZUGANG ZU VERSCHLUSSSACHEN DES GEHEIMHALTUNGSGRADS „RESTREINT UE/EU RESTRICTED“ ERFORDERN

11. Für die Erfüllung des Vertrags ist keine Sicherheitsüberprüfung von Personal erforderlich. Zugang zu Verschlusssachen des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“ können jedoch nur Mitarbeiter des Auftragnehmers erhalten, die diese Verschlusssachen zur Erfüllung des Vertrags benötigen (Grundsatz „Kenntnis nur, wenn nötig“), die vom Sicherheitsbeauftragten des Auftragnehmers über ihre Verantwortlichkeiten und die Folgen einer etwaigen Kompromittierung oder Verletzung der Sicherheit dieser Verschlusssachen belehrt wurden und die die Konsequenzen einer Nichteinhaltung des Schutzes von EU-VS schriftlich anerkannt haben.

12. Außer in den Fällen, in denen der öffentliche Auftraggeber seine schriftliche Zustimmung erteilt hat, dürfen der Auftragnehmer oder der Unterauftragnehmer Verschlusssachen des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“ nicht anderen Einrichtungen oder Personen als ihren Mitarbeitern, die Kenntnis von den Verschlusssachen haben müssen, zugänglich machen.

13. Der Auftragnehmer oder der Unterauftragnehmer müssen die Kennzeichnung mit einem Geheimhaltungsgrad für Verschlusssachen, die bei der Erfüllung eines Vertrags erstellt oder bereitgestellt werden, beibehalten und dürfen den Geheimhaltungsgrad einer Verschlusssache nicht ohne schriftliche Zustimmung des öffentlichen Auftraggebers aufheben.

14. Verschlusssachen des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“ müssen in verschließbaren Büromöbeln aufbewahrt werden, wenn sie nicht verwendet werden. Bei der Beförderung müssen die Dokumente in einem undurchsichtigen Umschlag mitgeführt werden. Dieser Umschlag mit den Dokumenten muss ununterbrochen im Besitz des Überbringers verbleiben und darf nicht geöffnet werden.

15. Der Auftragnehmer oder der Subauftragnehmer können der Kommission Dokumente des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“ durch kommerzielle Kurierdienste, Postdienste, als Handgepäck oder auf elektronischem Wege übermitteln. Diesbezüglich müssen der Auftragnehmer oder der Unterauftragnehmer die von der Kommission erstellten Programm- oder Projektsicherheitsanweisungen und/oder die Durchführungsbestimmungen der Kommission über den Geheimschutz in der Wirtschaft in Bezug auf als Verschlusssache eingestufte öffentliche Aufträge ([4]) beachten.

16. Nicht länger benötigte Dokumente des Geheimhaltungsgrads RESTREINT EU/EU RESTRICTED sind so zu vernichten, dass eine vollständige oder teilweise Wiederherstellung ausgeschlossen ist.

17. Die Sicherheitsakkreditierung des KIS des Auftragnehmers, mit dem EU-VS des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“ bearbeitet werden sollen, und jeder Zusammenschaltung dieses Systems mit anderen Systemen kann dem Sicherheitsbeauftragten des Auftragnehmers übertragen werden, wenn dies nach den nationalen Rechtsvorschriften zulässig ist. Wird die Akkreditierung übertragen, behalten die nationalen Sicherheitsbehörden/beauftragten Sicherheitsbehörden/Sicherheitsakkreditierungsstellen die Zuständigkeit für den Schutz von Verschlusssachen des Geheimhaltungsgrads RESTREINT UE/EU RESTRICTED, die vom Auftragnehmer bearbeitet werden, sowie das Recht, die vom Auftragnehmer ergriffenen Sicherheitsmaßnahmen zu kontrollieren. Darüber hinaus legt der Auftragnehmer dem öffentlichen Auftraggeber und, sofern dies aufgrund der nationalen Rechtsvorschriften vorgeschrieben ist, der zuständigen nationalen Sicherheitsakkreditierungsstelle eine Konformitätserklärung vor, mit der bescheinigt wird, dass das KIS sowie damit verbundene Zusammenschaltungen des Auftragnehmers für die Bearbeitung von EU-VS des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“ akkreditiert wurden.

BEARBEITUNG VON VERSCHLUSSSACHEN DES GEHEIMHALTUNGSGRADS „RESTREINT UE/EU RESTRICTED“ IN KOMMUNIKATIONS- UND INFORMATIONSSYSTEMEN (KIS)

18. Die Mindestanforderungen für KIS zur Bearbeitung von Verschlusssachen des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“ sind in Unteranhang E zu dieser Geheimschutzklausel enthalten.

BEDINGUNGEN, UNTER DENEN DER AUFTRAGNEHMER UNTERAUFTRÄGE VERGEBEN DARF

19. Vor einer etwaigen Untervergabe von Teilen eines als Verschlusssache eingestuften Auftrags holt der Auftragnehmer die Erlaubnis der betreffenden Kommissionsdienststelle in ihrer Eigenschaft als öffentlicher Auftraggeber ein.

([4]) Der öffentliche Auftraggeber sollte die Verweise einfügen, sobald die Durchführungsbestimmungen angenommen wurden.

20. Es kann kein Unterauftrag an ein Unternehmen vergeben werden, das in einem Drittstaat registriert ist, oder eine Einrichtung, die zu einer internationalen Organisation gehört, wenn dieser Drittstaat oder diese internationale Organisation weder ein Geheimschutzabkommen mit der EU noch eine Verwaltungsvereinbarung mit der Kommission geschlossen hat.

21. Hat der Auftragnehmer einen Unterauftrag vergeben, so gelten die Sicherheitsvorschriften des Vertrags entsprechend für den bzw. die Unterauftragnehmer und sein bzw. ihr Personal. In diesem Fall hat der Auftragnehmer dafür zu sorgen, dass alle Unterauftragnehmer diese Grundsätze auf ihre eigenen Unterauftragsvereinbarungen anwenden. Um eine angemessene Sicherheitsaufsicht zu gewährleisten, sind die nationalen Sicherheitsbehörden/beauftragten Sicherheitsbehörden des Auftragnehmers und des Unterauftragnehmers über die Vergabe sämtlicher Unteraufträge zu unterrichten, die Verschlusssachen der Geheimhaltungsgrade CONFIDENTIEL UE/EU CONFIDENTIAL und SECRET UE/EU SECRET betreffen. Gegebenenfalls ist den nationalen Sicherheitsbehörden/beauftragten Sicherheitsbehörden des Auftragnehmers und des Unterauftragnehmers eine Kopie der unterauftragsspezifischen Sicherheitsvorschriften vorzulegen. Die nationalen Sicherheitsbehörden/beauftragten Sicherheitsbehörden, denen die Sicherheitsvorschriften für als RESTREINT UE/EU RESTRICTED eingestufte Verträge zu melden sind, sind im Anhang der Durchführungsbestimmungen der Kommission über den Geheimschutz in der Wirtschaft in Bezug auf als Verschlusssache eingestufte öffentliche Aufträge ([1]) aufgeführt.

22. Der Auftragnehmer darf ohne vorherige schriftliche Zustimmung des öffentlichen Auftraggebers keine EU-VS an einen Unterauftragnehmer weitergeben. Sind EU-VS häufig oder routinemäßig an Unterauftragnehmer zu übermitteln, so kann der öffentliche Auftraggeber seine Zustimmung für eine bestimmte Dauer (z. B. 12 Monate) oder für die Laufzeit des Unterauftrags erteilen.

BESUCHE

Ist auf Besuche, die Verschlusssachen der Geheimhaltungsgrade „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“ betreffen, das Standardverfahren für Besuchsanträge anzuwenden, so muss der öffentliche Auftraggeber die Nummern 23, 24 und 25 aufnehmen und Nummer 26 streichen. Werden Besuche, die Verschlusssachen der Geheimhaltungsgrade „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“ betreffen, unmittelbar zwischen der entsendenden und der empfangenden Einrichtung durchgeführt, so muss der öffentliche Auftraggeber die Nummern 24 und 25 streichen und nur Nummer 26 aufnehmen.

23. Besuche, die einen tatsächlichen oder möglichen Zugang zu Verschlusssachen des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“ umfassen, werden unmittelbar zwischen der entsendenden und der empfangenden Einrichtung vereinbart, ohne dass das Verfahren nach den Nummern 24 bis 26 zu befolgen ist.

[24. Besuche, die einen tatsächlichen oder möglichen Zugang zu Verschlusssachen der Geheimhaltungsgrade „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“ umfassen, unterliegen dem folgenden Verfahren:

a) Der Sicherheitsbeauftragte der Einrichtung, die den Besucher entsendet, füllt alle relevanten Teile des Besuchsantragsformulars (Unteranhang C) aus und übermittelt den Antrag an deren nationale Sicherheitsbehörde/beauftragte Sicherheitsbehörde.

b) Die nationale Sicherheitsbehörde/beauftragte Sicherheitsbehörde der entsendenden Einrichtung muss die Sicherheitsüberprüfung des Besuchers bestätigen, bevor sie den Besuchsantrag an die nationale Sicherheitsbehörde/beauftragte Sicherheitsbehörde der empfangenden Einrichtung (oder an die Sicherheitsstelle der Kommission, wenn der Besuch in Räumlichkeiten der Kommission erfolgen soll) übermittelt.

c) Der Sicherheitsbeauftragte der entsendenden Einrichtung erhält daraufhin von seiner nationalen Sicherheitsbehörde/beauftragten Sicherheitsbehörde die Antwort der nationalen Sicherheitsbehörde/beauftragten Sicherheitsbehörde der empfangenden Einrichtung (oder der Sicherheitsstelle der Kommission), mit der dem Besuchsantrag stattgegeben oder der Antrag abgelehnt wird.

d) Ein Besuchsantrag gilt als genehmigt, wenn bis fünf Arbeitstage vor dem Datum des Besuchs keine Einwände erhoben werden.]

[25. Bevor die empfangende Einrichtung Besuchern Zugang zu Verschlusssachen der Geheimhaltungsgrade „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“ gewährt, muss sie die Genehmigung von ihrer nationalen Sicherheitsbehörde/beauftragten Sicherheitsbehörde erhalten haben.]

[26. Besuche, bei denen tatsächlich oder möglicherweise Zugang zu Verschlusssachen der Geheimhaltungsgrade „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“ gewährt wird, werden unmittelbar zwischen der entsendenden und der empfangenden Einrichtung vereinbart (ein Muster des Formulars, das zu diesem Zweck verwendet werden kann, ist in Unteranhang C enthalten).]

([1]) Der öffentliche Auftraggeber sollte die Verweise einfügen, sobald die Durchführungsbestimmungen angenommen wurden.

27. Besucher müssen ihre Identität bei der Ankunft in der empfangenden Einrichtung nachweisen, indem sie einen gültigen Personalausweis oder Reisepass vorlegen.

28. Die empfangende Einrichtung muss sicherstellen, dass alle Besucher registriert werden. Insbesondere müssen ihre Namen, die von ihnen vertretene Organisation, das Ablaufdatum ihrer Sicherheitsüberprüfung (falls zutreffend), das Datum des Besuchs und der/die Name(n) der besuchten Person(en) aufgezeichnet werden. Unbeschadet der europäischen Datenschutzvorschriften sind diese Aufzeichnungen für einen Zeitraum von mindestens fünf Jahren oder gegebenenfalls entsprechend den nationalen Rechtsvorschriften zu speichern.

BEWERTUNGSBESUCHE

29. Die Sicherheitsstelle der Kommission kann in Zusammenarbeit mit der zuständigen nationalen Sicherheitsbehörde/beauftragten Sicherheitsbehörde Besuche in Einrichtungen von Auftragnehmern oder Unterauftragnehmern durchführen, um zu prüfen, ob die Sicherheitsanforderungen für die Bearbeitung von EU-VS eingehalten werden.

EINSTUFUNGSLEITFADEN FÜR VERSCHLUSSSACHEN

30. Eine Liste aller Elemente des Vertrags, die im Zuge der Vertragserfüllung als Verschlusssache eingestuft werden oder einzustufen sind, die Vorschriften zur Einstufung sowie die anwendbaren Geheimhaltungsgrade sind im Einstufungsleitfaden für Verschlusssachen enthalten. Der Einstufungsleitfaden ist fester Bestandteil dieses Vertrags und befindet sich in Unteranhang B zum vorliegenden Anhang.

Unteranhang B

EINSTUFUNGSLEITFADEN FÜR VERSCHLUSSSACHEN

[Der jeweilige Wortlaut ist je nach Auftragsgegenstand anzupassen.]

Unteranhang C

BESUCHSANTRAG

(MUSTER)

Detaillierte Anweisungen für das Ausfüllen des Besuchsantrags

(Der Antrag ist ausschließlich in englischer Sprache einzureichen.)

HEADING	Bitte kreuzen Sie die zutreffenden Kästchen im Hinblick auf Besuchsart und Geheimhaltungsgrad an und machen Sie Angaben zur Zahl der zu besuchenden Standorte und der Besucher.
4. **ADMINISTRATIVE DATA**	Von der nationalen Sicherheitsbehörde/der beauftragten Sicherheitsbehörde auszufüllen.
5. **REQUESTING ORGANISATION OR INDUSTRIAL FACILITY**	Geben Sie bitte die vollständige Bezeichnung und die vollständige Postanschrift (ggf. einschließlich Postleitzahl, Stadt und Land) an.
6. **ORGANISATION OR INDUSTRIAL FACILITY TO BE VISITED**	Geben Sie bitte die vollständige Bezeichnung und die vollständige Postanschrift an. Anzugeben sind unter anderem Postleitzahl, Stadt, Land, Telex oder Faxnummer (falls zutreffend), Telefonnummer und E-Mail-Adresse. Bitte geben Sie den Namen sowie die Telefon-/Faxnummer(n) und die E-Mail-Adresse Ihres Hauptansprechpartners oder der Person an, mit der Sie den Besuch vereinbart haben. Hinweise: 1) Die Angabe der richtigen Postleitzahl ist wichtig, da ein Unternehmen verschiedene Räumlichkeiten haben kann. 2) Bei der manuellen Antragstellung kann Anhang 1 verwendet werden, wenn zwei oder mehr Einrichtungen in Verbindung mit demselben Gegenstand besucht werden müssen. Bei Verwendung eines Anhangs sollte Punkt 3 wie folgt lauten: „SEE ANNEX 1, NUMBER OF FAC: …“ (bitte Zahl der Räumlichkeiten angeben).
7. **DATES OF VISIT**	Bitte geben Sie das tatsächliche Datum oder den tatsächlichen Zeitraum (Datum bis Datum) des Besuchs im Format „Tag — Monat — Jahr“ an. Geben Sie gegebenenfalls ein alternatives Datum oder einen alternativen Zeitraum in Klammern an.
8. **TYPE OF INITIATIVE**	Bitte geben Sie an, ob der Besuch von der antragstellenden Organisation bzw. Einrichtung oder auf Einladung der zu besuchenden Einrichtung in die Wege geleitet wurde.
9. **THE VISIT RELATES TO:**	Bitte geben Sie die vollständige Bezeichnung des Projekts, des Auftrags oder der Ausschreibung an und verwenden Sie dabei ausschließlich gebräuchliche Abkürzungen.

10. **SUBJECT TO BE DISCUSSED/ JUSTIFICATION**	Geben Sie bitte eine kurze Begründung für den Besuch an. Verwenden Sie keine unverständlichen Abkürzungen. Hinweis: Bei wiederholten Besuchen sollten die Angaben unter diesem Punkt mit „Recurring visits“ beginnen (z. B. „Recurring visits to dicuss ___“).
11. **ANTICIPATED LEVEL OF CLASSIFIED INFORMATION TO BE INVOLVED**	Bitte SECRET UE/EU SECRET (S-UE/EU-S) bzw. CONFIDENTIEL UE/EU CONFIDENTIAL (C-UE/EU-C) angeben.
12. **PARTICULARS OF VISITOR**	Hinweis: Bei mehr als zwei Besuchern sollte Anhang 2 verwendet werden.
13. **THE SECURITY OFFICER OF THE REQUESTING ENTITY**	Unter diesem Punkt sind Name, Telefonnummer, Faxnummer und E-Mail-Adresse des Sicherheitsbeauftragten der antragstellenden Einrichtung anzugeben.
14. **CERTIFICATION OF SECURITY CLEARANCE**	Dieses Feld ist von der ausstellenden Behörde auszufüllen. Hinweise für die ausstellende Behörde: a) Bitte Namen, Anschrift, Telefonnummer, Faxnummer und E-Mail-Adresse angeben (Verwendung eines Vordrucks ist möglich). b) Bitte unterzeichnen und stempeln (falls zutreffend).
15. **REQUESTING SECURITY AUTHORITY**	Dieses Feld ist von der nationalen Sicherheitsbehörde/der beauftragten Sicherheitsbehörde auszufüllen. Hinweise für die betreffende Behörde: a) Bitte Namen, Anschrift, Telefonnummer, Faxnummer und E-Mail-Adresse angeben (Verwendung eines Vordrucks ist möglich). b) Bitte unterzeichnen und stempeln (falls zutreffend).

Alle Felder müssen ausgefüllt werden. Das Formular ist über vernetzte Verwaltungskanäle zu übermitteln ([2]).

([2]) Wurde vereinbart, dass Besuche, die einen tatsächlichen oder möglichen Zugang zu EU-VS der Geheimhaltungsgrade CONFIDENTIEL UE/EU CONFIDENTIAL und SECRET UE/EU SECRET umfassen, unmittelbar verabredet werden können, kann das ausgefüllte Formular unmittelbar an den Sicherheitsbeauftragten der zu besuchenden Einrichtung übermittelt werden.

REQUEST FOR VISIT

(MODEL)

To: _____

1. **TYPE OF VISIT REQUEST**	2. **TYPE OF INFORMATION**	3. **SUMMARY**
☐ Single ☐ Recurring ☐ Emergency ☐ Amendment ☐ Dates ☐ Visitors ☐ Facility For an amendment, insert the NSA/DSA original RFV Reference No_____	☐ C-UE/EU-C ☐ S-UE/EU-S	No of sites: _____ No of visitors: _____

4. **ADMINISTRATIVE DATA:**

Requester:	NSA/DSA RFV Reference No_____
To:	Date *(dd/mm/yyyy)*: _____/_____/_____

5. **REQUESTING ORGANISATION OR INDUSTRIAL FACILITY:**

NAME:

POSTAL ADDRESS:

E-MAIL ADDRESS:

FAX NO: TELEPHONE NO:

6. **ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED** *(Annex 1 to be completed)*

7. **DATE OF VISIT** *(dd/mm/yyyy)*: FROM _____/_____/_____ TO _____/_____/_____

8. **TYPE OF INITIATIVE:**

☐ Initiated by requesting organisation or facility

☐ By invitation of the facility to be visited

9. **THE VISIT RELATES TO CONTRACT:**

10. **SUBJECT TO BE DISCUSSED/REASONS/PURPOSE** *(Include details of host entity and any other relevant information. Abbreviations should be avoided):*

11. **ANTICIPATED HIGHEST CLASSIFICATION LEVEL OF INFORMATION/MATERIAL OR SITE ACCESS TO BE INVOLVED:**

12. **PARTICULARS OF VISITOR(S)** *(Annex 2 to be completed)*

13. **THE SECURITY OFFICER OF THE REQUESTING ORGANISATION OR INDUSTRIAL FACILITY:**

NAME:

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE:

14. **CERTIFICATION OF SECURITY CLEARANCE LEVEL:**

NAME:

ADDRESS:

STAMP

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE: DATE *(dd/mm/yyyy)*: _____/_____/_____

15. **REQUESTING NATIONAL SECURITY AUTHORITY/DESIGNATED SECURITY AUTHORITY:**

NAME:

ADDRESS:

TELEPHONE NO:

E-MAIL ADDRESS:

STAMP

SIGNATURE: DATE *(dd/mm/yyyy)*: _____/_____/_____

16. **REMARKS** *(Mandatory justification required in the case of an emergency visit)*:

<Platzhalter für Verweis auf die geltenden Datenschutzvorschriften und Link zu der vorgeschriebenen Auskunft an die betroffene Person, z. B. darüber, wie Artikel 13 der Datenschutz-Grundverordnung ([3]) umgesetzt wird.>

([3]) Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

ANNEX 1 to RFV FORM

ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED

1.

NAME:

ADDRESS:

TELEPHONE NO:

FAX NO:

NAME OF POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

NAME OF SECURITY OFFICER OR

SECONDARY POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

2.

NAME:

ADDRESS:

TELEPHONE NO:

FAX NO:

NAME OF POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

NAME OF SECURITY OFFICER OR

SECONDARY POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

(Continue as required)

<Platzhalter für Verweis auf die geltenden Datenschutzvorschriften und Link zu der vorgeschriebenen Auskunft an die betroffene Person, z. B. darüber, wie Artikel 13 der Datenschutz-Grundverordnung ([1]) umgesetzt wird.>

([1]) Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

ANNEX 2 to RFV FORM

PARTICULARS OF VISITOR(S)

1.

SURNAME:

FIRST NAMES *(as per passport)*:

DATE OF BIRTH *(dd/mm/yyyy)*: ____/____/____

PLACE OF BIRTH:

NATIONALITY:

SECURITY CLEARANCE LEVEL:

PP/ID NUMBER:

POSITION:

COMPANY/ORGANISATION:

2.

SURNAME:

FIRST NAMES *(as per passport)*:

DATE OF BIRTH *(dd/mm/yyyy)*: ____/____/____

PLACE OF BIRTH:

NATIONALITY:

SECURITY CLEARANCE LEVEL:

PP/ID NUMBER:

POSITION:

COMPANY/ORGANISATION:

(Continue as required)

<Platzhalter für Verweis auf die geltenden Datenschutzvorschriften und Link zu der vorgeschriebenen Auskunft an die betroffene Person, z. B. darüber, wie Artikel 13 der Datenschutz-Grundverordnung ([1]) umgesetzt wird.>

([1]) Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

Unteranhang D

AUSKUNFTSFORMULAR ZU SICHERHEITSBESCHEIDEN FÜR EINRICHTUNGEN

(MUSTER)

1. **Einleitung**

1.1. Nachstehend findet sich ein Muster eines Auskunftsformulars zu Sicherheitsbescheiden für Einrichtungen (im Folgenden „Auskunftsformular"), das dem raschen Informationsaustausch zwischen der nationalen Sicherheitsbehörde oder der beauftragten Sicherheitsbehörde, anderen zuständigen nationalen Sicherheitsbehörden und der Kommission (in ihrer Eigenschaft als öffentlicher Auftraggeber) im Hinblick auf Sicherheitsbescheide für Einrichtungen dient, die an als Verschlusssache eingestuften Ausschreibungen, Aufträgen oder Unteraufträgen beteiligt sind.

1.2. Das Auskunftsformular ist nur gültig, wenn es von der zuständigen nationalen Sicherheitsbehörde/beauftragten Sicherheitsbehörde oder einer anderen zuständigen Behörde abgestempelt wurde.

1.3. Das Auskunftsformular ist in einen Anfrage- und einen Antwortabschnitt gegliedert und kann für die oben genannten Zwecke oder für sonstige Zwecke, für die der Sicherheitsbescheid-Status einer bestimmten Einrichtung erforderlich ist, verwendet werden. Der Grund für das Auskunftsersuchen ist von der ersuchenden nationalen Sicherheitsbehörde/beauftragten Sicherheitsbehörde in Feld 7 des Anfrageabschnitts anzugeben.

1.4. Die Angaben im Auskunftsformular werden für gewöhnlich nicht als Verschlusssachen eingestuft. Dementsprechend sollte die Übermittlung eines Auskunftsformulars zwischen den jeweiligen nationalen Sicherheitsbehörden/beauftragten Sicherheitsbehörden/der Kommission vorzugsweise auf elektronischem Wege erfolgen.

1.5. Die nationalen Sicherheitsbehörden/beauftragten Sicherheitsbehörden sollten nach Möglichkeit innerhalb von zehn Arbeitstagen auf eine Anfrage mittels Auskunftsformular reagieren.

1.6. Sollten im Zusammenhang mit der Bescheinigung eines Sicherheitsbescheids Verschlusssachen übermittelt oder ein Auftrag vergeben werden, so ist die ausstellende nationale Sicherheitsbehörde/beauftragte Sicherheitsbehörde darüber zu unterrichten.

Verfahren und Anweisungen für die Verwendung des Auskunftsformulars zu Sicherheitsbescheiden für Einrichtungen

Diese ausführlichen Anweisungen sind für die nationale Sicherheitsbehörde/beauftragte Sicherheitsbehörde oder die Kommission in ihrer Eigenschaft als öffentlicher Auftraggeber bestimmt, die das Auskunftsformular ausfüllt. Das Formular sollte vorzugsweise in Großbuchstaben ausgefüllt werden.

KOPFZEILE	Der Antragsteller gibt die vollständige Bezeichnung der nationalen Sicherheitsbehörde/beauftragten Sicherheitsbehörde und die Länderbezeichnung an.
1. **ART DER ANFRAGE**	Der ersuchende öffentliche Auftraggeber kreuzt das entsprechende Kästchen für die Art der Anfrage mittels Auskunftsformular an. Bitte geben Sie das Niveau der beantragten Sicherheitsermächtigung an. Dabei sind die folgenden Abkürzungen zu verwenden: SECRET UE/EU SECRET = S-UE/EU-S CONFIDENTIEL UE/EU CONFIDENTIAL = C-UE/EU-C KIS = Kommunikations- und Informationssysteme für die Verarbeitung von Verschlusssachen

2. **ANGABEN ZUM ANTRAGSTELLER**	Die Felder 1 bis 6 bedürfen keiner weiteren Erklärung. In Feld 4 sollte der aus zwei Buchstaben bestehende Standard-Ländercode verwendet werden. Feld 5 ist fakultativ.
3. **GRUND DER ANFRAGE**	Bitte geben Sie den Grund für den Antrag, die Projektindikatoren sowie die Nummer des Auftrags oder der Ausschreibung an. Bitte geben Sie den Bedarf an Speicherkapazität, den KIS-Geheimhaltungsgrad usw. an. Ebenso sollten alle Fristen, Ablauf- und Vergabedaten, die sich auf die Ausstellung eines Sicherheitsbescheids für Unternehmen auswirken könnten, angegeben werden.
4. **ANTRAGSTELLENDE NATIONALE SICHERHEITSBEHÖRDE/BEAUFTRAGTE SICHERHEITSBEHÖRDE**	Geben Sie bitte den Namen des tatsächlichen Antragstellers (im Namen der nationalen Sicherheitsbehörde/beauftragten Sicherheitsbehörde) und das Datum des Antrags im Zahlenformat (TT/MM/JJJJ) an.
5. **ANTWORTABSCHNITT**	Felder 1-5: bitte zutreffende Felder ankreuzen bzw. ausfüllen. Feld 2: Ist die Ausstellung eines Sicherheitsbescheids für Einrichtungen im Gange, so sollte dem Antragsteller die erforderliche Bearbeitungsdauer mitgeteilt werden (sofern bekannt). Feld 6: a) Obwohl es je Land oder selbst je Einrichtung Unterschiede bei der Validierung gibt, wird empfohlen, das Ablaufdatum für den Sicherheitsbescheid anzugeben. b) Ist die Bescheinigung des Sicherheitsbescheids unbefristet, kann dieses Feld durchgestrichen werden. c) Entsprechend den jeweiligen nationalen Rechtsvorschriften obliegt es dem Antragsteller oder dem Auftragnehmer bzw. Unterauftragnehmer, eine Verlängerung des Sicherheitsbescheids zu beantragen.
6. **BEMERKUNGEN**	Hierunter können zusätzliche Angaben in Bezug auf den Sicherheitsbescheid, die Einrichtung oder die vorstehenden Punkte gemacht werden.
7. **AUSSTELLENDE NATIONALE SICHERHEITSBEHÖRDE/BEAUFTRAGTE SICHERHEITSBEHÖRDE**	Geben Sie bitte den Namen der ausstellenden Behörde (im Namen der nationalen Sicherheitsbehörde/beauftragten Sicherheitsbehörde) und das Datum der Antwort im Zahlenformat (TT/MM/JJJJ) an.

AUSKUNFTSFORMULAR ZU SICHERHEITSBESCHEIDEN FÜR EINRICHTUNGEN

(MUSTER)

Alle Felder müssen ausgefüllt werden. Das Formular ist über vernetzte Verwaltungskanäle oder Kanäle zwischen Behörden und internationalen Organisationen zu übermitteln.

ERSUCHEN UM BESCHEINIGUNG EINES SICHERHEITSBESCHEIDS FÜR EINRICHTUNGEN

AN: _____

(nationale Sicherheitsbehörde/beauftragte Sicherheitsbehörde, Länderbezeichnung)

Bitte füllen Sie die zutreffenden Antwortfelder aus:

[] Übermitteln Sie eine Bescheinigung eines Sicherheitsbescheids des Geheimhaltungsgrads [] S-UE/EU-S [] C-UE/EU-C

für die nachstehend aufgeführte Einrichtung

[] einschließlich des Schutzes von Verschlusssachen

[] einschließlich Kommunikations- und Informationssysteme (KIS) für die Verarbeitung von Verschlusssachen

[] Leiten Sie unmittelbar oder auf entsprechenden Antrag eines Auftragnehmers oder Unterauftragnehmers den Prozess zur Erlangung eines Sicherheitsbescheids für Einrichtungen bis einschließlich des Geheimhaltungsgrads ..... (Geheimhaltungsgrad ..... für den Schutz und Geheimhaltungsgrad ..... für das KIS) ein, sofern die Einrichtung über keine entsprechende Sicherheitsermächtigung verfügt.

Bestätigen Sie die Richtigkeit der Angaben zu der nachstehend aufgeführten Einrichtung und nehmen Sie gegebenenfalls Korrekturen/Ergänzungen vor.

1.	Vollständige Bezeichnung der Einrichtung:	Korrekturen/Ergänzungen:
.....		.....
2.	Vollständige Anschrift der Einrichtung:	
.....		.....
3.	Postanschrift (falls abweichend von 2.)	
.....		.....
4.	Postleitzahl/Stadt/Land	
.....		.....
5.	Name des Sicherheitsbeauftragten	
.....		.....
6.	Telefon/Fax/E-Mail des Sicherheitsbeauftragten	
.....		.....

7. Dieses Ersuchen ergeht aus folgenden Gründen (machen Sie bitte nähere Angaben zur vorvertraglichen Phase (Auswahl der Vorschläge), zum Vertrag oder Untervertrag, zum Programm/Projekt usw.):

.....

Antragsteller — nationale Sicherheitsbehörde/beauftragte Sicherheitsbehörde/Kommission als öffentlicher Auftraggeber: Bezeichnung: ..... Datum: (TT/MM/JJJJ) .....

ANTWORT (innerhalb von zehn Arbeitstagen)

Hiermit wird Folgendes bescheinigt:

1. [] Die oben genannte Einrichtung verfügt über einen Sicherheitsbescheid bis einschließlich des Geheimhaltungsgrads [] S-UE/EU-S

   [] C-UE/EU-C.

2. Die oben genannte Einrichtung ist in der Lage, Verschlusssachen zu schützen:

   [] ja, Geheimhaltungsgrad: ..... [] nein.

3. Die oben genannte Einrichtung verfügt über ein akkreditiertes/zugelassenes KIS:

   [] ja, Geheimhaltungsgrad: ..... [] nein.

4. [] Im Zusammenhang mit dem vorliegenden Ersuchen wurde der Prozess zur Erlangung eines Sicherheitsbescheids für Einrichtungen in die Wege geleitet. Sie werden benachrichtigt, wenn der Sicherheitsbescheid ausgestellt oder verweigert wurde.

5. [] Die oben genannte Einrichtung verfügt über keinen Sicherheitsbescheid.

6. Diese Bescheinigung ist befristet bis zum ..... (*TT/MM/JJJJ*) oder bis zu einem anderen, von der nationalen Sicherheitsbehörde/beauftragten Sicherheitsbehörde genannten Datum. Sollte die Zusicherung vor Ablauf ihrer Gültigkeitsdauer für ungültig erklärt werden oder sollten Änderungen bei den oben genannten Informationen eintreten, werden Sie darüber in Kenntnis gesetzt.

7. Bemerkungen:

   .....

Ausstellende nationale Sicherheitsbehörde/beauftragte Sicherheitsbehörde Bezeichnung: ..... Datum: (TT/MM/JJJJ) .....

<Platzhalter für Verweis auf die geltenden Datenschutzvorschriften und Link zu der vorgeschriebenen Auskunft an die betroffene Person, z. B. darüber, wie Artikel 13 der Datenschutz-Grundverordnung ([2]) umgesetzt wird.>

([2]) Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

Unteranhang E

Mindestanforderungen für den Schutz elektronischer EU-VS des Geheimhaltungsgrads RESTREINT UE/EU RESTRICTED, die im KIS des Auftragnehmers bearbeitet werden

Allgemeines

1. Der Auftragnehmer hat dafür zu sorgen, dass der Schutz von Verschlusssachen des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“ den in dieser Sicherheitsklausel festgelegten Mindestsicherheitsanforderungen und etwaigen sonstigen zusätzlichen Anforderungen des öffentlichen Auftraggebers oder gegebenenfalls der nationalen Sicherheitsbehörde oder der beauftragten Sicherheitsbehörde entspricht.

2. Der Auftragnehmer hat die in diesem Dokument genannten Sicherheitsanforderungen umzusetzen.

3. Für die Zwecke dieses Dokuments umfasst ein Kommunikations- und Informationssystem (KIS) alle Geräte und Anlagen, die für die Bearbeitung, Aufbewahrung bzw. Speicherung und Übermittlung von EU-VS eingesetzt werden, so z. B. Workstations, Drucker, Kopiergeräte, Faxgeräte, Server, Netzwerk- und Kommunikationscontroller, Laptops, Notebooks, Tablet-Computer, Smartphones und Wechseldatenspeicher wie USB-Datenträger, CDs, SD-Karten usw.

4. Spezielle Ausrüstung wie kryptografische Produkte muss im Einklang mit ihren speziellen sicherheitsbezogenen Betriebsverfahren geschützt werden.

5. Auftragnehmer müssen eine Struktur für die Sicherheitsverwaltung des KIS einrichten, mit den Verschlusssachen des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“ bearbeitet werden, und einen für die betreffende Einrichtung verantwortlichen Sicherheitsbeauftragten ernennen.

6. Der Einsatz von privaten IT (Hardware, Software oder Dienstleistungen) der Mitarbeiter des Auftragnehmers für die Aufbewahrung bzw. Speicherung oder die Verarbeitung von Verschlusssachen des Geheimhaltungsgrads RESTREINT UE/EU RESTRICTED ist nicht zulässig.

7. Die Akkreditierung eines KIS des Auftragnehmers, mit dem Verschlusssachen des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“ bearbeitet werden, muss von der Sicherheitsakkreditierungsstelle des betreffenden Mitgliedstaats genehmigt oder nach Maßgabe der nationalen Rechtsvorschriften dem Sicherheitsbeauftragten des Auftragnehmers übertragen werden.

8. Nur Verschlusssachen des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“, die unter Verwendung zugelassener kryptografischer Produkte verschlüsselt werden, dürfen (leitungsgebunden oder drahtlos) wie alle anderen nach dem Vertrag nicht als Verschlusssache eingestuften Informationen bearbeitet, gespeichert oder übermittelt werden. Diese kryptografischen Produkte müssen von der EU oder einem Mitgliedstaat zugelassen werden.

9. Externe Einrichtungen, die an Wartungs- und Reparaturarbeiten beteiligt sind, müssen vertraglich dazu verpflichtet werden, die in diesem Dokument niedergelegten geltenden Bestimmungen für die Bearbeitung von Verschlusssachen des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“ einzuhalten.

10. Auf Verlangen des öffentlichen Auftraggebers oder der zuständigen nationalen Sicherheitsbehörde/beauftragten Sicherheitsbehörde/Sicherheitsakkreditierungsstelle muss der Auftragnehmer den Nachweis für die Einhaltung der Sicherheitsklausel erbringen. Wird zudem eine Prüfung und Kontrolle der Prozesse und Einrichtungen des Auftragnehmers beantragt, um die Einhaltung dieser Anforderungen zu gewährleisten, so gestattet der Auftragnehmer Vertretern des öffentlichen Auftraggebers, der nationalen Sicherheitsbehörde/beauftragten Sicherheitsbehörde/Sicherheitsakkreditierungsstelle oder der zuständigen EU-Sicherheitsbehörde, eine entsprechende Prüfung und Kontrolle vorzunehmen.

Materieller Geheimschutz

11. Bereiche, in denen KIS zur Darstellung, Speicherung, Verarbeitung oder Übermittlung von Verschlusssachen des Geheimhaltungsgrads RESTREINT UE/EU RESTRICTED verwendet werden, oder Bereiche mit Servern, Netzmanagementsystemen, Netz- und Kommunikationscontrollern für solche KIS sollten als getrennte und kontrollierte Bereiche mit einem geeigneten Zugangskontrollsystem eingerichtet werden. Der Zugang zu diesen getrennten und kontrollierten Bereichen sollte auf Personen mit Einzelgenehmigung beschränkt werden. Unbeschadet der Randnummer 8 muss Ausrüstung nach Randnummer 3 in solchen getrennten und kontrollierten Bereichen aufbewahrt werden.

12. Es müssen Sicherheitsmechanismen und/oder -verfahren eingerichtet werden, um die Einführung oder Verbindung von Computer-Wechselspeichermedien (wie USB-Datenträgern, Massenspeichervorrichtungen oder CD-RW) in bzw. mit Komponenten im KIS zu regeln.

Zugang zu KIS

13. Der Zugang zum KIS eines Auftragnehmers, mit dem EU-VS bearbeitet werden, ist auf der Grundlage strikter Notwendigkeit und der Ermächtigung der Mitarbeiter zulässig.

14. Für alle KIS müssen aktualisierte Listen der zugelassenen Nutzer vorliegen. Alle Nutzer müssen zu Beginn jeder Verarbeitungssitzung authentifiziert werden.

15. Passwörter, die Teil der meisten Maßnahmen zur Identifizierung und Authentifizierung sind, müssen mindestens neun Zeichen enthalten, darunter Ziffern, Sonderzeichen und alphabetische Zeichen. Die Passwörter müssen mindestens alle 180 Tage geändert werden. Sie müssen umgehend geändert werden, wenn sie kompromittiert oder an Unbefugte weitergegeben wurden oder wenn Grund zur Annahme einer solchen Kompromittierung oder Weitergabe besteht.

16. Alle KIS müssen über interne Zugangskontrollen verfügen um zu verhindern, dass Unbefugte auf Verschlusssachen des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“ zugreifen und diese Verschlusssachen oder System- und Sicherheitskontrollen ändern. Die Nutzer müssen automatisch abgemeldet werden, wenn ihre Endgeräte über einen bestimmten Zeitraum inaktiv waren, oder das KIS muss nach 15 Minuten der Inaktivität einen passwortgeschützten Bildschirm aktivieren.

17. Jeder Nutzer des KIS erhält ein individuelles Nutzerkonto und eine individuelle Nutzer-ID. Die Nutzerkonten müssen automatisch gesperrt werden, sobald mindestens fünf aufeinander folgende Anmeldeversuche fehlgeschlagen sind.

18. Alle Nutzer des KIS müssen über ihre Verantwortlichkeiten und die Verfahren zum Schutz von als „RESTREINT UE/EU RESTRICTED“ eingestuften Verschlusssachen im KIS belehrt werden. Die Verantwortlichkeiten und die einzuhaltenden Verfahren müssen dokumentiert sein und von den Nutzern schriftlich anerkannt werden.

19. Die sicherheitsbezogenen Betriebsverfahren müssen für die Nutzer und Administratoren verfügbar sein und Beschreibungen der Sicherheitsfunktionen sowie eine dazugehörige Liste der Aufgaben, Anweisungen und Pläne enthalten.

Protokollierung, Prüfung und Reaktion auf Sicherheitsvorfälle

20. Jeder Zugriff auf das KIS muss protokolliert werden.

21. Die folgenden Ereignisse müssen aufgezeichnet werden:

    a) alle — erfolgreichen und fehlgeschlagenen — Anmeldungsversuche,

    b) Abmeldungen (ggf. auch wegen Zeitüberschreitung),

    c) Erstellung, Löschung oder Änderung von Zugangsrechten und Berechtigungen,

    d) Erstellung, Löschung oder Änderung von Passwörtern.

22. Zu allen oben aufgeführten Ereignissen sind mindestens folgende Angaben zu machen:

    a) Art des Ereignisses;

    b) Nutzer-ID;

    c) Datum und Uhrzeit;

    d) Geräte-ID.

23. Die Protokolle sollten einem Sicherheitsbeauftragten bei der Untersuchung möglicher Sicherheitsvorfälle helfen. Sie können auch zur Unterstützung etwaiger rechtlicher Ermittlungen im Falle eines Sicherheitsvorfalls verwendet werden. Alle Sicherheitsaufzeichnungen sollten regelmäßig überprüft werden, um mögliche Sicherheitsvorfälle zu ermitteln. Die Protokolle sind vor unautorisierter Löschung oder Änderung zu schützen.

24. Der Auftragnehmer muss über eine Strategie für die Reaktion auf Sicherheitsvorfälle verfügen. Nutzer und Administratoren müssen geschult werden, wie auf Vorfälle zu reagieren ist, wie sie zu melden sind und was im Notfall zu tun ist.

25. Die tatsächliche oder mutmaßliche Kompromittierung von Verschlusssachen des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“ ist dem öffentlichen Auftraggeber zu melden. Die Meldung muss eine Beschreibung der betreffenden Informationen und der Umstände der tatsächlichen oder mutmaßlichen Kompromittierung enthalten. Alle Nutzer des KIS müssen darüber belehrt werden, wie ein tatsächlicher oder mutmaßlicher Sicherheitsvorfall dem Sicherheitsbeauftragten zu melden ist.

Vernetzung und Zusammenschaltung

26. Wird ein KIS eines Auftragnehmers, mit dem Verschlusssachen des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“ bearbeitet werden, mit einem nicht akkreditierten KIS zusammengeschaltet, erhöht sich dadurch die Bedrohung sowohl für die Sicherheit des KIS als auch für die Sicherheit der mit diesem KIS bearbeiteten Verschlusssachen erheblich. Dies gilt auch für das Internet und andere öffentliche oder private KIS wie etwa andere KIS, die sich im Eigentum des Auftragnehmers oder Subunternehmers befinden. In diesem Fall muss der Auftragnehmer eine Risikobewertung durchführen, um die zusätzlichen Sicherheitsanforderungen zu ermitteln, die im Rahmen der Sicherheitsakkreditierung umzusetzen sind. Der Auftragnehmer legt dem öffentlichen Auftraggeber und, sofern dies aufgrund der nationalen Rechtsvorschriften vorgeschrieben ist, der zuständigen Sicherheitsakkreditierungsstelle eine Konformitätserklärung vor, mit der bescheinigt wird, dass das KIS sowie damit verbundene Zusammenschaltungen des Auftragnehmers für die Bearbeitung von EU-VS des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“ akkreditiert wurden.

27. Der Fernzugang von anderen Systemen zu LAN-Diensten (z. B. Fernzugang zu E-Mail und System-Fernunterstützung) ist verboten, sofern nicht besondere Sicherheitsmaßnahmen vorgenommen und vom öffentlichen Auftraggeber gebilligt und — wenn nationale Rechtsvorschriften dies vorschreiben — von der zuständigen Sicherheitsakkreditierungsstelle zugelassen werden.

Konfigurationsmanagement

28. Eine ausführliche Hardware- und Softwarekonfiguration, die aus den Akkreditierungs-/Zulassungsunterlagen (einschließlich der System- und Netzdiagramme) hervorgeht, muss verfügbar sein und regelmäßig gewartet werden.

29. Der Sicherheitsbeauftragte des Auftragnehmers führt Konfigurationskontrollen an der Hardware und Software durch, um sicherzustellen, dass keine unzulässige Hardware oder Software installiert wurde.

30. Änderungen an der Konfiguration des KIS des Auftragnehmers müssen auf ihre Sicherheitsauswirkungen hin überprüft und vom Sicherheitsbeauftragten sowie — falls nationale Rechtsvorschriften dies vorschreiben — von der Sicherheitsakkreditierungsstelle genehmigt werden.

31. Das System muss mindestens einmal vierteljährlich auf Sicherheitslücken gescannt werden. Software zur Erkennung von Schadprogrammen muss installiert sein und stets aktualisiert werden. Nach Möglichkeit sollte diese Software eine nationale oder anerkannte internationale Zulassung haben; andernfalls sollte sie ein allgemein anerkannter Industriestandard sein.

32. Der Auftragnehmer muss einen Betriebskontinuitätsplan erstellen. Es müssen Backup-Verfahren eingerichtet werden, die Folgendem Rechnung tragen:

    a) Häufigkeit von Backups;

    b) Aufbewahrung am Standort (Feuerschutzbehälter) oder außerhalb des Standorts;

    c) Kontrolle des autorisierten Zugangs zu Backup-Kopien.

Säuberung und Vernichtung

33. KIS oder Datenträger, die zu irgendeinem Zeitpunkt Verschlusssachen des Geheimhaltungsgrads RESTREINT UE/EU RESTRICTED enthielten, müssen vor ihrer Entsorgung komplett wie folgt gesäubert werden:

    a) Flash-Speicher (z. B. USB-Datenträger, SD-Karten, Solid-State-Drives (SSD), Hybridfestplatten) müssen mindestens dreimal überschrieben und anschließend überprüft werden, damit sichergestellt ist, dass der Originalinhalt nicht wiederhergestellt werden kann, oder die Speicherinhalte müssen mit einer zugelassenen Datenlöschsoftware gelöscht werden.

    b) Magnetische Medien (z. B. Festplatten) müssen überschrieben oder entmagnetisiert werden.

c) Optische Medien (z. B. CDs und DVDs) müssen geschreddert oder zersetzt werden.

d) Im Falle sonstiger Speichermedien sollte der öffentliche Auftraggeber oder gegebenenfalls die nationale Sicherheitsbehörde/beauftragte Sicherheitsbehörde/Sicherheitsakkreditierungsstelle hinsichtlich der zu erfüllenden Sicherheitsanforderungen zurate gezogen werden.

34. Datenträger müssen von Verschlusssachen des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“ gesäubert werden, bevor sie einer Einrichtung (z. B. zur Durchführung von Wartungsarbeiten) übergeben werden, die über keine Zugangsermächtigung für Verschlusssachen des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“ verfügt.

ANHANG IV

Sicherheitsbescheide und Sicherheitsüberprüfungen für Auftragnehmer, die Verschlusssachen des Geheimhaltungsgrads RESTREINT UE/EU RESTRICTED bearbeiten, und nationale Sicherheitsbehörden/beauftragte Sicherheitsbehörden, die eine Mitteilung von als Verschlusssache des Geheimhaltungsgrads RESTREINT UE/EU RESTRICTED eingestuften Aufträgen verlangen [1]

Mitgliedstaat	Sicherheitsbescheid für Einrichtungen		Mitteilung von Aufträgen oder Unteraufträgen, die Verschlusssachen des Geheimhaltungsgrads R-UE/EU-R umfassen, an nationale Sicherheitsbehörden/beauftragte Sicherheitsbehörden		Sicherheitsüberprüfung von Personal	
	JA	NEIN	JA	NEIN	JA	NEIN
Belgien		X		X		X
Bulgarien		X		X		X
Tschechien		X		X		X
Dänemark	X		X		X	
Deutschland		X		X		X
Estland	X		X			X
Irland		X		X		X
Griechenland	X			X	X	
Spanien		X	X			X
Frankreich		X		X		X
Kroatien		X	X			X
Italien		X	X			X
Zypern		X	X			X
Lettland		X		X		X

[1] Diese nationalen Anforderungen in Bezug auf Sicherheitsbescheide und Sicherheitsüberprüfungen sowie auf Mitteilungen betreffend Verträge, die Verschlusssachen des Geheimhaltungsgrads RESTREINT UE/EU RESTRICTED umfassen, dürfen anderen Mitgliedstaaten oder Auftragnehmer, die deren Hoheitsgewalt unterstehen, keine zusätzlichen Verpflichtungen auferlegen.
Hinweis: Verträge, die Verschlusssachen der Geheimhaltungsgrade CONFIDENTIEL UE/EU CONFIDENTIAL und SECRET UE/EU SECRET umfassen, sind in jedem Fall mitzuteilen.

Mitgliedstaat	Sicherheitsbescheid für Einrichtungen		Mitteilung von Aufträgen oder Unteraufträgen, die Verschlusssachen des Geheimhaltungsgrads R-UE/EU-R umfassen, an nationale Sicherheitsbehörden/beauftragte Sicherheitsbehörden		Sicherheitsüberprüfung von Personal	
	JA	NEIN	JA	NEIN	JA	NEIN
Litauen	X		X			X
Luxemburg	X		X		X	
Ungarn		X		X		X
Malta		X		X		X
Niederlande	X (nur für verteidigungsbezogene Aufträge)		X (nur für verteidigungsbezogene Aufträge)			X
Österreich		X		X		X
Polen		X		X		X
Portugal		X		X		X
Rumänien		X		X		X
Slowenien	X		X			X
Slowakei	X		X			X
Finnland		X		X		X
Schweden	X (nur für verteidigungsbezogene Aufträge)		X (nur für verteidigungsbezogene Aufträge)		X (nur für verteidigungsbezogene Aufträge)	
Vereinigtes Königreich		X		X		X

ANHANG V

LISTE DER DIENSTSTELLEN DER NATIONALEN SICHERHEITSBEHÖRDEN/BEAUFTRAGTEN SICHERHEITSBEHÖRDEN, DIE FÜR VERFAHREN IM ZUSAMMENHANG MIT DEM GEHEIMSCHUTZ IN DER WIRTSCHAFT ZUSTÄNDIG SIND

BELGIEN

National Security Authority
FPS Foreign Affairs
Rue des Petits Carmes 15
1000 Brussels
Tel.: +32 25014542 (Secretariat)
Fax +32 25014596
E-Mail: nvo-ans@diplobel.fed.be

BULGARIEN

1. State Commission on Information Security — National Security Authority
   4 Kozloduy Street
   1202 Sofia
   Tel.: +359 29835775
   Fax +359 29873750
   E-Mail: dksi@government.bg

2. Defence Information Service at the Ministry of Defence (security service)
   3 Dyakon Ignatiy Street
   1092 Sofia
   Tel.: +359 29227002
   Fax +359 29885211
   E-Mail: office@iksbg.org

3. State Intelligence Agency (security service)
   12 Hajdushka Polyana Street
   1612 Sofia
   Tel.: +359 29813221
   Fax +359 29862706
   E-Mail: office@dar.bg

4. State Agency for Technical Operations (security service)
   29 Shesti Septemvri Street
   1000 Sofia
   Tel.: +359 29824971
   Fax +359 29461339
   E-Mail: dato@dato.bg

   (Den oben aufgeführten zuständigen Behörden obliegt die Durchführung der Überprüfungsverfahren im Rahmen der Ausstellung von Sicherheitsbescheiden für juristische Personen, die einen als Verschlusssache eingestuften Vertrag abschließen wollen, und von Erklärungen über die Sicherheitsüberprüfung für Einzelpersonen, die einen als Verschlusssache eingestuften Vertrag für die Bedürfnisse dieser Behörden ausführen.)

5. State Agency National Security (security service)
   45 Cherni Vrah Blvd.
   1407 Sofia
   Tel.: +359 28147109
   Fax +359 29632188, +359 28147441
   E-Mail: dans@dans.bg

   (Oben stehender Sicherheitsdienst führt die Überprüfungsverfahren im Rahmen der Ausstellung von Sicherheitsbescheiden und Erklärungen über die Sicherheitsüberprüfung für alle sonstigen juristischen Personen bzw. Einzelpersonen im Land durch, die einen als Verschlusssache eingestuften Vertrag abschließen wollen bzw. ausführen.)

TSCHECHIEN

National Security Authority
Industrial Security Department
PO BOX 49
150 06 Praha 56
Tel.: +420 257283129
E-Mail: sbr@nbu.cz

DÄNEMARK

1. Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
2860 Søborg
Tel.: +45 33148888
Fax +45 33430190

2. Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)
Kastellet 30
2100 Copenhagen Ø
Tel.: +45 33325566
Fax +45 33931320

DEUTSCHLAND

1. Für Angelegenheiten in Bezug auf Strategien für den Geheimschutz in der Wirtschaft, Sicherheitsbescheide für Einrichtungen, Beförderungspläne (außer Kryptomaterial/Betriebs- und Geschäftsgeheimnissen):
Bundesministerium für Wirtschaft und Energie
Geheimschutz in der Wirtschaft — ZB3
Villemombler Str. 76
53123 Bonn
Tel.: +49 228996154028
Fax +49 228996152676
E-Mail: dsagermany-zb3@bmwi.bund.de (office email address)

2. Für Standardbesuchsanträge von/an deutsche(n) Unternehmen:
Bundesministerium für Wirtschaft und Energie
Geheimschutz in der Wirtschaft — ZB2
Villemombler Str. 76
53123 Bonn
Tel.: +49 228996152401
Fax +49 228996152603
E-Mail: zb2-international@bmwi.bund.de (office email address)

3. Beförderungspläne für Kryptomaterial:
Bundesamt für Sicherheit in der Informationstechnik (BSI)
National Distribution Agency/NDA-EU DEU
Mainzer Str. 84
53179 Bonn
Tel.: +49 2289995826052
Fax +49 228991095826052
E-Mail: NDAEU@bsi.bund.de

ESTLAND

National Security Authority Department
Estonian Foreign Intelligence Service
Rahumäe tee 4B
11316 Tallinn
Tel.: +372 6939211
Fax +372 6935001
E-Mail: nsa@fis.gov.ee

IRLAND

National Security Authority Ireland
Department of Foreign Affairs and Trade
76-78 Harcourt Street
Dublin 2
D02 DX45
Tel.: +353 14082724
E-Mail: nsa@dfa.ie

GRIECHENLAND

Hellenic National Defence General Staff
E' Division (Security INTEL, CI BRANCH)
E3 Directorate
Industrial Security Office
227-231 Mesogeion Avenue
15561 Holargos, Athens
Tel.: +30 2106572022, +30 2106572178
Fax +30 2106527612
E-Mail: daa.industrial@hndgs.mil.gr

SPANIEN

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Calle Argentona 30
28023 Madrid
Tel.: +34 913725000
Fax +34 913725808
E-Mail: nsa-sp@areatec.com
Bei Fragen, die die Sicherheitsüberprüfung von Personal betreffen: asip@areatec.com
In Bezug auf Beförderungspläne und internationale Besuche: sp-ivtco@areatec.com

FRANKREICH

National Security Authority (NSA) (für die Politik und Umsetzung in anderen Bereichen als der Verteidigungsindustrie)
Secrétariat général de la défense et de la sécurité nationale
Sous-direction Protection du secret (SGDSN/PSD)
51 boulevard de la Tour-Maubourg
75700 Paris 07 SP
Tel.: +33 171758193
Fax +33 171758200
E-Mail: ANSFrance@sgdsn.gouv.fr

Designated Security Authority (für die Umsetzung in der Verteidigungsindustrie)
Direction Générale de l'Armement
Service de la Sécurité de Défense et des systèmes d'Information (DGA/SSDI)
60 boulevard du général Martial Valin
CS 21623
75509 Paris CEDEX 15
Tel.: +33 988670421
E-Mail: für Formulare und ausgehende Besuchsanträge: dga-ssdi.ai.fct@intradef.gouv.fr
für eingehende Besuchsanträge: dga-ssdi.visit.fct@intradef.gouv.fr

KROATIEN

Office of the National Security Council
Croatian NSA
Jurjevska 34
10000 Zagreb
Tel.: +385 14681222
Fax +385 14686049
E-Mail: NSACroatia@uvns.hr

ITALIEN

Presidenza del Consiglio dei Ministri
D.I.S. — U.C.Se.
Via di Santa Susanna 15
00187 Roma
Tel.: +39 0661174266
Fax +39 064885273

ZYPERN

ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Λεωφόρος Στροβόλου, 172-174
Στρόβολος, 2048, Λευκωσία
Τηλέφωνα: +357 22807569, +357 22807764
Τηλεομοιότυπο: +357 22302351
E-Mail: cynsa@mod.gov.cy

Ministry of Defence
National Security Authority (NSA)
172-174, Strovolos Avenue
2048 Strovolos, Nicosia
Tel.: +357 22807569, +357 22807764
Fax +357 22302351
E-Mail: cynsa@mod.gov.cy

LETTLAND

National Security Authority
Constitution Protection Bureau of the Republic of Latvia
P.O. Box 286
Riga LV-1001
Tel.: +371 67025418, +371 67025463
Fax +371 67025454
E-Mail: ndi@sab.gov.lt, ndi@zd.gov.lv

LITAUEN

Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(The Commission for Secrets Protection Coordination of the Republic of Lithuania)
National Security Authority
Gedimino 40/1
LT-01110 Vilnius
Tel.: +370 70666703, +370 70666701
Fax +370 70666700
E-Mail: nsa@vsd.lt

LUXEMBURG

Autorité Nationale de Sécurité
207, route d'Esch
L-1471 Luxembourg
Tel.: +352 24782210
E-Mail: ans@me.etat.lu

UNGARN

National Security Authority of Hungary
H-1399 Budapest P.O. Box 710/50
H-1024 Budapest, Szilágyi Erzsébet fasor 11/B
Tel.: +36 13911862
Fax +36 13911889
E-Mail: nbf@nbf.hu

MALTA

Director of Standardisation
Designated Security Authority for Industrial Security
Standards & Metrology Institute
Malta Competition and Consumer Affairs Authority
Mizzi House
National Road
Blata I-Bajda HMR9010
Tel.: +356 23952000
Fax +356 21242406
E-Mail: certification@mccaa.org.mt

NIEDERLANDE

1. Ministry of the Interior and Kingdom Relations
PO Box 20010
2500 EA The Hague
Tel.: +31 703204400
Fax +31 703200733
E-Mail: nsa-nl-industry@minbzk.nl

2. Ministry of Defence
Industrial Security Department
PO Box 20701
2500 ES The Hague
Tel.: +31 704419407
Fax +31 703459189
E-Mail: indussec@mindef.nl

ÖSTERREICH

1. Bundeskanzleramt der Republik Österreich
Abteilung I/12, Büro der Informationssicherheitskommission
Ballhausplatz 2
1014 Vienna
Tel.: +43 153115202594
E-Mail: isk@bka.gv.at

2. Beauftragte Sicherheitsbehörde (DSA) im militärischen Bereich:
BMLVS/Abwehramt
Postfach 2000
1030 Wien
E-Mail: abwa@bmlvs.gv.at

POLEN

Internal Security Agency
Department for the Protection of Classified Information
Rakowiecka 2A
00-993 Warsaw
Tel.: +48 225857944
Fax +48 225857443
E-Mail: nsa@abw.gov.pl

PORTUGAL

Gabinete Nacional de Segurança
Serviço de Segurança Industrial
Rua da Junqueira nº 69
1300-342 Lisbon
Tel.: +351 213031710
Fax +351 213031711
E-Mail: sind@gns.gov.pt, franco@gns.gov.pt

RUMÄNIEN

Oficiul Registrului Național al Informațiilor Secrete de Stat — ORNISS
Romanian NSA — ORNISS — National Registry Office for Classified Information
4th Mures Street
012275 Bucharest
Tel.: +40 212075115
Fax +40 212245830
E-Mail: relatii.publice@orniss.ro, nsa.romania@nsa.ro

SLOWENIEN

Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
1000 Ljubljana
Tel.: +386 14781390
Fax +386 14781399
E-Mail: gp.uvtp@gov.si

SLOWAKEI

Národný bezpečnostný úrad
(National Security Authority)
Security Clearance Department
Budatínska 30
851 06 Bratislava
Tel.: +421 268691111
Fax +421 268691700
E-Mail: podatelna@nbu.gov.sk

FINNLAND

National Security Authority
Ministry for Foreign Affairs
P.O. Box 453
FI-00023 Government
E-Mail: NSA@formin.fi

SCHWEDEN

1. National Security Authority
   Utrikesdepartementet (Ministry for Foreign Affairs)
   UD SÄK/NSA
   SE-103 39 Stockholm
   Tel.: +46 84051000
   Fax +46 87231176
   E-Mail: ud-nsa@gov.se

2. DSA
   Försvarets Materielverk (Swedish Defence Materiel Administration)
   FMV Säkerhetsskydd
   SE-115 88 Stockholm
   Tel.: +46 87824000
   Fax +46 87826900
   E-Mail: security@fmv.se

VEREINIGTES KÖNIGREICH

UK National Security Authority
Room 335, 3rd Floor
70 Whitehall
London
SW1A 2AS
Tel.: +44 2072765497, +44 2072765645
E-Mail: UK-NSA@cabinet-office.x.gsi.gov.uk