II

(Atos não legislativos)

DECISÕES

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

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 a Decisão (UE, Euratom) 2015/443 da Comissão, de 13 de março de 2015, relativa à segurança na Comissão ([1]),

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 ([2]),

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 ([3]),

Considerando o seguinte:

(1) A Decisão (UE, Euratom) 2015/444 é aplicável a todos os serviços e em todas as instalações da Comissão.

(2) As medidas de segurança destinadas a proteger as informações classificadas da UE (a seguir designadas ICUE) ao longo do seu ciclo de vida devem ser proporcionais, em particular, à sua classificação de segurança.

(3) O artigo 4.º, n.º 3, o artigo 19.º, n.º 1, alínea c), e o artigo 22.º da Decisão (UE, Euratom) 2015/444 preveem a adoção de disposições mais pormenorizadas para completar e apoiar a aplicação da referida decisão através de regras de execução que regulem questões como o guia de classificação, as medidas de compensação para o manuseamento de ICUE fora de uma Zona de Segurança ou de uma Zona Administrativa e as responsabilidades da entidade de origem.

(4) Se necessário, devem ser adotadas regras de execução para completar ou apoiar a Decisão (UE, Euratom) 2015/444, em conformidade com o artigo 60.º da mesma decisão.

(5) As medidas de segurança adotadas para dar cumprimento à presente decisão devem respeitar os princípios de segurança da Comissão estabelecidos no artigo 3.º da Decisão (UE, Euratom) 2015/443.

(6) 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 ([4]).

(7) Em 4 de maio de 2016, a Comissão adotou uma decisão ([5]) 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,

([1]) JO L 72 de 17.3.2015, p. 41.
([2]) JO L 72 de 17.3.2015, p. 53.
([3]) JO L 6 de 11.1.2017, p. 40.
([4]) 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).
([5]) Decisão da Comissão, de 4 de maio de 2016, relativa a uma habilitação relativa à segurança [C(2016) 2797 final].

ADOTOU A PRESENTE DECISÃO:

CAPÍTULO 1

DISPOSIÇÕES GERAIS

Artigo 1.º

Objeto e âmbito de aplicação

1. A presente decisão estabelece as condições de manuseamento das informações classificadas da UE (ICUE) de nível CONFIDENTIEL UE/EU CONFIDENTIAL ([6]) e SECRET UE/EU SECRET ([7]), em conformidade com a Decisão (UE, Euratom) 2015/444.

2. A presente decisão é aplicável a todos os serviços e em todas as instalações da Comissão.

Artigo 2.º

Critérios de acesso às informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET

1. Pode ser concedido acesso a informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET após:

a) Ter sido determinada a necessidade de uma pessoa ter acesso a certas informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET para poder desempenhar funções ou realizar tarefas profissionais para a Comissão Europeia;

b) A pessoa em causa ter sido informada das regras e das normas de segurança aplicáveis e das orientações para a proteção das informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET;

c) A pessoa em causa ter reconhecido as suas responsabilidades em matéria de proteção das informações em causa; e

d) A pessoa em causa ter sido autorizada pela autoridade de segurança da Comissão a aceder a ICUE até ao nível adequado e até uma data especificada, em conformidade com o artigo 10.º, n.º 1, ponto 3, da Decisão (UE, Euratom) 2015/444.

2. Não devem ser confiadas aos estagiários da Comissão tarefas que requeiram acesso a informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET.

3. O acesso a essas informações por parte de outras categorias de pessoal deve ser recusado ou permitido em conformidade com o quadro constante do anexo.

CAPÍTULO 2

PRODUÇÃO DE INFORMAÇÕES COM CLASSIFICAÇÃO CONFIDENTIEL UE/EU CONFIDENTIAL E SECRET UE/EU SECRET

Artigo 3.º

Entidade de origem

Embora a entidade de origem, na aceção do artigo 1.º da Decisão (UE, Euratom) 2015/444, seja a instituição, agência ou organismo da União, o Estado-Membro, o Estado terceiro ou a organização internacional sob cuja autoridade tenham sido produzidas e/ou introduzidas nas estruturas da União informações classificadas, o redator de informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET não é necessariamente o mesmo.

([6]) Nos termos do artigo 3.º da Decisão (UE, Euratom) 2015/444, por informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL entende-se «informações e material cuja divulgação não autorizada possa prejudicar os interesses essenciais da União Europeia ou de um ou mais Estados-Membros».

([7]) Nos termos do artigo 3.º da Decisão (UE, Euratom) 2015/444, por informações com classificação SECRET UE/EU SECRET entende-se «informações e material cuja divulgação não autorizada possa prejudicar seriamente os interesses essenciais da União Europeia ou de um ou mais Estados-Membros».

Artigo 4.º

Atribuição de um nível de classificação

1. O pessoal que elabora um documento com base em informações na aceção do artigo 1.º deve ponderar sempre se o documento precisa de ser classificado. A classificação de um documento como ICUE implica uma avaliação e uma decisão da entidade de origem quanto à questão de saber se a divulgação do documento a pessoas não autorizadas causaria prejuízo aos interesses da União Europeia ou de um ou mais Estados-Membros. Se os autores tiverem dúvidas sobre a necessidade de o documento que estão a redigir receber a classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET, devem consultar o chefe de unidade ou o diretor responsável.

2. Um documento deve ser classificado, no mínimo, no nível CONFIDENTIEL UE/EU CONFIDENTIAL se a sua divulgação não autorizada for suscetível de, nomeadamente:

a) Causar um prejuízo substancial às relações diplomáticas, ou seja, dar origem a protestos formais ou a outras sanções;

b) Prejudicar a segurança ou a liberdade das pessoas;

c) Prejudicar a eficácia operacional ou a segurança do pessoal destacado dos Estados-Membros ou de outros contribuintes, ou a eficácia de operações de segurança ou de recolha de informações úteis;

d) Enfraquecer substancialmente a viabilidade financeira de organizações importantes;

e) Entravar investigações ou facilitar a criminalidade grave;

f) Prejudicar substancialmente os interesses financeiros, monetários, económicos e comerciais da União Europeia ou dos Estados-Membros;

g) Entravar seriamente o desenvolvimento ou o funcionamento de políticas importantes da União;

h) Paralisar ou perturbar de forma substancial atividades importantes da União;

i) Levar à descoberta de informações classificadas num nível mais elevado.

3. As informações devem ser classificadas, no mínimo, no nível SECRET UE/EU SECRET se a sua divulgação não autorizada for suscetível de, nomeadamente:

a) Provocar tensões internacionais;

b) Prejudicar gravemente as relações com países terceiros ou organizações internacionais;

c) Ameaçar diretamente a vida ou prejudicar gravemente a ordem pública ou a segurança ou a liberdade das pessoas;

d) Prejudicar gravemente a eficácia operacional ou a segurança do pessoal destacado dos Estados-Membros ou de outros contribuintes, ou a continuação da eficácia de operações de segurança ou de recolha de informações extremamente úteis;

e) Causar substanciais prejuízos materiais aos interesses financeiros, monetários, económicos e comerciais da União ou dos Estados-Membros;

f) Levar à descoberta de informações classificadas num nível mais elevado.

4. As entidades de origem podem decidir atribuir um nível de classificação normalizado às categorias de informações que produzem regularmente. Devem, no entanto, assegurar a atribuição do nível de classificação adequado aos elementos de informação individuais.

Artigo 5.º

Tratamento dos projetos

1. As informações devem ser classificadas assim que são produzidas. As notas pessoais, os anteprojetos ou as mensagens que contenham informações que justifiquem uma classificação de nível CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET devem ser marcadas como tal desde o início e produzidas e manuseadas em conformidade com o disposto na presente decisão.

2. Se o documento final deixar de justificar o nível de classificação inicial, deve ser desgraduado ou desclassificado.

Artigo 6.º

Registo do material de referência

A fim de permitir o exercício do controlo da entidade de origem, em conformidade com o artigo 14.º, as entidades de origem de documentos com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET devem manter um registo de todas as fontes classificadas utilizadas para a produção de documentos classificados, incluindo dados pormenorizados sobre as fontes provenientes dos Estados-Membros da UE, de organizações internacionais ou de países terceiros. Quando adequado, as informações classificadas agregadas devem ser marcadas de modo a preservar a identificação das entidades de origem dos materiais de referência classificados utilizados.

Artigo 7.º

Classificação de partes de um documento

1. Em conformidade com o artigo 22.º, n.º 6, da Decisão (UE, Euratom) 2015/444, a classificação geral de um documento deve ser pelo menos tão elevada como a da parte desse documento classificada ao nível mais elevado. Quando forem coligidas informações provenientes de várias fontes, o documento agregado final deve ser analisado para determinar o seu nível de classificação de segurança global, uma vez que pode justificar uma classificação mais elevada do que a das partes que o compõem.

2. Os documentos que contenham partes classificadas e partes não classificadas devem ser estruturados e marcados de modo que as componentes com níveis de classificação e/ou sensibilidade diferentes possam ser facilmente identificadas e separadas, se necessário. Deste modo, cada parte poderá ser manuseada de forma adequada quando for separada das outras componentes.

Artigo 8.º

Marca de classificação completa

1. As informações que justificam uma classificação devem ser marcadas e manuseadas como tal, independentemente da sua forma material. O nível de classificação deve ser comunicado claramente aos destinatários, quer através de uma marca de classificação, se a informação for transmitida por escrito, em papel, em suportes de armazenamento amovíveis ou num sistema de comunicação e informação (SCI), quer por meio de um aviso, se as informações forem transmitidas oralmente, por exemplo numa conversa ou numa apresentação. Os materiais classificados devem ser marcados materialmente de modo a permitir a fácil identificação da sua classificação de segurança.

2. Nos documentos, deve ser escrita a marca de classificação completa CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET em maiúsculas, em francês e inglês (primeiro em francês), em conformidade com o n.º 3. Esta marca não deve ser traduzida para outras línguas.

3. A marca de classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET é aposta do seguinte modo:

a) Ao centro nas partes superior e inferior de todas as páginas do documento;

b) A marca de classificação completa aparece numa só linha, sem espaços de cada lado da barra oblíqua;

c) Em maiúsculas de cor preta, com o tipo de letra «Times New Roman», tamanho 16 (se possível, mas pelo menos 14), em negrito, e com um bordo de cada lado.

4. Ao criar um documento CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET:

a) Todas as páginas devem ser marcadas de forma clara com o nível de classificação;

b) Todas as páginas devem ser numeradas;

c) O documento deve ostentar um número de referência, um número de registo e um assunto, que não constituem por si só informação classificada, a menos que estejam marcados como tal;

d) Todos os anexos e apêndices devem ser enumerados, sempre que possível, na primeira página; e

e) O documento deve ostentar a data da sua criação.

5. Sempre que possível, a marca SECRET UE/EU SECRET deve aparecer a vermelho.

Artigo 9.º

Marcas de classificação abreviadas C-UE/EU-C e S-UE/EU-S

Podem ser utilizadas as abreviaturas «C-UE/EU-C» e «S-UE/EU-S» para indicar o nível de classificação de partes de um documento CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET, respetivamente, ou quando não puder ser inserida a marca de classificação completa, por exemplo, num suporte de armazenamento amovível com pouca capacidade. Podem ser utilizadas igualmente no corpo do texto quando a utilização repetida das marcas de classificação por extenso se tornar pesada. A abreviatura não deve ser utilizada em vez da marca de classificação completa no cabeçalho e no rodapé do documento.

Artigo 10.º

Outros indicadores de segurança

1. Os documentos CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET podem ostentar outras marcas, ou «indicadores de segurança» que especifiquem, por exemplo, o domínio a que o documento diz respeito, ou indiquem uma distribuição específica baseada no princípio da necessidade de tomar conhecimento. Por exemplo:

COMUNICÁVEL AO LISTENSTAINE

2. Os documentos CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET podem conter uma advertência de segurança com instruções específicas sobre a forma de manusear e gerir os documentos.

3. Sempre que possível, qualquer indicação relativa à desgraduação ou desclassificação deve ser aposta na primeira página do documento aquando da sua criação. Por exemplo, pode ser utilizada a seguinte marca:

SECRET UE/EU SECRET até [dd.mm.aaaa] e **RESTREINT UE/EU RESTRICTED** a seguir

Artigo 11.º

Tratamento eletrónico

1. Os documentos CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET devem ser criados recorrendo a meios eletrónicos, sempre que estejam disponíveis.

2. Ao criar informações CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET, o pessoal da Comissão deve utilizar sistemas de comunicação e informação acreditados para o nível de classificação correspondente ou para um nível de classificação mais elevado. Em caso de dúvida quanto aos sistemas de comunicação e informação que podem ser utilizados, o pessoal deve consultar o seu responsável local de segurança (LSO). Consultando a autoridade de segurança da Comissão, podem ser aplicados procedimentos específicos em situações de emergência ou em caso de configurações técnicas específicas.

3. Como previsto no artigo 5.º, os documentos CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET, incluindo os que estiverem na fase de projeto, não podem ser enviados por correio eletrónico, impressos ou digitalizados em impressoras ou scâneres normalizados, ou manuseados nos dispositivos pessoais dos membros do pessoal. Só podem ser utilizadas impressoras ou fotocopiadoras ligadas a computadores autónomos protegidos das emissões eletromagnéticas ou a um sistema acreditado para imprimir documentos CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET.

Artigo 12.º

Registo para efeitos de segurança

1. As informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET devem ser registadas para fins de segurança antes da sua distribuição e aquando da sua receção. Devem ser registadas:

— quando chegam ou saem de uma entidade organizacional; e

— quando chegam ou saem de um sistema de comunicação e informação.

2. Este registo pode ser efetuado em papel ou em livros de registo eletrónicos.

3. Se as informações forem tratadas eletronicamente num sistemas de comunicação e informação, estes procedimentos de registo podem ser realizados por processos internos do próprio sistema. Nesse caso, o sistema de comunicação e informação deve incluir medidas destinadas a garantir a integridade dos livros de registo.

4. O responsável pelo controlo do registo deve manter um registo que contenha, pelo menos, as seguintes informações relativamente a cada documento:

a) A data em que o documento classificado final foi registado;

b) O nível de classificação;

c) Se for caso disso, a data de expiração do nível de classificação;

d) O nome do serviço de origem;

e) O ou os destinatários;

f) O objeto;

g) O número de referência do documento no serviço de origem;

h) O número de registo;

i) O número de cópias distribuídas;

j) Sempre que possível, o livro de registo das fontes utilizadas para a criação do documento;

k) A data de desgraduação ou de desclassificação do documento; e

l) Informações sobre a destruição (local, data, método, supervisão, certificado de destruição).

Artigo 13.º

Distribuição

O remetente de documentos CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET deve decidir a quem distribuir as informações, com base na necessidade de tomar conhecimento das mesmas. Deve ser elaborada uma lista de distribuição, a fim de aplicar mais rigorosamente o princípio da necessidade de tomar conhecimento.

CAPÍTULO 3

TRABALHAR COM INFORMAÇÕES COM CLASSIFICAÇÃO CONFIDENTIEL UE/EU CONFIDENTIAL E SECRET UE/EU SECRET EXISTENTES

Artigo 14.º

Controlo por parte da entidade de origem

1. A entidade de origem tem «controlo da entidade de origem» sobre as informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET que tiver criado. Deve ser solicitado o consentimento prévio, por escrito, da entidade de origem antes de as informações poderem ser:

a) Desclassificadas ou desgraduadas;

b) Utilizadas para fins diferentes dos estabelecidos pela entidade de origem;

c) Comunicadas a um país terceiro ou organização internacional;

d) Divulgadas a uma parte fora da Comissão, mas no interior da UE; ou

e) Divulgadas a um contratante ou potencial contratante situado num país terceiro.

2. Os titulares de informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET são pessoas devidamente autorizadas que receberam acesso às informações classificadas para poderem desempenhar as suas funções. São responsáveis pelo seu correto manuseamento, armazenamento e proteção, em conformidade com a Decisão (UE, Euratom) 2015/444. Contrariamente às entidades de origem das informações classificadas, os titulares não são autorizados a tomar decisões sobre a desgraduação, desclassificação ou ulterior comunicação de informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET.

3. Se não for possível identificar a entidade de origem de uma informação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET, o serviço da Comissão que tem essa informação classificada exerce o controlo de entidade de origem. O grupo de peritos de segurança da Comissão deve ser consultado antes de as informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET serem comunicadas a um país terceiro ou a uma organização internacional.

Artigo 15.º

Sistemas de comunicação e informação adequados para o manuseamento de informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET

1. As informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET devem ser manuseadas e transmitidas através de meios eletrónicos, se disponíveis. Apenas devem ser utilizados os sistemas de comunicação e informação e os equipamentos que tiverem sido acreditados pela Autoridade de Acreditação de Segurança da Comissão para o manuseamento de informações classificadas no nível pertinente ou num nível de classificação mais elevado.

2. Sempre que um serviço da Comissão disponha do equipamento adequado para manusear e enviar informações classificadas nesses níveis, deve ajudar, na medida das suas possibilidades, outras entidades da Comissão a manusear e enviar as informações de forma adequada.

Artigo 16.º

Medidas específicas aplicáveis às informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET em suportes de armazenamento amovíveis

1. A utilização de suportes de armazenamento amovíveis deve ser objeto de um controlo rigoroso e tida em conta. Apenas devem ser utilizados os suportes de armazenamento amovíveis fornecidos pela Comissão e encriptados por um produto aprovado pela autoridade de segurança da Comissão. Os suportes de armazenamento amovíveis pessoais e os suportes distribuídos gratuitamente em conferências, seminários, etc. não devem ser utilizados para transferir informações classificadas. Sempre que possível, devem ser utilizados suportes de armazenamento amovíveis com segurança Tempest, em conformidade com as orientações da autoridade de segurança da Comissão.

2. Quando um documento classificado for manuseado ou armazenado eletronicamente em suportes de armazenamento amovíveis, tais como memórias USB, CD ou cartões de memória, a marca de classificação deve ser claramente visível nas próprias informações mostradas, bem como no nome do ficheiro e no suporte de armazenamento amovível.

3. O pessoal deve ter em conta que, sempre que sejam armazenadas grandes quantidades de informações classificadas em suportes de armazenamento amovíveis, o dispositivo pode justificar um nível de classificação mais elevado.

4. Só podem ser utilizados para transferir informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET de ou para suportes de armazenamento amovíveis os sistemas de comunicação e informação que tiverem sido devidamente acreditados.

5. Ao descarregar estas informações para suportes de armazenamento amovíveis, devem ser tomadas precauções especiais, antes da transferência dos dados, para assegurar que os referidos suportes não contêm vírus nem *software* mal-intencionado.

6. Se for caso disso, os suportes de armazenamento amovíveis devem ser manuseados em conformidade com os procedimentos operacionais de segurança correspondentes ao sistema de cifragem utilizado.

7. Os documentos armazenados em suportes de armazenamento amovíveis que já não sejam necessários, ou que tenham sido transferidos para um sistema de comunicação e informação adequado, devem ser retirados ou apagados de forma segura utilizando produtos ou métodos aprovados. A menos que sejam armazenados num cofre adequado, os suportes de armazenamento amovíveis devem ser destruídos quando deixarem de ser necessários. As operações de destruição ou apagamento devem recorrer a métodos conformes com as regras de segurança da Comissão. Deve ser mantido um inventário dos suportes de armazenamento amovíveis e a sua destruição deve ser registada.

Artigo 17.º

Manuseamento e armazenamento de informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET

1. Nos termos do artigo 19.º, n.º 3, alínea a), da Decisão (UE, Euratom) 2015/444, as informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET devem ser manuseadas em Zonas de Segurança ([8]):

2. Nos termos do artigo 19.º, n.º 3, alínea b), da Decisão (UE, Euratom) 2015/444, estas informações podem ser manuseadas em Zonas Administrativas ([9]), desde que sejam protegidas do acesso de pessoas não autorizadas.

3. Estas informações podem ser manuseadas fora de Zonas de Segurança ou de Zonas Administrativas desde que o detentor se tenha comprometido a respeitar as medidas de compensação exigidas ao abrigo do artigo 19.º, n.º 3, alínea c), da Decisão (UE, Euratom) 2015/444, que devem incluir, pelo menos, as seguintes medidas:

— Os documentos CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET não devem ser lidos em locais públicos.

— As ICUE devem ser mantidas permanentemente sob o controlo pessoal do detentor.

— No caso dos documentos impressos, o titular deve ter notificado ao registo competente o manuseamento dos documentos classificados fora de uma Zona de Segurança e de uma Zona Administrativa.

— Os documentos devem ser armazenados num cofre apropriado quando não estiverem a ser lidos ou discutidos.

— As portas da sala devem manter-se fechadas durante a leitura ou o debate do documento.

— O conteúdo do documento não deve ser discutido ao telefone numa linha não protegida nem numa mensagem de correio eletrónico.

— O documento não pode ser fotocopiado nem digitalizado pelo titular. Só podem ser obtidas outras cópias do documento junto do registo.

— O documento só deve ser manuseado e conservado temporariamente fora de uma Zona Administrativa ou de uma Zona de Segurança durante o tempo estritamente necessário, após o que deve ser devolvido ao registo;

([8]) Definidas no artigo 18.º da Decisão (UE, Euratom) 2015/444.
([9]) Definidas no artigo 18.º da Decisão (UE, Euratom) 2015/444.

— A devolução do documento deve ser assinada.

— O titular não deve deitar fora nem destruir o documento classificado.

4. As informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET devem ser armazenadas em Zonas de Segurança, dentro de um contentor de segurança ou de uma casa-forte.

5. Pode ser solicitado aconselhamento adicional ao responsável local de segurança (LSO) do serviço competente da Comissão.

6. Devem ser comunicados ao LSO o mais rapidamente possível quaisquer suspeitas ou casos reais de incidentes de segurança relativos ao documento.

Artigo 18.º

Cópia e tradução de informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET

1. As informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET podem ser copiadas ou traduzidas a pedido do detentor, desde que a entidade de origem não tenha imposto reservas a esse respeito. No entanto, não podem ser feitas mais cópias do que as estritamente necessárias.

2. Quando apenas for reproduzida uma parte de um documento classificado, são aplicadas as mesmas condições que à cópia integral do documento. Os extratos também devem ser classificados no mesmo nível, a menos que a entidade de origem os tenha classificado especificamente num nível mais baixo, ou marcado como não classificados.

3. As medidas de segurança aplicáveis às informações originais são igualmente aplicadas às suas cópias e traduções.

Artigo 19.º

Princípios gerais aplicáveis ao transporte de informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET

1. Sempre que possível, as informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET que tenham de sair das Zonas de Segurança ou das Zonas Administrativas devem ser enviadas por via eletrónica através de meios devidamente acreditados e/ou protegidas por produtos criptográficos aprovados.

2. Em função dos meios disponíveis ou das circunstâncias, as informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET poderão ser transportadas fisicamente, em mão própria, sob a forma de documentos impressos ou em suportes de armazenamento amovíveis. Deve ser dada preferência à utilização de suportes de armazenamento amovíveis para transferir informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET em relação ao envio de documentos impressos.

3. Apenas devem ser utilizados os suportes de armazenamento amovíveis encriptados por um produto aprovado pela autoridade de segurança da Comissão. As informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET contidas em suportes de armazenamento amovíveis que não estejam protegidos por um produto de cifragem aprovado pela autoridade de segurança da Comissão devem ser manuseadas da mesma forma que as informações impressas.

4. A remessa poderá conter mais de um elemento de ICUE, desde que seja respeitado o princípio da necessidade de ter conhecimento.

5. A embalagem utilizada deve assegurar que o conteúdo não é visível. As informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET devem ser transportadas em duas camadas de embalagens opacas, tais como sobrescritos, capas opacas ou uma pasta para documentos. A embalagem exterior não deve ostentar qualquer indicação da natureza ou do nível de classificação do seu conteúdo. A camada interior da embalagem deve ser marcada como CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET. Ambas as camadas devem indicar o nome do destinatário, o seu cargo e o seu endereço, bem como um endereço de retorno caso a entrega não possa ser efetuada.

6. Os membros do pessoal ou os serviços de correio rápido que transportarem em mãos informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET devem receber uma autorização de segurança e um certificado de correio rápido.

7. O sobrescrito ou embalagem não deve ser aberto durante o percurso. A autorização de segurança concedida ao serviço de correio rápido não o autoriza a aceder ao conteúdo das informações classificadas.

8. Os eventuais incidentes de segurança relativos a informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET que sejam transportadas por membros do pessoal ou serviços de correio rápido devem ser comunicados para investigação subsequente à Direção de Segurança da Direção-Geral dos Recursos Humanos e Segurança, através do LSO do serviço competente da Comissão.

Artigo 20.º

Transporte em mão própria de suportes de armazenamento amovíveis

1. Os suportes de armazenamento amovíveis destinados a transportar informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET devem ser acompanhados de uma declaração de expedição em que sejam mencionados os suportes de armazenamento amovíveis que contêm as informações classificadas, bem como todos os ficheiros neles contidos, de modo a permitir ao destinatário efetuar as verificações necessárias e confirmar a receção.

2. Só devem ser armazenados nos suportes de armazenamento amovíveis os documentos a transmitir. Por exemplo, todas as informações classificadas contidas numa única memória USB devem ter o mesmo destinatário. O remetente deve ter em conta que o armazenamento de grandes quantidades de informações classificadas em dispositivos deste tipo poderá justificar a atribuição de um nível de classificação mais elevado ao dispositivo no seu conjunto.

3. Só devem ser utilizados suportes de armazenamento amovíveis com a marca de classificação adequada para o transporte de informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET.

4. Toda as informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET salvaguardadas em suportes amovíveis devem ser registadas para fins de segurança.

Artigo 21.º

Transporte de documentos CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET dentro dos edifícios da Comissão

1. O pessoal que possui uma autorização de segurança pode transportar documentos com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET dentro dos edifícios da Comissão, mas esses documentos devem ficar sempre na posse do detentor e não podem ser lidos em público.

2. Os documentos com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET não podem ser enviados por correio interno.

Artigo 22.º

Transporte de documentos CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET dentro da União

1. As informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET podem ser transportadas por membros do pessoal ou estafetas da Comissão em qualquer lugar da União, desde que respeitem as seguintes instruções:

a) Devem ser utilizados sobrescritos ou embalagens duplos opacos para transmitir informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET. O exterior não deve ostentar qualquer indicação da natureza ou do nível de classificação do seu conteúdo;

b) As informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET devem ficar sempre na posse do portador; e

c) O sobrescrito ou embalagem não deve ser aberto durante o percurso e as informações não devem ser lidas em locais públicos.

2. O pessoal do registo que pretenda enviar informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL para outros locais da União pode providenciar para que sejam transmitidas por um dos seguintes meios:

— serviços postais nacionais que garantam o seguimento da remessa ou certos serviços comerciais de correio rápido que garantam o transporte em mão própria, desde que cumpram os requisitos estabelecidos no artigo 24.º da presente decisão;

— estafeta militar, correio oficial ou mala diplomática.

3. O pessoal que pretenda enviar informações com classificação SECRET UE/EU SECRET para outros Estados-Membros da UE pode providenciar com o respetivo registo para que sejam enviadas por estafeta militar, correio oficial ou mala diplomática, mas não pelos serviços postais ou por serviços comerciais de correio rápido.

4. Os membros do pessoal ou estafetas oficiais da Comissão que transportem informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET devem levar consigo, para cada remessa, um certificado de estafeta emitido pelo registo do respetivo serviço que ateste que estão autorizados a transportá-la.

Artigo 23.º

Transporte de informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET do ou para o território de um país terceiro

1. As informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET podem ser transportadas em mão própria pelo pessoal entre o território da União e o território de um país terceiro.

2. O pessoal do registo pode prever o transporte por estafeta militar ou mala diplomática.

3. Quando transportarem em mão própria documentos impressos ou suportes de armazenamento amovíveis classificados como CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET, os membros do pessoal devem respeitar todas as seguintes medidas adicionais:

— Quando se deslocarem em transportes públicos, as informações classificadas devem ser colocadas numa pasta para documentos ou num saco mantido sob a guarda pessoal do portador. Estas informações não podem ser deixadas em nenhum compartimento para bagagem.

— A camada interior da embalagem deve ostentar um selo oficial que indique que se trata de uma remessa oficial que não deve ser submetida a um controlo de segurança.

— O portador deve possuir um certificado de estafeta que ateste que está autorizado a transportar a remessa com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET, emitido pelo registo do serviço competente.

Artigo 24.º

Transporte por serviços comerciais de correio rápido

1. Para efeitos da presente decisão, por «serviços comerciais de correio rápido» entende-se os serviços postais nacionais e as empresas de correio rápido que oferecem um serviço em que as informações são entregues em troca de um pagamento e são transportadas pessoalmente ou seguidas.

2. Os serviços comerciais de correio rápido podem transmitir informações CONFIDENTIEL UE/EU CONFIDENTIAL no interior de um Estado-Membro ou de um Estado-Membro para outro. Os serviços comerciais de correio rápido podem transmitir informações com classificação SECRET UE/EU SECRET unicamente dentro de um Estado-Membro, mas não no estrangeiro.

3. Os serviços comerciais de correio rápido devem ser informados de que só podem entregar remessas CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET ao responsável do controlo do registo, ao seu substituto devidamente autorizado ou ao destinatário previsto.

4. Os serviços comerciais de correio rápido podem recorrer aos serviços de um subcontratante. No entanto, a responsabilidade pelo cumprimento da presente decisão incumbe à empresa de correio rápido.

5. Os serviços prestados pelos serviços comerciais de correio rápido que consistam na transmissão eletrónica de documentos enviados por correio registado não podem ser utilizados para as informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET.

Artigo 25.º

Preparação das ICUE para transporte por serviços comerciais de correio rápido

1. Ao preparar as remessas classificadas, o remetente deve ter em conta que os serviços comerciais de correio rápido só entregam as remessas CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET ao destinatário previsto, ao seu substituto devidamente autorizado, ao agente de controlo do registo ou ao seu substituto devidamente autorizado, ou a um rececionista.

2. Quando essas informações forem enviadas por um serviço comercial de correio rápido aprovado, a remessa deve ser preparada e embalada do seguinte modo:

a) A remessa deve ser enviada em sobrescritos duplos (devendo o sobrescrito interior revelar qualquer tentativa de o abrir) ou outro material de embalagem seguro.

b) O nível de classificação deve ser claramente visível no sobrescrito interior ou na camada interior da embalagem.

c) A classificação não pode ser indicada no sobrescrito exterior ou na camada exterior da embalagem.

d) Os sobrescritos ou camadas tanto interiores como exteriores da embalagem devem ser claramente endereçados a uma pessoa identificada no destinatário previsto e incluir um endereço de retorno.

e) Deve ser colocado um formulário de recibo de registo dentro do sobrescrito interior ou na camada interior da embalagem, que o destinatário deve preencher e devolver. O recibo de registo, que não deve ser classificado, deve mencionar o número de referência, a data e o número da cópia do documento, mas não o objeto.

f) O sobrescrito ou embalagem exterior deve conter recibos de entrega. O recibo de entrega, que não deve ser classificado, deve mencionar o número de referência, a data e o número da cópia do documento, mas não o objeto.

g) O serviço de correio rápido deve obter a prova da entrega da remessa no documento de assinaturas e registo e fornecê-la ao remetente, ou obter recibos ou números de encomenda.

3. O remetente deve contactar o destinatário indicado antes da expedição da remessa a fim de combinar uma data e hora adequadas para a entrega.

4. O remetente é o único responsável por qualquer remessa enviada por um serviço comercial de correio rápido. Em caso de perda ou de entrega atrasada da remessa, o remetente deve comunicar o facto à autoridade de segurança da Comissão, que se encarregará do seguimento do incidente de segurança.

Artigo 26.º

Outras condições de manuseamento específicas

1. Devem ser respeitadas todas as condições de transporte estabelecidas num acordo de segurança das informações ou em acordos administrativos. Em caso de dúvida, o pessoal deve consultar o respetivo registo ou a Direção de Segurança da Direção-Geral dos Recursos Humanos e da Segurança.

2. O requisito da dupla embalagem pode ser dispensado no caso das informações classificadas protegidas por produtos criptográficos aprovados. Contudo, para efeitos de expedição, e também pelo facto de o meio de armazenamento amovível ostentar uma marca de classificação de segurança explícita, o meio de armazenamento deve ser transportado pelo menos num sobrescrito comum, mas poderá exigir medidas de proteção material adicionais, como, por exemplo, a utilização de saquetas almofadadas.

CAPÍTULO 4

REUNIÕES CLASSIFICADAS

Artigo 27.º

Preparação de reuniões CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET

1. As reuniões em que esteja prevista a discussão de informações com classificação CONFIDENTIEL UE/EU CONFIDENTIEL ou SECRET UE/EU SECRET só podem ser realizadas em salas de reuniões que tenham sido acreditadas ao nível adequado ou superior. Quando estas salas não estiverem disponíveis, o pessoal deve consultar a autoridade de segurança da Comissão.

2. Regra geral, as ordens de trabalhos não devem ser classificadas. O facto de a ordem de trabalhos de uma reunião mencionar documentos classificados não implica que a ordem de trabalhos deva automaticamente ser classificada. Os pontos da ordem de trabalhos devem ser redigidos de modo a evitar pôr em risco a proteção dos interesses da União ou de um ou mais Estados-Membros.

3. Os organizadores das reuniões devem recordar aos participantes que quaisquer observações sobre pontos da ordem de trabalhos com classificação CONFIDENTIEL UE/EU CONFIDENTIEL ou SECRET UE/EU SECRET não podem ser enviadas por correio eletrónico nem por outros meios que não tenham sido devidamente acreditados em conformidade com o artigo 11.º da presente decisão.

4. Os organizadores das reuniões devem esforçar-se por agrupar de forma consecutiva na ordem de trabalhos os pontos com classificação CONFIDENTIEL UE/EU CONFIDENTIEL e SECRET UE/EU SECRET, a fim de facilitar o bom funcionamento da reunião. Durante os debates dos pontos classificados, só podem estar presentes as pessoas com necessidade de tomar conhecimento, as que têm uma credenciação de segurança para o nível adequado e as pessoas autorizadas, se for caso disso.

5. A própria convocatória deve prevenir os participantes de que na reunião serão debatidos temas classificados e que serão aplicadas as medidas de segurança correspondentes.

6. Deve ser recordado aos participantes que os dispositivos eletrónicos portáteis devem ficar no exterior da sala de reunião durante os debates de pontos CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET.

7. Antes da reunião, os organizadores devem elaborar uma lista completa dos participantes.

Artigo 28.º

Acesso dos participantes às reuniões CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET

1. Os organizadores da reunião devem informar a autoridade de segurança da Comissão de quaisquer visitantes externos que assistirem à reunião CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET nas instalações da Comissão.

2. Os participantes deverão provar que possuem uma credenciação de segurança do pessoal de nível adequado válida, a fim de poderem participar na discussão de pontos CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET.

Artigo 29.º

Equipamento eletrónico na sala de reunião CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET

1. Só podem ser utilizados sistemas informáticos acreditados em conformidade com o artigo 11.º da presente decisão quando forem transmitidas informações classificadas, por exemplo durante uma apresentação em que sejam mostradas informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET ou quando forem organizadas videoconferências.

2. O presidente deve assegurar-se de que os dispositivos eletrónicos portáteis não autorizados foram deixados no exterior da sala de reuniões.

Artigo 30.º

Procedimentos a seguir durante as reuniões CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET

1. No início do debate classificado, o presidente deve anunciar aos presentes que a reunião vai passar para «modo classificado». As portas devem ser fechadas.

2. Será assinado e entregue aos participantes e aos intérpretes apenas o número necessário de documentos, se for caso disso, no início do debate.

3. Os documentos CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET não podem ser deixados sem vigilância durante os intervalos da reunião.

4. No final da reunião, deve ser recordado aos participantes e aos intérpretes que não devem deixar sem vigilância na sala quaisquer documentos classificados ou notas que tiverem tomado. Os documentos com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET que não forem solicitados pelos participantes no final da reunião e, em qualquer caso, todos os documentos dos intérpretes, devem ser assinados e devolvidos ao responsável do controlo do registo com vista à sua destruição em destruidoras adequadas.

5. Durante a reunião, deve ser elaborada a lista dos participantes e um resumo de quaisquer informações classificadas partilhadas com os Estados-Membros e comunicadas oralmente a países terceiros ou a organizações internacionais, a fim de serem registados nos resultados dos trabalhos.

Artigo 31.º

Intérpretes e tradutores

Só podem ter acesso a informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET os intérpretes e tradutores autorizados que tenham uma credenciação de segurança e estejam cobertos pelo Estatuto do Pessoal ou pelo Regime Aplicável aos Outros Agentes da União Europeia ou que tenham uma relação contratual com a Comissão.

CAPÍTULO 5

PARTILHA E TROCA DE INFORMAÇÕES COM CLASSIFICAÇÃO CONFIDENTIEL UE/EU CONFIDENTIAL E SECRET UE/EU SECRET

Artigo 32.º

Consentimento da entidade de origem

Se a Comissão não for a entidade de origem das informações classificadas cuja comunicação ou partilha se pretende, ou do material de referência que possam conter, o serviço da Comissão que tem essas informações classificadas deve solicitar à entidade de origem que dê o consentimento prévio por escrito para a sua comunicação. Se a entidade de origem não puder ser identificada, o serviço da Comissão que tem essas informações classificadas deve exercer o controlo enquanto entidade de origem.

Artigo 33.º

Partilha de informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET com outras entidades da União

1. As informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET só devem ser partilhadas com outra instituição, órgão ou organismo da União se o destinatário tiver necessidade de tomar conhecimento das mesmas e se a entidade tiver um acordo jurídico correspondente com a Comissão.

2. Na Comissão, o registo de ICUE gerido pelo Secretariado-Geral deve ser, regra geral, o principal ponto de entrada e de saída para os intercâmbios de informações classificadas com outras instituições, agências, organismos ou serviços da União. A autoridade de segurança da Comissão deve ser consultada sempre que existam motivos de segurança, organizacionais ou operacionais que tornem mais adequado que os registos locais de ICUE funcionem como ponto de entrada e de saída nas matérias da competência do serviço em causa.

Artigo 34.º

Troca de informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET com os Estados-Membros

1. As informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET podem ser partilhadas com os Estados-Membros se o destinatário tiver necessidade de tomar conhecimento das mesmas e possuir uma credenciação de segurança.

2. As informações classificadas dos Estados-Membros que ostentem uma marca de classificação nacional equivalente ([10]) e tenham sido disponibilizadas à Comissão devem beneficiar do mesmo nível de proteção que as informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET.

Artigo 35.º

Troca de informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET com países terceiros e organizações internacionais

1. As informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET só podem ser comunicadas a países terceiros ou organizações internacionais se o destinatário tiver necessidade de tomar conhecimento das mesmas e se o país ou organização internacional dispuser de um quadro jurídico ou administrativo adequado, como por exemplo um acordo de segurança das informações ou um convénio administrativo com a Comissão. As disposições desses acordos ou convénios prevalecem sobre as disposições da presente decisão.

2. Regra geral, o registo de ICUE gerido pelo Secretariado-Geral constitui o principal ponto de entrada e de saída de todas as informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET trocadas entre a Comissão e países terceiros e organizações internacionais. A autoridade de segurança da Comissão deve ser consultada sempre que existam motivos de segurança, organizacionais ou operacionais que tornem mais adequado que os registos locais de ICUE funcionem como ponto de entrada e de saída nas matérias da competência do serviço em causa.

3. Quaisquer informações classificadas recebidas de um país terceiro ou de uma organização internacional devem ser registadas, para fins de segurança. Por conseguinte, o pessoal deve contactar o registo se receber informações classificadas provenientes de fontes fora do circuito habitual do registo.

4. A fim de assegurar a rastreabilidade, as informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET devem ser registadas:

— quando chegam ou saem de uma entidade organizacional; e

— quando chegam ou saem de um sistema de comunicação e informação.

5. Esse registo pode ser efetuado em papel ou em livros de registo eletrónicos.

6. Os procedimentos de registo das informações classificadas manuseadas num sistema de comunicação e informação acreditado podem ser executados por processos internos do próprio sistema. Nesse caso, o sistema de comunicação e informação deve incluir medidas destinadas a garantir a integridade dos livros de registo.

7. As informações classificadas recebidas de países terceiros ou de organizações internacionais devem beneficiar de um nível de proteção equivalente ao das ICUE que ostentem a marca de classificação equivalente, conforme previsto no respetivo acordo de segurança das informações ou convénio administrativo.

Artigo 36.º

Comunicação ad hoc excecional de informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET

1. Sempre que a Comissão ou um dos seus serviços determinar que existe uma necessidade excecional de comunicar informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET a um país terceiro, uma organização internacional ou uma entidade da UE, mas não exista um acordo de segurança das informações ou um convénio administrativo, deve ser seguido o procedimento de comunicação *ad hoc* excecional.

([10]) O quadro de equivalências das marcas dos Estados-Membros figura no anexo I da Decisão (UE, Euratom) 2015/444.

2. Os serviços da Comissão devem contactar a autoridade de segurança da Comissão, que consultará o Grupo de Peritos de Segurança da Comissão.

3. Após consulta do Grupo de Peritos de Segurança da Comissão, a Comissão pode, com base numa proposta do membro da Comissão responsável pelas questões de segurança, autorizar a comunicação das informações em causa.

CAPÍTULO 6

FIM DE VIDA DAS INFORMAÇÕES COM CLASSIFICAÇÃO CONFIDENTIEL UE/EU CONFIDENTIAL E SECRET UE/EU SECRET

Artigo 37.º

Quando desgraduar e desclassificar

1. As informações só permanecem classificadas enquanto necessitarem de proteção. A «desgraduação» significa uma redução do nível de classificação de segurança. A «desclassificação» significa que as informações deixam de ser consideradas classificadas. Aquando da produção de ICUE, a entidade de origem indica, sempre que possível, se as mesmas podem ser desgraduadas ou desclassificadas numa determinada data ou após um acontecimento concreto. Caso contrário, a entidade de origem deve reanalisar as informações e avaliar os riscos pelo menos de cinco em cinco anos, a fim de determinar se o nível de classificação inicial continua a ser adequado.

2. Os documentos da Comissão também podem ser desgraduados ou desclassificados numa base *ad hoc*, por exemplo na sequência de um pedido de acesso do público.

Artigo 38.º

Responsabilidade pela desgraduação ou desclassificação

1. As informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET não podem ser desgraduadas ou desclassificadas sem a autorização da entidade de origem.

2. O serviço da Comissão que cria um documento classificado é responsável por decidir se o mesmo pode ser desgraduado ou desclassificado. Na Comissão, todos os pedidos de desgraduação e desclassificação devem ser submetidos à consulta do chefe de unidade ou do diretor do serviço de origem. Se o serviço tiver compilado informações classificadas provenientes de várias fontes, deve, em primeiro lugar, solicitar o consentimento das partes que tiverem fornecido material de origem, incluindo os Estados-Membros, outros organismos da UE, países terceiros ou organizações internacionais.

3. Se o serviço de origem da Comissão já não existir e as suas responsabilidades tiverem sido assumidas por outro serviço, a decisão de desgraduação ou desclassificação deve ser tomada por este último. Se o serviço de origem já não existir e as suas responsabilidades tiverem sido assumidas por outro serviço, a decisão de desgraduação ou desclassificação deve ser tomada conjuntamente pelos chefes de unidade ou os diretores das direções-gerais destinatárias.

4. O serviço responsável pela desgraduação ou desclassificação deve trabalhar em conjunto com o respetivo registo com vista a determinar as modalidades práticas para proceder à desgraduação ou desclassificação.

Artigo 39.º

Informações sensíveis não classificadas

Sempre que da reanálise de um documento resultar a decisão de o desclassificar, deve ser ponderado se o documento deve ostentar a marca de distribuição «informações sensíveis não classificadas» na aceção do artigo 9.º da Decisão (UE, Euratom) 2015/443.

Artigo 40.º

Indicação de que um documento foi desgraduado ou desclassificado

1. A marca de classificação original na parte superior e inferior de cada página deve ser riscada de forma visível (não suprimida) utilizando a funcionalidade «riscado» no caso de formatos eletrónicos, ou de forma manual nos documentos impressos.

2. A primeira página (capa) deve ostentar um carimbo que indique que o documento foi desgraduado ou desclassificado e preenchida com os dados da autoridade responsável pela desgraduação ou desclassificação e a data correspondente.

3. Os destinatários originais das informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET devem ser informados da desgraduação ou desclassificação. Os destinatários iniciais são responsáveis por informar quaisquer destinatários subsequentes a quem tenham enviado as informações originais com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET ou posto em cópia da sua remessa.

4. O Serviço do Arquivo Histórico da União Europeia deve ser informado de todas as decisões de desclassificação tomadas.

5. Todas as traduções de informações classificadas estão sujeitas aos mesmos procedimentos de desgraduação ou desclassificação que a versão linguística original.

Artigo 41.º

Desgraduação ou desclassificação parcial de informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET

1. Deve também ser possível proceder a uma desgraduação ou desclassificação parcial (por exemplo, os anexos ou apenas determinados parágrafos). O procedimento deve ser idêntico ao da desgraduação ou desclassificação de um documento na íntegra.

2. Depois da desclassificação parcial («limpeza») de informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET, deve ser produzido um extrato desclassificado.

3. As partes que permaneçam classificadas devem ser substituídas pela menção:

PARTE QUE NÃO DEVE SER DESCLASSIFICADA

quer no corpo do próprio texto, se a parte que permanece classificada fizer parte de um parágrafo, quer como parágrafo, se a parte que permanece classificada for um parágrafo específico ou mais de um parágrafo.

4. Se um anexo completo não puder ser desclassificado e, por conseguinte, tiver sido retirado do extrato, deve ser feita uma menção específica do facto no texto.

Artigo 42.º

Destruição e apagamento rotineiros de informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET

1. A Comissão não deve acumular grandes quantidades de informações classificadas.

2. Os serviços de origem devem reanalisar os documentos, pelo menos de cinco em cinco anos, para destruição ou apagamento. Devem ser reanalisadas periodicamente tanto as informações armazenadas em papel como as armazenadas em sistemas de comunicação e informação.

3. O pessoal não deve destruir quaisquer documentos impressos com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET de que já não necessite, mas sim solicitar ao seu responsável do controlo do registo que proceda à destruição dos documentos, sob reserva de eventuais requisitos de arquivo aplicáveis ao documento original.

4. O pessoal não é obrigado a informar a entidade de origem do apagamento de cópias de documentos com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET.

5. Os projetos que contenham informações classificadas devem ser sujeitos aos mesmos métodos de eliminação que os documentos classificados finalizados.

6. Só serão utilizadas destruidoras aprovadas para a destruição de documentos CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET. As destruidoras de nível 5 DIN 66399 são adequadas para destruir documentos CONFIDENTIEL UE/EU CONFIDENTIAL. As destruidoras de nível 6 DIN 66399 são adequadas para destruir documentos SECRET UE/EU SECRET.

7. As partículas das destruidoras aprovadas podem ser eliminadas como resíduos de escritório normais.

8. O responsável pelo controlo do registo deve criar certificados de destruição e atualizar em conformidade os livros de registo eletrónicos e outras informações de registo.

9. Todos os suportes e dispositivos que contenham informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET devem ser limpos de forma adequada quando chegam ao fim da sua vida útil. Os dados eletrónicos devem ser destruídos ou apagados dos recursos informáticos e dos suportes de armazenamento associados de uma forma que dê garantias razoáveis de que as informações não podem ser recuperadas. A limpeza deve eliminar os dados do dispositivo de armazenamento, bem como todos os rótulos, marcas e registos de atividade.

10. Os suportes de dados informáticos devem ser entregues ao LSO ou ao responsável local da segurança informática e/ou ao responsável do controlo do registo para destruição e eliminação.

Artigo 43.º

Evacuação e destruição de informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET em situações de emergência

1. O chefe de serviço deve conceber, aprovar e, se necessário, ativar planos de evacuação e destruição de emergência para proteger as ICUE que corram um risco significativo de cair na posse de mãos não autorizadas durante uma crise. Por ordem de prioridade, e em função da natureza da situação de emergência, deve ser estudada a possibilidade de:

1) Deslocar as ICUE para um local seguro alternativo, se possível uma Zona de Segurança dentro do mesmo edifício;

2) Levar as ICUE para um local seguro alternativo, se possível uma Zona de Segurança noutro edifício, de preferência um edifício da Comissão;

3) Destruir as ICUE, utilizando, se possível, os meios de destruição aprovados.

2. Quando tiverem sido ativados os planos de emergência, deve ser dada prioridade à mudança ou à destruição das informações com classificação SECRET UE/EU SECRET e depois a quaisquer informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL.

3. Os próprios dados operacionais dos planos de evacuação e de destruição de emergência devem ser classificados como «RESTREINT UE/EU RESTRICTED». Deve ser conservada uma cópia em cada cofre onde sejam armazenadas informações com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET, de modo a estar acessível em caso de emergência.

Artigo 44.º

Arquivo

1. As decisões de arquivar ou não e em que momento, bem como as medidas práticas correspondentes a tomar, devem ser conformes com a política da Comissão em matéria de gestão de documentos.

2. Os documentos com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET não devem ser enviados para o Arquivo Histórico da União Europeia em Florença.

CAPÍTULO 7

DISPOSIÇÕES FINAIS

Artigo 45.º

Transparência

A presente decisão é levada ao conhecimento do pessoal da Comissão e de todas as pessoas às quais se aplica, e é publicada no *Jornal Oficial da União Europeia*.

Artigo 46.º

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 17 de outubro de 2019.

Pela Comissão,

Em nome do Presidente,

Günther OETTINGER

Membro da Comissão

ANEXO

Categorias de pessoal que podem ter acesso a informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET se delas tiverem necessidade para o desempenho das suas tarefas profissionais

Categorias de pessoal da Comissão	Acesso às informações C-UE/EU- C e S-UE/EU-S	Condições
Funcionários	Sim	Inquérito + instruções + reconhecimento + autorização + necessidade de tomar conhecimento
Agentes temporários	Sim	Inquérito + instruções + reconhecimento + autorização + necessidade de tomar conhecimento
Agentes contratuais	Sim	Inquérito + instruções + reconhecimento + autorização + necessidade de tomar conhecimento
Peritos nacionais destacados (PND)	Sim	Unicamente se tiverem recebido uma autorização dos Estados-Membros antes de assumirem as suas funções + informações da Comissão + reconhecimento + autorização da Comissão + necessidade de tomar conhecimento
Estagiários	Não	Nenhuma exceção possível
Qualquer outra categoria de pessoal (pessoal temporário, pessoal externo que trabalha nas instalações da Comissão, etc.)	Não	Consultar a autoridade de segurança da Comissão para eventuais exceções