2024/1418

24.5.2024

Decisão Delegada n.º 19/2024 relativa às regras de execução aplicáveis ao manuseamento de informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET

O COMITÉ ADMINISTRATIVO DO TRIBUNAL DE CONTAS EUROPEU,

tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente o artigo 287.º,

tendo em conta a Decisão n.º 41/2021 do Tribunal de Contas sobre as regras de segurança aplicáveis à proteção das informações classificadas da UE (ICUE) ([1]), em seguida designada por «Decisão n.º 41/2021»,

tendo em conta a política de segurança das informações do Tribunal de Contas (DEC 127/15 FINAL) e a política de classificação de informações (Comunicação ao Pessoal n.º 123/20) ([2]),

tendo em conta o debate que teve lugar no Comité Administrativo, na sua reunião de 18 de março de 2024,

considerando que a Decisão n.º 41/2021 é aplicável a todos os serviços e instalações do Tribunal de Contas,

considerando que a Decisão n.º 41/2021 prevê, no artigo 1.º, n.º 3, que devem ser adotadas disposições que assegurem que o pessoal do Tribunal de Contas que necessite de aceder a níveis mais elevados de ICUE o possa fazer em instalações adequadas de outras instituições ou organismos da UE,

considerando que a Decisão n.º 41/2021 prevê, nos artigos 1.º, n.º 3, e 5.º, n.º 6, que o Tribunal de Contas pode celebrar um contrato de nível de serviço com outra instituição da UE situada no Luxemburgo com vista a poder manusear e armazenar informações com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior numa Zona de Segurança dessa instituição, e que foi assinado um Memorando de Entendimento com a Direção-Geral dos Recursos Humanos e da Segurança da Comissão Europeia em 25 de setembro de 2023 sobre a utilização da sua Zona de Segurança no Luxemburgo,

considerando que as medidas de segurança destinadas a proteger as ICUE ao longo do seu ciclo de vida devem ser proporcionais, em particular, à sua classificação de segurança,

considerando que as medidas de segurança destinadas a proteger a confidencialidade, integridade e disponibilidade das informações comunicadas ao Tribunal de Contas devem ser adequadas à natureza e ao tipo de informações em questão,

considerando que a Decisão n.º 41/2021 prevê, no artigo 3.º, n.º 3, que as ICUE devem ser protegidas através de medidas de segurança física, e as informações classificadas como CONFIDENTIEL UE/EU CONFIDENTIAL ou superior devem, além disso, ser protegidas por medidas de segurança relativas ao pessoal,

considerando que a Decisão n.º 41/2021 prevê, no artigo 10.º, n.º 10, que o Comité Administrativo deve adotar uma decisão delegada que estabeleça as regras aplicáveis à sua execução e, nos artigos 8.º, n.º 1, e 10.º, n.º 1, que estas regras devem reger questões como o manuseamento e armazenamento de ICUE e as quebras de segurança,

considerando que o Tribunal de Contas assegurou, através da Decisão n.º 41/2021, que as suas medidas de segurança para garantir um elevado nível de proteção das ICUE são equivalentes às estabelecidas pelas regras de proteção das ICUE adotadas pelas outras instituições, órgãos e organismos da UE,

considerando que entrou em vigor um acordo administrativo mínimo entre o Tribunal de Contas e a Comissão, o Conselho e o Serviço Europeu para a Ação Externa (SEAE) em 27 de janeiro de 2023,

([1]) JO L 256 de 19.7.2021, p. 106.
([2]) Disponível em https://www.eca.europa.eu/pt/legal-framework.

DECIDE:

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 ([3]) e SECRET UE/EU SECRET ([4]), em conformidade com a Decisão n.º 41/2021 do Tribunal de Contas.

2. A presente decisão é aplicável a todos os serviços e instalações do Tribunal de Contas. Aplica-se também às suas câmaras de auditoria e comités, que são incluídos no termo «serviços» para efeitos da presente decisão.

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 o Tribunal de Contas;

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 por escrito as suas responsabilidades em matéria de proteção das informações em causa;

d) a pessoa ter obtido credenciação de segurança e ter-lhe sido concedida autorização de acesso pelo Diretor dos Recursos Humanos, Finanças e Serviços Gerais do Tribunal de Contas até ao nível pertinente e até uma data especificada, em conformidade com o artigo 4.º, n.º 4, da Decisão n.º 41/2021.

2. Não devem ser confiadas aos estagiários do Tribunal de Contas 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.

([3]) Nos termos do artigo 1.º, n.º 2, alínea a), da Decisão n.º 41/2021, entende-se por informações CONFIDENTIEL UE/EU CONFIDENTIAL «informações e material cuja divulgação não autorizada possa prejudicar os interesses essenciais da União Europeia ou de um ou mais Estados-Membros».

([4]) Nos termos do artigo 1.º, n.º 2, alínea a), da Decisão n.º 41/2021, entende-se por informações SECRET UE/EU SECRET «informações e material cuja divulgação não autorizada possa prejudicar seriamente os interesses essenciais da União Europeia ou de um ou mais Estados-Membros».

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 2.º, alínea m), da Decisão n.º 41/2021, seja a instituição, órgão ou organismo da UE, 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.

Artigo 4.º

Atribuição de um nível de classificação

1. 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 significativo às relações diplomáticas, ou seja, dar origem a protestos formais ou a outras sanções;

b) prejudicar a segurança ou a liberdade individuais,

c) causar danos à eficácia operacional ou à segurança do pessoal destacado dos Estados-Membros ou de outros contribuintes, ou à eficácia de operações valiosas de segurança ou de informações;

d) enfraquecer substancialmente a viabilidade financeira de organizações importantes;

e) prejudicar investigações ou facilitar a criminalidade grave;

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

g) impedir gravemente o desenvolvimento ou o funcionamento de políticas importantes da União;

h) paralisar ou perturbar de forma substancial atividades da União;

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

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

a) criar 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 individuais;

d) causar graves danos à eficácia operacional ou à segurança do pessoal destacado dos Estados-Membros ou de outros contribuintes, ou à eficácia contínua de operações de segurança ou de informações de grande valor;

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.

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

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, após confirmação pela entidade de origem do documento de que é seguro fazê-lo.

Artigo 6.º

Registo do material de referência

A fim de permitir o controlo por parte da entidade de origem, em conformidade com o artigo 14.º da presente decisão, 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 ponto 12 da política de segurança das informações do Tribunal de Contas, a classificação geral de um documento deve ser pelo menos a mesma que 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), 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 aposta 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 do presente artigo. Esta marca não deve ser traduzida para outras línguas.

3. A marca de classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET deve ser 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 todos os lados.

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) a data de criação deve ser indicada no documento.

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

Artigo 9.º

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

Podem ser utilizadas as abreviaturas C-UE/EU-C e S-EU/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 colocada a marca de classificação completa, por exemplo num suporte de armazenamento amovível com pouca capacidade. Podem ser utilizadas igualmente no corpo do texto se a utilização repetida da marca de classificação completa se tornar pesada. No cabeçalho e no rodapé do documento, a forma abreviada não deve substituir a marca de classificação completa.

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 com classificação 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.

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

SECRET UE/EU SECRET até [dd.mm.aaaa] e RESTREINT UE/EU RESTRICTED após essa data

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 estes estejam disponíveis.

2. Ao criar informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET, o pessoal do Tribunal de Contas deve utilizar um sistema de comunicação e informação acreditado pelo menos para o nível de classificação correspondente. Em caso de dúvida, deve consultar o Responsável pela Segurança das Informações do Tribunal de Contas.

3. Os documentos CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET, incluindo os que estiverem na fase de projeto (ver o artigo 5.º da presente decisão), 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 de 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 quando da sua receção. O registo deve ser efetuado:

— quando as informações chegam à Zona de Segurança da Comissão no Luxemburgo, ou saem dela, sendo a utilização dessa zona objeto de um memorando de entendimento celebrado pelo Tribunal de Contas;

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

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

3. Se as informações forem manuseadas eletronicamente num sistema de comunicação e informação, o registo pode também ser abrangido por processos desse próprio sistema. Neste caso, o sistema de comunicação e informação deve incluir medidas para garantir a integridade dos registos.

4. O Responsável do Controlo do Registo deve conservar um registo que contenha, para cada documento, pelo menos as seguintes informações:

a) a data de registo do documento classificado final;

b) o nível de classificação;

c) se for caso disso, a data de caducidade do nível de classificação;

d) o nome do serviço de origem;

e) o/os destinatário/os;

f) o objeto;

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

h) o número de registo nacional;

i) o número de cópias distribuídas;

j) sempre que possível, o registo das fontes utilizadas para criar o documento;

k) a data de desgraduação ou de desclassificação do documento;

l) informações sobre a sua 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. Se necessário, 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

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 seu consentimento prévio, por escrito, 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 do Tribunal de Contas, mas no interior da UE.

2. Os detentores 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 n.º 41/2021. Contrariamente às entidades de origem das informações classificadas, os detentores não são autorizados a tomar decisões sobre a desgraduação, desclassificação ou a 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 do Tribunal de Contas que tem a informação classificada exerce o «controlo da entidade de origem». Caso o detentor das informações considere necessária a divulgação de informações CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET a um país terceiro ou a uma organização internacional, o Tribunal de Contas solicita o parecer de uma das partes signatárias de um acordo de segurança das informações com o país terceiro ou a organização internacional em questão ([5]).

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

As informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET devem ser manuseadas e transmitidas por via eletrónica, se possível. Em conformidade com o artigo 6.º da Decisão n.º 41/2021, só podem ser utilizados os sistemas de comunicação e informação e os equipamentos acreditados pelo Tribunal de Contas ou por outra instituição, órgão ou organismo da UE para este efeito

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, tais como memórias USB, CD, DVD ou cartões de memória (incluindo dispositivos SSD ([6])), deve ser rigorosamente controlada e contabilizada. Apenas são utilizados os suportes de armazenamento amovíveis fornecidos pelo Tribunal de Contas ou por outra instituição, órgão ou organismo da UE e aprovados pelo Responsável pela Segurança das Informações, bem como encriptados por um produto que este tenha aprovado. Os suportes de armazenamento amovíveis pessoais e os suportes distribuídos gratuitamente em conferências, seminários, etc. não são utilizados para transferir informações classificadas. Sempre que possível, deverão ser utilizados suportes de armazenamento amovíveis com segurança TEMPEST, em conformidade com as orientações do Responsável pela Segurança das Informações.

([5]) Para mais informações, ver o artigo 35.º da presente decisão.
([6]) Dispositivos semicondutores para armazenamento ou dispositivos/unidades de estado sólido.

2. Quando um documento classificado for manuseado ou armazenado eletronicamente em suportes de armazenamento amovíveis, 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, os dispositivos podem justificar um nível de classificação mais elevado.

4. Só são utilizados sistemas de comunicação e informação devidamente acreditados para transferir informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET para suportes de armazenamento amovíveis ou que provenham deles.

5. Antes de descarregar estas informações para suportes de armazenamento amovíveis, devem ser tomadas precauções especiais 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 colocados num cofre apropriado, os suportes de armazenamento amovíveis devem ser destruídos quando deixarem de ser necessários. As operações de destruição ou apagamento devem cumprir as regras de segurança do Tribunal de Contas. Deve ser mantido um inventário dos suportes de armazenamento amovíveis e a sua destruição é 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 5.º, n.ºs 5 e 6, da Decisão n.º 41/2021, as informações CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET devem ser manuseadas numa Zona de Segurança ([7]). Estas informações também podem ser consultadas pelo pessoal do Tribunal de Contas nas Zonas de Segurança de outra instituição da UE.

2. Nos termos do artigo 5.º, n.º 6, da Decisão n.º 41/2021, e se tal for especificamente acordado pela entidade de origem, estas informações podem ser manuseadas, a título excecional, na Zona Administrativa ([8]) do Tribunal de Contas, desde que as ICUE estejam protegidas para evitar o acesso de pessoas não autorizadas.

3. Em tempos de crise ou em caso de emergência, estas informações podem ser manuseadas fora de uma Zona de Segurança ou Administrativa, desde que o detentor se tenha comprometido a aplicar medidas de compensação que incluam, pelo menos, o seguinte:

— 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 de documentos em papel, o detentor notifica o Registo das ICUE, o mais rapidamente possível e em função da natureza da situação de crise ou de emergência, de que os documentos classificados estão a ser manuseados fora de uma Zona de Segurança ou Administrativa;

— os documentos devem ser armazenados em cofres apropriados quando não estiverem a ser lidos ou discutidos;

— as portas da sala devem manter-se fechadas durante a leitura ou o debate dos documentos;

— o conteúdo dos documentos não é discutido ao telefone numa linha não protegida ou por correio eletrónico;

— o detentor não deve fotocopiar nem digitalizar documentos; só o Registo das ICUE fornece cópias adicionais;

([7]) Tal como definido no artigo 18.º da 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).

([8]) Definidas no anexo da Decisão n.º 41/2021.

— os documentos só podem ser manuseados e mantidos temporariamente fora de uma Zona Administrativa ou de Segurança durante o tempo estritamente necessário, após o que devem ser devolvidos ao Registo das ICUE;

— a devolução dos documentos deve ser acompanhada de uma assinatura;

— o detentor não deve deitar fora os documentos classificados nem destrui-los.

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 pela Segurança das Informações.

6. Devem ser comunicados ao Responsável pela Segurança das Informações, 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. O Tribunal de Contas pode igualmente solicitar à entidade de origem que forneça uma cópia traduzida para inglês.

2. Quando apenas for reproduzida uma parte de um documento classificado, aplicam-se as mesmas condições que à cópia integral do documento. Os extratos devem ser classificados ao mesmo nível, a menos que a entidade de origem os tenha especificamente classificado num nível inferior ou marcado como não classificados.

3. As medidas de segurança aplicáveis às informações originais devem ser 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 de uma Zona de Segurança ou Zona Administrativa devem ser, em conformidade com o artigo 17.º, n.º 2, da presente decisão, enviadas por via eletrónica através de meios devidamente acreditados e/ou protegidas por produtos criptográficos aprovados.

2. Em função dos meios disponíveis e das circunstâncias específicas, as informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET podem 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. Nos termos do artigo 6.º, n.º 8, da Decisão n.º 41/2021, os suportes de armazenamento amovíveis devem ser encriptados por meio de um produto aprovado para a proteção das ICUE, quer pelo Conselho, ou pelo seu Secretário-Geral, na sua capacidade de autoridade de aprovação criptográfica, quer por outra instituição, órgão ou organismo da UE. 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 desta forma devem ser manuseadas da mesma forma que as informações impressas.

4. As remessas podem conter mais de um elemento de ICUE, desde que seja respeitado o princípio da necessidade de ter conhecimento.

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

6. O pessoal ou os serviços de correio rápido que transportem em mão própria informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET devem receber uma autorização de segurança e um certificado de estafeta.

7. Os sobrescritos e as embalagens não são abertos durante o percurso. A autorização de segurança concedida aos estafetas não lhes confere o direito de acederem às informações classificadas constantes da remessa.

8. Nos termos do artigo 5.º, n.º 12, da Decisão n.º 41/2021, a entidade de origem pode igualmente impor medidas de segurança física adicionais para proteger as informações de divulgação não autorizada durante o transporte.

9. Quaisquer suspeitas ou casos reais de incidentes de segurança que envolvam informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET transportadas pelo pessoal ou por serviços de correio rápido devem ser comunicados ao Responsável pela Segurança das Informações para investigação subsequente o mais rapidamente possível.

Artigo 20.º

Transporte em mão própria de suportes de armazenamento amovíveis

1. Os suportes de armazenamento amovíveis utilizados para o transporte de informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET devem ser acompanhados de uma nota de envio com informações pormenorizadas sobre estes suportes e todos os ficheiros neles contidos, de modo que o destinatário possa efetuar as verificações necessárias e confirmar a receção.

2. Os dispositivos devem conter apenas as ICUE transportadas. Todas as informações classificadas contidas num único dispositivo devem ter o mesmo destinatário. O remetente tem em conta que o armazenamento de grandes quantidades de informações classificadas no mesmo dispositivo pode 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. Todas as informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET guardadas em suportes de armazenamento amovíveis devem ser registadas para fins de segurança.

Artigo 21.º

Transporte de documentos com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET nos serviços e nas instalações do Tribunal de Contas

1. O pessoal habilitado com autorização de segurança pode transportar documentos com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET nos serviços e nas instalações do Tribunal de Contas, mas os documentos não devem deixar a posse do portador nem ser lidos em público.

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

Artigo 22.º

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

1. As informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET podem ser transportadas por membros do pessoal ou estafetas do Tribunal de Contas ou da instituição, órgão ou organismo da UE de origem, em qualquer lugar da União, desde que se respeitam as seguintes instruções:

a) as embalagens e os sobrescritos utilizados para transmitir informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET devem ser duplos e opacos. A embalagem exterior deve ser selada e não dar 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 ficam sempre na posse do portador;

c) o sobrescrito ou embalagem não é aberto durante o percurso, e as informações não são 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 estas sejam transmitidas por um dos seguintes meios:

a) 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 23.º da presente decisão;

b) estafeta militar, correio oficial ou mala diplomática, em coordenação com o pessoal do Serviço de Registos.

3. O pessoal que pretenda enviar informações com classificação SECRET UE/EU SECRET para outros locais da União pode apenas contactar o Responsável do Controlo do Registo para que estas sejam transmitidas por estafeta militar, correio oficial ou mala diplomática, e não por um serviço postal ou um serviço de correio comercial.

4. O pessoal do Tribunal de Contas ou o correio oficial que sejam portadores de informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET devem possuir um certificado de estafeta para cada remessa. O certificado deve ser emitido pelo Responsável do Controlo do Registo e indicar que o portador está autorizado a transportar a remessa.

Artigo 23.º

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

1. As informações com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET podem ser transportadas em mão própria pelo pessoal do Tribunal de Contas ou da instituição, órgão ou organismo da UE de origem, entre o território da União e o território de um país terceiro.

2. O pessoal do Registo pode providenciar o transporte por estafeta militar ou mala diplomática.

3. Quando transportar em mão própria documentos impressos ou suportes de armazenamento amovíveis classificados como CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET, o pessoal deve respeitar todas as seguintes medidas adicionais:

— quando se deslocar 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 devem 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 é submetida a controlos de segurança;

— O portador deve possuir um certificado de estafeta emitido pelo Responsável do Controlo do Registo atestando que está autorizado a transportar a remessa com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET.

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 pagamento e são transportadas pessoalmente ou seguidas.

2. Os serviços comerciais de correio rápido podem transportar informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL dentro de um Estado-Membro da UE ou entre dois Estados-Membros. Podem transmitir informações SECRET UE/EU SECRET dentro de um Estado-Membro, mas não para o estrangeiro.

3. Os serviços comerciais de correio rápido devem receber instruções no sentido de apenas entregarem remessas com classificação 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.

Artigo 25.º

Preparação das ICUE para transporte por serviços comerciais de correio rápido

1. Ao preparar remessas classificadas, o remetente deve ter em conta que os serviços comerciais de correio rápido só podem entregar remessas com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET ao Responsável do Controlo do Registo, ao seu substituto devidamente autorizado ou ao destinatário previsto.

2. As remessas de informações enviadas através de um serviço comercial de correio rápido aprovado devem ser preparadas e embaladas do seguinte modo:

a) As informações devem ser colocadas num sobrescrito duplo opaco (devendo o sobrescrito interior revelar qualquer tentativa de o abrir) ou noutro material de embalagem seguro.

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

c) A embalagem exterior deve ser selada e não ostentar qualquer marca de classificação.

d) Os sobrescritos ou camadas tanto interiores como exteriores da embalagem devem ser claramente endereçados a uma pessoa devidamente identificada pelo seu nome no destinatário previsto e indicar um endereço de devolução.

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

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

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

3. Antes de enviar uma remessa, o remetente combina com o destinatário indicado uma data e uma 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 atraso na entrega da remessa, o remetente deve informar o Responsável pela Segurança das Informações e o do Controlo do Registo, que procedem ao seguimento do incidente de segurança.

Artigo 26.º

Outras condições de manuseamento específicas

1. Devem ser respeitadas todas as condições de transporte adicionais estabelecidas num acordo de segurança das informações ou em acordos administrativos. Em caso de dúvida, o pessoal consulta o Responsável pela Segurança das Informações ou o Responsável do Controlo do Registo.

2. O requisito de dupla embalagem pode ser dispensado no caso das informações classificadas protegidas por produtos criptográficos aprovados. Contudo, para efeitos de expedição, e porque o meio de armazenamento amovível ostenta uma marca de classificação de segurança explícita, este deve ser transportado pelo menos num sobrescrito opaco fechado, se necessário recorrendo a medidas de proteção material adicionais, como, por exemplo, um sobrescrito almofadado.

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 CONFIDENTIAL ou SECRET UE/EU SECRET só devem ser realizadas em salas de reuniões que tenham sido acreditadas ao nível adequado ou superior. O Tribunal de Contas pode utilizar salas de reunião na Zona de Segurança de outra instituição da UE. Quando estas salas não estiverem disponíveis, o pessoal deve solicitar aconselhamento ao Responsável pela Segurança das Informações.

2. Regra geral, as ordens de trabalhos não são classificadas. O facto de a ordem de trabalhos de uma reunião mencionar documentos classificados não implica que seja automaticamente classificada. Os pontos da ordem de trabalhos devem ser redigidos de modo a evitar pôr em risco os interesses da União ou de qualquer Estado-Membro.

3. Os organizadores das reuniões recordam aos participantes que quaisquer observações sobre pontos da ordem de trabalhos com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET não devem ser enviadas por correio eletrónico nem por quaisquer 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 CONFIDENTIAL e SECRET UE/EU SECRET, a fim de facilitar o bom funcionamento da reunião. Só as pessoas com necessidade de tomar conhecimento, que disponham de uma credenciação de segurança de nível adequado e que tenham sido devidamente autorizadas, podem estar presentes durante o debate dos pontos classificados.

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

6. Os organizadores das reuniões devem recordar aos participantes que devem deixar fora da sala de reuniões os dispositivos eletrónicos portáteis durante o debate de pontos CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET.

7. Os organizadores devem elaborar antecipadamente uma lista completa dos participantes. Em conformidade com o artigo 4.º, n.º 6, da Decisão n.º 41/2021, devem informar igualmente o Responsável pela Segurança das Informações, em tempo útil, das datas, horas, locais e listas de participantes.

Artigo 28.º

Acesso dos participantes a uma reunião CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET

1. Os organizadores das reuniões devem informar o Responsável pela Segurança das Informações e o Responsável do Controlo do Registo de quaisquer visitantes externos que participem numa reunião CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET organizada pelo Tribunal de Contas.

2. Os participantes têm de provar que possuem uma credenciação de segurança do pessoal de nível adequado válida, a fim de poderem participar no debate de pontos CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET.

Artigo 29.º

Equipamento eletrónico em salas de reunião CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET

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

Artigo 30.º

Procedimentos a seguir durante uma reunião CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET

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

2. No início do debate, deve ser entregue aos participantes e aos intérpretes apenas o número necessário de documentos, se for caso disso.

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

4. No final da reunião, é 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 não exigidos pelos participantes no final da reunião, bem como todos os documentos utilizados pelos intérpretes, devem ser assinados e devolvidos ao Responsável do Controlo do Registo para eliminação em destruidoras aprovadas ([9]).

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 devem ter acesso a informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET os intérpretes e tradutores devidamente autorizados que disponham de credenciação de segurança e que estejam abrangidos pelo Estatuto do Pessoal ou pelo Regime Aplicável aos Outros Agentes da União Europeia ([10]) ou aqueles que tenham uma relação contratual com o Tribunal de Contas ou outra instituição da UE.

([9]) Para mais informações, ver o artigo 42.º, n.º 6, da presente decisão.

([10]) Regulamento n.º 31 (CEE) que fixa o Estatuto dos Funcionários e o Regime aplicável aos outros agentes, com a última redação (JO 45 de 14.6.1962, p. 1385/62) (https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:01962R0031-20230101).

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 o Tribunal de Contas 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 do Tribunal de Contas que tem as informações classificadas deve solicitar à entidade de origem o consentimento prévio por escrito para a sua comunicação. Se não for possível identificar a entidade de origem, o serviço do Tribunal de Contas que tem a informação classificada deve exercer o «controlo da 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 podem ser partilhadas com outra instituição, órgão ou organismo da UE se o destinatário tiver necessidade de tomar conhecimento e a entidade tiver um acordo jurídico correspondente com o Tribunal de Contas.

2. No Tribunal de Contas, o Registo das ICUE deve ser, regra geral, o principal ponto de entrada e de saída para os intercâmbios de informações classificadas com outras instituições, órgãos ou organismos da União.

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 e tiver obtido credenciação de segurança.

2. As informações classificadas dos Estados-Membros que ostentem uma marca de classificação nacional equivalente ([11]) e tenham sido disponibilizadas ao Tribunal de Contas 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 o país ou a organização internacional dispuser de um quadro jurídico ou administrativo adequado, como por exemplo um acordo de segurança das informações ou um convénio administrativo com o Tribunal de Contas. As disposições desses acordos ou convénios prevalecem sobre as da presente decisão.

2. Regra geral, o Registo das ICUE 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 o Tribunal de Contas e países terceiros e organizações internacionais.

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

3. Todas as informações classificadas recebidas de um país terceiro ou de uma organização internacional devem ser registadas para efeitos de segurança. Por conseguinte, o pessoal deve contactar o Registo das ICUE se receber informações classificadas provenientes de fora do circuito habitual de 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 a uma Zona de Segurança ou saem dela;

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

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 acordo de segurança das informações ou convénio administrativo aplicável.

Artigo 36.º

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

1. Sempre que o Tribunal de Contas 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.

2. Os serviços do Tribunal de Contas devem contactar o Responsável pela Segurança das Informações e a entidade de origem. O Tribunal de Contas solicita o parecer de uma das partes signatárias de um acordo de segurança das informações com a entidade da UE, o país terceiro ou a organização internacional em questão.

3. Após esta consulta, o Colégio do Tribunal de Contas pode, com base numa proposta do Secretário-Geral, autorizar a divulgação 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 efetuar uma desgraduação ou desclassificação

1. As informações só permanecem classificadas enquanto necessitarem de proteção. Entende-se por desgraduação a redução do nível de classificação de segurança. A desclassificação significa que as informações deixam de ser consideradas classificadas. Quando 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 do Tribunal de Contas 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 do Tribunal de Contas que cria um documento classificado é responsável por decidir se o mesmo pode ser desgraduado ou desclassificado. No Tribunal de Contas, todos os pedidos de desgraduação e desclassificação devem ser submetidos à consulta do chefe ou do diretor do serviço de origem ou do responsável de tarefa. Se o serviço tiver compilado informações classificadas provenientes de várias fontes, deve, em primeiro lugar, solicitar o consentimento das partes que tenham fornecido material de origem, incluindo os Estados-Membros, outros organismos da UE, países terceiros ou organizações internacionais.

3. Se o serviço de origem do Tribunal de Contas já não existir e as suas atribuições tiverem sido transferidas para outro serviço, a decisão de desgraduação ou desclassificação é tomada por este último. Se o serviço de origem já não existir e as suas atribuições não tiverem sido transferidas para outro serviço, a decisão de desgraduação ou desclassificação deve ser tomada conjuntamente pelos diretores do Tribunal de Contas.

4. O serviço responsável pela desgraduação ou desclassificação deve trabalhar com o Registo das ICUE sobre as modalidades práticas de 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 informações sensíveis não classificadas na aceção do ponto 16 da política de classificação das informações do Tribunal de Contas ([12]) e do capítulo 4 das suas orientações relativas à classificação e manuseamento das informações não classificadas da UE.

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 (e não suprimida), utilizando a funcionalidade «riscado» no caso de formatos eletrónicos, ou de forma manual nos documentos impressos.

2. A primeira página (capa) deve ser carimbada com a indicação de que o documento é desgraduado ou desclassificado e preenchida com os dados da autoridade responsável pela desgraduação ou desclassificação e a data correspondente.

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

4. O Serviço de Arquivos do Tribunal de Contas 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.

([12]) Disponível em https://www.eca.europa.eu/pt/legal-framework.

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. A desclassificação parcial de informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET resulta na produção de um extrato desclassificado.

3. No extrato desclassificado, as partes que permaneçam classificadas devem ser substituídas pela menção:

PARTE QUE NÃO DEVE SER DESCLASSIFICADA

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

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. O Tribunal de Contas 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 efeitos de destruição ou apagamento. Este procedimento é aplicável periodicamente tanto às informações em papel como às armazenadas em sistemas de comunicação e informação.

3. O pessoal não deve proceder à destruição de quaisquer documentos em papel CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET de que já não necessite, mas solicitar ao Responsável do Controlo do Registo que os destrua, sob reserva de quaisquer 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 devem ser utilizadas destruidoras aprovadas para eliminar documentos com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e 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 do Controlo do Registo deve emitir certificados de destruição e atualizar os livros de registo eletrónicos e outras informações de registo em conformidade.

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 termo do seu ciclo de vida. 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 implica eliminar todos 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 Responsável pela Segurança das Informações para destruição e eliminação após o Responsável do Controlo do Registo ter sido informado.

Artigo 43.º

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

1. Em conformidade com o Memorando de Entendimento celebrado entre o Tribunal de Contas e a Direção-Geral dos Recursos Humanos e da Segurança da Comissão sobre a utilização da sua Zona de Segurança, é aplicável o procedimento de emergência estabelecido pela Comissão para a salvaguarda das informações classificadas. Se necessário, o responsável local de segurança da Direção de Segurança da Comissão no Luxemburgo terá acesso seguro ao Tribunal de Contas, a fim de aplicar o procedimento de emergência estabelecido pela Comissão e ativar quaisquer planos de evacuação e destruição de emergência para salvaguardar ICUE que corram um risco significativo de cair em 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:

i) deslocar as ICUE para um local seguro alternativo, se possível uma Zona de Segurança no mesmo edifício;

ii) evacuar as ICUE para um local seguro alternativo, se possível uma Zona de Segurança num edifício diferente, de preferência de uma instituição da UE;

iii) destruir as ICUE, utilizando, se possível, um dos meios de destruição aprovados.

2. Se forem ativados os planos de emergência, será dada prioridade à mudança ou à destruição das informações com classificação SECRET UE/EU SECRET primeiro e das informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL em seguida.

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 utilizado para armazenar informações com 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 de segurança das informações, a política de classificação de informações e a política de arquivamento do Tribunal de Contas.

2. Os documentos com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET não são enviados para os Arquivos Históricos da União Europeia em Florença.

CAPÍTULO 7

DISPOSIÇÕES FINAIS

Artigo 45.º

Transparência

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

Artigo 46.º

Entrada em vigor

Após a sua adoção pelo Comité Administrativo, a presente decisão entra em vigor no dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*.

Feito no Luxemburgo, em 19 de março de 2024.

Pelo Comité Administrativo do Tribunal de Contas
O Presidente
Tony MURPHY

ANEXO

Categorias de pessoal que podem ter acesso a informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET quando forem necessárias para o exercício das suas funções

Categorias de pessoal do Tribunal de Contas	Acesso às informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET	Condições
Membros	Sim	Instruções + reconhecimento
Funcionários	Sim	Verificação + instruções + reconhecimento + necessidade de tomar conhecimento
Agentes temporários	Sim	Verificação + instruções + reconhecimento + necessidade de tomar conhecimento
Agentes contratuais	Sim	Verificação + instruções + reconhecimento + necessidade de tomar conhecimento
Peritos nacionais destacados dos Estados-Membros da UE	Sim	Apenas se autorizado pelos Estados-Membros de origem antes de assumirem as suas funções + instruções (pelo Tribunal de Contas) + reconhecimento + autorização do Tribunal de Contas + necessidade de tomar conhecimento
Estagiários	Não	Nenhuma exceção possível
Qualquer outra categoria de pessoal (pessoal contratado a agências de trabalho temporário, pessoal externo que trabalha nas instalações do Tribunal de Contas, etc.)	Não	Nenhuma exceção possível