DECISÃO (UE, Euratom) 2021/259 DA COMISSÃO

de 10 de fevereiro de 2021

que estabelece regras de execução relativas à segurança industrial no que respeita às subvenções classificadas

A COMISSÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente o artigo 249.º,

Tendo em conta o Tratado que institui a Comunidade Europeia da Energia Atómica, nomeadamente o artigo 106.º,

Tendo em conta o Regulamento (UE, Euratom) 2018/1046 do Parlamento Europeu e do Conselho, de 18 de julho de 2018, relativo às disposições financeiras aplicáveis ao orçamento geral da União, que altera os Regulamentos (UE) n.º 1296/2013, (UE) n.º 1301/2013, (UE) n.º 1303/2013, (UE) n.º 1304/2013, (UE) n.º 1309/2013, (UE) n.º 1316/2013, (UE) n.º 223/2014 e (UE) n.º 283/2014, e a Decisão n.º 541/2014/UE, e revoga o Regulamento (UE, Euratom) n.º 966/2012 ([1]),

Tendo em conta a Decisão (UE, Euratom) 2015/443 da Comissão, de 13 de março de 2015, relativa à segurança na Comissão ([2]),

Tendo em conta a Decisão (UE, Euratom) 2015/444 da Comissão, de 13 de março de 2015, relativa às regras de segurança aplicáveis à proteção das informações classificadas da UE ([3]),

Tendo em conta a Decisão (UE, Euratom) 2017/46 da Comissão, de 10 de janeiro de 2017, relativa à segurança dos sistemas de comunicação e de informação na Comissão Europeia ([4]),

Após consulta do grupo de peritos de segurança da Comissão, em conformidade com o artigo 41.º, n.º 5, da Decisão (UE, Euratom) 2015/444,

Considerando o seguinte:

(1) Os artigos 41.º, 42.º, 47.º e 48.º da Decisão (UE, Euratom) 2015/444 preveem o estabelecimento de disposições mais pormenorizadas para complementar e apoiar o capítulo 6 da referida decisão na aplicação das regras em matéria de segurança industrial, que regem questões como a concessão de convenções de subvenção classificadas, a credenciação de segurança da empresa, a credenciação de segurança do pessoal, as visitas e a transmissão e o transporte de informações classificadas da União Europeia (ICUE).

(2) A Decisão (UE, Euratom) 2015/444 estabelece que as convenções de subvenção classificadas devem ser executadas em estreita cooperação com a autoridade nacional de segurança, a autoridade de segurança designada ou qualquer outra autoridade competente do Estado-Membro em causa. Os Estados-Membros acordaram em garantir que qualquer entidade sob a sua jurisdição que possa receber ou gerar informações classificadas originárias da Comissão possua credenciação de segurança ao nível adequado e seja capaz de providenciar uma proteção adequada equivalente à estabelecida nas regras de segurança do Conselho da União Europeia aplicáveis à proteção das informações classificadas da UE que ostentem uma marca de classificação correspondente, como estabelecido no Acordo entre os Estados-Membros da União Europeia, reunidos no Conselho, sobre a proteção das informações classificadas trocadas no interesse da União Europeia (2011/C 202/05) ([5]).

([1]) JO L 193 de 30.7.2018, p. 1.
([2]) JO L 72 de 17.3.2015, p. 41.
([3]) JO L 72 de 17.3.2015, p. 53.
([4]) JO L 6 de 11.1.2017, p. 40.
([5]) JO C 202 de 8.7.2011, p. 13.

(3) O Conselho, a Comissão e a Alta Representante da União para os Negócios Estrangeiros e a Política de Segurança acordaram em assegurar a máxima coerência na aplicação das regras de segurança relativas à proteção das ICUE, tendo em conta as suas necessidades institucionais e organizacionais específicas, em conformidade com as declarações anexadas à ata da sessão do Conselho em que foi adotada a Decisão 2013/488/UE do Conselho ([6]) relativa às regras de segurança aplicáveis à proteção das informações classificadas da UE.

(4) Por conseguinte, as regras de execução da Comissão em matéria de segurança industrial no que diz respeito às subvenções classificadas devem também assegurar a máxima coerência e ter em conta as orientações sobre segurança industrial aprovadas pelo Comité de Segurança do Conselho em 13 de dezembro de 2016.

(5) Em 4 de maio de 2016, a Comissão adotou uma decisão ([7]) que habilita o membro da Comissão responsável pelas questões de segurança a adotar, em nome da Comissão e sob a sua responsabilidade, as regras de execução previstas no artigo 60.º da Decisão (UE, Euratom) 2015/444,

ADOTOU A PRESENTE DECISÃO:

CAPÍTULO 1

DISPOSIÇÕES GERAIS

Artigo 1.

Objeto e âmbito de aplicação

1. A presente decisão estabelece regras de execução em matéria de segurança industrial no que respeita às subvenções classificadas na aceção da Decisão (UE, Euratom) 2015/444, nomeadamente o respetivo capítulo 6.

2. A presente decisão estabelece requisitos específicos para assegurar a proteção das informações classificadas da UE (ICUE) aquando da publicação de convites à apresentação de propostas, da concessão de subvenções e da execução das convenções de subvenção classificadas celebradas pela Comissão Europeia.

3. A presente decisão aplica-se às subvenções que impliquem informações classificadas nos seguintes níveis:

a) RESTREINT UE/EU RESTRICTED;

b) CONFIDENTIEL UE/EU CONFIDENTIAL;

c) SECRET UE/EU SECRET.

4. A presente decisão é aplicável sem prejuízo das regras específicas estabelecidas noutros atos jurídicos, como as relativas ao Programa Europeu de Desenvolvimento Industrial no domínio da Defesa.

Artigo 2.

Responsabilidades no seio da Comissão

1. No âmbito das suas responsabilidades, o gestor orçamental da autoridade que concede a subvenção a que se refere o Regulamento (UE, Euratom) 2018/1046 do Parlamento Europeu e do Conselho assegura que a subvenção classificada cumpre o disposto na Decisão (UE, Euratom) 2015/444 e nas suas normas de execução.

([6]) Decisão 2013/488/UE do Conselho, de 23 de setembro de 2013, relativa às regras de segurança aplicáveis à proteção das informações classificadas da UE (JO L 274 de 15.10.2013, p. 1).

([7]) Decisão da Comissão de 4.5.2016 relativa a uma habilitação em matéria de segurança [C(2016) 2797 final].

2. Para o efeito, o gestor orçamental competente solicita, em todas as fases, o parecer da autoridade de segurança da Comissão sobre questões relacionadas com os elementos de segurança da convenção de subvenção classificada, ou do programa ou projeto classificados, e informa o responsável local de segurança sobre as convenções de subvenção classificadas celebradas. A decisão sobre o nível de classificação de assuntos específicos incumbe à autoridade que concede a subvenção e deve ser tomada levando em devida conta o Guia da Classificação de Segurança.

3. Quando forem aplicadas as instruções de segurança relativas a um programa ou um projeto a que se refere o artigo 5.º, n.º 3, a autoridade que concede a subvenção e a autoridade de segurança da Comissão assumem as responsabilidades que lhes são cometidas nessas instruções.

4. Respeitando os requisitos das presentes regras de execução, a autoridade de segurança da Comissão coopera estreitamente com as autoridades nacionais de segurança (ANS) e as autoridades de segurança designadas (ASD) dos Estados-Membros em causa, nomeadamente no que diz respeito à credenciação de segurança da empresa (CSE) e à credenciação de segurança do pessoal (CSP), aos procedimentos de visita e aos planos de transporte.

5. Quando a gestão das subvenções estiver a cargo de agências de execução ou de outros organismos de financiamento da UE e as regras específicas estabelecidas noutros atos jurídicos referidos no artigo 1.º, n.º 4 não se aplicarem:

a) O serviço delegante da Comissão exerce os direitos relativos à entidade de origem das ICUE geradas no contexto das subvenções, se as modalidades de delegação assim o previrem;

b) O serviço delegante da Comissão é responsável pela determinação da classificação de segurança;

c) Os pedidos de informação sobre a credenciação de segurança e as notificações às ANS e/ou ASD devem ser enviados por intermédio da autoridade de segurança da Comissão.

CAPÍTULO 2

MANUSEAMENTO DOS CONVITES A APRESENTAÇÃO DE PROPOSTAS PARA SUBVENÇÕES CLASSIFICADAS

Artigo 3.

Princípios básicos

1. As partes classificadas das subvenções são executadas exclusivamente por beneficiários registados num Estado-Membro ou por beneficiários registados num país terceiro ou estabelecidos por uma organização internacional, desde que esse país terceiro ou organização internacional tenham celebrado um acordo de segurança das informações com a União ou celebrado um convénio administrativo com a Comissão ([8]).

2. Antes de publicar um convite à apresentação de propostas para uma subvenção classificada, a autoridade que concede a subvenção determina a classificação de segurança das informações que podem ser fornecidas aos requerentes. A autoridade que concede a subvenção determina igualmente a classificação de segurança máxima de todas as informações utilizadas ou geradas na execução da convenção de subvenção, programa ou projeto ou, pelo menos, o volume e o tipo de informações que previsivelmente serão geradas ou manuseadas e a necessidade de um sistema de comunicação e informação (SCI) classificado.

3. A autoridade que concede a subvenção assegura que os convites à apresentação de propostas para subvenções classificadas fornecem informações sobre as obrigações de segurança especiais relacionadas com as informações classificadas. A documentação relativa aos convites deve incluir esclarecimentos sobre os prazos para os beneficiários obterem a CSE, caso lhes seja exigida. Os anexos I e II contêm amostras de modelos de informações sobre as condições dos convites à apresentação de propostas.

([8]) A lista dos acordos celebrados pela UE e dos convénios administrativos celebrados pela Comissão Europeia, ao abrigo dos quais podem ser trocadas informações classificadas da UE com países terceiros e organizações internacionais, pode ser consultada no sítio Web da Comissão.

4. A autoridade que concede a subvenção assegura que as informações com classificação RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET só são divulgadas aos requerentes depois de estes terem assinado um acordo de não divulgação que os obrigue a manusear e proteger as ICUE de acordo com o disposto na Decisão (UE, Euratom) 2015/444, nas suas regras de execução e nas regras nacionais aplicáveis.

5. No caso de serem fornecidas aos requerentes informações RESTREINT UE/EU RESTRICTED, os requisitos mínimos referidos no artigo 5.º, n.º 7, da presente decisão são incluídos no convite ou nos acordos de não divulgação celebrados na fase de apresentação de propostas.

6. Todos os requerentes e beneficiários que tenham de proceder ao manuseamento ou armazenamento de informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET nas suas instalações, quer durante a fase de apresentação de propostas quer durante a execução da própria convenção de subvenção classificada, devem ter uma CSE ao nível exigido, exceto nos casos referidos no n.º 9. São seguidamente apresentados os três cenários que poderão surgir durante a fase de apresentação de propostas para uma subvenção classificada que implique ICUE de nível CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET:

a) Durante a fase de apresentação de propostas, não é concedido acesso a ICUE de nível CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET:

   Quando o convite diz respeito a uma subvenção que implique ICUE de nível CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET mas não exija que o requerente manuseie essas informações na fase de apresentação de propostas, os requerentes desprovidos de uma CSE ao nível exigido não são excluídos do processo por esse motivo.

b) Acesso a ICUE de nível CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET nas instalações da autoridade que concede a subvenção durante a fase de apresentação de propostas:

   É concedido acesso aos requerentes que tenham uma CSP ao nível exigido e que tenham necessidade de tomar conhecimento.

c) Manuseamento ou armazenamento de ICUE de nível CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET nas instalações do requerente durante a fase de apresentação de propostas:

   Se o convite à apresentação de propostas exigir que os requerentes procedam ao manuseamento ou armazenamento de ICUE nas suas instalações, os requerentes devem ter uma CSE ao nível exigido. Em tais circunstâncias, a autoridade que concede a subvenção obtém, por intermédio da autoridade de segurança da Comissão, uma garantia da ANS ou ASD competente de que foi concedida ao requerente uma CSE adequada antes de as ICUE lhe terem sido fornecidas. É concedido acesso aos requerentes que tenham uma CSP ao nível exigido e que tenham necessidade de tomar conhecimento.

7. Em princípio, não é exigida uma CSE ou uma CSP para aceder a informações RESTREINT UE/EU RESTRICTED, quer na fase da apresentação de propostas, quer na fase de execução da convenção de subvenção. Nos casos em que os Estados-Membros exijam uma CSE ou uma CSP para convenções de subvenção ou subcontratos de nível RESTREINT UE/EU RESTRICTED ao abrigo das respetivas disposições legislativas e regulamentares nacionais, conforme enumerado no anexo IV, esses requisitos nacionais não devem impor obrigações adicionais a outros Estados-Membros nem excluir requerentes, beneficiários ou subcontratantes de Estados-Membros que não tenham esses requisitos para o acesso a informações RESTREINT UE/EU RESTRICTED decorrentes de convenções de subvenção ou de subcontratos conexos ou de um concurso para esse efeito. Estas convenções de subvenção devem ser executadas nos Estados-Membros em conformidade com as respetivas disposições legislativas e regulamentares nacionais.

8. Quando for necessária uma CSE para o manuseamento de um convite à apresentação de propostas e para a execução de uma convenção de subvenção classificada, a autoridade que concede a subvenção apresenta, por intermédio da autoridade de segurança da Comissão, um pedido à ANS ou ASD do beneficiário, utilizando uma ficha de informação de credenciação de segurança da empresa (FICSE) ou outro formulário eletrónico equivalente estabelecido. O anexo III, apêndice D, apresenta um exemplo de FICSE ([9]). A resposta a uma FICSE é dada, na medida do possível, no prazo de dez dias úteis a contar da data de apresentação do pedido.

9. Quando as entidades públicas dos Estados-Membros ou entidades sob o controlo do respetivo governo participam em subvenções classificadas que exigem CSE e quando, ao abrigo da legislação nacional, não são emitidas CSE para essas entidades, a autoridade que concede a subvenção verifica junto da ANS ou ASD em causa, por intermédio da autoridade de segurança da Comissão, se essas entidades públicas estão aptas a manusear as ICUE ao nível exigido.

([9]) Outros formulários utilizados podem diferir, na sua conceção, do exemplo apresentado nas presentes regras de execução.

10. Quando é exigida uma CSP para a execução de uma convenção de subvenção classificada e quando, de acordo com as regras nacionais, é necessária uma CSE antes de ser concedida uma CSP, a autoridade que concede a subvenção verifica junto da ANS ou ASD do beneficiário, por intermédio da autoridade de segurança da Comissão, utilizando uma FICSE, se o beneficiário possui uma CSE ou se está em curso o processo de credenciação correspondente. Neste caso, a Comissão não emite pedidos de CSP utilizando a ficha de informação de credenciação de segurança do pessoal (FICSP).

Artigo 4.

Subcontratação em subvenções classificadas

1. As condições em que um beneficiário pode subcontratar tarefas associadas a ICUE são definidas no convite à apresentação de propostas e na convenção de subvenção. Estas condições devem incluir o requisito de que todas as FICSE sejam apresentadas por intermédio da autoridade de segurança da Comissão. A subcontratação está sujeita ao consentimento prévio, por escrito, da autoridade que concede a subvenção. Quando aplicável, a subcontratação deve respeitar o ato de base que institui o programa.

2. As partes classificadas das subvenções são subcontratadas exclusivamente a entidades registadas num Estado-Membro ou a entidades registadas num país terceiro ou estabelecidas por uma organização internacional, desde que esse país terceiro ou organização internacional tenha celebrado um acordo de segurança das informações com a União ou celebrado um convénio administrativo com a Comissão ([10]).

CAPÍTULO 3

MANUSEAMENTO DE SUBVENÇÕES CLASSIFICADAS

Artigo 5.

Princípios básicos

1. Quando da concessão de uma subvenção classificada, a autoridade que concede a subvenção, juntamente com a autoridade de segurança da Comissão, assegura que as obrigações do beneficiário em matéria de proteção das ICUE utilizadas ou geradas na execução da convenção de subvenção sejam parte integrante da dita convenção. Os requisitos de segurança específicos da subvenção assumem a forma de cláusulas adicionais de segurança (CAS). O anexo III contém um exemplo de um modelo de CAS.

2. Antes de assinar uma subvenção classificada, a autoridade que concede a subvenção aprova um Guia da Classificação de Segurança (GCS) para as tarefas a executar e as informações geradas na execução da subvenção, ou a nível do programa ou do projeto, quando aplicável. O GCS faz parte das CAS.

3. Os requisitos de segurança específicos do programa ou do projeto assumem a forma de instruções de segurança do programa (ou projeto) (ISP). As ISP podem ser elaboradas com base nas disposições do modelo de CAS que figura no anexo III. As ISP são elaboradas pelo serviço da Comissão responsável pela gestão do programa ou projeto, em estreita cooperação com a autoridade de segurança da Comissão, e submetidas a parecer ao Grupo de Peritos de Segurança da Comissão. Quando uma convenção de subvenção faz parte de um programa ou projeto com as suas próprias ISP, as CAS da convenção de subvenção assumem uma forma simplificada e incluem uma referência às disposições de segurança estabelecidas nas ISP do programa ou projeto.

4. Exceto nos casos referidos no artigo 3.º, n.º 9, a convenção de subvenção classificada não pode ser assinada antes de a ANS ou ASD do requerente ter confirmado a CSE do requerente, ou, quando a convenção de subvenção classificada for atribuída a um consórcio, até que a ANS ou ASD de, pelo menos, um requerente, no âmbito do consórcio, ou mais, se necessário, tenha confirmado a CSE desse requerente.

5. Em princípio, e salvo disposição em contrário noutras regras pertinentes, a autoridade que concede a subvenção é considerada a entidade de origem das ICUE geradas na execução da convenção de subvenção.

([10]) A lista dos acordos celebrados pela UE e dos convénios administrativos celebrados pela Comissão Europeia, ao abrigo dos quais podem ser trocadas informações classificadas da UE com países terceiros e organizações internacionais, pode ser consultada no sítio Web da Comissão.

6. A autoridade que concede a subvenção, por intermédio da autoridade de segurança da Comissão, notifica as ANS e/ou ASD de todos os beneficiários e subcontratantes da assinatura de convenções de subvenção classificadas ou de subcontratos classificados e de eventuais prorrogações ou cessações antecipadas dos mesmos. O anexo IV apresenta uma lista dos requisitos nacionais.

7. As convenções de subvenção que implicam informações com classificação RESTREINT UE/EU RESTRICTED incluem uma cláusula de segurança que torna as disposições estabelecidas no anexo III, apêndice E, vinculativas para os beneficiários. Essas convenções de subvenção incluem CAS que estabelecem, no mínimo, os requisitos para o manuseamento de informações RESTREINT UE/EU RESTRICTED, incluindo aspetos relacionados com a garantia da informação e requisitos específicos a cumprir pelos beneficiários no atinente à acreditação do respetivo sistema de comunicação e informação (SCI) que manuseia as informações RESTREINT UE/EU RESTRICTED.

8. Quando tal é exigido pelas disposições legislativas e regulamentares nacionais dos Estados-Membros, as ANS ou ASD asseguram que os beneficiários ou subcontratantes sob a sua jurisdição cumpram as disposições de segurança aplicáveis à proteção das informações RESTREINT UE/EU RESTRICTED e efetuem visitas de verificação às instalações dos beneficiários ou subcontratantes situadas no seu território. Se as ANS ou ASD não tiverem essa obrigação, a autoridade que concede a subvenção assegura que os beneficiários aplicam as disposições de segurança estabelecidas no anexo III, apêndice E.

Artigo 6.

Acesso a ICUE pelo pessoal dos beneficiários e subcontratantes

1. A autoridade que concede a subvenção assegura que as convenções de subvenção classificadas incluam disposições que prevejam que só seja concedido acesso a ICUE ao pessoal de um beneficiário ou subcontratante que, para a execução da convenção de subvenção classificada ou do subcontrato classificado, tenha necessidade desse acesso, se:

a) Tiver sido estabelecido que o pessoal em causa tem necessidade de tomar conhecimento;

b) Para informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET, o pessoal em causa possuir a credenciação de segurança ao nível adequado, concedida pela respetiva ANS ou ASD ou por outra autoridade de segurança competente;

c) O pessoal em causa tiver sido informado das regras de segurança aplicáveis à proteção de ICUE e tiver reconhecido as suas responsabilidades no que respeita à proteção dessas informações.

2. Quando aplicável, o acesso a ICUE também deve estar em conformidade com o ato de base que institui o programa e ter em conta eventuais marcas adicionais definidas no GCS.

3. Se o beneficiário ou subcontratante pretender contratar um nacional de um país terceiro para um lugar que implique o acesso a ICUE com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET, cabe ao beneficiário ou subcontratante iniciar o procedimento de credenciação de segurança dessa pessoa, em conformidade com as disposições legislativas e regulamentares nacionais aplicáveis no local onde o acesso às ICUE deve ser concedido.

Artigo 7.

Acesso a ICUE por parte de peritos que participam em controlos, exames ou auditorias

1. As pessoas externas («peritos») que participam em controlos, exames ou auditorias realizados pela autoridade que concede a subvenção ou em análises do desempenho dos beneficiários que necessitam de ter acesso a informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET só podem obter um contrato se possuírem a credenciação de segurança ao nível adequado, concedida pela respetiva ANS ou ASD ou por outra autoridade de segurança competente. A autoridade que concede a subvenção, por intermédio da autoridade de segurança da Comissão, procede à verificação e, se necessário, solicita à ANS ou ASD que dê início ao processo de verificação no que respeita aos peritos pelo menos seis meses antes do início dos respetivos contratos.

2. Antes da assinatura do contrato, os peritos devem ser informados das regras de segurança aplicáveis à proteção de ICUE e devem ter reconhecido as suas responsabilidades no que respeita à proteção dessas informações.

CAPÍTULO 4

VISITAS ASSOCIADAS AS CONVENÇÕES DE SUBVENÇÃO CLASSIFICADAS

Artigo 8.

Princípios básicos

1. Quando a autoridade que concede a subvenção, os peritos, os beneficiários ou os subcontratantes necessitam de aceder a informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET nas instalações uns dos outros no contexto da execução de uma convenção de subvenção classificada, devem ser organizadas visitas em ligação com as ANS ou ASD ou com outras autoridades de segurança competentes a que o assunto diga respeito.

2. As visitas referidas no n.º 1 estão sujeitas aos seguintes requisitos:

a) A finalidade oficial da visita deve estar relacionada com a subvenção classificada;

b) Os visitantes devem ter uma CSP ao nível exigido e devem ter necessidade de tomar conhecimento de tais informações para acederem às ICUE utilizadas ou geradas na execução de uma subvenção classificada.

Artigo 9.

Pedidos de visita

1. As visitas dos beneficiários ou subcontratantes a instalações de outros beneficiários ou subcontratantes, ou a instalações da autoridade que concede a subvenção, que impliquem o acesso a informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET devem ser organizadas de acordo com o seguinte procedimento:

a) O responsável de segurança da instalação que envia o visitante deve preencher todas as partes relevantes do formulário de pedido de visita (PDV) e apresentar o pedido à ANS ou ASD da instalação. O modelo de formulário de PDV consta do anexo III, apêndice C;

b) A ANS ou ASD da instalação de envio tem de confirmar a CSP do visitante antes de apresentar o PDV à ANS ou ASD da instalação de acolhimento (ou à autoridade de segurança da Comissão, se se tratar de uma visita às instalações da autoridade que concede a subvenção);

c) O responsável de segurança da instalação de envio obtém então da sua ANS ou ASD a resposta da ANS ou ASD da instalação de acolhimento (ou da autoridade de segurança da Comissão), aceitando ou recusando o PDV;

d) Se não forem levantadas objeções até cinco dias úteis antes da data da visita, o PDV é considerado aprovado.

2. As visitas de funcionários da autoridade que concede a subvenção, de peritos ou de auditores às instalações dos beneficiários ou subcontratantes que impliquem o acesso a informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET devem ser organizadas de acordo com o seguinte procedimento:

a) O visitante deve preencher todas as partes relevantes do formulário de PDV e apresentá-lo à autoridade de segurança da Comissão;

b) A autoridade de segurança da Comissão confirma a CSP do visitante antes de submeter o PDV à ANS ou ASD da instalação de acolhimento;

c) A autoridade de segurança da Comissão obtém uma resposta da ANS ou ASD da instalação de acolhimento, autorizando ou recusando o PDV;

d) Se não forem levantadas objeções até cinco dias úteis antes da data da visita, o PDV é considerado aprovado.

3. Um PDV pode abranger uma única visita ou visitas recorrentes. No caso de visitas recorrentes, o PDV pode ser válido, no máximo, até um ano a contar da data de início solicitada.

4. O período de validade do PDV não pode exceder o período de validade da CSP do visitante.

5. Regra geral, o PDV é apresentado à autoridade de segurança competente da instalação de acolhimento pelo menos 15 dias úteis antes da data da visita.

Artigo 10.

Procedimentos relativos às visitas

1. Antes de autorizar o acesso dos visitantes a ICUE, o responsável de segurança da instalação de acolhimento deve cumprir todos os procedimentos e regras de segurança relativos a visitas estabelecidos pela sua ANS ou ASD.

2. Os visitantes devem comprovar a sua identidade ao chegarem à instalação de acolhimento mediante a apresentação do bilhete de identidade ou passaporte válidos. Essas informações de identificação devem corresponder às informações indicadas no PDV.

3. A instalação de acolhimento deve assegurar que sejam mantidos registos de todos os visitantes, incluindo os seus nomes, a organização que representam, a data de termo da CSP, a data da visita e os nomes das pessoas visitadas. Esses registos devem ser conservados por um período mínimo de cinco anos, ou mais se tal for exigido pelas regras e regulamentos nacionais do país onde está situada a instalação de acolhimento.

Artigo 11.

Visitas organizadas diretamente

1. No contexto de projetos específicos, as ANS ou ASD competentes e a autoridade de segurança da Comissão podem acordar um procedimento ao abrigo do qual as visitas realizadas no âmbito de uma subvenção classificada específica podem ser organizadas diretamente entre o responsável de segurança do visitante e o responsável de segurança da instalação a visitar. O modelo de formulário a utilizar para este efeito é apresentado no anexo III, apêndice C. Este procedimento excecional é estabelecido nas ISP ou noutras disposições específicas. Nesses casos, não se aplicam os procedimentos estabelecidos no artigo 9.º e no artigo 10.º, n.º 1.

2. As visitas que impliquem o acesso a informações com classificação RESTREINT UE/EU RESTRICTED devem ser organizadas diretamente entre a entidade de envio e a entidade de acolhimento, sem necessidade de seguir os procedimentos estabelecidos no artigo 9.º e no artigo 10.º, n.º 1.

CAPÍTULO 5

TRANSMISSÃO E TRANSPORTE DE ICUE NA EXECUÇÃO DE CONVENÇÕES DE SUBVENÇÃO CLASSIFICADAS

Artigo 12.

Princípios básicos

A autoridade que concede a subvenção assegura que todas as decisões relacionadas com a transferência e o transporte de ICUE estão conformes com a Decisão (UE, Euratom) 2015/444 e com as suas regras de execução, bem como com as condições da convenção de subvenção classificada, incluindo o consentimento da entidade de origem.

Artigo 13.

Manuseamento eletrónico

1. O manuseamento e a transmissão eletrónicos de ICUE processam-se nos termos estabelecidos nos capítulos 5 e 6 da Decisão (UE, Euratom) 2015/444 e nas suas regras de execução.

Os sistemas de comunicação e informação que sejam propriedade de um beneficiário e sejam utilizados para o manuseamento de ICUE na execução da convenção de subvenção (SCI do beneficiário) estão sujeitos a acreditação pela autoridade de acreditação de segurança (AAS) responsável. Todas as transmissões eletrónicas de ICUE devem ser protegidas por produtos criptográficos aprovados nos termos do artigo 36.º, n.º 4, da Decisão (UE, Euratom) 2015/444. Devem ser aplicadas medidas de segurança TEMPEST em conformidade com o artigo 36.º, n.º 6, da referida decisão.

2. A acreditação de segurança do SCI do beneficiário que manuseia ICUE ao nível de classificação RESTREINT UE/EU RESTRICTED e qualquer interligação do mesmo pode ser delegada no responsável de segurança de um beneficiário, se tal for permitido pelas disposições legislativas e regulamentares nacionais. Quando essa tarefa é delegada, o beneficiário é responsável pela aplicação dos requisitos mínimos de segurança descritos nas CAS ao manusear informações com a classificação RESTREINT UE/EU RESTRICTED no seu SCI. No entanto, as ANS ou ASD e AAS competentes continuam a ser responsáveis pela proteção das informações RESTREINT UE/EU RESTRICTED manuseadas pelo beneficiário e a ter o direito de inspecionar as medidas de segurança tomadas pelo beneficiário. Além disso, o beneficiário deve fornecer à autoridade que concede a subvenção e, se as disposições legislativas e regulamentares nacionais o exigirem, à AAS nacional competente, uma declaração de conformidade certificando que o SCI do beneficiário e as interligações conexas foram acreditados para o manuseamento de ICUE ao nível RESTREINT UE/EU RESTRICTED ([11]).

Artigo 14.

Transporte por serviços comerciais de estafeta

O transporte de ICUE por serviços comerciais de estafeta deve respeitar as disposições pertinentes da Decisão (UE, Euratom) 2019/1962 da Comissão ([12]) que estabelece regras de execução aplicáveis ao manuseamento de informações com classificação RESTREINT UE/EU RESTRICTED e da Decisão (UE, Euratom) 2019/1961 da Comissão ([13]) que estabelece regras de execução aplicáveis ao manuseamento de informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET.

Artigo 15.

Transporte em mão própria

1. O transporte em mão própria de informações classificadas está sujeito a requisitos de segurança rigorosos.

2. As informações RESTREINT UE/EU RESTRICTED podem ser transportadas por mão própria por pessoal do beneficiário dentro da União, desde que sejam cumpridos os seguintes requisitos:

a) O sobrescrito ou a embalagem utilizados são opacos e não contêm qualquer indicação sobre a classificação do seu conteúdo;

b) As informações classificadas não saem das mãos do portador;

c) O sobrescrito ou a embalagem não são abertos durante o percurso.

3. Para informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET, o transporte em mão própria por pessoal do beneficiário num Estado-Membro é organizado com antecedência entre a entidade expedidora e a entidade recetora. A autoridade ou instalação expedidora informa a autoridade ou instalação recetora dos dados relativos à remessa, incluindo a referência, a classificação, a hora prevista de chegada e o nome do serviço de estafeta. É permitido esse transporte em mão própria, desde que sejam cumpridos os seguintes requisitos:

a) As informações classificadas são transportadas num duplo sobrescrito ou numa dupla embalagem;

b) O sobrescrito ou a embalagem exteriores estão protegidos e não contêm qualquer indicação sobre a classificação do seu conteúdo, devendo o sobrescrito interior indicar o nível de classificação;

c) As ICUE não saem das mãos do portador;

d) O sobrescrito ou a embalagem não são abertos durante o percurso;

e) O sobrescrito ou a embalagem são transportados numa pasta que possa ser fechada à chave ou num contentor aprovado similar, de dimensões e peso tais que possam ser mantidos permanentemente na posse do portador e não ser enviados para um compartimento de bagagens;

f) O estafeta está munido de um certificado de estafeta emitido pela respetiva autoridade de segurança competente que o autoriza a transportar a remessa classificada identificado.

([11]) Os requisitos mínimos aplicáveis a sistemas de comunicação e informação que manuseiam ICUE ao nível RESTREINT UE/EU RESTRICTED constam do anexo III, apêndice E.

([12]) Decisão (UE, Euratom) 2019/1962 da Comissão, de 17 de outubro de 2019, que estabelece regras de execução aplicáveis ao manuseamento de informações com classificação RESTREINT UE/EU RESTRICTED (JO L 311 de 2.12.2019, p. 21).

([13]) Decisão (UE, Euratom) 2019/1961 da Comissão, de 17 de outubro de 2019, que estabelece regras de execução aplicáveis ao manuseamento de informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET (JO L 311 de 2.12.2019, p. 1).

4. Para o transporte em mão, efetuado por pessoal do beneficiário, de informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET de um Estado-Membro para outro, são aplicáveis as seguintes regras adicionais:

a) O estafeta é responsável por guardar em segurança o material classificado transportado até à sua entrega ao destinatário;

b) Em caso de violação da segurança, a ANS ou ASD do expedidor pode solicitar que as autoridades do país em que se verificou a violação de segurança procedam a uma investigação, comuniquem as suas constatações e tomem medidas legais ou outras, conforme adequado;

c) O estafeta foi informado de todas as obrigações de segurança a observar durante o transporte e assinou uma declaração adequada;

d) As instruções destinadas ao estafeta estão apensas ao certificado de estafeta;

e) O estafeta recebeu uma descrição da remessa e um itinerário;

f) Os documentos são devolvidos à ANS ou ASD emissora no termo da ou das deslocações ou mantidos à disposição pelo destinatário para fins de controlo;

g) Caso as autoridades aduaneiras ou de imigração ou a polícia de fronteiras solicitem o exame e a inspeção da remessa, estas são autorizadas a abrir e a examinar partes suficientes da remessa que lhes permitam determinar que esta não contém material distinto do declarado;

h) As autoridades aduaneiras são instadas a respeitar a autoridade oficial dos documentos de expedição e dos documentos de autorização transportados pelo estafeta.

Se uma remessa for aberta pelas autoridades aduaneiras, tal deve ser feito fora da vista de pessoas não autorizadas e, sempre que possível, na presença do estafeta. O estafeta deve solicitar que a remessa seja reembalada e que as autoridades que efetuam a inspeção voltem a selar a remessa e confirmem, por escrito, que abriram a remessa.

5. O transporte em mão, por pessoal do beneficiário, de informações com classificação RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET para um país terceiro ou uma organização internacional está sujeito às disposições do acordo de segurança das informações ou do convénio administrativo celebrado, respetivamente, entre a União ou a Comissão e esse país terceiro ou organização internacional.

CAPÍTULO 6

PLANEAMENTO DE CONTINUIDADE DAS ATIVIDADES

Artigo 16.

Planos de contingência e medidas de recuperação

A autoridade que concede a subvenção assegura que a convenção de subvenção classificada exija que os beneficiários estabeleçam planos de contingência das atividades (PCA) para proteger as ICUE manuseadas no contexto da execução da subvenção classificada em situações de emergência e prevejam medidas de prevenção e recuperação no contexto do planeamento da continuidade das atividades, a fim de minimizar o impacto de incidentes relacionados com o manuseamento e o armazenamento das ICUE. Os beneficiários devem confirmar à autoridade que concede a subvenção que os seus planos de contingência das atividades estão em vigor.

Artigo 17.

Entrada em vigor

A presente decisão entra em vigor no vigésimo dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*.

Feito em Bruxelas, em 10 de fevereiro de 2021.

Pela Comissão,
Em nome da Presidente,
Johannes HAHN
Membro da Comissão

ANEXO I

INFORMAÇÕES NORMALIZADAS NO CONVITE À APRESENTAÇÃO DE PROPOSTAS

(a adaptar ao convite utilizado)

Segurança

Os projetos que implicam informações classificadas da UE devem ser submetidos a um controlo de segurança para autorizar o financiamento e podem ser sujeitos a regras de segurança específicas [detalhadas nas cláusulas adicionais de segurança (CAS) que figuram em anexo à convenção de subvenção].

Estas regras [regidas pela Decisão (UE, Euratom) 2015/444 ([1]) e/ou pelas normas nacionais] preveem, por exemplo, que:

— Os projetos que implicam informações com classificação TRES SECRET UE/EU TOP SECRET (ou equivalente) **NÃO** podem ser financiados;

— As informações classificadas devem ser marcadas de acordo com as instruções de segurança aplicáveis constantes das CAS;

— As informações com níveis de classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior (e RESTREINT UE/EU RESTRICTED, se exigido pelas regras nacionais):

  — só podem ser criadas ou consultadas em instalações com credenciação de segurança da empresa pela autoridade nacional de segurança competente (ANS), em conformidade com as regras nacionais;

  — só podem ser manuseadas numa zona securizada acreditada pela ANS competente;

  — só podem ser consultadas e manuseadas por pessoas com credenciação de segurança do pessoal (CSP) válida e que tenham necessidade de tomar conhecimento;

— No final da subvenção, as informações classificadas devem ser devolvidas ou continuar a ser objeto de proteção em conformidade com as regras aplicáveis;

— As tarefas da ação que impliquem informações classificadas da UE (ICUE) só podem ser subcontratadas mediante a aprovação prévia, por escrito, da autoridade que concede a subvenção, e apenas a entidades estabelecidas num Estado-Membro ou num país terceiro com um acordo de segurança das informações com a UE (ou um convénio administrativo com a Comissão);

— A divulgação de ICUE a terceiros está sujeita à aprovação prévia, por escrito, da autoridade que concede a subvenção.

Note-se que, dependendo do tipo de atividade, a credenciação de segurança da empresa pode ter de ser fornecida antes da assinatura da subvenção. A autoridade que concede a subvenção avaliará a necessidade de proceder à credenciação em cada caso e fixará a respetiva data de entrega durante a preparação da subvenção. Note-se que, **em circunstância alguma**, poderemos assinar uma convenção de subvenção sem que pelo menos um dos beneficiários no âmbito de um consórcio obtenha a credenciação de segurança da empresa.

Podem ser acrescentadas à convenção de subvenção outras recomendações de segurança sob a forma de prestações de segurança (*por exemplo, criar um grupo consultivo em matéria de segurança, limitar o nível de pormenor, utilizar cenários falsos, excluir a utilização de informações classificadas, etc.*).

Os beneficiários devem garantir que os seus projetos não estão sujeitos a requisitos de segurança nacionais/de países terceiros suscetíveis de afetar a execução ou de pôr em causa a concessão da subvenção (*por exemplo, restrições tecnológicas, classificação de segurança nacional, etc.*). A autoridade que concede a subvenção deve ser notificada imediatamente de quaisquer problemas potenciais de segurança.

[OPÇÃO adicional para os acordos-quadro de parceria: no caso dos acordos-quadro de parceria, tanto as candidaturas a acordos-quadro de parceria como as candidaturas a subvenções podem ter de ser submetidas a um controlo de segurança.]

([1]) Ver Decisão (UE, Euratom) 2015/444 da Comissão, de 13 de março de 2015, relativa às regras de segurança aplicáveis à proteção das informações classificadas da UE (JO L 72 de 17.3.2015, p. 53).

ANEXO II

CLÁUSULAS-TIPO DAS CONVENÇÕES DE SUBVENÇÃO

(a adaptar à convenção de subvenção utilizada)

13.2 Segurança – Informações classificadas

As partes devem manusear as informações classificadas (UE ou nacionais) em conformidade com a legislação da UE ou a legislação nacional aplicável em matéria de informações classificadas [em particular, a Decisão (UE, Euratom) 2015/444 da Comissão ([1]) e as respetivas regras de execução].

As (eventuais) regras de segurança específicas constam do anexo 5.

ANEXO 5

Segurança — Informações classificadas da UE

[OPÇÃO para ações com informações classificadas da UE (norma): se a ação implicar a utilização ou a geração de informações classificadas da UE, essas informações devem ser tratadas em conformidade com o Guia da Classificação de Segurança (GCS) e com as cláusulas adicionais de segurança (CAS), conforme estabelecido no anexo 1 e na Decisão (UE, Euratom) 2015/444 e respetivas regras de execução, até serem desclassificadas.

As prestações que contenham informações classificadas da UE devem ser apresentadas em conformidade com procedimentos especiais acordados com a autoridade que concede a subvenção.

As tarefas da ação que impliquem informações classificadas da UE só podem ser subcontratadas mediante a aprovação prévia explícita, por escrito, da autoridade que concede a subvenção e apenas a entidades estabelecidas num Estado-Membro ou num país terceiro que tenha um acordo de segurança das informações com a UE (ou um convénio administrativo com a Comissão).

As informações classificadas da UE não devem ser divulgadas a terceiros (incluindo participantes na execução da ação) sem a aprovação prévia explícita, por escrito, da autoridade que concede a subvenção.]

([1]) Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53).

ANEXO III

[Anexo IV (da ……)]

CLÁUSULAS ADICIONAIS DE SEGURANÇA (CAS) [1]

[Modelo]

[1] O presente modelo de CAS aplica-se quando a Comissão é considerada a entidade de origem das informações classificadas criadas e manuseadas para a execução da convenção de subvenção. Quando a entidade de origem das informações classificadas criadas e manuseadas para a execução da convenção de subvenção não for a Comissão, e os Estados-Membros que participam na subvenção estabelecerem um quadro de segurança específico, podem aplicar-se outros modelos de CAS.

Apêndice A

REQUISITOS DE SEGURANÇA

A autoridade que concede a subvenção deve incluir os seguintes requisitos de segurança nas cláusulas adicionais de segurança (CAS). Algumas cláusulas podem não ser aplicáveis à convenção de subvenção. Essas cláusulas são indicadas entre parênteses retos.

A lista das cláusulas não é exaustiva. Podem ser acrescentadas outras cláusulas em função da natureza da subvenção classificada.

CONDIÇÕES GERAIS [*N.B.: aplicável a todas as convenções de subvenção classificadas*]

1. Estas cláusulas adicionais de segurança (CAS) são parte integrante da convenção de subvenção classificada [ou do subcontrato] e descrevem os requisitos de segurança específicos da convenção de subvenção. O incumprimento destes requisitos pode constituir motivo suficiente para a rescisão da convenção de subvenção.

2. Os beneficiários das subvenções estão sujeitos a todas as obrigações estabelecidas na Decisão (UE, Euratom) 2015/444 da Comissão ([2]) (a seguir designada «DC 2015/444») e nas respetivas regras de execução ([3]). Se o beneficiário da subvenção se deparar com um problema de aplicação do quadro jurídico aplicável num dado Estado-Membro, deve recorrer à autoridade de segurança da Comissão e à autoridade nacional de segurança (ANS) ou à autoridade de segurança designada (ASD).

3. As informações classificadas geradas na execução da convenção de subvenção devem ser marcadas como informações classificadas da UE (ICUE) ao nível de classificação de segurança, conforme determinado no Guia da Classificação de Segurança (GCS) no apêndice B dessas cláusulas. Um desvio em relação ao nível de classificação de segurança estipulado pelo GCS só é admissível com autorização escrita da autoridade que concede a subvenção.

4. Os direitos da entidade de origem de ICUE criadas e manuseadas para a execução da convenção de subvenção classificada são exercidos pela Comissão, enquanto autoridade que concede a subvenção.

5. O beneficiário ou subcontratante não deve utilizar, sem o consentimento escrito da autoridade que concede a subvenção, informações ou material fornecidos por essa autoridade ou em nome dela produzidos para outra finalidade que não a da convenção de subvenção.

6. Quando for necessária uma credenciação de segurança da empresa (CSE) para a execução de uma convenção de subvenção, o beneficiário deve solicitar à autoridade que concede a subvenção que dê seguimento ao pedido de CSE.

7. O beneficiário deve investigar todas as violações de segurança relacionadas com as ICUE e comunicá-las à autoridade que concede a subvenção logo que possível. O beneficiário ou subcontratante deve informar imediatamente a ANS ou ASD e, se as disposições legislativas e regulamentares nacionais o permitirem, a autoridade de segurança da Comissão de todos os casos em que se tem conhecimento ou motivos para suspeitar que as ICUE fornecidas ou geradas nos termos da convenção de subvenção foram perdidas ou divulgadas a pessoas não autorizadas.

([2]) Decisão (UE, Euratom) 2015/444 da Comissão, de 13 de março de 2015, relativa às regras de segurança aplicáveis à proteção das informações classificadas da UE (JO L 72 de 17.3.2015, p. 53).

([3]) A autoridade que concede a subvenção deve inserir as referências após a adoção destas regras de execução.

8. Após o termo da convenção de subvenção, o beneficiário ou subcontratante deve devolver à autoridade que concede a subvenção, o mais rapidamente possível, todas as ICUE na sua posse. Quando viável, o beneficiário ou subcontratante pode destruir as ICUE em vez de as devolver. Tal deve ser efetuado em conformidade com as disposições legislativas e regulamentares nacionais do país em que o beneficiário está estabelecido, com o acordo prévio da autoridade de segurança da Comissão, e de acordo com as instruções desta autoridade. As ICUE devem ser destruídas de forma a não poderem ser reconstituídas, quer no todo, quer em parte.

9. Se o beneficiário ou subcontratante estiver autorizado a conservar ICUE após a rescisão ou o termo da convenção de subvenção, as ICUE devem continuar a ser protegidas em conformidade com a DC 2015/444 e com as respetivas regras de execução ([4]).

10. O manuseamento, o tratamento e a transmissão por via eletrónica de ICUE devem respeitar as disposições estabelecidas nos capítulos 5 e 6 da DC 2015/444. Estas incluem, nomeadamente, o requisito de submeter a acreditação os sistemas de comunicação e informação que sejam propriedade do beneficiário e utilizados para o manuseamento de ICUE na execução da convenção de subvenção (seguidamente designados «SCI do beneficiário») ([5]); de proteger qualquer transmissão eletrónica de ICUE por produtos criptográficos aprovados nos termos do artigo 36.º, n.º 4, da DC 2015/444, e de aplicar medidas de segurança TEMPEST em conformidade com o artigo 36.º, n.º 6, da mesma decisão.

11. O beneficiário ou subcontratante deve dispor de planos de contingência das atividades (PCA) com vista a proteger as ICUE manuseadas no desempenho da convenção de subvenção classificada em situações de emergência e estabelecer medidas de prevenção e de recuperação a fim de minimizar o impacto de incidentes associados ao manuseamento e ao armazenamento de ICUE. O beneficiário ou subcontratante deve informar a autoridade que concede a subvenção do seu PCA.

CONVENÇÕES DE SUBVENÇÃO QUE NECESSITAM DE ACESSO A INFORMAÇÕES COM CLASSIFICAÇÃO RESTREINT UE/EU RESTRICTED

12. Em princípio, não é necessária uma credenciação de segurança do pessoal (CSP) para cumprimento da convenção de subvenção ([6]). No entanto, as informações ou o material com classificação RESTREINT UE/EU RESTRICTED devem estar acessíveis apenas ao pessoal do beneficiário que delas necessite para a execução da convenção de subvenção (princípio da necessidade de tomar conhecimento), que tenha sido devidamente informado pelo responsável da segurança do beneficiário sobre as suas responsabilidades e sobre as consequências de um eventual comprometimento ou violação da segurança dessas informações e que tenha reconhecido por escrito as consequências da não proteção das ICUE.

13. Exceto nos casos em que a autoridade que concede a subvenção tenha dado o seu consentimento por escrito, o beneficiário ou subcontratante não pode dar acesso a informações ou a material com classificação RESTREINT UE/EU RESTRICTED a entidades ou pessoas que não sejam o seu pessoal que tenha necessidade de tomar conhecimento.

14. O beneficiário ou subcontratante deve manter as marcas de classificação de segurança das informações classificadas geradas ou fornecidas durante a execução de uma convenção de subvenção e não deve desclassificar informações sem o consentimento escrito da autoridade que concede a subvenção.

15. As informações ou o material com classificação RESTREINT UE/EU RESTRICTED devem ser armazenados em móveis de escritório fechados à chave quando não estiverem a ser utilizados. Quando em trânsito, os documentos devem ser transportados dentro de um sobrescrito opaco. Os documentos não devem sair das mãos do portador nem ser abertos durante o percurso.

([4]) A autoridade que concede a subvenção deve inserir as referências após a adoção destas regras de execução.

([5]) A parte que procede à acreditação terá de fornecer à autoridade que concede a subvenção uma declaração de conformidade, por intermédio da autoridade de segurança da Comissão, e em coordenação com a autoridade de acreditação de segurança nacional (AAS) competente.

([6]) Se os beneficiários provierem de Estados-Membros que exijam CSP e/ou CSE para subvenções com classificação RESTREINT UE/EU RESTRICTED, a autoridade que concede a subvenção enumera nas CAS os respetivos requisitos de CSP e CSE para os beneficiários em causa.

16. O beneficiário ou subcontratante pode transmitir documentos com classificação RESTREINT UE/EU RESTRICTED à autoridade que concede a subvenção recorrendo a empresas de estafetas, serviços postais, transporte em mão própria ou meios eletrónicos. Para o efeito, o beneficiário ou subcontratante deve seguir as instruções de segurança do programa (ou projeto) (ISP) emitidas pela Comissão e/ou as regras de execução da Comissão relativas à segurança industrial no que respeita às subvenções classificadas ([7]).

17. Quando já não forem necessários, os documentos com classificação RESTREINT UE/EU RESTRICTED devem ser destruídos de forma a não poderem ser reconstituídos, quer total quer parcialmente.

18. A acreditação de segurança do SCI do beneficiário que manuseia ICUE ao nível de classificação RESTREINT UE/EU RESTRICTED e qualquer interligação do mesmo pode ser delegada no responsável de segurança do beneficiário, se tal for permitido pelas disposições legislativas e regulamentares nacionais. Nos casos em que a acreditação é assim delegada, as ANS/ASD ou as autoridades de acreditação de segurança (AAS) continuam a ser responsáveis pela proteção das informações RESTREINT UE/EU RESTRICTED manuseadas pelo beneficiário e a ter o direito de inspecionar as medidas de segurança tomadas pelo beneficiário. Além disso, o beneficiário deve fornecer à autoridade que concede a subvenção e, se as disposições legislativas e regulamentares nacionais o exigirem, à AAS nacional competente, uma declaração de conformidade que certifique que o SCI do beneficiário e as interligações conexas foram acreditados para o manuseamento de ICUE ao nível RESTREINT UE/EU RESTRICTED.

MANUSEAMENTO DE INFORMAÇÕES COM CLASSIFICAÇÃO RESTREINT UE/EU RESTRICTED EM SISTEMAS DE COMUNICAÇÃO E INFORMAÇÃO (SCI)

19. Os requisitos mínimos aplicáveis aos SCI que manuseiam informações com a classificação RESTREINT UE/EU RESTRICTED constam do apêndice E destas CAS.

CONDIÇÕES EM QUE O BENEFICIÁRIO PODE SUBCONTRATAR

20. O beneficiário deve obter a autorização da autoridade que concede a subvenção antes de subcontratar qualquer parte de uma convenção de subvenção classificada.

21. Não podem ser adjudicados subcontratos a uma entidade registada num país terceiro ou a uma entidade pertencente a uma organização internacional, se esse país terceiro ou organização internacional não tiverem celebrado um acordo de segurança das informações com a UE ou um convénio administrativo com a Comissão.

22. Quando o beneficiário procede a uma subcontratação, as disposições de segurança da convenção de subvenção aplicam-se, *mutatis mutandis*, ao(s) subcontratante(s) e ao respetivo pessoal. Nesse caso, cabe ao beneficiário assegurar que todos os subcontratantes aplicam estes princípios nas suas próprias disposições de subcontratação. A fim de assegurar uma supervisão da segurança adequada, a autoridade de segurança da Comissão deve notificar as ANS e/ou ASD do beneficiário e do subcontratante da atribuição de todos os subcontratos classificados conexos de nível CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET. Quando adequado, as ANS e/ou ASD do beneficiário e do subcontratante devem receber uma cópia das disposições de segurança específicas do subcontrato. As ANS e ASD que exigem a notificação das disposições de segurança das convenções de subvenção classificadas ao nível RESTREINT UE/EU RESTRICTED são enumeradas no anexo às regras de execução da Comissão relativas à segurança industrial no que respeita às convenções de subvenção classificadas ([8]).

23. O beneficiário não pode comunicar ICUE a um subcontratante sem a aprovação prévia, por escrito, da autoridade que concede a subvenção. Se forem enviadas ICUE a subcontratantes de forma frequente ou rotineira, a autoridade que concede a subvenção pode dar a sua aprovação por um período determinado (por exemplo, 12 meses) ou durante o período de vigência do subcontrato.

([7]) A autoridade que concede a subvenção deve inserir as referências após a adoção destas regras de execução.
([8]) A autoridade que concede a subvenção deve inserir as referências após a adoção destas regras de execução.

VISITAS

Se for aplicável o procedimento normal de pedido de visita (PDV) a visitas que impliquem informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET, a autoridade que concede a subvenção deve integrar os n.os 24, 25 e 26 e suprimir o n.o 27. Se forem organizadas visitas que impliquem informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET diretamente entre o estabelecimento de envio e o estabelecimento de acolhimento, a autoridade que concede a subvenção deve suprimir os n.os 25 e 26 e integrar apenas o n.o 27.

24. As visitas que impliquem o acesso efetivo ou potencial a informações com classificação RESTREINT UE/EU RESTRICTED devem ser organizadas diretamente entre a entidade de envio e a entidade de acolhimento, sem necessidade de seguir os procedimentos estabelecidos nos n.os 25 a 27 abaixo.

[25. As visitas que impliquem o acesso efetivo ou potencial a informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET estão sujeitas ao seguinte procedimento:

a) O responsável de segurança da instalação que envia o visitante deve preencher todas as partes relevantes do formulário de pedido de visita (PDV) (apêndice C) e apresentar o pedido à ANS ou ASD da instalação;

b) A ANS ou ASD da instalação de envio tem de confirmar a CSP do visitante antes de apresentar o PDV à ANS ou ASD da instalação de acolhimento (ou à autoridade de segurança da Comissão, se a visita for efetuada às instalações da autoridade que concede a subvenção);

c) O responsável de segurança da instalação de envio obtém então da sua ANS ou ASD a resposta da ANS ou ASD da instalação de acolhimento (ou da autoridade de segurança da Comissão), aceitando ou recusando o PDV;

d) Se não forem levantadas objeções até cinco dias úteis antes da data da visita, o PDV é considerado aprovado.]

[26. Antes de dar ao(s) visitante(s) acesso a informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET, a instalação de acolhimento deve ter recebido autorização da sua ANS ou ASD.]

[27. As visitas que impliquem acesso efetivo ou potencial a informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET devem ser organizadas diretamente entre o estabelecimento de envio e o estabelecimento de acolhimento (consta do apêndice C um exemplo do formulário que pode ser utilizado para esse efeito).]

28. Os visitantes devem comprovar a sua identidade à chegada à instalação de acolhimento mediante a apresentação de bilhete de identidade ou passaporte válidos.

29. A instalação que acolhe a visita deve assegurar que sejam mantidos registos de todos os visitantes. Estes devem incluir os seus nomes, a organização que representam, a data de termo da CSP (se aplicável), a data da visita e o nome da(s) pessoa(s) visitada(s). Sem prejuízo das regras europeias em matéria de proteção de dados, esses registos devem ser conservados por um período não inferior a cinco anos ou em conformidade com as normas e regulamentações nacionais, conforme adequado.

VISITAS DE AVALIAÇÃO

30. A autoridade de segurança da Comissão pode, em cooperação com as ANS ou ASD competentes, efetuar visitas às instalações de beneficiários ou subcontratantes a fim de verificar se os requisitos de segurança aplicáveis ao manuseamento de ICUE estão a ser cumpridos.

GUIA DA CLASSIFICAÇÃO DE SEGURANÇA

31. O Guia da Classificação de Segurança (GCS) contém uma lista de todos os elementos da convenção de subvenção que são classificados ou a classificar no decurso da execução da mesma, as regras correspondentes e a especificação dos níveis de classificação de segurança aplicáveis. O GCS é parte integrante da presente convenção de subvenção e consta do apêndice B do presente anexo.

Apêndice B

GUIA DA CLASSIFICAÇÃO DE SEGURANÇA

[texto específico a adaptar em função do objeto da convenção de subvenção]

Apêndice C

PEDIDO DE VISITA (MODELO)

INSTRUÇÕES PORMENORIZADAS PARA O PREENCHIMENTO DO PEDIDO DE VISITA

(O pedido deve ser apresentado apenas em inglês)

HEADING	Assinalar as caixas relativas ao tipo de visita e ao tipo de informação e indicar o número de locais a visitar e o número de visitantes.
4. **ADMINISTRATIVE DATA**	A preencher pela ANS/ASD requerente.
5. **REQUESTING ORGANISATION OR INDUSTRIAL FACILITY**	Indicar o nome completo e o endereço postal. Incluir a cidade, o Estado e o código postal, conforme aplicável.
6. **ORGANISATION OR INDUSTRIAL FACILITY TO BE VISITED**	Indicar o nome completo e o endereço postal. Incluir a cidade, o Estado, o código postal, o número de telex ou fax (se aplicável), o número de telefone e o endereço de correio eletrónico. Indicar o nome e os números de telefone/fax e o endereço de correio eletrónico do seu principal ponto de contacto ou da pessoa com quem marcou a visita. Observações: 1) É importante indicar o código postal correto (código zip), uma vez que uma empresa pode ter várias instalações. 2) Quando o pedido é preenchido manualmente, pode ser utilizado o anexo 1 quando da visita de duas ou mais instalações sobre um mesmo assunto. Quando é utilizado um anexo, o ponto 3 deve indicar: «VER ANEXO 1, NÚMERO DE INSTAL:..» (indicar o número de instalações).
7. **DATES OF VISIT**	Indicar a data ou o período efetivos (de data a data) da visita com o formato «dia — mês — ano». Quando aplicável, indicar uma data ou um período alternativos entre parênteses.
8. **TYPE OF INITIATIVE**	Especificar se a visita é da iniciativa da organização ou instalação requerente ou se é um convite da instalação a visitar.
9. **THE VISIT RELATES TO:**	Indicar o nome completo do projeto, do contrato ou do convite à apresentação de propostas usando apenas abreviaturas utilizadas correntemente.
10. **SUBJECT TO BE DISCUSSED/ JUSTIFICATION**	Apresentar uma breve descrição do(s) motivo(s) da visita. Não utilizar abreviaturas sem explicação. Observações: No caso de visitas recorrentes, este ponto deve indicar a menção «Visitas recorrentes» como primeiras palavras no elemento de dados (por exemplo, «Visitas recorrentes para debater _____»).
11. **ANTICIPATED LEVEL OF CLASSIFIED INFORMATION TO BE INVOLVED**	Indicar SECRET UE/EU SECRET (S-UE/EU-S) ou CONFIDENTIEL UE/EU CONFIDENTIAL (C-UE/EU-C), conforme adequado.

12. **PARTICULARS OF VISITOR**	Observação: quando a visita é efetuada por dois visitantes, deve ser utilizado o anexo 2.
13. **THE SECURITY OFFICER OF THE REQUESTING ENTITY**	Este ponto diz respeito ao nome, números de telefone e de fax, bem como ao endereço de correio eletrónico do responsável da segurança da instalação requerente.
14. **CERTIFICATION OF SECURITY CLEARANCE**	Este campo deve ser preenchido pela autoridade de certificação. Notas relativas à autoridade de certificação: a. Indicar o nome, endereço, número de telefone, número de fax e endereço de correio eletrónico (pode ser pré-impresso). b. Este ponto deve ser assinado e carimbado (se aplicável).
15. **REQUESTING SECURITY AUTHORITY**	Este campo deve ser preenchido pela ANS/ASD. Nota para a ANS/ASD: a. Indicar o nome, endereço, número de telefone, número de fax e endereço de correio eletrónico (pode ser pré-impresso). b. Este ponto deve ser assinado e carimbado (se aplicável).

Devem ser preenchidos todos os campos e o formulário deve ser apresentado através de canais intergovernamentais ([9]).

PEDIDO DE VISITA

(MODELO)

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

([9]) Se tiver sido acordado que as visitas que impliquem o acesso efetivo ou potencial a ICUE de nível CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET podem ser organizadas diretamente, o formulário preenchido pode ser apresentado diretamente ao responsável de segurança do estabelecimento a visitar.

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:

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE:

STAMP

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)*:**

<Espaço reservado para a referência à legislação aplicável em matéria de dados pessoais e para a hiperligação para as informações obrigatórias para o titular dos dados, por exemplo, de que forma é aplicado o artigo 13.º do Regulamento Geral sobre a Proteção de Dados ([10]).>

([10]) Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1).

ANEXO 1 do FORMULÁRIO DE PDV

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)***

<Espaço reservado para a referência à legislação aplicável em matéria de dados pessoais e para a hiperligação para as informações obrigatórias para o titular dos dados, por exemplo, de que forma é aplicado o artigo 13.º do Regulamento Geral sobre a Proteção de Dados ([11]).>

([11]) Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1).

ANEXO 2 do FORMULÁRIO DE PDV

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)***

<Espaço reservado para a referência à legislação aplicável em matéria de dados pessoais e para a hiperligação para as informações obrigatórias para o titular dos dados, por exemplo, de que forma é aplicado o artigo 13.º do Regulamento Geral sobre a Proteção de Dados ([12]).>

([12]) Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1).

APÊNDICE D

FICHA DE INFORMAÇÃO DA CREDENCIAÇÃO DE SEGURANÇA DA EMPRESA (FICSE) (MODELO)

1. **INTRODUÇÃO**

1.1. É apenso um modelo de Ficha de Informação de Credenciação de Segurança da Empresa (FICSE) que permite um rápido intercâmbio de informações entre a autoridade nacional de segurança (ANS) ou a autoridade de segurança designada (ASD), outras autoridades nacionais de segurança competentes e a autoridade de segurança da Comissão (que atua em nome das autoridades que concedem as subvenções) no que respeita à credenciação de segurança da empresa (CSE) de uma instalação que intervém nas candidaturas relativas a convenções de subvenção classificadas ou a subcontratos classificados e na sua execução.

1.2. A FICSE só é válida quando carimbada pela ANS, a ASD ou outra autoridade competente.

1.3. A FICSE está dividida numa secção de pedido e numa secção de resposta e pode ser utilizada para os fins supramencionados ou para quaisquer outros fins para os quais seja necessário o estatuto de CSE de uma determinada instalação. O motivo do pedido deve ser indicado pela ANS ou ASD requerente no campo 7 da secção de pedido.

1.4. Os dados contidos na FICSE não são normalmente classificados; por conseguinte, quando do envio de uma FICSE entre as ANS/ASD/Comissão, é preferível fazê-lo por via eletrónica.

1.5. As ANS/ASD devem envidar todos os esforços para responder a um pedido de FICSE no prazo de dez dias úteis.

1.6. No caso de transferência de informações classificadas ou de concessão de uma subvenção ou de um subcontrato relacionado com essa garantia, a ANS ou ASD emissora deve ser informada.

Procedimentos e instruções para a utilização da Ficha de Informação de Credenciação de Segurança da Empresa (FICSE)

Estas instruções pormenorizadas destinam-se à ANS ou ASD, ou à autoridade que concede a subvenção e à autoridade de segurança da Comissão que preenchem a FICSE. O pedido deve, de preferência, ser datilografado em maiúsculas.

CABEÇALHO	O requerente insere a designação completa da ANS/ASD e o nome do país.
1. **TIPO DE PEDIDO**	A autoridade que concede a subvenção requerente seleciona a caixa adequada para o tipo de pedido de FICSE. Indicar o nível de credenciação de segurança solicitado. Devem ser utilizadas as seguintes abreviaturas: SECRET UE/EU SECRET = S-UE/EU-S CONFIDENTIEL UE/EU CONFIDENTIAL = C-UE/EU-C CIS = Sistemas de comunicação e informação para o tratamento de informações classificadas
2. **INFORMAÇÕES SOBRE O ASSUNTO**	Os campos 1 a 6 não necessitam de explicação. No campo 4 deve ser utilizado o código de país normalizado de duas letras. O campo 5 é facultativo.
3. **MOTIVO DO PEDIDO**	Indicar o motivo específico do pedido, os indicadores de projeto e o número do convite à apresentação de propostas ou da subvenção. Especificar as necessidades em matéria de capacidade de armazenamento, nível de classificação do SCI, etc. Devem ser indicados os prazos/ as datas de termo/ as datas de concessão que possam ter uma incidência na finalização de uma CSE.

4. **ANS/ASD REQUERENTE**	Indicar o nome do requerente efetivo (em nome da ANS/ASD) e a data do pedido em formato numérico (dd/mm/aaaa).
5. **SECÇÃO DE RESPOSTA**	Campos 1-5: selecionar os campos adequados. Campo 2: se estiver em curso uma CSE, recomenda-se que seja dada ao requerente uma indicação do tempo necessário para o tratamento (se conhecido). Campo 6: a) Embora a validação seja diferente consoante o país ou até mesmo consoante a instalação, recomenda-se que seja indicada a data de termo da CSE. b) Nos casos em que a data de termo da garantia CSE seja indeterminada, este campo pode ser riscado. c) Em conformidade com as respetivas regras e regulamentos nacionais, o requerente, ou o beneficiário ou subcontratante, é responsável pela apresentação de um pedido de renovação da CSE.
6. **OBSERVAÇÕES**	Podem ser utilizadas para fornecer informações adicionais no que diz respeito à CSE, à instalação ou aos elementos supramencionados.
7. **ANS/ASD EMISSORA**	Indicar o nome da autoridade emissora (em nome da ANS/ASD) e a data da resposta em formato numérico (dd/mm/aaaa).

FICHA DE INFORMAÇÃO DA CREDENCIAÇÃO DE SEGURANÇA DA EMPRESA (FICSE) (MODELO)

Devem ser preenchidos todos os campos, e o formulário deve ser enviado através de canais intergovernamentais ou canais entre administrações públicas e organizações internacionais.

PEDIDO DE GARANTIA DA CREDENCIAÇÃO DE SEGURANÇA DA EMPRESA

À ATENÇÃO DE: _____

(nome do país da ANS/ASD)

Preencher as caixas de resposta, quando aplicável:

[ ] Fornecer uma garantia CSE ao nível de: [ ] S-UE/EU-S [ ] C-UE/EU-C

para a instalação abaixo

[ ] Incluindo a salvaguarda de material/informações classificados

[ ] Incluindo sistemas de comunicação e informação (SCI) para o tratamento de informações classificadas

[ ] Iniciar, diretamente ou a pedido de um beneficiário ou subcontratante, o processo de obtenção de uma CSE até ao nível de ....., inclusive, com nível de salvaguarda ..... e nível de SCI ....., se a instalação não dispuser atualmente desses níveis de capacidades.

Confirmar a exatidão dos dados da instalação a seguir enumerados e apresentar correções/aditamentos se necessário.

1. Nome completo da instalação: Correções/Aditamentos:

....

2. Endereço completo da instalação:

....

3. Endereço postal (se diferente do indicado no ponto 2)

....

4. Zip/código postal/cidade/país

....

5. Nome do responsável de segurança

.....
.....

6. N.º de telefone/n.º de fax/endereço de correio eletrónico do responsável de segurança

....

7. O presente pedido é apresentado pelo(s) motivo(s) a seguir indicado(s): [fornecer informações sobre a fase pré-contratual (seleção de propostas), a subvenção ou o subcontrato, o programa/projeto, etc.]

.....

ANS/ASD /autoridade que concede a subvenção requerente: Nome: ..... Data: (dd/mm/aaaa) .....

RESPOSTA (no prazo de dez dias úteis)

Certifica-se que:

1. [ ] A referida instalação dispõe de uma CSE até ao nível de [ ] S-UE/EU-S, inclusive.

   [ ] C-UE/EU-C.

2. A referida instalação tem capacidade para salvaguardar informações/material classificados:

   [ ] sim, nível: ..... [ ] não.

3. A instalação supramencionada dispõe de um SCI acreditado/autorizado:

   [ ] sim, nível: ..... [ ] não.

4. [ ] em relação ao pedido supramencionado, foi iniciado o processo de CSE. Será informado quando a CSE tiver sido aprovada ou recusada.

5. [ ] a instalação acima referida não dispõe de uma CSE.

6. Esta garantia de CSE termina na seguinte data: ..... (*dd/mm/aaaa*), ou conforme recomendação da ANS/ASD. Será informado em caso de invalidação antecipada ou de alterações às informações supramencionadas.

7. Observações:
   .....

ANS/ASD emissora Nome: ..... *Data (dd/mm/aaaa):* .....

<Espaço reservado para a referência à legislação aplicável em matéria de dados pessoais e para a hiperligação para as informações obrigatórias para o titular dos dados, por exemplo, de que forma é aplicado o artigo 13.º do Regulamento Geral sobre a Proteção de Dados ([13]).>

([13]) Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1).

Apêndice E

Requisitos mínimos para a proteção de ICUE em formato eletrónico do nível RESTREINT UE/EU RESTRICTED manuseadas no SCI do beneficiário

Considerações gerais

1. Cabe ao beneficiário assegurar que a proteção de informações RESTREINT UE/EU RESTRICTED cumpra os requisitos mínimos de segurança estabelecidos nesta cláusula de segurança, bem como quaisquer outros requisitos adicionais aconselhados pela autoridade que concede a subvenção ou, se aplicável, pela autoridade nacional de segurança (ANS) ou pela autoridade de segurança designada (ASD).

2. O beneficiário é responsável pelo cumprimento dos requisitos de segurança identificados no presente documento.

3. Para fins do presente documento, um sistema de comunicação e informação (SCI) abrange todos os equipamentos utilizados para o manuseamento, armazenamento e transmissão de ICUE, incluindo estações de trabalho, impressoras, fotocopiadoras, copiadoras, máquinas de fax, servidores, sistemas de gestão de rede, controladores de rede e controladores de comunicações, computadores portáteis, *notebooks*, tabletes, telemóveis inteligentes e suportes de armazenamento amovíveis, como chaves USB, CD, cartões SD, etc.

4. Os equipamentos especiais, como produtos criptográficos, devem ser protegidos em conformidade com os seus procedimentos operacionais de segurança (POS) específicos.

5. Os beneficiários devem estabelecer uma estrutura responsável pela gestão da segurança dos SCI que manuseiam informações com classificação RESTREINT UE/EU RESTRICTED e nomear um responsável de segurança da instalação em causa.

6. Não é autorizada, para fins de armazenamento ou tratamento de informações RESTREINT UE/EU RESTRICTED, a utilização de soluções informáticas (*hardware*, *software* ou serviços) que sejam propriedade do pessoal do beneficiário.

7. A acreditação do SCI do beneficiário que manuseia informações com a classificação RESTREINT UE/EU RESTRICTED deve ser aprovada pela autoridade de acreditação de segurança (AAS) do Estado-Membro em causa ou delegada no responsável de segurança do beneficiário, em conformidade com as disposições legislativas e regulamentares nacionais.

8. Só as informações com classificação RESTREINT UE/EU RESTRICTED encriptadas com produtos criptográficos aprovados podem ser manuseadas, armazenadas ou transmitidas (por ligações com ou sem fios) como qualquer outra informação não classificada no âmbito da convenção de subvenção. Esses produtos criptográficos devem ser aprovados pela UE ou por um Estado-Membro.

9. As instalações externas envolvidas em trabalhos de manutenção/reparação devem estar contratualmente obrigadas a cumprir as disposições aplicáveis ao manuseamento de informações com classificação RESTREINT UE/EU RESTRICTED, conforme estabelecido no presente documento.

10. A pedido da autoridade que concede a subvenção ou da ANS, ASD ou AAS competente, o beneficiário deve fornecer provas da conformidade com a cláusula de segurança da convenção de subvenção. Caso seja também solicitada a realização de uma auditoria e inspeção dos processos e instalações do beneficiário por forma a assegurar o cumprimento desses requisitos, os beneficiários devem autorizar os representantes da autoridade que concede a subvenção, a ANS, ASD e/ou SAA, ou a autoridade de segurança da UE competente a proceder a essa auditoria e inspeção.

Segurança física

11. Os espaços em que os SCI são utilizados para visualizar, armazenar, tratar ou transmitir informações RESTREINT UE/EU RESTRICTED ou os espaços onde estão instalados os servidores, os sistemas de gestão de rede, os controladores de rede e os controladores de comunicações para os referidos SCI devem ser estabelecidos como zonas separadas e controladas, com um sistema de controlo de acesso adequado. O acesso a estas zonas separadas e controladas deve ser limitado às pessoas com autorização específica. Sem prejuízo do disposto no n.º 8, o equipamento descrito no n.º 3 deve ser armazenado nessas zonas separadas e controladas.

12. Devem ser implementados mecanismos e/ou procedimentos de segurança a fim de regulamentar a instalação ou ligação de suportes informáticos amovíveis (como chaves USB, dispositivos de armazenamento maciço de dados ou CD-RW) a componentes do SCI.

Acesso ao SCI

13. É permitido o acesso ao SCI de um beneficiário que manuseie ICUE segundo o princípio da estrita necessidade de tomar conhecimento e com base numa autorização concedida ao pessoal.

14. Todos os SCI devem dispor de listas atualizadas dos utilizadores autorizados. Todos os utilizadores devem ser autenticados no início de cada sessão de tratamento.

15. As senhas, que fazem parte da maioria das medidas de segurança de identificação e autenticação, devem ter pelo menos nove carateres e incluir carateres numéricos e carateres «especiais» (se o sistema o permitir), bem como carateres alfabéticos. As senhas devem ser alteradas pelo menos de 180 em 180 dias. Devem ser alteradas o mais rapidamente possível se tiverem sido comprometidas ou divulgadas a uma pessoa não autorizada ou se houver suspeitas de tal comprometimento ou divulgação.

16. Todos os SCI devem ter controlos internos de acesso para impedir que utilizadores não autorizados acedam ao sistema ou modifiquem informações com a classificação RESTREINT UE/EU RESTRICTED e modifiquem os controlos de segurança e os controlos do sistema. Os utilizadores devem ser automaticamente desligados do SCI se os seus terminais estiverem inativos durante um período predeterminado ou o SCI deve ativar um economizador de ecrã protegido por senha após 15 minutos de inatividade.

17. A cada utilizador do SCI é atribuída uma conta de utilizador única e uma identificação única. As contas de utilizador devem ser automaticamente bloqueadas quando são efetuadas, pelo menos, cinco tentativas incorretas de acesso sucessivas.

18. Todos os utilizadores do SCI devem ser informados das suas responsabilidades e dos procedimentos a seguir para fins de proteção das informações com classificação RESTREINT UE/EU RESTRICTED no SCI. As responsabilidades e os procedimentos a seguir devem ser documentados e reconhecidos por escrito pelos utilizadores.

19. Devem estar ao dispor dos utilizadores e administradores procedimentos operacionais de segurança, que devem incluir descrições das funções de segurança e a lista associada de tarefas, instruções e planos.

Contabilização, auditoria e resposta a incidentes

20. Devem ser registados todos os acessos ao SCI.

21. Devem ser registados os seguintes eventos:

    a) Todas as tentativas de início de sessão, com ou sem sucesso;

    b) Encerramento de sessão (incluindo, quando aplicável, por inatividade);

    c) Criação, supressão ou alteração de direitos de acesso e privilégios;

    d) Criação, supressão ou alteração de senhas.

22. Relativamente a todos os eventos supramencionados, devem ser comunicadas, no mínimo, as seguintes informações:

    a) Tipo de evento;

    b) Identificação do utilizador;

    c) Data e hora;

    d) Identificação do dispositivo.

23. Os registos devem ajudar o responsável de segurança no exame dos potenciais incidentes de segurança. Podem também ser utilizados para apoiar inquéritos judiciais em caso de incidente de segurança. Todos os registos de segurança devem ser regularmente verificados a fim de detetar potenciais incidentes de segurança. Os registos devem ser protegidos contra eliminação ou alteração não autorizadas.

24. O beneficiário deve dispor de uma estratégia de resposta consolidada para fazer face a incidentes de segurança. Os utilizadores e administradores devem receber instruções sobre a forma de responder a incidentes, de os comunicar e de atuar face a uma emergência.

25. O comprometimento ou a suspeita de comprometimento de informações com classificação RESTREINT UE/EU RESTRICTED devem ser comunicados à autoridade que concede a subvenção. O relatório deve conter uma descrição das informações em causa e uma descrição das circunstâncias do comprometimento ou da suspeita de comprometimento. Todos os utilizadores do SCI devem ser informados sobre a forma de comunicar ao responsável de segurança eventuais incidentes ou suspeita de incidentes.

Ligação em rede e interligação

26. Quando o SCI de um beneficiário que manuseia informações com a classificação RESTREINT UE/EU RESTRICTED está interligado a um SCI que não está acreditado, tal aumenta significativamente a ameaça tanto à segurança do SCI como às informações RESTREINT UE/EU RESTRICTED manuseadas por esse SCI. É o caso da Internet e de outros SCI públicos ou privados, como outros SCI pertencentes ao beneficiário ou ao subcontratante. Nesse caso, o beneficiário deve efetuar uma avaliação dos riscos a fim de identificar os requisitos de segurança adicionais que devem ser aplicados no âmbito do processo de acreditação de segurança. O beneficiário deve fornecer à autoridade que concede a subvenção e, se as disposições legislativas e regulamentares nacionais o exigirem, à AAS competente uma declaração de conformidade que certifique que o SCI do beneficiário e as interligações conexas foram acreditados para o manuseamento de ICUE do nível RESTREINT UE/EU RESTRICTED.

27. É proibido o acesso remoto a serviços LAN a partir de outros sistemas (por exemplo, acesso remoto a correio eletrónico e apoio remoto ao sistema) a menos que sejam implementadas medidas de segurança especiais acordadas pela autoridade que concede a subvenção e, quando exigido pelas disposições legislativas e regulamentares nacionais, que estas sejam aprovadas pela AAS competente.

Gestão da configuração

28. Deve estar disponível e ser objeto de manutenção regular uma configuração pormenorizada do *hardware* e *software*, conforme estabelecida na documentação de acreditação/aprovação (incluindo diagramas de sistema e de rede).

29. O responsável de segurança do beneficiário deve proceder a verificações da configuração do *hardware* e do *software*, a fim de garantir que não foi instalado *hardware* ou *software* não autorizado.

30. As alterações à configuração do SCI do beneficiário devem ser avaliadas em função das suas implicações em termos de segurança e devem ser aprovadas pelo responsável de segurança e, quando exigido pelas disposições legislativas e regulamentares nacionais, pela AAS.

31. O sistema deve ser analisado, pelo menos uma vez por trimestre, a fim de detetar eventuais vulnerabilidades de segurança. Deve ser instalado e regularmente atualizado *software* para detetar *software* malicioso. Se possível, esse *software* deve ser objeto de uma aprovação nacional ou de uma aprovação reconhecida a nível internacional; caso contrário deve corresponder a uma norma amplamente aceite no setor.

32. O beneficiário deve elaborar um plano de continuidade das atividades. Devem ser estabelecidos procedimentos de salvaguarda no que diz respeito aos seguintes aspetos:

    a) Frequência das cópias de segurança;

    b) Requisitos de armazenamento no local (contentores à prova de fogo) ou fora do local;

    c) Controlo do acesso autorizado a cópias de segurança.

Limpeza definitiva e destruição de dados

33. No caso de SCI ou de suportes de armazenamento de dados que tenham contido, em qualquer momento, informações com a classificação RESTREINT UE/EU RESTRICTED, deve ser efetuada a seguinte limpeza definitiva de todo o sistema ou dos suportes de armazenamento antes da sua eliminação:

    a) As memórias *flash* (por exemplo, chaves USB, cartões SD, unidades de estado sólido, discos rígidos híbridos), devem ser sujeitas a um processo de reescrita de dados sobre dados, pelo menos, três vezes e em seguida verificadas a fim de garantir que o conteúdo original não possa ser recuperado, ou ser limpas utilizando um *software* de eliminação de dados aprovado;

    b) Os suportes magnéticos (por exemplo, discos rígidos) devem ser sujeitos a um processo de reescrita de dados sobre dados ou desmagnetizados;

    c) Os suportes óticos (por exemplo, CD e DVD) devem ser triturados ou desintegrados;

    d) Quanto a outros suportes de armazenamento, a autoridade que concede a subvenção ou, quando adequado, a ANS, ASD ou AAS, devem ser consultadas sobre os requisitos de segurança a cumprir.

34. Todos os suportes de armazenamento de dados que contenham informações com classificação RESTREINT UE/EU RESTRICTED devem ser objeto de limpeza definitiva antes de serem entregues a uma entidade que não esteja autorizada a aceder a informações com classificação RESTREINT UE/EU RESTRICTED (por exemplo, para trabalhos de manutenção).

ANEXO IV

Credenciação de segurança do pessoal e da empresa para beneficiários ou subcontratantes que manuseiem informações com classificação RESTREINT UE/EU RESTRICTED e ANS/ASD que exigem a notificação de convenções de subvenção classificadas de nível RESTREINT UE/EU RESTRICTED [1]

Estado-Membro	CSE		Notificação à ANS e/ou ASD de uma convenção de subvenção ou subcontrato que implique informações R-UE/EU-R		CSP	
	SIM	NÃO	SIM	NÃO	SIM	NÃO
Bélgica		**X**		**X**		**X**
Bulgária		**X**		**X**		**X**
Chéquia		**X**		**X**		**X**
Dinamarca	**X**		**X**		**X**	
Alemanha		**X**		**X**		**X**
Estónia	**X**		**X**			**X**
Irlanda		**X**		**X**		**X**
Grécia	**X**			**X**	**X**	
Espanha		**X**	**X**			**X**
França		**X**		**X**		**X**
Croácia		**X**	**X**			**X**
Itália		**X**	**X**			**X**
Chipre		**X**	**X**			**X**
Letónia		**X**		**X**		**X**
Lituânia	**X**		**X**			**X**
Luxemburgo	**X**		**X**		**X**	
Hungria		**X**		**X**		**X**
Malta		**X**		**X**		**X**
Países Baixos	**X** (apenas para convenções de subvenção e subcontratos relacionados com a defesa)		**X** (apenas para convenções de subvenção e subcontratos relacionados com a defesa)			**X**
Áustria		**X**		**X**		**X**
Polónia		**X**		**X**		**X**

[1] Estes requisitos nacionais aplicáveis às CSE/CSP e às notificações relativas a convenções de subvenção que impliquem o manuseamento de informações RESTREINT UE/EU RESTRICTED não devem impor obrigações adicionais a outros Estados-Membros ou beneficiários e subcontratantes sob a sua jurisdição.
N.B.: as notificações de convenções de subvenção que impliquem informações CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET são obrigatórias.

Portugal		**X**		**X**		**X**
Roménia		**X**		**X**		**X**
Eslovénia	**X**		**X**			**X**
Eslováquia	**X**		**X**			**X**
Finlândia		**X**		**X**		**X**
Suécia		**X**		**X**		**X**

ANEXO V

LISTA DAS AUTORIDADES NACIONAIS DE SEGURANÇA / SERVIÇOS DAS AUTORIDADES DE SEGURANÇA DESIGNADAS RESPONSÁVEIS PELO TRATAMENTO DOS PROCEDIMENTOS RELATIVOS À SEGURANÇA INDUSTRIAL

BÉLGICA

Autorité nationale de Sécurité
SPF Affaires étrangères
Rue des Petits Carmes 15
1000 Bruxelas

Tel. +32 25014542 (secretariado)

Fax +32 25014596

Endereço de correio eletrónico: nvo-ans@diplobel.fed.be

BULGÁRIA

1. State Commission on Information Security – National Security Authority
   4 Kozloduy Street
   1202 Sófia
   Tel. +359 29835775
   Fax +359 29873750
   Endereço de correio eletrónico: dksi@government.bg

2. Defence Information Service at the Ministry of Defence (security service)
   3 Dyakon Ignatiy Street
   1092 Sófia
   Tel. +359 29227002
   Fax +359 29885211
   Endereço de correio eletrónico: office@iksbg.org

3. State Intelligence Agency (security service)
   12 Hajdushka Polyana Street
   1612 Sófia
   Tel. +359 29813221
   Fax +359 29862706
   Endereço de correio eletrónico: office@dar.bg

4. State Agency for Technical Operations (security service)
   29 Shesti Septemvri Street
   1000 Sófia
   Tel. +359 29824971
   Fax +359 29461339
   Endereço de correio eletrónico: dato@dato.bg

(As autoridades competentes acima enumeradas executam os procedimentos de verificação aplicáveis à emissão de CSE a entidades jurídicas que se candidatem à celebração de um contrato classificado, e de CSP a pessoas singulares que executam um contrato classificado para satisfazer as necessidades dessas autoridades.)

5. State Agency National Security (security service)

   45 Cherni Vrah Blvd.

   1407 Sófia

   Tel. +359 28147109

   Fax +359 29632188, +359 28147441

   Endereço de correio eletrónico: dans@dans.bg

(O serviço de segurança supramencionado executa os procedimentos de verificação aplicáveis à emissão de CSE e CSP a todas as outras entidades jurídicas e pessoas singulares no país que sejam candidatas à celebração de um contrato classificado ou de uma convenção de subvenção classificada ou à execução de um contrato classificado ou de uma convenção de subvenção classificada.)

CHÉQUIA

National Security Authority
Industrial Security Department
PO BOX 49
150 06 Praga 56

Tel. +420 257283129

Endereço de correio eletrónico: sbr@nbu.cz

DINAMARCA

1. Politiets Efterretningstjeneste
   [Serviço de Informações de Segurança da Dinamarca]

   Klausdalsbrovej 1

   2860 Søborg

   Tel. +45 33148888

   Fax +45 33430190

2. Forsvarets Efterretningstjeneste
   [Serviço de Informações de Defesa da Dinamarca]
   Kastellet 30
   2100 Copenhaga Ø

   Tel. +45 33325566

   Fax +45 33931320

ALEMANHA

1. Para questões relativas à política de segurança industrial, CSE, planos de transporte (exceto para cripto/CCI):
   Federal Ministry for Economic Affairs and Energy

   Industrial Security Division - RS3

   Villemombler Str. 76

   53123 Bona

   Tel. +49 228996154028

   Fax +49 228996152676

   Endereço de correio eletrónico: dsagermany-rs3@bmwi.bund.de (endereço eletrónico do serviço)

2. Para pedidos de visita normalizados de/a empresas alemãs:

Federal Ministry for Economic Affairs and Energy

Industrial Security Division – RS2
Villemombler Str. 76
53123 Bona

Tel. +49 228996152401

Fax +49 228996152603

Endereço de correio eletrónico: rs2-international@bmwi.bund.de (endereço eletrónico do serviço)

3. Planos de transporte para material criptográfico:

Federal Office for Information Security (BSI)
National Distribution Agency / NDA-EU DEU
Mainzer Str. 84
53179 Bona

Tel. +49 2289995826052

Fax +49 228991095826052

Endereço de correio eletrónico: NDAEU@bsi.bund.de

ESTÓNIA

National Security Authority Department
Estonian Foreign Intelligence Service
Rahumäe tee 4B
11316 Taline

Tel. +372 6939211

Fax +372 6935001

Endereço de correio eletrónico: nsa@fis.gov.ee

IRLANDA

National Security Authority Ireland
Department of Foreign Affairs and Trade
76-78 Harcourt Street
Dublim 2
D02 DX45

Tel. +353 14082724

Endereço de correio eletrónico: nsa@dfa.ie

GRÉCIA

Hellenic National Defence General Staff
E' Division (Security INTEL, CI BRANCH)
E3 Directorate
Industrial Security Office
227-231 Mesogeion Avenue
15561 Holargos, Atenas

Tel. +30 2106572022, +30 2106572178

Fax +30 2106527612

Endereço de correio eletrónico: daa.industrial@hndgs.mil.gr

ESPANHA

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Calle Argentona 30
28023 Madrid

Tel. +34 912832583, +34 912832752, +34 913725928

Fax +34 913725808

Endereço de correio eletrónico: nsa-sp@areatec.com

Para informações relativas a programas classificados: programas.ons@areatec.com

Para questões relativas à credenciação de segurança do pessoal: hps.ons@areatec.com

Para planos de transporte e visitas internacionais: sp-ivtco@areatec.com

FRANÇA

Autoridade Nacional de Segurança (ANS) (para questões de política e de execução noutros domínios que não a indústria da defesa)
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

Endereço de correio eletrónico: ANSFrance@sgdsn.gouv.fr

Autoridade de Segurança Designada (para a execução na indústria da defesa)
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

Endereço de correio eletrónico: para formulários e PDV saídos: dga-ssdi.ai.fct@intradef.gouv.fr

para PDV entrados: dga-ssdi.visit.fct@intradef.gouv.fr

CROÁCIA

Office of the National Security Council
Croatian NSA
Jurjevska 34
10000 Zagrebe

Tel. +385 14681222

Fax +385 14686049

Endereço de correio eletrónico: NSACroatia@uvns.hr

ITÁLIA

Presidenza del Consiglio dei Ministri
D.I.S. - U.C.Se.
Via di Santa Susanna 15
00187 Roma

Tel. +39 0661174266

Fax +39 064885273

CHIPRE

ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Λεωφόρος Στροβόλου, 172-174
Στρόβολος, 2048, Λευκωσία

Τηλέφωνα: +357 22807569, +357 22807764

Τηλεομοιότυπο: +357 22302351

Endereço de correio eletrónico: cynsa@mod.gov.cy

Ministry of Defence
National Security Authority (NSA)
172-174, Strovolos Avenue
2048 Strovolos, Nicósia

Tel. +357 22807569, +357 22807764

Fax +357 22302351

Endereço de correio eletrónico: cynsa@mod.gov.cy

LETÓNIA

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

Endereço de correio eletrónico: ndi@sab.gov.lv, ndi@zd.gov.lv

LITUÂNIA

Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(Comissão para a Coordenação da Proteção dos Segredos da República da Lituânia)
National Security Authority
Pilaitės pr. 19
LT-06264 Vílnius

Tel. +370 70666128

Endereço de correio eletrónico: nsa@vsd.lt

LUXEMBURGO

Autorité Nationale de Sécurité
207, route d'Esch
L-1471 Luxemburgo

Tel. +352 24782210

Endereço de correio eletrónico: ans@me.etat.lu

HUNGRIA

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

Endereço de correio eletrónico: 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

Endereço de correio eletrónico: certification@mccaa.org.mt

PAÍSES BAIXOS

1. Ministry of the Interior and Kingdom Relations

   PO Box 20010
   2500 EA Den Haag

   Tel. +31 703204400

   Fax +31 703200733

   Endereço de correio eletrónico: nsa-nl-industry@minbzk.nl

2. Ministry of Defence

   Industrial Security Department

   PO Box 20701
   2500 ES Den Haag

   Tel. +31 704419407

   Fax +31 703459189

   Endereço de correio eletrónico: indussec@mindef.nl

ÁUSTRIA

1. Federal Chancellery of Austria
   Department I/10, Federal Office for Information Security

   Ballhausplatz 2
   10104 Viena

   Tel. +43 153115202594

   Endereço de correio eletrónico: isk@bka.gv.at

2. ASD no domínio militar:
   BMLV/Abwehramt

   Postfach 2000
   1030 Viena

   Endereço de correio eletrónico: abwa@bmlvs.gv.at

POLÓNIA

Internal Security Agency
Department for the Protection of Classified Information
Rakowiecka 2A
00-993 Varsóvia

Tel. +48 225857944

Fax +48 225857443

Endereço de correio eletrónico: nsa@abw.gov.pl

PORTUGAL

Gabinete Nacional de Segurança
Serviço de Segurança Industrial
Rua da Junqueira, n.º 69
1300-342 Lisboa

Tel. +351 213031710

Fax +351 213031711

Endereço de correio eletrónico: sind@gns.gov.pt, franco@gns.gov.pt

ROMÉNIA

Oficiul Registrului Național al Informațiilor Secrete de Stat - ORNISS
[ANS romena: ORNISS - Gabinete Nacional de Registo de Informações Classificadas]
4th Mures Street
012275 Bucareste

Tel. +40 212075115

Fax +40 212245830

Endereço de correio eletrónico: relatii.publice@orniss.ro, nsa.romania@nsa.ro

ESLOVÉNIA

Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
1000 Liubliana

Tel. +386 14781390

Fax +386 14781399

Endereço de correio eletrónico: gp.uvtp@gov.si

ESLOVÁQUIA

Národný bezpečnostný úrad
(Autoridade Nacional de Segurança)
Security Clearance Department
Budatínska 30
851 06 Bratislava

Tel. +421 268691111

Fax +421 268691700

Endereço de correio eletrónico: podatelna@nbu.gov.sk

FINLÂNDIA

National Security Authority
Ministry for Foreign Affairs
P.O. Box 453
FI-00023 Government

Endereço de correio eletrónico: NSA@formin.fi

SUÉCIA

1. National Security Authority

   Utrikesdepartementet (Ministério dos Negócios Estrangeiros)
   UD SÄK / NSA
   SE-103 39 Estocolmo
   Tel. +46 84051000
   Fax +46 87231176
   Endereço de correio eletrónico: ud-nsa@gov.se

2. ASD

   Försvarets Materielverk [Administração do Equipamento de Defesa da Suécia]
   FMV Säkerhetsskydd
   SE-115 88 Estocolmo
   Tel. +46 87824000
   Fax +46 87826900
   Endereço de correio eletrónico: security@fmv.se