IV

(Informações)

INFORMAÇÕES DAS INSTITUIÇÕES, ÓRGÃOS E ORGANISMOS DA UNIÃO EUROPEIA

PARLAMENTO EUROPEU

DECISÃO DA MESA DO PARLAMENTO EUROPEU

de 6 de Junho de 2011

sobre as regras que regem o tratamento de informações confidenciais pelo Parlamento Europeu

(2011/C 190/02)

A MESA DO PARLAMENTO EUROPEU,

Tendo em conta o n.º 12 do artigo 23.º do Regimento do Parlamento Europeu,

considerando o seguinte:

(1) Tendo em conta o Acordo-Quadro sobre as relações entre o Parlamento Europeu e a Comissão Europeia [1], assinado em 20 de Outubro de 2010 («Acordo-Quadro»), é necessário rever a Decisão da Mesa, de 13 de Novembro de 2006, sobre as regras que regem o tratamento administrativo de documentos confidenciais.

(2) O Tratado de Lisboa confere novas competências ao Parlamento Europeu e, para que este possa desenvolver actividades em domínios que exigem um certo grau de confidencialidade, é necessário estabelecer princípios de base, normas mínimas de segurança e procedimentos adequados para o tratamento de informações confidenciais, incluindo informações classificadas, pelo Parlamento Europeu.

(3) As regras previstas na presente decisão destinam-se a garantir normas equivalentes de protecção e a compatibilidade com as regras adoptadas por outras instituições, órgãos, organismos e agências estabelecidos por força ou com base nos Tratados ou pelos Estados-Membros, a fim de facilitar o bom funcionamento do processo decisório a nível da União Europeia.

(4) As disposições da presente decisão são adoptadas sem prejuízo do artigo 15.º do Tratado sobre o Funcionamento da União Europeia (TFUE) e do Regulamento (CE) n.º 1049/2001 do Parlamento Europeu e do Conselho, de 30 de Maio de 2001, relativo ao acesso do público aos documentos do Parlamento Europeu, do Conselho e da Comissão [2].

(5) As disposições da presente decisão são adoptadas sem prejuízo do artigo 16.º do TFUE e do Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de Dezembro de 2000, relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados [3],

ADOPTOU A PRESENTE DECISÃO:

Artigo 1.º

Objectivo

A presente decisão rege a produção, a recepção, a transmissão e o armazenamento de informações pelo Parlamento Europeu a fim de proteger de forma adequada a sua natureza confidencial. Dá aplicação, em particular, ao anexo 2 do Acordo-Quadro.

[1] JO L 304 de 20.11.2010, p. 47.

[2] JO L 145 de 31.5.2001, p. 43.

[3] JO L 8 de 12.1.2001, p. 1.

Artigo 2.º

Definições

Para efeitos da presente decisão, entende-se por:

a) «Informação», uma informação oral ou escrita, seja qual for o seu suporte ou o seu autor;

b) «Informações confidenciais», «informações classificadas da UE» e «outras informações confidenciais» não classificadas;

c) «Informações classificadas da UE», informações ou materiais classificados como «TRÈS SECRET UE/EU TOP SECRET», «SECRET UE/EU SECRET», «CONFIDENTIEL UE/EU CONFIDENTIAL» ou «RESTREINT UE/EU RESTRICTED», cuja divulgação não autorizada possa causar prejuízos de diversos níveis aos interesses da UE ou de um ou vários dos seus Estados-Membros, quer tais informações tenham origem nas instituições, órgãos, organismos e agências estabelecidos por força ou com base nos Tratados, quer provenham de Estados-Membros, de países terceiros ou de organizações internacionais. Neste contexto:

— «TRÈS SECRET UE/EU TOP SECRET» é a classificação de informações e materiais cuja divulgação não autorizada possa prejudicar de forma excepcionalmente grave os interesses essenciais da União Europeia ou de um ou vários dos seus Estados-Membros,

— «SECRET UE/EU SECRET» é a classificação de informações e materiais cuja divulgação não autorizada possa prejudicar gravemente os interesses essenciais da União Europeia ou de um ou vários dos seus Estados-Membros,

— «CONFIDENTIEL UE/EU CONFIDENTIAL» é a classificação de informações e materiais cuja divulgação não autorizada possa prejudicar os interesses essenciais da União ou de um ou vários dos seus Estados-Membros,

— «RESTREINT UE/EU RESTRICTED» é a classificação de informações e materiais cuja divulgação não autorizada possa ser desfavorável para os interesses da União ou de um ou vários dos seus Estados-Membros;

d) «Outras informações confidenciais», outras informações não classificadas, incluindo informações abrangidas por regras relativas à protecção de dados ou pela obrigação de sigilo profissional, produzidas no Parlamento Europeu ou transmitidas por outras instituições, órgãos, organismos e agências estabelecidos por força ou com base nos Tratados ou pelos Estados-Membros ao Parlamento Europeu;

e) «Documento», uma informação registada, independentemente da sua forma física ou das suas características;

f) «Material», um documento ou parte de maquinaria ou equipamento, produzido ou em processo de produção;

g) «Necessidade de tomar conhecimento», a necessidade de uma pessoa aceder a informações confidenciais para desempenhar uma função oficial ou executar uma tarefa;

h) «Autorização», uma decisão (decisão de habilitação) adoptada pelo Presidente, se disser respeito a deputados ao Parlamento Europeu, ou pelo Secretário-Geral, se disser respeito a funcionários do Parlamento Europeu e a outros agentes do Parlamento ao serviço dos grupos políticos, de conceder acesso individual a informações classificadas da UE até um determinado nível, com base no resultado positivo de um inquérito de segurança (procedimento de habilitação) efectuado por uma autoridade nacional nos termos da lei nacional e do anexo I, parte 2;

i) «Desgraduação», uma redução do nível de classificação;

j) «Desclassificação», a supressão de qualquer classificação;

k) «Entidade de origem», o autor devidamente autorizado de informações classificadas da UE ou de outras informações confidenciais;

l) «Indicações de segurança», as medidas técnicas de aplicação estabelecidas no anexo II [1].

Artigo 3.º

Princípios de base e normas mínimas

1. O tratamento de informações confidenciais pelo Parlamento Europeu obedece aos princípios de base e às normas mínimas estabelecidos no anexo I, parte 1.

2. O Parlamento Europeu cria um sistema de gestão da segurança das informações em conformidade com esses princípios de base e essas normas mínimas cujo objectivo consiste em facilitar o trabalho parlamentar e administrativo e, simultaneamente, assegurar a protecção das informações confidenciais tratadas pelo Parlamento Europeu, respeitando plenamente as regras estabelecidas pela entidade de origem das informações que figuram nas indicações de segurança.

O tratamento de informações confidenciais por meio dos sistemas de informação automatizados do Parlamento Europeu é efectuado com base no conceito de garantia da segurança da informação e estabelecido nas indicações de segurança.

[1] Anexo a adoptar.

3. Os deputados ao Parlamento Europeu podem consultar informações classificadas até ao nível «CONFIDENTIEL UE/EU CONFIDENTIAL», inclusive, sem necessidade de habilitação de segurança. Caso se trate de informações classificadas como «CONFIDENTIEL UE/EU CONFIDENTIAL», devem assinar uma declaração sob compromisso de honra de que não divulgarão o conteúdo dessas informações a terceiros. As informações com uma classificação superior a «CONFIDENTIEL UE/EU CONFIDENTIAL» só são colocadas à disposição dos deputados que disponham do nível de habilitação de segurança adequado.

4. Os funcionários do Parlamento Europeu e outros agentes do Parlamento ao serviço dos grupos políticos podem consultar informações classificadas se tiverem uma razão válida para delas tomarem conhecimento, e podem consultar informações com uma classificação superior a «RESTREINT UE/EU RESTRICTED» se dispuserem do nível de habilitação de segurança adequado.

Artigo 4.º

Produção de informações confidenciais e tratamento administrativo pelo Parlamento Europeu

1. O Presidente do Parlamento Europeu, os presidentes das comissões parlamentares interessadas e o Secretário-Geral e/ou qualquer pessoa por este devidamente autorizada por escrito podem produzir informações confidenciais e/ou informações classificadas, tal como estabelecido nas indicações de segurança.

2. Ao produzir informações classificadas, a entidade de origem aplica o nível adequado de classificação, em conformidade com as normas e definições internacionais que figuram no anexo I. Regra geral, a entidade de origem indica igualmente os destinatários que podem ser autorizados a consultar as informações em função do nível de classificação. Esta informação é comunicada ao Serviço de Informações Confidenciais (SIC) quando os documentos forem depositados no SIC.

3. As informações confidenciais abrangidas pelo sigilo profissional são tratadas em conformidade com as instruções de tratamento definidas nas indicações de segurança.

Artigo 5.º

Recepção de informações confidenciais pelo Parlamento Europeu

1. As informações confidenciais recebidas pelo Parlamento Europeu são comunicadas do seguinte modo:

— Informações classificadas da UE do nível «RESTREINT EU/EU RESTRICTED» e outras informações confidenciais, ao secretariado da instância parlamentar ou do titular de um cargo que apresentou o pedido,

— Informações classificadas da UE do nível «CONFIDENTIEL UE/EU CONFIDENTIAL» e superior, ao SIC.

2. O registo, o armazenamento e a rastreabilidade das informações confidenciais são assegurados pelo secretariado da instância parlamentar ou do titular de um cargo que recebeu as informações ou pelo SIC.

3. No caso de informações confidenciais transmitidas pela Comissão nos termos do Acordo-Quadro, as modalidades acordadas nos termos do anexo II, ponto 3.2, do Acordo-Quadro (estabelecidas por comum acordo e referentes aos destinatários, ao processo de consulta, ou seja, sala de leitura segura e reuniões à porta fechada, ou a outras matérias) para preservar a confidencialidade das informações são depositadas, juntamente com as informações confidenciais, no secretariado da instância parlamentar ou do titular de um cargo ou no SIC quando as informações estiverem classificadas com o nível «CONFIDENTIEL UE/EU CONFIDENTIAL» ou superior.

4. As modalidades referidas no n.º 3 podem ser igualmente aplicadas, com as necessárias adaptações, à transmissão de informações confidenciais por outras instituições, órgãos, organismos e agências estabelecidos por força ou com base nos Tratados ou pelos Estados-Membros.

5. A transmissão de informações classificadas da UE do nível «TRÈS SECRET UE/EU TOP SECRET» ao Parlamento Europeu está sujeita a outras modalidades, a acordar entre a instância parlamentar ou o titular de um cargo que apresentou o pedido de informação e as instituições da UE ou os Estados-Membros que as transmitem. A Conferência dos Presidentes cria um comité de supervisão encarregado de garantir um nível de protecção adequado a esse nível de classificação.

Artigo 6.º

Transmissão de informações classificadas da UE a terceiros pelo Parlamento Europeu

O Parlamento Europeu pode transmitir, sob reserva de consentimento da entidade de origem, informações classificadas da UE a outras instituições, órgãos, organismos e agências estabelecidos por força ou com base nos Tratados ou aos Estados-Membros, desde que estes assegurem que, aquando do tratamento de informações classificadas da UE, sejam aplicadas, nos seus serviços e instalações, regras equivalentes às previstas na presente decisão.

Artigo 7.º

Armazenamento e consulta de informações confidenciais em zonas protegidas (salas de leitura segura)

1. As salas de leitura segura devem dispor de um sistema de armazenamento seguro e não podem conter fotocopiadoras, telefones, fax, *scanners* ou qualquer outro equipamento técnico de reprodução ou transmissão de documentos.

2. O acesso a uma sala de leitura segura rege-se pelas seguintes condições:

a) Só têm acesso à sala de leitura segura as seguintes pessoas:

— os deputados ao Parlamento Europeu, os funcionários do Parlamento Europeu e outros agentes do Parlamento ao serviço dos grupos políticos, devidamente identificados, de acordo com as modalidades referidas no artigo 4.º, n.º 2, ou no artigo 5.º, n.ºs 3 e 4,

— os funcionários do Parlamento Europeu responsáveis pela gestão do SIC,

— se necessário, os funcionários do Parlamento Europeu responsáveis pela segurança e pela prevenção de incêndios.

A limpeza da zona segura é efectuada apenas na presença e sob apertada vigilância de um funcionário do SIC;

b) Cada pessoa que pretenda aceder a informações confidenciais comunica com antecedência o seu nome ao SIC. O SIC verifica a identidade de cada pessoa que apresente um pedido de consulta dessas informações e, se necessário, verifica se essa pessoa dispõe do nível de habilitação de segurança exigido e se está autorizada a consultá-las de acordo com as modalidades referidas no artigo 4.º, n.º 2, ou no artigo 5.º, n.ºs 3 e 4;

c) O SIC tem competência para recusar o acesso à sala a qualquer pessoa não autorizada a entrar nela nos termos das alíneas a) e b). Qualquer objecção à decisão do SIC é apresentada ao Presidente, no caso dos deputados ao Parlamento Europeu, ou ao Secretário-Geral, nos restantes casos.

3. A consulta de informações confidenciais na sala de leitura segura rege-se pelas seguinte regras:

a) As pessoas autorizadas a consultar as informações e que tenham apresentado o pedido a que se refere o n.º 2, alinea b), devem comparecer pessoalmente no SIC.

Salvo em circunstâncias excepcionais (por exemplo, caso tenha sido apresentado um número elevado de pedidos de consulta num curto período), a consulta de informações confidenciais na sala de leitura segura só é autorizada a uma pessoa de cada vez, na presença de um funcionário do SIC.

Esse funcionário informa a pessoa assim autorizada das obrigações que lhe incumbem e, nomeadamente, requer-lhe que assine uma declaração sob compromisso de honra de que não divulgará o conteúdo das informações a terceiros;

b) Durante a consulta não é permitido o contacto com o exterior (inclusive por meio de telefones ou de outras tecnologias), a tomada de notas, nem a fotocópia ou fotografia das informações confidenciais consultadas;

c) Antes de autorizar uma pessoa a abandonar a sala de leitura segura, o funcionário do SIC referido na alínea a) certifica-se de que as informações confidenciais consultadas se mantêm presentes, intactas e completas.

4. Em caso de infracção às regras acima definidas, o funcionário responsável do SIC informa o Secretário-Geral, o qual submete o assunto ao Presidente, caso o infractor seja um deputado ao Parlamento Europeu.

Artigo 8.º

Normas mínimas aplicáveis a outras consultas de informações confidenciais

1. No que diz respeito ao tratamento administrativo de informações confidenciais numa reunião à porta fechada, o secretariado da instância parlamentar ou do titular de um cargo responsável pela reunião assegura que:

— Só sejam autorizadas a entrar na sala as pessoas designadas para participar na reunião e que disponham do nível de habilitação exigido em matéria de segurança;

— Todos os documentos sejam numerados, distribuídos no início da reunião e recolhidos no final, e que não sejam tomadas notas nem feitas fotocópias ou fotografias desses documentos;

— A acta da reunião não mencione o conteúdo do debate sobre as informações apreciadas segundo o procedimento confidencial;

— As informações confidenciais prestadas oralmente a destinatários no Parlamento Europeu sejam sujeitas ao nível equivalente de protecção aplicado às informações confidenciais escritas. Tal pode incluir uma declaração sob compromisso de honra dos destinatários das informações de que não divulgarão o seu conteúdo a terceiros.

2. O tratamento administrativo de informações confidenciais pelo secretariado da instância parlamentar ou do titular de um cargo fora da reunião à porta fechada rege-se pelas seguintes regras:

— Os documentos em papel são entregues pessoalmente ao responsável pelo secretariado, que os regista e acusa a sua recepção;

— Esses documentos são guardados em locais fechados à chave, sob a responsabilidade do secretariado, quando não estiverem a ser efectivamente utilizados;

— Sem prejuízo do tratamento administrativo de informações confidenciais numa reunião à porta fechada previsto no n.º 1, esses documentos não devem, em circunstância alguma, ser reproduzidos, gravados noutro suporte ou transmitidos a terceiros;

— O acesso a esses documentos é limitado aos seus destinatários e, em conformidade com as modalidades referidas no artigo 4.º, n.º 2, ou no artigo 5.º, n.ºs 3 e 4, é feito sob a supervisão do secretariado;

— O secretariado mantém um registo das pessoas que consultaram os documentos, bem como da data e da hora das consultas. Esse registo é transmitido ao SIC para efeitos da elaboração do relatório anual referido no artigo 12.º

Artigo 9.º

Arquivo de informações confidenciais

1. É assegurado um sistema de arquivo seguro nas instalações do Parlamento Europeu.

As informações confidenciais depositadas a título definitivo no SIC ou no secretariado da instância parlamentar ou do titular de um cargo são transferidas para o arquivo seguro do SIC seis meses após a última consulta e, no máximo, um ano depois de terem sido depositadas.

2. A gestão dos arquivos seguros é assegurada pelo SIC, em conformidade com as normas de arquivo habituais.

3. As informações confidenciais guardadas nos arquivos seguros podem ser consultadas nas seguintes condições:

— Só são autorizadas a consultar essas informações as pessoas identificadas, nominalmente ou por força das suas funções, na ficha de acompanhamento preenchida aquando do depósito das informações confidenciais;

— O pedido de consulta de informações confidenciais deve ser apresentado ao SIC, o qual assegura a transferência do documento em questão para a sala de leitura segura;

— Aplicam-se os procedimentos e as condições de consulta de informações confidenciais definidos no artigo 7.º

Artigo 10.º

Desgraduação e desclassificação de informações classificadas da UE

1. As informações classificadas da UE só podem ser desgraduadas ou desclassificadas com a autorização da entidade de origem e, se necessário, após discussão com as outras partes interessadas. A desgraduação ou a desclassificação são confirmadas por escrito. A entidade de origem tem a responsabilidade de informar da alteração os seus destinatários, e estes, por seu turno, são responsáveis por informar da alteração quaisquer destinatários subsequentes aos quais tenham enviado o documento ou facultado uma cópia do mesmo. Se possível, as entidades de origem especificam nos documentos classificados a data, o período ou a ocorrência após os quais os conteúdos podem ser desgraduados ou desclassificados. Caso contrário, devem rever os documentos de cinco em cinco anos, no máximo, a fim de verificar se é necessário manter a classificação original.

2. A desclassificação de documentos guardados nos arquivos seguros tem lugar, no máximo, ao fim de 30 anos, nos termos do Regulamento (CEE, Euratom) n.º 354/83 do Conselho, de 1 de Fevereiro de 1983, relativo à abertura ao público dos arquivos históricos da Comunidade Económica Europeia e da Comunidade Europeia da Energia Atómica ([1]). A desclassificação é efectuada pela entidade de origem das informações classificadas ou pelo serviço que no momento seja competente para o efeito, em conformidade com o anexo I, parte 1, ponto 10.

Artigo 11.º

Violação da confidencialidade das informações

1. As violações da confidencialidade em geral e da presente decisão em particular implicam, no caso dos deputados ao Parlamento Europeu, a aplicação das disposições em matéria de sanções previstas no Regimento do Parlamento Europeu.

2. As violações da confidencialidade cometidas por membros do pessoal implicam a aplicação dos procedimentos e sanções previstos, respectivamente, pelo Estatuto dos Funcionários e pelo Regime Aplicável aos Outros Agentes da União Europeia, estabelecidos no Regulamento (CEE, Euratom, CECA) n.º 259/68 ([2]) («Estatuto dos Funcionários»).

3. O Presidente e o Secretário-Geral determinam os inquéritos necessários.

Artigo 12.º

Adaptação da presente decisão e das suas normas de execução e relatório anual sobre a aplicação da presente decisão

1. O Secretário-Geral propõe as adaptações necessárias da presente decisão e dos anexos que lhe dão execução e transmite essas propostas à Mesa para decisão.

2. O Secretário-Geral apresenta à Mesa um relatório anual sobre a aplicação da presente decisão.

([1]) JO L 43 de 15.2.1983, p. 1.
([2]) JO L 56 de 4.3.1968, p. 1.

Artigo 13.º

Disposições transitórias e finais

1. As informações confidenciais existentes no SIC ou nos arquivos antes da aplicação da presente decisão são automaticamente classificadas como «RESTREINT UE/EU RESTRICTED», a menos que a entidade de origem decida não as classificar ou atribuir-lhes uma classificação superior ou uma marcação no prazo de um ano a contar da data de entrada em vigor da presente decisão.

2. Se a entidade de origem das informações confidenciais decidir atribuir-lhes uma classificação superior, essas informações são classificadas no nível mais baixo possível pela entidade de origem ou pelos seus delegados, em articulação com o SIC e em conformidade com os critérios estabelecidos no anexo I.

3. É revogada a Decisão da Mesa, de 13 de Novembro de 2006, sobre as regras que regem o tratamento administrativo de documentos confidenciais.

4. É revogada a Decisão da Mesa, de 24 de Outubro de 2005, pela qual é conferido mandato ao Secretário-Geral para criar um comité de desclassificação e para tomar decisões relativas à desclassificação.

Artigo 14.º

Entrada em vigor

1. A presente decisão entra em vigor na data da sua publicação no *Jornal Oficial da União Europeia*.

2. É aplicável a partir de 1 de Julho de 2011.

ANEXO I

PARTE 1

PRINCÍPIOS DE BASE E NORMAS MÍNIMAS DE SEGURANÇA PARA A PROTECÇÃO DE INFORMAÇÕES CONFIDENCIAIS

1. Introdução

As presentes disposições estabelecem os princípios de base e as normas mínimas de segurança que deverão ser respeitadas pelo Parlamento Europeu em todos os seus locais de trabalho, bem como por todos os destinatários de informações classificadas da UE e de outras informações confidenciais, de modo que a segurança seja salvaguardada e que todas as pessoas interessadas possam ter a certeza de que foi estabelecida uma norma comum de protecção. São completadas por regras que regem o tratamento de informações confidenciais pelas comissões parlamentares e por outras instâncias parlamentares ou por titulares de um cargo.

2. Princípios gerais

A política de segurança do Parlamento Europeu é parte integrante da sua política geral de gestão interna e baseia-se, portanto, nos princípios que regem essa política geral. Esses princípios compreendem a legalidade, a transparência, a responsabilidade, a subsidiariedade e a proporcionalidade.

O princípio de legalidade implica a necessidade de que a execução das funções de segurança se mantenha estritamente dentro do quadro jurídico, e de respeitar as exigências legais aplicáveis. Significa, igualmente, que as responsabilidades em matéria de segurança devem assentar em disposições jurídicas apropriadas. Aplicam-se na íntegra as disposições do Estatuto dos Funcionários, nomeadamente o artigo 17.º, relativo à obrigação de o pessoal se abster de qualquer revelação não autorizada de informações recebidas no exercício das suas funções, e o título VI, relativo às medidas disciplinares. Por último, significa que as quebras de segurança nos domínios de responsabilidade do Parlamento Europeu devem ser tratadas em conformidade com a política do Parlamento Europeu em matéria de medidas disciplinares.

O princípio de transparência implica a necessidade de clareza em todas as regras e disposições de segurança, a fim de se obter um equilíbrio entre os diferentes serviços e os diferentes domínios (segurança física em comparação com a protecção das informações, etc.), e de uma política coerente e estruturada de sensibilização para as questões de segurança. Significa igualmente que são necessárias directrizes escritas claras para a aplicação das medidas de segurança.

O princípio de responsabilidade significa que as responsabilidades no domínio da segurança devem ser claramente definidas. Além disso, implica a necessidade de verificar regularmente se essas responsabilidades foram adequadamente cumpridas.

O princípio de subsidiariedade significa que a segurança deve ser organizada ao nível mais baixo possível e tão próximo quanto possível das direcções-gerais e dos serviços do Parlamento Europeu. O princípio de proporcionalidade significa que as actividades de segurança se devem limitar estritamente ao mínimo necessário, e que as medidas de segurança devem ser proporcionais aos interesses a proteger e às ameaças reais ou potenciais a esses interesses, a fim de permitir que estes sejam defendidos de um modo que cause o mínimo de perturbação possível.

3. Bases da segurança da informação

As bases de uma boa segurança da informação são:

a) No Parlamento Europeu, um serviço responsável pela segurança das informações (INFOSEC), encarregado de trabalhar com as autoridades de segurança pertinentes a fim de prestar informações e aconselhamento sobre ameaças técnicas à segurança e sobre os meios de protecção contra essas ameaças;

b) Uma estreita cooperação entre os serviços do Parlamento Europeu responsáveis pela segurança e os serviços de segurança das outras instituições da UE.

4. Princípios da segurança da informação

4.1. *Objectivos*

Os objectivos principais da segurança da informação são os seguintes:

a) Salvaguardar as informações classificadas da UE e outras informações confidenciais dos riscos de espionagem, fuga ou divulgação não autorizada;

b) Salvaguardar as informações da UE tratadas em sistemas e redes de comunicação e informação das ameaças à sua confidencialidade, integridade e disponibilidade;

c) Salvaguardar as instalações do Parlamento Europeu que albergam informações classificadas da UE dos riscos de sabotagem ou de danos intencionais;

d) Em caso de falha, avaliar os danos causados, limitar as suas consequências, realizar inquéritos de segurança e adoptar as medidas correctivas necessárias.

4.2. *Classificação*

4.2.1. No que respeita à confidencialidade, é necessário cautela e experiência na selecção das informações e dos materiais a proteger e na avaliação do grau de protecção requerido. É fundamental que o grau de protecção corresponda à importância securitária de cada elemento de informação e de cada peça de material a proteger. A fim de assegurar o bom fluxo da informação, devem ser evitadas tanto a sobreclassificação como a subclassificação.

4.2.2. O sistema de classificação é o instrumento que permite pôr em prática os princípios definidos na presente secção; é utilizado um sistema semelhante de classificação no planeamento e na organização da luta contra a espionagem, a sabotagem, o terrorismo e outras ameaças, por forma a garantir a máxima protecção das instalações mais importantes que alberguem informações classificadas da UE e dos pontos mais sensíveis no interior dessas instalações.

4.2.3. A responsabilidade pela classificação das informações incumbe exclusivamente à entidade de origem das mesmas.

4.2.4. O nível de classificação baseia-se exclusivamente no conteúdo das informações em causa.

4.2.5. Quando vários elementos de informação estiverem agrupados, o nível de classificação a aplicar ao conjunto deve ser pelo menos idêntico à classificação mais elevada aplicada individualmente a esses elementos. A um conjunto de informações pode, porém, ser atribuída uma classificação mais elevada do que a atribuída às suas partes constituintes.

4.2.6. As classificações são atribuídas e mantidas apenas quando e durante o período necessário.

4.3. *Objectivos das medidas de segurança*

As medidas de segurança devem:

a) Abranger todas as pessoas que tenham acesso a informações classificadas da UE, os suportes das informações classificadas da UE e outras informações confidenciais, bem como todos os locais que as alberguem essas informações e as instalações importantes;

b) Ser concebidas para detectar as pessoas cuja posição possa pôr em perigo a segurança dessas informações e das instalações importantes que as alberguem, e para proceder à sua exclusão ou afastamento;

c) Impedir que pessoas não autorizadas tenham acesso a essas informações ou a instalações que as alberguem;

d) Assegurar que essas informações apenas sejam difundidas às pessoas que delas precisem de tomar conhecimento, princípio fundamental em todos os aspectos da segurança;

e) Assegurar a integridade (ou seja, impedir a deterioração, a alteração não autorizada ou a eliminação não autorizada) e a disponibilidade (às pessoas com necessidade e autorização de acesso) de todas as informações confidenciais, tanto classificadas como não classificadas, especialmente das informações armazenadas, tratadas ou transmitidas sob forma electromagnética.

5. **Normas mínimas comuns**

O Parlamento Europeu deve assegurar que todos os destinatários de informações classificadas da UE, tanto no interior da instituição como dependentes da sua competência, nomeadamente todos os seus serviços e prestadores de serviços, cumpram normas mínimas comuns de segurança, por forma que essas informações possam ser transmitidas com a certeza de que serão tratadas com iguais precauções. Estas normas mínimas devem incluir critérios para a habilitação de segurança de funcionários do Parlamento Europeu e de outros agentes do Parlamento ao serviço dos grupos políticos, e procedimentos para a protecção das informações confidenciais.

O Parlamento Europeu só autorizará o acesso de entidades externas a essas informações na condição de estas serem tratadas de acordo com disposições pelo menos estritamente equivalentes às normas mínimas comuns.

Estas normas mínimas serão igualmente aplicadas quando o Parlamento Europeu confiar a entidades industriais ou outras, por contrato ou convenção de subvenção, tarefas que envolvam informações confidenciais.

6. **Medidas de segurança aplicáveis aos funcionários do Parlamento Europeu e a outros agentes do Parlamento ao serviço dos grupos políticos**

6.1. *Instruções de segurança aplicáveis aos funcionários do Parlamento Europeu e a outros agentes do Parlamento ao serviço dos grupos políticos*

Os funcionários do Parlamento Europeu e outros agentes do Parlamento ao serviço dos grupos políticos que ocupem lugares em que possam ter acesso a informações classificadas da UE receberão instruções completas, ao assumirem as suas funções e, posteriormente, a intervalos regulares, sobre a necessidade de segurança e sobre os meios de a conseguir. Essas pessoas devem atestar por escrito ter lido e compreendido totalmente as disposições de segurança aplicáveis.

6.2. *Responsabilidades dos gestores*

Os gestores deverão saber quais os membros do seu pessoal que trabalham com informações classificadas ou que têm acesso a sistemas de comunicação ou informação protegidos, e deverão registar e relatar todos os incidentes e vulnerabilidades manifestas susceptíveis de afectar a segurança.

6.3. *Estatuto de segurança dos funcionários do Parlamento Europeu e dos outros agentes do Parlamento ao serviço dos grupos políticos*

Devem ser definidos procedimentos para garantir que, quando forem comunicadas informações desfavoráveis relativamente a um funcionário do Parlamento Europeu ou a um agente do Parlamento ao serviço de um grupo político, sejam tomadas medidas para determinar se o trabalho dessa pessoa a põe em contacto com informações classificadas ou se tem acesso a sistemas de comunicação ou de informação protegidos, e para que o serviço competente do Parlamento Europeu seja informado. Se se verificar que essa pessoa constitui um risco para a segurança, deverá ser afastada ou proibida de desempenhar funções em que possa pôr em perigo a segurança.

7. **Segurança física**

Entende-se por segurança física a aplicação de medidas de protecção física e técnica para impedir o acesso não autorizado a informações classificadas da UE.

7.1. *Necessidade de protecção*

O grau das medidas de segurança física a aplicar para assegurar a protecção das informações classificadas da UE deve ser proporcional à classificação, ao volume e às ameaças a que estão expostos os materiais e as informações existentes. Todos os detentores de informações classificadas da UE deverão aplicar práticas uniformes em matéria de classificação dessas informações e respeitar normas comuns de protecção no que se refere ao armazenamento, à transmissão e à eliminação de informações e de materiais que necessitem de protecção.

7.2. *Controlo*

Antes de abandonarem locais onde existam informações classificadas da UE, as pessoas responsáveis pela guarda das mesmas devem assegurar que essas informações se encontram guardadas em condições de segurança e que todos os dispositivos de segurança foram activados (fechaduras, alarmes, etc.). Deverão ser efectuadas outras acções de controlo independentes após as horas de serviço.

7.3. *Segurança dos edifícios*

Os edifícios onde existam informações classificadas da UE ou sistemas de comunicação ou informação protegidos devem ser protegidos contra o acesso de pessoas não autorizadas.

O tipo de protecção proporcionada às informações classificadas da UE, como, por exemplo, janelas com grades, fechaduras nas portas, guardas nas entradas, sistemas automatizados de controlo de acesso, controlos e patrulhas de segurança, sistemas de alarme, sistemas de detecção de intrusos e cães de guarda, dependerá:

a) Da classificação, do volume e da localização das informações e dos materiais a proteger no interior do edifício;

b) Da qualidade dos contentores de segurança das informações e dos materiais em causa; e

c) Das características físicas e da localização do edifício.

O tipo de protecção proporcionada aos sistemas de comunicação e informação dependerá da avaliação do valor das informações e dos materiais em causa e dos danos potenciais em caso de falha de segurança, das características físicas e da localização do edifício em que o sistema se encontrar e da localização desse sistema no interior do edifício.

7.4. *Planos de emergência*

É necessário elaborar com antecedência planos pormenorizados para a protecção das informações classificadas em caso de emergência.

8. **Indicadores de segurança, marcações, aposição e gestão da classificação**

8.1. *Indicadores de segurança*

Não são permitidas outras classificações para além das definidas no artigo 2.º da presente decisão.

Pode ser utilizado um indicador de segurança acordado para limitar no tempo a validade de uma classificação (ou seja, o momento da desgraduação ou da desclassificação automática das informações classificadas). Esse indicador será «ATÉ … (hora/data)» ou «ATÉ … (ocorrência)».

Serão aplicados indicadores de segurança adicionais, tais como CRYPTO ou qualquer outro indicador de segurança reconhecido a nível da UE, caso sejam necessários uma distribuição limitada e um tratamento especial, além do indicado pela classificação de segurança.

Os indicadores de segurança só podem ser utilizados em associação com uma classificação.

8.2. *Marcações*

Pode ser aposta uma marcação para indicar o domínio abrangido por um documento ou uma distribuição específica com base no princípio da necessidade de tomar conhecimento, ou (no caso de informações não classificadas) para indicar o fim de uma proibição.

As marcações não constituem uma classificação e não podem ser utilizadas como alternativas a esta.

8.3. *Aposição das classificações e dos indicadores de segurança*

As classificações são apostas do seguinte modo:

a) Nos documentos com a classificação «RESTREINT UE/EU RESTRICTED», por meios mecânicos ou electrónicos;

b) Nos documentos com a classificação «CONFIDENTIEL UE/EU CONFIDENTIAL», por meios mecânicos ou manualmente, ou por impressão em papel pré-carimbado, consignado num registo;

c) Nos documentos com a classificação «SECRET UE/EU SECRET» e «TRÈS SECRET UE/EU TOP SECRET», por meios mecânicos ou manualmente.

Os indicadores de segurança são apostos imediatamente abaixo da classificação, por meios idênticos aos utilizados na aposição das classificações.

8.4. *Gestão da classificação*

8.4.1. Generalidades

As informações são classificadas apenas em caso de necessidade. A classificação deve ser indicada de forma clara e correcta e só será mantida enquanto as informações necessitarem de protecção.

A responsabilidade pela classificação de informações ou por qualquer desgraduação ou desclassificação subsequentes incumbe exclusivamente à entidade de origem.

Os funcionários do Parlamento Europeu e outros agentes do Parlamento procedem à classificação, desgraduação ou desclassificação das informações mediante instruções ou por delegação do Secretário-Geral.

Os procedimentos pormenorizados para o tratamento de documentos classificados devem ser concebidos de modo a garantir que estes sejam objecto de uma protecção adequada às informações que contenham.

O número de pessoas autorizadas a produzir documentos com a classificação «TRÈS SECRET UE/EU TOP SECRET» deve ser o mais reduzido possível, e os seus nomes devem constar de uma lista elaborada pelo SIC.

8.4.2. Aplicação da classificação

A classificação de um documento é determinada pelo nível de sensibilidade do seu conteúdo, em conformidade com as definições contidas no artigo 2.º, alínea c). É importante que a classificação seja utilizada de forma correcta e comedida, especialmente no que se refere à classificação «TRÈS SECRET UE/EU TOP SECRET».

A classificação de uma carta ou nota de envio de documentos deve ser equivalente ao nível mais alto de classificação dos documentos anexos. A entidade de origem deve indicar claramente em que nível essa carta ou nota de envio deverá ser classificada quando for separada dos documentos anexos.

A entidade de origem de um documento a classificar deverá ter em conta as regras acima indicadas e abster-se de proceder a sobreclassificações ou subclassificações.

Cada uma das páginas, parágrafos, secções, anexos, apêndices, adendas e documentos anexos de um determinado documento pode exigir uma classificação diferente, e deve ser classificado em conformidade. A classificação do documento no seu todo deve ser a da sua parte com a classificação mais elevada.

9. **Inspecções**

A Direcção do Parlamento Europeu responsável pela segurança, eventualmente assistida pelo SIC, efectua inspecções periódicas das medidas de segurança tomadas para proteger as informações classificadas da UE.

A Direcção do Parlamento Europeu responsável pela segurança e os serviços de segurança de outras instituições, órgãos, organismos e agências estabelecidos por força ou com base nos Tratados que detenham informações classificadas da UE podem igualmente decidir realizar avaliações interpares das medidas de segurança tomadas para proteger as informações classificadas da UE.

10. **Procedimento de desclassificação**

10.1. O SIC examina as informações classificadas da UE e apresenta propostas de desclassificação à entidade de origem de um documento o mais tardar no 25.º ano seguinte à data da sua criação. Os documentos que não tenham sido desclassificados aquando de um primeiro exame devem ser reexaminados periodicamente pelo menos de cinco em cinco anos.

10.2. Além de se aplicar a documentos efectivamente guardados nos arquivos seguros e devidamente classificados, o processo de desclassificação pode cobrir também outras informações confidenciais existentes nos arquivos seguros ou no Centro de Arquivo e Documentação do Parlamento Europeu (CARDOC).

10.3. Cabe ao SIC informar, em nome da entidade de origem, os destinatários do documento da alteração de classificação, e estes, por seu turno, são responsáveis por informar os destinatários subsequentes aos quais tenham enviado o documento ou facultado uma cópia do mesmo.

10.4. A desclassificação não afecta nenhuma das marcações que possam aparecer no documento.

10.5. A classificação inicial que figura no cimo e no fundo de cada página deve ser barrada. A primeira página (capa) do documento deve ser carimbada e completada com a referência do SIC.

10.6. O texto do documento desclassificado deve ser anexado à ficha electrónica ou ao sistema equivalente em que tenha sido registado.

10.7. No caso dos documentos abrangidos pelas excepções relativas à vida privada e à integridade dos indivíduos ou aos interesses comerciais das pessoas singulares ou colectivas, e no caso dos documentos sensíveis, aplica-se o disposto no artigo 2.º do Regulamento (CEE, Euratom) n.º 354/83.

10.8. Além do disposto nos pontos 10.1 a 10.7, aplicam-se as seguintes regras:

a) No que diz respeito aos documentos de terceiros, o SIC consulta os terceiros em causa antes de proceder à desclassificação. Os terceiros dispõem de oito semanas para apresentarem observações;

b) No que diz respeito à excepção relativa à vida privada e à integridade dos indivíduos, o processo de desclassificação tem em conta, em particular, o consentimento da pessoa em causa, a impossibilidade de identificar a pessoa em causa e/ou o facto de essa pessoa já não estar viva;

c) No que diz respeito aos interesses comerciais das pessoas singulares ou colectivas, a pessoa em causa pode ser notificada mediante publicação no *Jornal Oficial da União Europeia* e dispor de um prazo de quatro semanas para apresentar observações.

PARTE 2

PROCEDIMENTO DE HABILITAÇÃO DE SEGURANÇA

11. **Procedimento de habilitaçãode segurança para os deputados ao Parlamento Europeu**

11.1. À luz das prerrogativas e competências do Parlamento Europeu, pode ser concedido aos seus deputados acesso a informações classificadas da UE até ao nível «CONFIDENTIEL UE/EU CONFIDENTIAL», inclusive, sem habilitação de segurança. No caso das informações com a classificação «CONFIDENTIEL UE/EU CONFIDENTIAL», os deputados devem assinar uma declaração sob compromisso de honra de que não divulgarão a terceiros o conteúdo dessas informações.

11.2. A fim de terem acesso a informações com a classificação «TRÈS SECRET UE/EU TOP SECRET» e «SECRET UE/EU SECRET», os deputados ao Parlamento Europeu devem ter sido autorizados pelo procedimento referido nos pontos 11.3 e 11.4.

11.3. A autorização só é concedida aos deputados ao Parlamento Europeu que tenham sido objecto de um inquérito de segurança pelas autoridades nacionais competentes dos Estados-Membros, em conformidade com o procedimento referido nos pontos 11.9 a 11.14. O Presidente é responsável pela concessão da autorização aos deputados.

11.4. O Presidente pode conceder a autorização após ter obtido o parecer das autoridades nacionais competentes dos Estados-Membros com base no inquérito de segurança efectuado nos termos dos pontos 11.8 a 11.13.

11.5. A Direcção do Parlamento Europeu responsável pela segurança mantém uma lista actualizada de todos os deputados ao Parlamento Europeu aos quais tenha sido concedida uma autorização, incluindo uma autorização temporária nos termos do ponto 11.15.

11.6. A autorização é válida por um período de cinco anos ou enquanto durarem as tarefas para as quais foi concedida, prevalecendo o prazo que for mais curto. Pode ser renovada pelo procedimento estabelecido no ponto 11.4.

11.7. A autorização é retirada pelo Presidente caso este considere que existem motivos fundamentados para o fazer. Qualquer decisão de retirar uma autorização é notificada ao deputado ao Parlamento Europeu em questão, que pode pedir para ser ouvido pelo Presidente antes de a retirada produzir efeitos, e à autoridade nacional competente.

11.8. O inquérito de segurança é efectuado com a assistência do deputado ao Parlamento Europeu em questão e a pedido do Presidente. A autoridade nacional competente para a realização do inquérito de segurança é a do Estado-Membro de que o deputado em questão for nacional.

11.9. No âmbito do inquérito de segurança, o deputado ao Parlamento Europeu em questão deve preencher um formulário de informação pessoal.

11.10. O Presidente deve especificar no seu pedido às autoridades nacionais competentes o nível de informações classificadas a disponibilizar ao deputado ao Parlamento Europeu em questão, para que aquelas autoridades possam proceder ao inquérito de segurança.

11.11. A integralidade do processo de inquérito de segurança realizado pelas autoridades nacionais competentes, juntamente com os resultados obtidos, deve respeitar a legislação em vigor na matéria no Estado-Membro em questão, inclusive em matéria de recurso.

11.12. Se as autoridades nacionais competentes do Estado-Membro emitirem um parecer positivo, o Presidente pode conceder a autorização ao deputado em questão.

11.13. Um parecer negativo das autoridades nacionais competentes é notificado ao deputado ao Parlamento Europeu, que pode pedir para ser ouvido pelo Presidente. Caso o considere necessário, o Presidente pode pedir esclarecimentos adicionais às autoridades nacionais competentes. Se o parecer negativo for confirmado, a autorização não é concedida.

11.14. Todos os deputados ao Parlamento Europeu aos quais seja concedida uma autorização nos termos do ponto 11.3 recebem as instruções consideradas necessárias sobre a protecção de informações classificadas e sobre os meios de assegurar essa protecção no momento em que a autorização lhes for concedida e, posteriormente, a intervalos regulares. Esses deputados assinam uma declaração confirmando que receberam essas instruções.

11.15. Em circunstâncias excepcionais, o Presidente, depois de ter notificado as autoridades nacionais competentes e na condição de não ter obtido resposta destas no prazo de um mês, pode conceder uma autorização temporária a um deputado ao Parlamento Europeu por um período não superior a seis meses, sujeita aos resultados do inquérito de segurança referido no ponto 11.11. As autorizações temporárias assim concedidas não dão acesso às informações classificadas como «TRÈS SECRET UE/EU TOP SECRET».

12. **Procedimento de habilitação de segurança para os funcionários do Parlamento Europeu e outros agentes ao serviço dos grupos políticos do Parlamento**

12.1. Só têm acesso a informações classificadas os funcionários do Parlamento Europeu e outros agentes ao serviço dos grupos políticos do Parlamento que, devido às suas funções e às exigências do serviço, necessitem de tomar conhecimento ou de aceder a tais informações.

12.2. Para terem acesso a informações com a classificação «TRÈS SECRET UE/EU TOP SECRET», «SECRET UE/EU SECRET» e «CONFIDENTIEL UE/EU CONFIDENTIAL», as pessoas referidas no ponto 12.1 devem ter obtido uma autorização nos termos do procedimento referido nos pontos 12.3 e 12.4.

12.3. A autorização só é concedida às pessoas referidas no ponto 12.1 que tenham sido objecto de um inquérito de segurança pelas autoridades nacionais competentes dos Estados-Membros, em conformidade com o procedimento referido nos pontos 12.9 a 12.14. O Secretário-Geral é responsável pela concessão da autorização aos funcionários do Parlamento Europeu e aos outros agentes do Parlamento ao serviço dos grupos políticos.

12.4. O Secretário-Geral concede a autorização após ter obtido o parecer das autoridades nacionais competentes dos Estados-Membros com base no inquérito de segurança efectuado nos termos dos pontos 12.8 a 12.13.

12.5. A Direcção do Parlamento Europeu responsável pela segurança mantém uma lista actualizada de todos os lugares que exigem uma habilitação de segurança, indicados pelos serviços pertinentes do Parlamento Europeu, e de todas as pessoas às quais tenha sido concedida uma autorização, incluindo uma autorização temporária.

12.6. A autorização é válida por um período de cinco anos ou enquanto durarem as tarefas para as quais foi concedida, prevalecendo o prazo que for mais curto. Pode ser renovada pelo procedimento estabelecido no ponto 12.4.

12.7. A autorização é retirada pelo Secretário-Geral caso este considere que existem motivos fundamentados para o fazer. Qualquer decisão de retirar uma autorização é notificada ao funcionário do Parlamento Europeu ou outro agente do Parlamento ao serviço de um grupo político em questão, que pode pedir para ser ouvido pelo Secretário-Geral antes de a retirada produzir efeitos, e à autoridade nacional competente.

12.8. O inquérito de segurança é efectuado com a assistência da pessoa interessada e a pedido do Secretário-Geral. A autoridade nacional competente para a realização do inquérito de segurança é a do Estado-Membro de que a pessoa em questão for nacional. Quando a legislação nacional o permitir, as autoridades nacionais competentes podem realizar inquéritos em relação a cidadãos estrangeiros que solicitem o acesso a informações classificadas com o nível «CONFIDENTIEL UE/EU CONFIDENTIAL» ou superior.

12.9. No âmbito do inquérito de segurança, o funcionário do Parlamento Europeu ou outro agente do Parlamento ao serviço de um grupo político em questão deve preencher um formulário de informação pessoal.

12.10. O Secretário-Geral deve especificar no seu pedido às autoridades nacionais competentes o nível de informações classificadas a disponibilizar à pessoa em questão, para que aquelas autoridades possam proceder ao inquérito de segurança e dar o seu parecer quanto ao nível de autorização que será adequado conceder a essa pessoa.

12.11. A integralidade do processo de inquérito de segurança realizado pelas autoridades nacionais competentes, juntamente com os resultados obtidos, deve respeitar a legislação em vigor na matéria no Estado-Membro em questão, inclusive em matéria de recurso.

12.12. Se as autoridades nacionais competentes do Estado-Membro emitirem um parecer positivo, o Secretário-Geral pode conceder a autorização à pessoa em questão.

12.13. Um parecer negativo das autoridades nacionais competentes é notificado ao funcionário do Parlamento Europeu ou ao outro agente do Parlamento ao serviço de um grupo político em questão, que pode pedir para ser ouvido pelo Secretário-Geral. Caso o considere necessário, o Secretário-Geral pode pedir esclarecimentos adicionais às autoridades nacionais competentes. Se o parecer negativo for confirmado, a autorização não é concedida.

12.14. Todos os funcionários do Parlamento Europeu e outros agentes do Parlamento ao serviço dos grupos políticos aos quais seja concedida uma autorização nos termos dos pontos 12.4 e 12.5 recebem as instruções consideradas necessárias sobre a protecção de informações classificadas e os meios de assegurar essa protecção no momento em que a autorização lhes for concedida e, posteriormente, a intervalos regulares. Esses funcionários e agentes assinam uma declaração confirmando que receberam essas instruções e comprometem-se a respeitá-las.

12.15. Em circunstâncias excepcionais, o Secretário-Geral, depois de ter notificado as autoridades nacionais competentes e na condição de não ter obtido resposta destas no prazo de um mês, pode conceder uma autorização temporária a um funcionário do Parlamento Europeu ou a outro agente do Parlamento ao serviço de um grupo político por um período não superior a seis meses, sujeita aos resultados do inquérito de segurança referido no ponto 12.11. As autorizações temporárias assim concedidas não dão acesso às informações classificadas como «TRÈS SECRET UE/EU TOP SECRET».