

Jornal Oficial

da União Europeia

C 190



Edição em língua
portuguesa

Comunicações e Informações

56.º ano
29 de junho de 2013

Número de informação Índice Página

IV *Informações*

INFORMAÇÕES DAS INSTITUIÇÕES, ÓRGÃOS E ORGANISMOS DA UNIÃO EUROPEIA

Serviço Europeu para a Ação Externa

2013/C 190/01 Decisão da Alta Representante da União para os Negócios Estrangeiros e a Política de Segurança, de 19 de abril de 2013, relativa às regras de segurança aplicáveis ao Serviço Europeu para a Ação Externa 1

INFORMAÇÕES DOS ESTADOS-MEMBROS

2013/C 190/02 Informações comunicadas pelos Estados-Membros relativas a auxílios estatais concedidos nos termos do Regulamento (CE) n.º 800/2008 da Comissão, que declara certas categorias de auxílios compatíveis com o mercado comum, em aplicação dos artigos 87.º e 88.º do Tratado (Regulamento geral de isenção por categoria) ⁽¹⁾ 47

2013/C 190/03 Informações comunicadas pelos Estados-Membros relativas a auxílios estatais concedidos em conformidade com o Regulamento (CE) n.º 1857/2006 da Comissão relativo à aplicação dos artigos 87.º e 88.º do Tratado aos auxílios estatais a favor das pequenas e médias empresas que se dedicam à produção de produtos agrícolas e que altera o Regulamento (CE) n.º 70/2001 62

2013/C 190/04 Informações comunicadas pelos Estados-Membros relativas a auxílios estatais concedidos nos termos do Regulamento (CE) n.º 800/2008 da Comissão, que declara certas categorias de auxílios compatíveis com o mercado comum, em aplicação dos artigos 87.º e 88.º do Tratado (Regulamento geral de isenção por categoria) ⁽¹⁾ 65

PT

Preço:
4 EUR

⁽¹⁾ Texto relevante para efeitos do EEE

(continua no verso da capa)

V Avisos

PROCEDIMENTOS RELATIVOS À EXECUÇÃO DA POLÍTICA DE CONCORRÊNCIA

Comissão Europeia

2013/C 190/05

Auxílio estatal — República Helénica — Auxílio estatal SA.31155 (2013/C) (ex 2013/NN) (ex 2010/N) — Auxílios estatais a favor do Hellenic Postbank S.A. através da criação e da capitalização do banco de transição «New Hellenic Postbank S.A.» — Convite à apresentação de observações nos termos do artigo 108.º, n.º 2, do TFUE ⁽¹⁾

70



⁽¹⁾ Texto relevante para efeitos do EEE

IV

(Informações)

INFORMAÇÕES DAS INSTITUIÇÕES, ÓRGÃOS E ORGANISMOS DA UNIÃO EUROPEIA

SERVIÇO EUROPEU PARA A AÇÃO EXTERNA

DECISÃO DA ALTA REPRESENTANTE DA UNIÃO PARA OS NEGÓCIOS ESTRANGEIROS E A POLÍTICA DE SEGURANÇA

de 19 de abril de 2013

relativa às regras de segurança aplicáveis ao Serviço Europeu para a Ação Externa

(2013/C 190/01)

A ALTO REPRESENTANTE DA UNIÃO PARA OS NEGÓCIOS ESTRANGEIROS E A POLÍTICA DE SEGURANÇA,

peçoal, ativos físicos, informações e visitantes e cumpra o dever de diligência que lhe compete;

Tendo em conta a Decisão 2010/427/UE do Conselho, de 26 de julho de 2010, que estabelece a organização e o funcionamento do Serviço Europeu para a Ação Externa ⁽¹⁾ («SEAE»),

(3) Mais concretamente, deve ser garantido um nível de proteção ao pessoal colocado sob a responsabilidade do SEAE, aos ativos físicos do SEAE, incluindo sistemas de comunicação e informação, informações e visitantes, conforme com as melhores práticas seguidas no Conselho, na Comissão, nos Estados-Membros e, se for caso disso, nas organizações internacionais;

Tendo em conta o parecer do Comité referido no artigo 9.º, n.º 6, da Decisão da Alta Representante, de 15 de junho de 2011, relativa às regras de segurança aplicáveis ao Serviço Europeu para a Ação Externa ⁽²⁾,

(4) As regras de segurança aplicáveis ao SEAE devem contribuir para um quadro geral completo e mais coerente na UE tendo em vista a proteção de Informações Classificadas da UE (a seguir designadas «ICUE»), com base em, e mantendo tanta coerência quanto possível com, as regras de segurança do Conselho da União Europeia (a seguir designado «o Conselho») e as disposições em matéria de segurança da Comissão Europeia;

Tendo em conta o parecer do Comité referido no artigo 10.º, n.º 1, da Decisão 2010/427/UE do Conselho, de 26 de julho de 2010, que estabelece a organização e o funcionamento do Serviço Europeu para a Ação Externa,

Considerando o seguinte:

(1) O SEAE, enquanto órgão da União Europeia (UE) funcionalmente autónomo, deve ter regras de segurança, tal como referido no artigo 10.º, n.º 1, da Decisão 2010/427/UE do Conselho;

(5) O SEAE, o Conselho e a Comissão estão empenhados em aplicar normas de segurança equivalentes para proteção das ICUE;

(2) A Alta Representante da União para os Negócios Estrangeiros e a Política de Segurança (a seguir designada «Alta Representante» ou «AR») deve decidir das regras de segurança aplicáveis ao SEAE, cobrindo todos os aspetos da segurança, para assegurar que este serviço efetue uma gestão eficaz dos riscos a que estejam sujeitos o respetivo

(6) A presente decisão é aprovada sem prejuízo dos artigos 15.º e 16.º do Tratado sobre o Funcionamento da União Europeia (TFUE) e dos instrumentos que lhe dão execução;

(7) É necessário estabelecer a organização da segurança no SEAE e a atribuição de funções de segurança no âmbito das estruturas do SEAE;

⁽¹⁾ JO L 201 de 3.8.2010, p. 30.

⁽²⁾ JO C 304 de 15.10.2011, p. 5.

- (8) A Alta Representante deve apoiar-se nas competências relevantes existentes nos Estados-Membros, no Secretariado-Geral do Conselho e na Comissão Europeia, conforme necessário;
- (9) A Alta Representante deve tomar todas as medidas adequadas necessárias para aplicar essas regras com o apoio dos Estados-Membros, do Secretariado-Geral do Conselho e da Comissão,

APROVOU A PRESENTE DECISÃO:

Artigo 1.º

Objeto e âmbito de aplicação

A presente decisão estabelece as regras de segurança aplicáveis ao Serviço Europeu para a Ação Externa (a seguir designadas «regras de segurança do SEAE»).

Nos termos do artigo 10.º, n.º 1, da Decisão 2010/427/UE do Conselho, de 26 de julho de 2010, que estabelece a organização e o funcionamento do Serviço Europeu para a Ação Externa, esta é aplicável ao pessoal do SEAE e a todo o pessoal das delegações da União, independentemente do seu estatuto administrativo ou da sua origem, e estabelece o quadro regulamentar geral para assegurar uma gestão eficaz dos riscos a que estejam sujeitos o pessoal do SEAE, tal como referido no artigo 2.º, instalações, os ativos físicos, as informações e os visitantes do SEAE.

Artigo 2.º

Definições

Para efeitos da presente decisão, entende-se por:

- a) «Pessoal do SEAE», funcionários e outros agentes do SEAE, incluindo pessoal dos serviços diplomáticos dos Estados-Membros nomeados como agentes temporários e peritos nacionais destacados, na aceção do artigo 6.º da Decisão 2010/427/UE do Conselho, de 26 de julho de 2010, que estabelece a organização e o funcionamento do Serviço Europeu para a Ação Externa.
- b) «Pessoal sob responsabilidade do SEAE», o pessoal do SEAE e todo o pessoal das delegações da União, independentemente do seu estatuto administrativo ou da sua origem, bem como, no contexto da presente decisão, a Alta Representante e, se for caso disso, outro pessoal residente nas instalações da Sede do SEAE.
- c) «Pessoas a cargo», os membros da família do pessoal sob responsabilidade do SEAE nas delegações da União que façam parte do respetivo agregado familiar conforme notificado ao Ministério de Negócios Estrangeiros do Estado receptor.
- d) «Instalações do SEAE», todos os estabelecimentos do SEAE, incluindo edifícios, escritórios, salas e outras áreas, bem como zonas em que se encontrem sistemas de comunicação e de informação (incluindo as que manuseiam ICUE), em que o SEAE realize atividades permanentes ou temporárias.
- e) «Interesses de segurança do SEAE», pessoal sob responsabilidade do SEAE, instalações, pessoas a cargo, ativos físicos, incluindo sistemas de comunicação e informação, informações e visitantes do SEAE.
- f) «ICUE», quaisquer informações ou material designado por uma classificação de segurança da UE cuja divulgação não autorizada possa causar prejuízos de vária ordem aos interesses da União Europeia ou de um ou mais Estados-Membros.

Outras definições são apresentadas nos anexos relevantes e no Apêndice A.

Artigo 3.º

Dever de diligência

1. As regras de segurança do SEAE visam cumprir o dever de diligência do SEAE.
2. O dever de diligência do SEAE inclui as diligências devidas na aplicação de todas as medidas razoáveis para implementar medidas de segurança de modo a impedir danos razoavelmente previsíveis a interesses de segurança do SEAE.
3. Tendo em conta o dever de diligência dos Estados-Membros, das instituições ou órgãos da UE e de outras partes com o pessoal em delegações da União e/ou em instalações de delegações da União, ou tal responsabilidade a cargo do SEAE quando as delegações da União estão alojadas em instalações de outras partes supramencionadas, o SEAE deve celebrar convénios administrativos com cada uma das entidades acima que especificuem os respetivos papéis e responsabilidades, tarefas e mecanismos de cooperação.

Artigo 4.º

Segurança física e de infraestruturas

1. O SEAE deve implementar todas as medidas de segurança física adequadas (quer sejam permanentes ou temporárias), nomeadamente disposições para o controlo do acesso, em todas as instalações do SEAE, para a proteção dos interesses de segurança do SEAE. Tais medidas devem ser tidas em conta na conceção e no planeamento de novas instalações ou antes do arrendamento de instalações existentes.

2. Em países terceiros, o SEAE deve implementar também eventuais medidas adicionais de segurança física adequadas, permanentes ou temporárias, para a proteção dos respetivos interesses de segurança.

Para isso, podem impor-se obrigações ou restrições especiais ao pessoal sob responsabilidade do SEAE e às pessoas a seu cargo, por razões de segurança, durante um período específico e em zonas específicas.

3. As medidas referidas nos n.ºs 1 e 2 devem ser proporcionais aos riscos avaliados.

Artigo 5.º

Proteção das informações classificadas

1. A proteção das ICUE é regida pelos requisitos previstos na presente decisão e em particular no Anexo A. Cabe ao detentor de quaisquer ICUE a responsabilidade pela sua proteção nestes termos.

2. O SEAE deve assegurar que o acesso a informações classificadas será concedido apenas a quem satisfaça as condições definidas no artigo 5.º do Anexo A.

3. As condições em que os agentes locais podem ter acesso a ICUE devem também ser definidas pela Alta Representante, em conformidade com as regras para a proteção das ICUE previstas no Anexo A da presente decisão.

4. A Direção da Segurança do SEAE gere uma base de dados com o estatuto de credenciação de segurança de todo o pessoal sob responsabilidade do SEAE e dos contratantes do SEAE.

5. Quando os Estados-Membros introduzem, nas estruturas ou redes do SEAE, informações classificadas que ostentem uma marca de classificação de segurança nacional, o SEAE deve proteger essas informações nos termos dos requisitos aplicáveis às ICUE de nível equivalente, tal como estabelecido nas regras aplicáveis no Anexo A da presente decisão.

6. As zonas no SEAE onde são armazenadas informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior, ou com classificação de nível equivalente, são consideradas zonas de segurança em conformidade com as regras estabelecidas no anexo A da presente decisão e devem ser aprovadas pela autoridade de segurança do SEAE.

7. Os procedimentos para executar responsabilidades de Alto Representante no quadro de acordos ou nos convénios administrativos para o intercâmbio de ICUE com Estados terceiros ou

organizações internacionais são descritos nos anexos A e A VI da presente decisão.

Artigo 6.º

Incidentes e emergências de segurança

1. A fim de assegurar uma resposta pronta e eficaz a incidentes de segurança, o SEAE deve definir um processo para comunicar tais incidentes e emergências, que deve estar operacional vinte e quatro horas por dia, sete dias por semana e abranger todos os tipos de incidentes de segurança ou ameaças aos interesses de segurança do SEAE (por exemplo, acidentes, conflitos, atos mal-intencionados, atos criminosos, raptos e situações de tomada de reféns, emergências médicas, incidentes com sistemas de informação e comunicação, ciberataques, etc.).

2. Deverão criar-se canais de ligação de emergência entre a Sede do SEAE, as delegações da União, o Conselho, a Comissão, os Representantes Especiais da UE e os Estados-Membros, para prestar apoio na gestão de incidentes de segurança que envolvam pessoal e das respetivas consequências, incluindo planos de contingência.

3. Esta gestão de incidentes de segurança incluirá, nomeadamente:

— procedimentos para apoiar eficazmente o processo de tomada de decisões relativo a um incidente de segurança que envolva pessoal, incluindo decisões relativas à extração ou suspensão de uma missão, e

— uma política e procedimentos para recuperação de pessoal — por exemplo, no caso de desaparecimento de pessoal ou rapto e situações de reféns — tendo em conta as responsabilidades especiais dos Estados-Membros, das Instituições da UE e do SEAE nesta matéria. A necessidade de competências específicas, no âmbito da gestão de tais operações neste contexto, deve ser considerada tendo em conta os recursos que poderão ser disponibilizados pelos Estados-Membros.

4. O SEAE deve celebrar convénios administrativos adequados para comunicar incidentes de segurança nas delegações da União. Sempre que adequado, devem informar-se os Estados-Membros, a Comissão, qualquer outra autoridade relevante, bem como os Comitês de Segurança relevantes.

5. Os processos de gestão de incidentes serão executados e revistos com regularidade

Artigo 7.º

Segurança dos sistemas de comunicação e informação

1. O SEAE protege as informações tratadas nos sistemas de comunicação e informação (SCI) contra as ameaças à confidencialidade, integridade, disponibilidade, autenticidade e não rejeição.

2. A autoridade de segurança do SEAE aprova regras, uma política de segurança e um programa de segurança para proteção de todos os SCI pertencentes ao SEAE ou por ele operados, tal como definido no artigo 12.º, secção I, n.º 1.

3. As regras, a política e o programa devem estar em conformidade e a respetiva implementação será realizada em colaboração próxima com os do Conselho e da Comissão e, sempre que adequado, com as políticas de segurança aplicadas pelos Estados-Membros.

4. Todos os SCI que tratem informações classificadas devem ser submetidos a um processo de acreditação. O SEAE deve aplicar um sistema de gestão da acreditação de segurança em consulta com o Secretariado-Geral do Conselho e a Comissão.

5. Quando a proteção de ICUE manuseada pelo SEAE for assegurada por produtos criptográficos, estes devem ser aprovados pela Autoridade de Aprovação Criptográfica do SEAE sob recomendação do Comité de Segurança do Conselho.

6. A autoridade de segurança do SEAE criará, na medida do necessário, as seguintes funções em matéria de garantia de informação:

- a) Uma autoridade de garantia da informação;
- b) Uma autoridade TEMPEST;
- c) Uma autoridade de aprovação criptográfica;
- d) Uma autoridade de distribuição criptográfica.

7. Para cada sistema, a autoridade de segurança do SEAE criará as seguintes funções:

- a) Uma autoridade de acreditação de segurança;
- b) Uma autoridade operacional de garantia da informação.

8. As regras de execução do presente artigo no que respeita à proteção das ICUE são estabelecidas nos Anexos A e A IV.

Artigo 8.º

Quebras de segurança e comprometimento de informações classificadas

1. As quebras de segurança resultam de atos ou omissões de uma pessoa que são contrários às regras de segurança estabelecidas na presente decisão e/ou às políticas de segurança ou diretrizes que estabeleçam quaisquer medidas necessárias para a sua implementação, como aprovado nos termos do artigo 20.º, n.º 1.

2. Os comprometimentos de informações classificadas resultam da divulgação integral ou parcial das mesmas a pessoas ou entidades não autorizadas.

3. Qualquer quebra ou suspeita de quebra de segurança e qualquer comprometimento ou suspeita de comprometimento de informações classificadas será imediatamente comunicado à Direção da Segurança do SEAE, que tomará as medidas adequadas, tal como definido no anexo A.

4. Quem for responsável pela quebra das regras de segurança previstas na presente decisão, ou pelo comprometimento de informações classificadas, está passível de ação disciplinar e/ou judicial, nos termos das disposições legislativas e regulamentares aplicáveis, tal como disposto no artigo 11.º, n.º 3 do Anexo A.

Artigo 9.º

Investigação de incidentes, quebras e/ou comprometimentos de segurança e medidas corretivas

1. A Direção da Segurança do SEAE, assistida por peritos dos Estados-Membros e/ou de outras instituições da UE se apropriado, e com autorização do diretor operacional sempre que necessário, deverá:

- a) Realizar investigações ou verificações, consoante o caso:
 - i) sempre que haja conhecimento ou motivos razoáveis para presumir que houve comprometimento ou perda de informação classificada relevante para o SEAE,
 - ii) em casos concretos ou de suspeitas de quebra de segurança ou outros incidentes de segurança ou ameaças aos interesses de segurança do SEAE;
- b) Implementar quaisquer medidas corretivas necessárias resultantes de investigações, sempre que adequado.

2. Os investigadores deverão ter acesso a toda a informação necessária para a realização de tais investigações e deverão receber o apoio total de todos os serviços do SEAE nesta matéria.

Os investigadores podem tomar medidas adequadas para salvarguardar o rasto de indícios de forma equivalente à gravidade da questão sob investigação.

3. Quando o acesso a informação for relativo a dados pessoais, incluindo os constantes dos sistemas de informação e comunicação, tal acesso deve estar em conformidade com o Regulamento (CE) n.º 45/2001.

4. Quando for necessário criar uma base de dados de investigação que contenha dados pessoais, a Autoridade Europeia para a Proteção de Dados (AEPD) será notificada, tal como disposto no regulamento supramencionado.

Artigo 10.º

Gestão dos riscos de segurança

1. A fim de determinar as suas necessidades em matéria de proteção e segurança, o SEAE deve desenvolver uma metodologia global de avaliação dos riscos de segurança, em cooperação estreita com a Direção da Segurança da Comissão e, se adequado, com o Gabinete de Segurança do Secretariado-Geral do Conselho.

2. Os riscos a que os interesses de segurança do SEAE estão expostos são sujeitos a um processo de gestão. Este processo terá por objetivo determinar os riscos de segurança conhecidos, definir as medidas de segurança destinadas a reduzir esses riscos para um nível aceitável e aplicar tais medidas de acordo com o conceito de defesa em profundidade. A eficácia das medidas e o nível de risco serão sujeitos a avaliação contínua.

3. Os papéis, responsabilidades e tarefas estabelecidos na presente decisão não prejudicam a responsabilidade de cada membro do pessoal sob responsabilidade do SEAE; em particular, o pessoal da UE em missão em países terceiros deve demonstrar bom senso e discernimento no que se refere à sua própria proteção e segurança e cumprir todas as regras, regulamentos, procedimentos e instruções aplicáveis em matéria de segurança.

4. O SEAE deve tomar todas as medidas razoáveis para garantir a proteção dos seus interesses de segurança e para impedir danos razoavelmente previsíveis aos mesmos.

5. As medidas de segurança no SEAE para proteção de ICUE ao longo do seu ciclo de vida devem ser proporcionais, designadamente ao seu nível de classificação de segurança, à forma e ao volume das informações ou do material, à localização e construção das instalações que albergam ICUE e à ameaça, incluindo a avaliação local da ameaça, de atos mal-intencionados e/ou atividades criminosas, nomeadamente de espionagem, sabotagem e terrorismo.

Artigo 11.º

Sensibilização e formação em matéria de segurança

1. A autoridade de segurança do SEAE deve garantir que sejam elaborados e executados programas de sensibilização e formação em matéria de segurança e que o pessoal sob responsabilidade do SEAE e, se for caso disso, as pessoas a seu cargo, beneficiem das ações de formação e sensibilização necessárias em função dos riscos inerentes ao seu local de trabalho ou residência.

2. Antes de lhes ser facultado acesso às ICUE e, posteriormente, a intervalos regulares, o pessoal deve ser informado e

reconhecer as suas responsabilidades na proteção das ICUE de acordo com as regras adotadas nos termos do artigo 5.º.

Artigo 12.º

Organização da segurança no SEAE

Secção 1

Disposições gerais

1. O diretor operacional é a autoridade de segurança do SEAE. Nessa qualidade, o diretor operacional garante que:

- a) As medidas de segurança sejam coordenadas, conforme necessário, com as autoridades competentes dos Estados-Membros, do Secretariado-Geral do Conselho e da Comissão e, se for caso disso, de países terceiros ou de organizações internacionais, em todas as questões de segurança pertinentes para as atividades do SEAE, nomeadamente no que se refere à natureza das ameaças à segurança dos interesses de segurança do SEAE, bem como os meios de proteção contra essas ameaças;
- b) Os aspetos de segurança sejam plenamente tidos em conta desde o início de todas as atividades do SEAE;
- c) O acesso a informações classificadas seja concedido apenas a quem satisfaça as condições definidas no artigo 5.º do Anexo A.
- d) Seja criado um sistema de registo que garanta que informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior sejam manuseadas nos termos da presente decisão no SEAE e quando comunicadas a Estados-Membros da UE, Instituições, órgãos ou agências da UE ou outros destinatários. Manter-se-á um registo separado de todas as ICUE comunicadas pelo SEAE a Estados terceiros e organizações internacionais, bem como de todas as informações classificadas recebidas de Estados terceiros e organizações internacionais;
- e) Sejam realizadas as inspeções de segurança referidas no artigo 15.º;
- f) Sejam realizadas investigações sobre qualquer quebra de segurança real ou suspeita, assim como sobre qualquer comprometimento real ou suspeito ou perda de informações classificadas detidas ou emanadas do SEAE, e seja solicitado às autoridades de segurança competentes que prestem assistência nessas investigações;
- g) Sejam estabelecidos mecanismos e planos de gestão adequados dos incidentes e consequências, a fim de dar uma resposta pronta e eficaz a incidentes de segurança;
- h) Sejam tomadas medidas adequadas caso algum indivíduo não cumpra a presente decisão;

- i) Sejam instauradas medidas físicas e organizativas adequadas para a proteção dos interesses de segurança do SEAE.

Neste contexto, em consulta com o secretário-geral executivo, o diretor operacional:

— define a categoria de segurança das delegações, em consulta com a Comissão,

— decide, após consulta à AR, quando evacuar pessoal das delegações se a situação de segurança assim o exigir,

— decide que medidas aplicar para a proteção de pessoas a cargo, se for caso disso, tendo em conta convénios com instituições da UE, tal como referido no artigo 3.º, n.º 3,

— aprova a política de comunicação criptográfica, nomeadamente o programa de instalação de produtos e mecanismos criptográficos.

2. O diretor operacional é assistido nesta tarefa pelo Diretor Executivo dos Serviços de Administração e Finanças, pelo Chefe da Direção da Segurança do SEAE e, quando adequado, pelo Diretor Executivo de Resposta a Crises e Coordenador Operacional.

3. Como autoridade de segurança do SEAE, o diretor operacional pode delegar tarefas neste âmbito, quando for caso disso.

4. Cada Chefe de departamento/divisão é responsável pela implementação de regras para proteção de ICUE no/a respetivo/a departamento/divisão.

Mantendo-se responsável tal como supramencionado, cada Chefe de departamento/divisão designa pessoal para uma função de Coordenador de Segurança Departamental, com recursos adequados à quantidade de ICUE manuseadas por cada departamento/divisão.

Os Coordenadores de Segurança Departamental assistem e apoiam o Chefe de departamento/divisão, sempre que adequado, na execução de tarefas relacionadas com segurança, tais como:

- a) Desenvolver requisitos de segurança adicionais adequados às necessidades específicas do/a departamento/divisão;
- b) Comunicar informações de segurança periódicas aos membros do/a departamento/divisão;
- c) Garantir que o princípio da necessidade de tomar conhecimento é respeitado pelo/a departamento/divisão;

- d) Manter uma lista atualizada de códigos e chaves de segurança;

- e) Manter procedimentos e medidas de segurança;

- f) Comunicar quaisquer quebras e/ou comprometimento de segurança de ICUE ao diretor e à Direção da Segurança;

- g) Realizar reuniões de balanço com os membros do pessoal que deixem de exercer funções no SEAE;

- h) Apresentar relatórios com regularidade a toda a hierarquia sobre as matérias de segurança do/a departamento/divisão;

- i) Colaborar com a Direção da Segurança do SEAE em questões de segurança.

Qualquer atividade ou questão que possa afetar a segurança deve ser atempadamente notificada à Direção da Segurança do SEAE.

5. Cada Chefe de delegação da União é responsável pela aplicação de todas as medidas relativas à segurança da delegação da União.

Secção 2

A Direção da Segurança do SEAE

1. O SEAE tem uma Direção da Segurança. A Direção deverá:

- a) Gerir, coordenar, supervisionar e/ou executar todas as medidas de segurança em todas as instalações sob responsabilidade do SEAE, na Sede, na UE e em Estados terceiros;
- b) Assegurar coerência e consistência com a presente decisão e com as disposições de execução de qualquer atividade que possa afetar a proteção dos interesses de segurança do SEAE;
- c) Ser a principal conselheira da AR, do secretário-geral executivo e do diretor operacional em todas as questões de segurança;
- d) Ser assistida pelos serviços competentes dos Estados-Membros, em conformidade com o disposto no artigo 10.º, n.º 3, da Decisão 2010/427/UE do Conselho, que estabelece a organização e o funcionamento do SEAE, a Direção da Segurança;

e) Apoiar as atividades da Autoridade de Acreditação de Segurança do SEAE através da realização de avaliações da segurança física das Condições Gerais de Segurança (CGS)/Condições Locais de Segurança (CLS) dos sistemas de comunicação e informação que manuseiam ICUE e das instalações a ser autorizadas para manuseamento e armazenamento de ICUE.

2. O Chefe da Direção da Segurança do SEAE é responsável por:

a) Assegurar a proteção geral dos interesses de segurança do SEAE;

b) Elaborar, rever e atualizar as regras de segurança, bem como coordenar medidas de segurança com as autoridades competentes dos Estados-Membros e, se for caso disso, com as autoridades competentes de Estados terceiros e organizações internacionais ligadas à UE através de acordos e/ou convênios de segurança;

c) Apoiar os procedimentos do Comité de Segurança do SEAE, tal como definido no artigo 14.º, n.º 1, da presente decisão;

d) Colaborar com quaisquer parceiros ou autoridades para além dos referidos na alínea b) em questões de segurança, se for caso disso;

e) Ordenar em termos de prioridade e apresentar propostas para a gestão do orçamento para a segurança na Sede e nas delegações da União.

3. O Chefe da Direção da Segurança do SEAE deverá:

a) Assegurar que as quebras e os comprometimentos de segurança são registados e que se iniciam e realizam investigações quando necessário;

b) Reunir-se regularmente, e sempre que necessário, para debater domínios de interesse comum com o Diretor da Segurança do Secretariado-Geral do Conselho e o Diretor da Segurança da Comissão.

4. A Direção da Segurança do SEAE deve estabelecer contacto e manter uma colaboração estreita com:

— os departamentos responsáveis pela segurança nos Ministérios de Negócios Estrangeiros dos Estados-Membros,

— as Autoridades Nacionais de Segurança (ANS) e/ou as outras autoridades de segurança competentes dos Estados-Membros, para permitir a assistência das mesmas no que compete à informação necessária para avaliar os perigos e ameaças que o SEAE, o pessoal, as atividades, os ativos e recursos e as informações classificadas do SEAE podem enfrentar no seu local de atividade habitual,

— as autoridades de segurança competentes dos Estados-Membros ou Estados de acolhimento no território em que o SEAE possa exercer atividades, no que compete a qualquer questão relacionada com a proteção do pessoal, da atividade, dos ativos e recursos e das informações classificadas enquanto se encontram no seu território,

— o Gabinete de Segurança do Secretariado-Geral do Conselho e a Direção da Segurança da Direção-Geral dos Recursos Humanos e da Segurança da Comissão e, quando oportuno, com os departamentos de segurança de outras instituições, órgãos e agências da UE,

— os departamentos de segurança de Estados terceiros ou organizações internacionais com vista a uma eventual coordenação útil, e

— as ANS dos Estados-Membros, no que compete a qualquer questão relativa à proteção de ICUE.

Secção 3

Delegações da União

1. Cada Chefe de delegação da União é responsável pela implementação e gestão local de todas as medidas relativas à proteção dos interesses de segurança do SEAE nas instalações e competências da delegação da União.

Aplicará, em consulta com as autoridades competentes do Estado de acolhimento sempre que necessário, todas as medidas razoavelmente aplicáveis para assegurar que as medidas físicas e organizacionais adequadas estão em vigor para atingir este objetivo.

O Chefe de delegação definirá procedimentos de segurança para a proteção das pessoas a cargo, tal como definido no artigo 2.º, alínea c), quando adequado, tendo em conta qualquer convénio administrativo, tal como referido no artigo 3.º, n.º 3. O Chefe de delegação apresentará um relatório anual sobre todas as questões de segurança na sua esfera de responsabilidade ao Chefe da Direção da Segurança do SEAE.

Será assistido nessas funções pela Direção da Segurança do SEAE, pelo pessoal do SEAE na delegação que exerce tarefas e funções inerentes à segurança e por pessoal de segurança destacado caso necessário.

2. Além disso, o Chefe de delegação irá:

— criar planos de segurança e contingência detalhados para a delegação, com base em procedimentos operacionais normalizados genéricos,

— estabelecer um sistema 24/7 eficaz para gerir incidentes e emergências de segurança no âmbito da operação da delegação,

- assegurar que todo o pessoal destacado na delegação está coberto por seguro consoante as condições na área,
 - assegurar que a segurança faz parte da formação inicial da delegação da União administrada a todo o pessoal destacado na delegação previamente ou na chegada à delegação, e
 - assegurar que quaisquer recomendações feitas após avaliações da segurança são implementadas e apresentar relatórios escritos em intervalos regulares sobre a sua implementação e sobre outras questões de segurança à Autoridade de Segurança do SEAE.
3. Sendo responsável e responsabilizável por salvaguardar a gestão da segurança, bem como por assegurar resiliência coletiva, o Chefe de delegação pode delegar a execução das suas tarefas de segurança ao Coordenador de Segurança da Delegação («CSD»), sendo o Chefe de Delegação Adjunto ou, quando ninguém for nomeado, uma alternativa adequada.

Nomeadamente, podem atribuir-se as seguintes responsabilidades ao CSD:

- concertar-se com as autoridades competentes da nação de acolhimento e os equivalentes adequados nas embaixadas e missões diplomáticas dos Estados-Membros em questões de segurança,
 - aplicar procedimentos de gestão de segurança adequados relativos aos interesses de segurança do SEAE, incluindo a proteção de ICUE,
 - informar o pessoal sobre as regras de segurança que lhes são aplicáveis e sobre os riscos específicos no país de acolhimento,
 - apresentar pedidos à Direção da Segurança do SEAE no que compete às posições que exigem uma Certificação de Segurança do Pessoal (CSP), e
 - manter o Chefe de delegação, o Oficial de Segurança Regional (OSR) e a Direção da Segurança do SEAE permanentemente informados no que se refere a incidentes ou desenvolvimentos na zona que afetem a proteção dos interesses de segurança do SEAE.
4. O Chefe da delegação pode delegar tarefas de segurança de cariz administrativo ou técnico ao Chefe de Administração e a outros membros do pessoal da delegação.

5. A Delegação da União é assistida por um Oficial de Segurança Regional (OSR). Os OSR desempenham os papéis definidos abaixo nas delegações em cada uma das respetivas zonas geográficas de responsabilidade.

Sob certas circunstâncias, quando a situação de segurança assim o exige, um OSR pode ser destacado para uma delegação específica como residente a tempo inteiro.

Pode ser necessário que um OSR seja destacado para uma área exterior à sua zona de responsabilidade atual, incluindo a Sede em Bruxelas ou até assumir um posto residencial de acordo com a situação de segurança relevante em qualquer país e conforme exigido pela Direção da Segurança do SEAE.

6. Os OSR estão sob o controlo hierárquico imediato da Direção da Segurança do SEAE, mas sob o controlo funcional e administrativo direto do Chefe de delegação pertinente. Devem assistir o Chefe de delegação e o pessoal da delegação na organização e implementação de todas as medidas físicas, organizacionais e processuais relativas à segurança de todo o pessoal da delegação independentemente da sua origem administrativa

7. Os OSR aconselham e apoiam o Chefe de delegação e o pessoal da delegação. Caso seja adequado, nomeadamente se um OSR for residente a tempo inteiro, pode assistir uma delegação da União na gestão e implementação da segurança, incluindo na preparação de contratos de segurança, na gestão de credenciações e nas credenciações.

Artigo 13.º

Operações PCSD e Representantes Especiais da UE

A Direção da Segurança do SEAE assiste e aconselha o Diretor da Direção-Geral de Gestão de Crises e Planeamento (DGCP), o Diretor-Geral do Estado-Maior da União Europeia (EMUE), o Comandante de Operações Civas a cargo da Capacidade Civil de Planeamento e Condução (CPCC) e os Comandantes das Operações Militares da UE no que respeita a aspetos de segurança de operações PCSD, bem como os Representantes Especiais da UE sobre aspetos de segurança do seu mandato, complementares às disposições específicas que existem neste âmbito sobre as políticas relevantes adotadas pelo Conselho.

Artigo 14.º

O Comité de Segurança do SEAE

1. É criado um Comité de Segurança do SEAE.

O Comité será presidido pelo diretor operacional, ou por um seu delegado, e reúne-se segundo as instruções do Presidente ou a pedido de qualquer dos seus membros. A Direção da Segurança do SEAE apoia o Presidente na sua função e presta assistência administrativa, quando necessário, aos procedimentos do Comité.

2. O Comité de Segurança do SEAE será composto por representantes de:

- todos os Estados-Membros,
- o Gabinete de Segurança do Secretariado-Geral do Conselho,
- a Direção de Segurança da Direção-Geral dos Recursos Humanos e da Segurança da Comissão.

Uma delegação de um Estado-Membro para o Comité de Segurança do SEAE pode consistir em membros de:

- a Autoridade Nacional de Segurança e/ou a Autoridade de Segurança Designada,
- os departamentos responsáveis pela segurança nos Ministérios de Negócios Estrangeiros.

3. Os representantes do Comité podem ser acompanhados e aconselhados por peritos se considerarem necessário. Os representantes de outras instituições, agências ou órgãos da UE podem ser convidados a participar em debates sobre questões relevantes para a sua segurança.

4. Sem prejuízo do disposto no n.º 5, o Comité de Segurança do SEAE deverá assistir o SEAE, através de consultas, em todas as questões de segurança relevantes para as atividades do SEAE, para a Sede e as delegações da União.

Em particular, sem prejuízo do disposto no n.º 5, o Comité de Segurança do SEAE:

- a) Deve ser consultado em questões de:
- políticas de segurança, diretrizes, conceitos ou outros documentos metodológicos relativos à segurança, nomeadamente no que respeita à proteção de informações classificadas e às medidas a tomar em caso de incumprimento das regras de segurança por parte do pessoal do SEAE,
 - aspetos de segurança técnica que possam influenciar a decisão da AR de apresentar uma recomendação ao Conselho para a abertura de negociações para acordos de segurança das informações a que se refere o artigo 10.º, n.º 1, alínea a) do Anexo A,
 - quaisquer alterações à presente decisão.
- b) Pode ser consultado ou informado, sempre que adequado, acerca de assuntos relacionados com a segurança do pessoal e dos ativos na Sede do SEAE e nas delegações da União, sem prejuízo do disposto no Artigo 3.º, n.º 3;

c) Deve ser informado de quaisquer comprometimentos ou perdas de ICUE ocorridas no SEAE.

5. Qualquer alteração às regras relacionadas com a proteção das ICUE constantes da presente decisão e do respetivo Anexo A necessitam de um parecer favorável por unanimidade dos Estados-Membros representados no Comité de Segurança do SEAE. Tal parecer favorável por unanimidade é também necessário previamente a:

- iniciar negociações de convénios administrativos a que se refere o artigo 10.º, n.º 1, alínea b) do Anexo A,
- divulgar informações classificadas nas circunstâncias excecionais referidas no n.º 9, n.º 11 e n.º 12 do Anexo A VI,
- assumir a responsabilidade como entidade de origem das informações nas circunstâncias referidas no artigo 10.º, n.º 4, última frase do Anexo A.

Quando for necessário um parecer favorável unânime, tal será conseguido quando não forem formuladas objeções pelas delegações dos Estados-Membros durante os procedimentos do Comité.

6. O Comité de Segurança do SEAE terá plenamente em conta as políticas e orientações em matéria de segurança em vigor no Conselho e na Comissão.

7. O Comité de Segurança do SEAE recebe a lista das inspeções anuais do SEAE e, quando finalizados, os relatórios das inspeções.

8. Organização das reuniões:

- O Comité de Segurança do SEAE reúne-se pelo menos duas vezes por ano. As reuniões adicionais, na sua configuração de pleno direito ou em ANS/ASD ou em formato de segurança do MNE, podem ser organizadas pelo Presidente ou solicitadas pelos membros do Comité.
- O Comité de Segurança do SEAE organiza as suas atividades de forma a poder formular recomendações sobre domínios de segurança específicos. Pode estabelecer outras subformações especializadas, consoante as necessidades. O Comité define os mandatos dessas subformações especializadas, as quais lhe apresentam relatórios das suas atividades.
- A Direção da Segurança do SEAE é responsável pela preparação de tópicos para debate. O presidente fixa a ordem de trabalhos provisória de cada reunião. Os membros do Comité podem propor tópicos adicionais para discussão.

*Artigo 15.º***Inspecções de segurança**

1. A autoridade de segurança do SEAE assegura a realização de inspecções de segurança, com regularidade, na Sede do SEAE e nas delegações da União a fim de avaliar a adequação das medidas de segurança e de verificar a sua conformidade com a presente decisão. A Direção de Segurança do SEAE pode, se adequado, destacar peritos contribuintes para participar nas inspecções de segurança às agências e aos órgãos da UE ao abrigo do Capítulo 2 do Título V do TUE.

2. As Inspecções de Segurança do SEAE são realizadas sob a autoridade da Direção da Segurança do SEAE e, se adequado, com o apoio de peritos em segurança em representação de outras instituições ou Estados-Membros da UE, nomeadamente no contexto dos convénios referidos no artigo 3.º, n.º 3.

3. O SEAE pode recorrer, conforme necessário, aos conhecimentos especializados dos Estados-Membros, do Secretariado-Geral do Conselho e da Comissão.

Quando necessário, podem convidar-se peritos em segurança competentes sediados em Missões de Estados-Membros em Estados terceiros e/ou representantes dos departamentos de segurança diplomática dos Estados-Membros a participar na inspeção de segurança da delegação da União.

4. As regras de execução deste artigo no que respeita à proteção de ICUE são estabelecidas no Anexo A III.

*Artigo 16.º***Visitas de Avaliação**

São organizadas visitas de avaliação para avaliar a eficácia das medidas de segurança aplicadas num Estado terceiro ou organização internacional para proteção das ICUE trocadas sob um convénio administrativo a que se refere o artigo 10.º, n.º 1, alínea b) do Anexo A.

A Direção da Segurança do SEAE pode, se adequado, destacar peritos contribuintes para participar nas visitas a Estados terceiros ou organizações internacionais com as quais a UE tenha concluído um Acordo de segurança das informações a que se refere o artigo 10.º, n.º 1, alínea a) do Anexo A.

*Artigo 17.º***Planeamento da continuidade das atividades**

A Direção da Segurança do SEAE apoiará o diretor operacional na gestão dos aspetos ligados à segurança dos processos de continuidade das atividades do SEAE como parte integrante do planeamento global da continuidade das atividades do SEAE.

*Artigo 18.º***Conselhos de viagem para missões no exterior da UE**

A Direção da Segurança do SEAE assegura a disponibilidade de conselhos de viagem no que respeita a missões do pessoal sob responsabilidade do SEAE no exterior da UE, apoiando-se nos recursos de todos os serviços competentes do SEAE, nomeadamente o Gabinete de Crise, o INTCEN, os departamentos geográficos e as delegações da União.

A Direção da Segurança do SEAE presta, sob pedido e apoiando-se nos recursos supramencionados, aconselhamento de viagem específico no que respeita a missões do pessoal sob responsabilidade do SEAE em Estados terceiros que apresentem alto risco ou um nível de risco mais elevado.

*Artigo 19.º***Saúde e segurança**

As regras de segurança do SEAE complementam as regras do SEAE para a proteção da saúde e segurança, tal como aprovado pela Alta Representante.

*Artigo 20.º***Aplicação e revisão**

1. A autoridade de segurança do SEAE aprova, após consulta com o Comité de Segurança do SEAE se adequado, políticas ou diretrizes de segurança que estabeleçam quaisquer medidas necessárias para a implementação destas regras no SEAE e cria a capacidade adequada para abranger todos os aspetos da segurança, em cooperação estreita com as autoridades de segurança competentes dos Estados-Membros e com o apoio dos serviços relevantes das Instituições da UE.

2. Em conformidade com o disposto no do artigo 4.º, n.º 5 da Decisão 2010/427/UE do Conselho, de 26 de julho de 2010, que estabelece a organização e o funcionamento do Serviço Europeu para a Ação Externa, pode recorrer-se, se necessário, a disposições transitórias através de acordos a nível dos serviços com os serviços competentes do Secretariado-Geral do Conselho e da Comissão.

3. A AR garante a coerência global na aplicação da presente decisão e reaprecia regularmente as presentes regras de segurança.

4. As regras de segurança do SEAE serão implementadas em cooperação estreita com as autoridades de segurança competentes dos Estados-Membros, com o Gabinete de Segurança do Secretariado-Geral do Conselho e com a Direção de Segurança da Direção-Geral dos Recursos Humanos e da Segurança da Comissão

5. O SEAE assegura que todos os aspetos do processo de segurança são considerados no sistema de resposta à crise do SEAE.

6. O diretor operacional, enquanto Autoridade de Segurança, e o chefe da Direção da Segurança do SEAE asseguram a implementação da presente decisão.

Artigo 21.º

Substituição de decisões anteriores

1. A presente decisão revoga e substitui a Decisão da Alta Representante da União para os Negócios Estrangeiros e a Política de Segurança, de 15 de junho de 2011, relativa às regras de segurança aplicáveis ao Serviço Europeu para a Ação Externa ⁽¹⁾.

2. A presente decisão revoga e substitui a Decisão da Alta Representante da União para os Negócios Estrangeiros e a Política de Segurança, de 23 de fevereiro de 2011, relativa à Designação e às tarefas da Autoridade de Segurança Destacada do Serviço Europeu para a Ação Externa.

Artigo 22.º

Disposições finais

A presente decisão entra em vigor na data da sua assinatura.

Será publicada no *Jornal Oficial da União Europeia*.

As autoridades competentes no SEAE informam devida e prontamente todo o pessoal abrangido pela presente decisão e respetivos anexos, acerca do conteúdo, entrada em vigor e quaisquer alterações subsequentes.

Feito em Bruxelas, em 19 de abril de 2013.

A Alta Representante
C. ASHTON

⁽¹⁾ JO C 304 de 15.10.2011, p. 5.

ANEXO A

PRINCÍPIOS E NORMAS PARA A PROTEÇÃO DE ICUE*Artigo 1.º***Objeto, âmbito de aplicação e definições**

1. O presente anexo define os princípios básicos e as normas mínimas de segurança aplicáveis à proteção das ICUE.
2. Estes princípios básicos e normas mínimas são aplicáveis ao SEAE e ao pessoal sob responsabilidade do SEAE, tal como referido e definido respetivamente nos artigos 1.º e 2.º da presente decisão.

*Artigo 2.º***Definição de ICUE, classificações e marcas de segurança**

1. Entende-se por «informações classificadas da UE» (ICUE) quaisquer informações ou material designado por uma classificação de segurança da UE cuja divulgação não autorizada possa causar prejuízos de várias ordens aos interesses da União Europeia ou de um ou mais Estados-Membros.
2. As ICUE serão classificadas num dos seguintes níveis:
 - a) TRÈS SECRET UE/EU TOP SECRET: informações e material cuja divulgação não autorizada possa prejudicar de forma excepcionalmente grave os interesses essenciais da União Europeia ou de um ou mais Estados-Membros.
 - b) 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.
 - c) 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.
 - d) RESTREINT UE/EU RESTRICTED: informações e material cuja divulgação não autorizada possa ser desfavorável aos interesses da União Europeia ou de um ou mais Estados-Membros.
3. As ICUE ostentam uma marca de classificação de segurança nos termos do disposto no n.º 2. Podem ostentar marcas adicionais que designem o domínio de atividade a que se referem, identifiquem a entidade de origem, limitem a distribuição, restrinjam a utilização ou indiquem a comunicabilidade.

*Artigo 3.º***Gestão das classificações**

1. O SEAE garante que as ICUE sejam devidamente classificadas e claramente identificadas como informações classificadas, e mantenham o seu nível de classificação durante o tempo necessário.
2. As ICUE não podem ser desgraduadas nem desclassificadas e nenhuma das marcas a que se refere o artigo 2.º, n.º 3, pode ser alterada ou suprimida sem o consentimento prévio, por escrito, da entidade de origem.
3. A autoridade de segurança do SEAE aprova, após consulta do Comité de Segurança do SEAE em conformidade com o artigo 14.º, n.º 5, da presente decisão, uma política de segurança para a produção de ICUE, que compreende um guia prático de classificação.

*Artigo 4.º***Proteção das informações classificadas**

1. As ICUE são protegidas nos termos da presente decisão.
2. Cabe ao detentor de quaisquer ICUE a responsabilidade pela sua proteção nos termos da presente decisão.

3. Quando os Estados-Membros introduzirem nas estruturas ou redes do SEAE informações classificadas que ostentem uma marca de classificação de segurança nacional, o SEAE protege essas informações nos termos dos requisitos aplicáveis às ICUE de nível equivalente, de acordo com a tabela de equivalências das classificações de segurança constante do Apêndice B da Decisão 2011/292/UE do Conselho, de 31 de março de 2011, relativa às regras de segurança aplicáveis à proteção das informações classificadas da UE.

O SEAE estabelece procedimentos adequados para manter registos rigorosos relativos à entidade de origem de

- informações classificadas recebidas pelo SEAE; e
- material de referência incluído em informações classificadas emanadas do SEAE.

O Comité de Segurança do SEAE será informado acerca destes procedimentos.

4. As grandes quantidades ou o acervo de ICUE podem justificar um nível de proteção correspondente a uma classificação mais elevada do que a dos seus componentes.

Artigo 5.º

Segurança do pessoal para manuseamento de informações classificadas da UE

1. A segurança do pessoal consiste na aplicação de medidas que se destinam a garantir que o acesso às ICUE só seja concedido a quem:

- tenha necessidade de tomar conhecimento das informações;
- para efeitos de acesso a informação com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior, possua a credenciação de segurança para o nível adequado ou outra autorização devidamente emitida, em virtude das funções que exerce, nos termos das disposições legislativas e regulamentares nacionais; e
- tenha sido informado das responsabilidades que lhe cabem.

2. Os procedimentos de certificação de segurança do pessoal (CSP) permitem verificar se determinada pessoa pode ter acesso a ICUE, tendo em conta a sua lealdade, idoneidade e fiabilidade.

3. Todas as pessoas são informadas das suas responsabilidades no que respeita à proteção das ICUE nos termos da presente decisão e reconhecem essas mesmas responsabilidades, por escrito, antes de lhes ser facultado o acesso a ICUE e, posteriormente, a intervalos regulares.

4. As regras de execução do presente artigo são estabelecidas no Anexo A I.

Artigo 6.º

Segurança física das informações classificadas da UE

1. A segurança física consiste na aplicação de medidas físicas e técnicas de proteção destinadas a dissuadir o acesso não autorizado a ICUE.

2. São concebidas medidas de segurança física que permitam impedir a entrada sub-reptícia ou forçada de intrusos, dissuadir, impedir e detetar ações não autorizadas e permitir uma diferenciação do pessoal no que se refere ao acesso a ICUE, segundo o princípio da necessidade de tomar conhecimento de tais informações. Essas medidas são determinadas com base num processo de gestão de risco.

3. São aplicadas medidas de segurança física em todas as instalações, edifícios, gabinetes, salas e outras zonas onde sejam manuseadas ou armazenadas ICUE, nomeadamente zonas em que se encontrem sistemas de comunicação e de informação, tal como definidos no artigo 8.º, n.º 2.

4. As zonas onde sejam armazenadas informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior são instituídas como zonas de segurança, nos termos do Anexo A II, e aprovadas pela autoridade de segurança do SEAE.

5. Só são utilizados equipamentos ou dispositivos aprovados para proteger as ICUE de nível CONFIDENTIEL UE/EU CONFIDENTIAL ou superior.
6. As regras de execução do presente artigo são estabelecidas no Anexo A II.

Artigo 7.º

Gestão das informações classificadas

1. A gestão das informações classificadas consiste na aplicação de medidas administrativas de controlo das ICUE ao longo do seu ciclo de vida que visam complementar as medidas previstas nos artigos 5.º, 6.º e 8.º e contribuir, deste modo, para dissuadir e detetar a perda ou o comprometimento deliberados ou acidentais de informações e para recuperar essas informações em caso de perda ou comprometimento. Estas medidas dizem respeito, nomeadamente, à produção, registo, cópia, tradução, transporte, manuseamento, armazenamento e destruição de ICUE.
2. As informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior são registadas, para fins de segurança, antes da distribuição e no momento da receção. Para o efeito, as autoridades competentes do SEAE criam um sistema de registo. As informações com classificação TRÈS SECRET UE/EU TOP SECRET são inscritas em registos próprios.
3. Os serviços e instalações onde se proceda ao manuseamento ou armazenamento de ICUE são periodicamente inspecionados pela autoridade de segurança do SEAE.
4. As ICUE devem ser transmitidas entre diferentes serviços e instalações fora do perímetro das zonas fisicamente protegidas de acordo com as regras a seguir enunciadas:
 - a) As ICUE são, regra geral, transmitidas por meios eletrónicos protegidos por produtos criptográficos aprovados nos termos do artigo 7.º n.º 5, da presente decisão e de acordo com Procedimentos Operacionais de Segurança (POS) claramente definidos;
 - b) Se não se utilizarem os meios referidos na alínea a), as ICUE são transportadas:
 - i) em suporte eletrónico (chaves USB, CD, discos rígidos) protegido por produtos criptográficos aprovados nos termos do artigo 7.º, n.º 5, da presente decisão, ou
 - ii) em todos os demais casos, nas condições estipuladas pela autoridade de segurança do SEAE, de acordo com as medidas de proteção pertinentes estabelecidas na Secção V do Anexo A III.
5. As regras de execução do presente artigo são estabelecidas no Anexo A III.

Artigo 8.º

Proteção das ICUE manuseadas nos sistemas de comunicação e informação

1. A garantia da informação (GI) no domínio dos sistemas de comunicação e informação consiste na confiança em que esses sistemas protegem as informações neles manuseadas e funcionam como for necessário, quando for necessário, sob o controlo de utilizadores legítimos. Uma GI eficaz deve assegurar níveis adequados de confidencialidade, integridade, disponibilidade, não rejeição e autenticidade. A GI baseia-se num processo de gestão de risco.
2. Um sistema de comunicação e informação (SCI) consiste num sistema que permita o manuseamento automatizado de informações. Um sistema de comunicação e informação compreende todos os ativos necessários ao seu funcionamento, designadamente infraestrutura, organização, pessoal e recursos em matéria de informação. O presente anexo é aplicável a qualquer SCI do SEAE em que sejam manuseadas ICUE.
3. As ICUE devem ser manuseadas pelos SCI de acordo com o conceito de GI.
4. Todos os SCI que tratem ICUE devem ser submetidos a um processo de acreditação. A acreditação visa obter a garantia de que foram tomadas todas as medidas de segurança adequadas e de que foi alcançado um nível suficiente de proteção das ICUE e do próprio SCI, nos termos da presente decisão. A declaração de acreditação determina o nível máximo de classificação das informações que podem ser manuseadas pelo SCI e os termos e condições correspondentes.

5. Os SCI em que sejam manuseadas informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior são protegidos de forma a impedir o comprometimento das informações devido a emanações eletromagnéticas não intencionais («medidas de segurança TEMPEST»).
6. Quando a proteção de ICUE for assegurada por produtos criptográficos, estes são aprovados em conformidade com o artigo 7.º, n.º 5, da presente decisão.
7. Durante a transmissão de ICUE por via eletrónica, são utilizados produtos criptográficos aprovados. Não obstante este requisito, podem ser aplicados procedimentos específicos, em circunstâncias de emergência ou configurações técnicas específicas, nos termos do Anexo A IV.
8. Em conformidade com o artigo 7.º, n.º 6, da presente decisão, as seguintes funções em matéria de GI serão criadas na medida do necessário:
 - a) Uma Autoridade de GI (AGI);
 - b) Uma Autoridade TEMPEST (AT);
 - c) Uma Autoridade de Aprovação Criptográfica (AAC);
 - d) Uma Autoridade de Distribuição Criptográfica (ADC).
9. Ao abrigo do artigo 7.º, n.º 7 da presente decisão, será criado, para cada sistema:
 - a) Uma Autoridade de Acreditação de Segurança (AAS);
 - b) Uma Autoridade Operacional de GI.
10. As regras de execução do presente artigo são estabelecidas no Anexo A IV.

Artigo 9.º

Segurança industrial

1. Entende-se por «segurança industrial» a aplicação de medidas destinadas a garantir a proteção das ICUE pelos contratantes ou subcontratantes no âmbito das negociações pré-contratuais e durante a vigência dos contratos classificados. Estes contratos não devem, regra geral, envolver o acesso a informações com classificação TRÈS SECRET UE/EU TOP SECRET.
2. O SEAE pode confiar tarefas que envolvam ou impliquem o acesso a ICUE ou o seu manuseamento ou armazenamento a entidades industriais ou outras registadas num Estado-Membro ou num Estado terceiro que tenha celebrado um acordo de segurança das informações ou um convénio administrativo a que se refere o artigo 10.º, n.º 1 do Anexo A.
3. Ao adjudicar contratos classificados a entidades industriais ou outras, o SEAE, na qualidade de entidade adjudicante, garante o cumprimento das normas mínimas de segurança industrial estabelecidas na presente decisão, às quais o contrato fará referência. Assegura o cumprimento de tais normas mínimas através das ANS/ASD relevantes.
4. Os contratantes ou subcontratantes registados num determinado Estado-Membro que participem na execução de contratos ou subcontratos que exijam o manuseamento e armazenamento de informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET dentro das suas próprias instalações, seja na execução do contrato, seja na fase pré-contratual, deverão possuir uma Credenciação de Segurança da Empresa (CSE) para o nível de classificação adequado, concedida pela ANS, ASD ou por qualquer outra autoridade de segurança competente do respetivo Estado-Membro.

5. O pessoal do contratante ou subcontratante que tenha de aceder a informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET para a execução de contratos classificados deve possuir uma CSP, emitida pela respetiva Autoridade Nacional de Segurança (ANS), Autoridade de Segurança Designada (ASD) ou por qualquer outra autoridade de segurança competente nos termos das disposições legislativas e regulamentares nacionais e das normas mínimas estabelecidas no Anexo A I.
6. As regras de execução do presente artigo são estabelecidas no Anexo A V.

Artigo 10.º

Intercâmbio de informações classificadas com Estados terceiros e organizações internacionais

1. O SEAE só pode trocar ICUE com um Estado terceiro ou uma organização internacional se:
- a) Estiver em vigor um acordo de segurança das informações entre a UE e um Estado terceiro ou organização internacional, celebrado nos termos do artigo 37.º do TUE e do artigo 218.º do TFUE; ou
 - b) Estiver em vigor um convénio administrativo entre a AR e as autoridades de segurança competentes do respetivo Estado terceiro ou organização internacional, para o intercâmbio de informações com classificação, em princípio, não superior a RESTREINT UE/EU RESTRICTED, celebrado em conformidade com o procedimento definido no artigo 14.º, n.º 5 da presente decisão; ou
 - c) For aplicável um acordo-quadro de participação ou um acordo de participação ad hoc entre a UE e o respetivo Estado terceiro no contexto de uma operação PCSD de gestão de crises, celebrado nos termos do artigo 37.º do TUE e do artigo 218.º do TFUE,

e as condições definidas nesse instrumento forem cumpridas.

As exceções à regra geral supramencionada são estabelecidas na Secção V do Anexo A VI.

2. Os convénios administrativos a que se refere o n.º 1, alínea b), contêm disposições destinadas a assegurar que, ao receberem ICUE, os Estados terceiros e as organizações internacionais concedam a essas informações uma proteção que seja adequada ao respetivo nível de classificação e obedeça a normas mínimas não menos rigorosas do que as estabelecidas na presente decisão.

O intercâmbio de informações com base em acordos a que se refere o n.º 1, alínea c) deve ser limitado a informações respeitantes a operações PCSD em que o Estado terceiro em questão participa com base neste acordos e em conformidade com respetivas disposições.

3. As visitas a Estados terceiros ou organizações internacionais, a que se refere o artigo 16.º da presente decisão, são organizadas a fim de avaliar a eficácia das medidas de segurança aplicadas para proteção das ICUE trocadas.

4. A decisão de comunicar ICUE detidas pelo SEAE a um Estado terceiro ou organização internacional é tomada caso a caso, em função da natureza e do teor dessas informações, da necessidade que o destinatário tenha de tomar conhecimento das mesmas, e das vantagens que daí advenham para a UE.

O SEAE deve solicitar o consentimento, por escrito, de qualquer entidade que tenha fornecido informações classificadas como material de referência para ICUE de que a SEAE seja a entidade de origem, a fim de estabelecer que não existem objeções à comunicação das mesmas.

Se as informações classificadas cuja comunicação se pretende não emanarem do SEAE, o SEAE solicita à entidade de origem que dê, por escrito, o consentimento prévio para a sua comunicação.

Todavia, se o SEAE não conseguir identificar a entidade de origem, a autoridade de segurança do SEAE assume a responsabilidade em seu lugar, após obtenção do parecer favorável por unanimidade dos Estados-Membros representados no Comité de Segurança do SEAE.

5. As regras de execução do presente artigo são estabelecidas no Anexo A VI.

Artigo 11.º

Quebras de segurança e comprometimento de informações classificadas

1. Qualquer quebra ou suspeita de quebra de segurança e qualquer comprometimento ou suspeita de comprometimento de informações classificadas será imediatamente comunicado à Direção da Segurança do SEAE, que informará, sempre que adequado, a Direção de Segurança da Direção-Geral dos Recursos Humanos e da Segurança da Comissão, bem como o Gabinete de Segurança do Secretariado-Geral do Conselho, o(s) Estado(s)-Membro(s) em questão ou outra entidade relevante.

2. Sempre que haja conhecimento ou motivos razoáveis para presumir que houve comprometimento ou perda de informações classificadas, a Direção da Segurança do SEAE informa desse facto a Direção da Segurança da Comissão, o Gabinete de Segurança do Secretariado-Geral do Conselho ou a ANS do(s) Estado(s)-Membro(s) em questão, ou outra entidade relevante, conforme adequado, e toma as medidas apropriadas nos termos das disposições legislativas e regulamentares pertinentes para:

- a) Avaliar os danos eventualmente causados aos interesses da UE ou dos Estados-Membros;
- b) Tomar as medidas adequadas para impedir novas ocorrências;
- c) Salvar provas;
- d) Garantir que o caso seja investigado por elementos do pessoal não diretamente envolvidos na quebra de segurança, a fim de determinar os factos ocorridos;
- e) Notificar as autoridades competentes dos efeitos da ocorrência e da ação tomada; e
- f) Informar a entidade de origem.

3. Os membros do pessoal sob responsabilidade do SEAE que são responsáveis pela violação das regras de segurança estabelecidas na presente decisão são passíveis de ação disciplinar nos termos das disposições regulamentares aplicáveis.

Quem for responsável pelo comprometimento ou pela perda de informações classificadas é passível de ação disciplinar e/ou judicial nos termos das disposições legislativas e regulamentares aplicáveis.

A Direção de Segurança da Direção-Geral dos Recursos Humanos e da Segurança da Comissão, o Gabinete de Segurança do Secretariado-Geral do Conselho ou a ANS do(s) Estado(s)-Membro(s) em questão, ou outra entidade relevante, devem ser imediatamente informados, sempre que adequado.

4. No decorrer de uma investigação a um comprometimento ou quebra de segurança, o Chefe da Direção da Segurança do SEAE pode suspender o acesso da pessoa em questão às ICUE e às instalações do SEAE. A Direção de Segurança da Direção-Geral dos Recursos Humanos e da Segurança da Comissão, o Gabinete de Segurança do Secretariado-Geral do Conselho ou a ANS do(s) Estado(s)-Membro(s) ou outra entidade relevante, devem ser imediatamente informados da presente decisão.

ANEXO A I

REQUISITOS DE SEGURANÇA DO PESSOAL**I. INTRODUÇÃO**

1. O presente anexo estabelece as regras de execução do artigo 5.º do Anexo A. Nele se definem não só os critérios a ter em conta pelo SEAE para determinar se, com base nas suas lealdade, idoneidade e fiabilidade, uma dada pessoa pode ser autorizada a ter acesso a ICUE, mas também os procedimentos administrativos e de investigação a seguir para esse efeito.
2. A «Certificação de Segurança do Pessoal» (CSP) para acesso a ICUE consiste numa declaração de uma autoridade competente de um Estado-Membro feita depois de concluída uma investigação de segurança conduzida pelas autoridades competentes de um Estado-Membro, e pela qual se atesta que uma dada pessoa pode aceder a ICUE até determinado nível (CONFIDENTIEL UE/EU CONFIDENTIAL ou superior), e até determinada data, desde que tenha sido comprovada a sua «necessidade de tomar conhecimento»; diz-se da pessoa nestas condições que «possui credenciação de segurança»;
3. O «Certificado de Credenciação de Segurança do Pessoal» (CCSP) é um certificado emitido pela autoridade de segurança do SEAE que indica a credenciação de segurança de uma pessoa e apresenta o nível de ICUE a que a mesma pode ter acesso, o período de validade da CSP e o prazo de validade do próprio certificado.
4. A «Autorização para acesso a ICUE» é uma autorização dada pela Autoridade de Segurança do SEAE, tomada nos termos da presente decisão após emissão de uma CSP pelas autoridades competentes de um Estado-Membro, e pela qual se atesta que uma dada pessoa pode aceder a ICUE até determinado nível (CONFIDENTIEL UE/EU CONFIDENTIAL ou superior), e até determinada data, desde que tenha sido comprovada a sua «necessidade de tomar conhecimento»; diz-se da pessoa nestas condições que «possui credenciação de segurança».

II. AUTORIZAÇÃO DE ACESSO ÀS ICUE

5. O acesso a informações com classificação RESTREINT UE/EU RESTRICTED não exige uma credenciação de segurança e é concedido após:
 - a) Identificação do vínculo de natureza estatutária ou contratual ao SEAE;
 - b) Confirmação da necessidade de tomar conhecimento de tais informações;
 - c) Comunicação das regras e procedimentos de segurança aplicáveis à proteção das ICUE à pessoa e reconhecimento pela mesma, por escrito, das suas responsabilidades no que respeita à proteção dessas informações em conformidade com a presente decisão.
6. Ninguém pode ser autorizado a ter acesso a informações da UE com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior sem que:
 - a) Tenha ficado comprovada a sua necessidade de tomar conhecimento de tais informações;
 - b) Lhe tenha sido conferida a CSP para o nível adequado ou outra autorização devidamente emitida em virtude das funções que exerce nos termos das disposições legislativas e regulamentares nacionais; e
 - c) Tenha sido informado das regras e procedimentos de segurança aplicáveis à proteção das ICUE e tenha reconhecido, por escrito, as suas responsabilidades no que respeita à proteção dessas informações.
7. O SEAE identificará os cargos que, nas respetivas estruturas, exigem o acesso a informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior e para os quais é, por esse motivo, necessária uma CSP para o nível adequado, a que se refere o supramencionado artigo 4.º.
8. O pessoal do SEAE deve declarar se têm cidadania em mais do que um país.

Procedimento de solicitação de CSP no SEAE

9. No que respeita ao pessoal do SEAE, a Autoridade do SEAE Investida do Poder de Nomeação enviará o questionário de segurança do pessoal, preenchido, à ANS do Estado-Membro de nacionalidade da pessoa, solicitando que seja levada a cabo uma investigação de segurança para o nível de ICUE às quais a pessoa deverá ter acesso.
10. Quando uma pessoa tem cidadania em mais do que um país, o pedido de verificação será endereçado à ANS do país correspondente à nacionalidade a partir da qual a pessoa foi recrutada.
11. Se o SEAE tomar conhecimento de informações relevantes para a investigação de segurança a respeito de alguém que tenha solicitado uma CSP, o SEAE informará desse facto a ANS competente, nos termos das regras e regulamentações pertinentes.

12. Após a conclusão da investigação de segurança, a ANS competente notifica a Direção da Segurança do SEAE do resultado da referida investigação.
- Se da investigação de segurança se concluir que não há garantidamente conhecimento de fatores desfavoráveis que ponham em dúvida a lealdade, a idoneidade e a fiabilidade da pessoa, a Autoridade do SGC Investida do Poder de Nomeação pode conceder à pessoa em questão uma CSP UE e autorizá-la a ter acesso a ICUE até ao nível adequado e até determinada data;
 - O SEAE toma todas as medidas adequadas para que as condições ou restrições impostas pela ANS sejam devidamente implementadas. A ANS é informada do resultado.
 - Se da investigação de segurança se não concluir pela existência dessa garantia, a Autoridade de Segurança do SEAE notificará do facto a pessoa em causa, que poderá pedir para ser ouvida pela referida Autoridade. A Autoridade de Segurança do SEAE poderá pedir à ANS competente quaisquer outros esclarecimentos que esta possa prestar nos termos das respetivas disposições legislativas e regulamentares nacionais. Se as conclusões se confirmarem, não será concedida uma Autorização para acesso a ICUE. Neste caso, o SEAE toma todas as medidas adequadas para que seja negado ao candidato qualquer acesso a ICUE.
13. A investigação de segurança, em conjunto com os resultados obtidos, em que o SEAE baseia a sua decisão de conceder ou não uma autorização para acesso a ICUE, ficará sujeita às disposições legislativas e regulamentares pertinentes em vigor no Estado-Membro em questão, incluindo em matéria de recurso. As decisões tomadas pela Autoridade de Segurança do SEAE são passíveis de recurso nos termos do Estatuto dos Funcionários da União Europeia e do Regime Aplicável aos Outros Agentes da União Europeia, previstos no Regulamento (CEE, Euratom, CECA) n.º 259/68 ⁽¹⁾ (a seguir designado «Estatuto do Pessoal»).
14. A garantia em que se baseia a CSP, desde que se mantenha válida, abrangerá quaisquer funções que a pessoa em causa venha a desempenhar no SEAE, no Secretariado-Geral do Conselho ou na Comissão.
15. Se o período de serviço da pessoa não tiver começado no prazo de 12 meses a contar da notificação dos resultados da investigação de segurança à Autoridade de Segurança do SEAE, ou se houver uma interrupção de 12 meses ou mais no serviço durante a qual a pessoa não exerça funções no SEAE, em outras Instituições, agências ou órgãos da UE ou na administração de um Estado-Membro, que exija acesso a informação classificada, os referidos resultados serão remetidos à ANS competente, para confirmação de que continuam a ser válidos e pertinentes.
16. Se o SEAE tomar conhecimento de informações a respeito da existência de qualquer risco para a segurança que provenha de alguém que tenha uma CSP válida, o SEAE informará desse facto a ANS competente, nos termos das regras e regulamentações pertinentes. Quando a ANS comunicar ao SEAE que retirou a alguém que possua uma Autorização válida para acesso a ICUE a garantia que lhe fora dada nos termos do ponto 12, alínea a), a Autoridade de Segurança do SEAE pode pedir à ANS quaisquer esclarecimentos que esta possa prestar nos termos das respetivas disposições legislativas e regulamentares nacionais. Se as informações desfavoráveis forem confirmadas, a Autorização supramencionada será retirada e a pessoa em causa será excluída do acesso às ICUE e afastada de funções no âmbito das quais esse acesso seja possível ou a pessoa possa prejudicar a segurança.
17. A decisão de retirar uma Autorização para acesso a ICUE a um membro do pessoal do SEAE e, se necessário, as razões que a motivaram serão notificadas à pessoa em causa, que pode pedir para ser ouvida pela Autoridade de Segurança do SEAE. As informações prestadas pela ANS ficarão sujeitas às disposições legislativas e regulamentares pertinentes em vigor no Estado-Membro em questão, incluindo em matéria de recurso. As decisões tomadas pela Autoridade de Segurança do SEAE são passíveis de recurso nos termos do Estatuto do Pessoal.
18. Antes de assumirem funções, os peritos nacionais destacados para um cargo no SEAE que exija o acesso a informação com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior deverão apresentar à Autoridade de Segurança do SEAE uma CSP válida para efeitos de acesso ao nível pertinente das ICUE. O processo supramencionado deve ser gerido pelo Estado-Membro remetente.

Registos de CSP

19. O SEAE manterá uma base de dados com o estatuto de credenciação de segurança de todo o pessoal sob responsabilidade do SEAE e do pessoal dos contratantes do SEAE. Esses registos incluirão o nível das ICUE a que a pessoa pode ter acesso (CONFIDENTIEL UE/EU CONFIDENTIAL ou superior), a data de concessão e o período de validade da CSP.
20. Devem estabelecer-se procedimentos de coordenação adequados com os Estados-Membros e outras Instituições, agências e órgãos da UE para garantir que o SEAE possui um registo rigoroso e abrangente dos estatutos de credenciação de segurança de todo o pessoal sob responsabilidade do SEAE e dos funcionários dos contratantes do SEAE.

⁽¹⁾ JO L 56 de 4.3.1968, p. 1

21. A Autoridade de Segurança do SEAE poderá emitir um Certificado de Credenciação de Segurança do Pessoal (CCSP), indicando o nível de ICUE a que a pessoa pode ter acesso (CONFIDENTIEL UE/EU CONFIDENTIAL ou superior), o período de validade da CSP e o prazo de validade do próprio certificado.

Isenção do requisito de Credenciação de Segurança do Pessoal

22. Quem estiver devidamente autorizado a aceder a ICUE em virtude das funções que exerce nos termos das respetivas disposições legislativas e regulamentares nacionais deve ser informado pela Direção da Segurança do SEAE, consoante adequado, das suas obrigações de segurança no que respeita à proteção das ICUE.

III. EDUCAÇÃO E SENSIBILIZAÇÃO PARA A SEGURANÇA

23. Antes de serem autorizadas a aceder a ICUE, todas as pessoas confirmarão por escrito que compreenderam as obrigações a que estão sujeitas no que respeita à proteção das ICUE e as consequências do comprometimento de ICUE. O SEAE conservará um registo dessas declarações escritas.
24. Todas as pessoas autorizadas a aceder a ICUE ou que precisem de manusear ICUE serão inicialmente sensibilizadas e periodicamente informadas das ameaças existentes para a segurança e deverão comunicar imediatamente às autoridades de segurança competentes qualquer atitude ou atividade que considerem suspeita ou pouco habitual.
25. Todas as pessoas com acesso a ICUE são sujeitas a medidas contínuas de segurança do pessoal (isto é, acompanhamento posterior) durante o período em que manuseiam ICUE. A segurança contínua do pessoal é da responsabilidade de:
- a) Pessoas com acesso a ICUE: as pessoas são pessoalmente responsáveis pela sua conduta de segurança e deverão comunicar imediatamente às autoridades de segurança competentes qualquer atitude ou atividade que considerem suspeita ou pouco habitual e quaisquer circunstâncias pessoais que possam afetar a sua CSP ou a Autorização para acesso a ICUE.
 - b) Superiores hierárquicos: são responsáveis por garantir que o pessoal tem conhecimento das medidas e responsabilidades de segurança para proteção das ICUE, por controlar a conduta de segurança do pessoal e por lidar pessoalmente com questões de segurança preocupantes ou comunicar às autoridades de segurança adequadas quaisquer informações adversas que possam afetar a CSP do pessoal ou a Autorização para acesso a ICUE.
 - c) Intervenientes no domínio da segurança da organização de segurança do SEAE a que se refere o artigo 12.º da presente decisão: são responsáveis por realizar reuniões de sensibilização em matéria de segurança para assegurar que o pessoal na sua área é informado periodicamente, por fomentar uma cultura de segurança forte na sua área de responsabilidade, por definir medidas de controlo da conduta de segurança do pessoal e por comunicar às autoridades de segurança adequadas quaisquer informações adversas que possam afetar a CSP de alguém.
 - d) O SEAE e os Estados-Membros: estabelecerão os canais necessários para comunicar informação que possa afetar a CSP de alguém ou a Autorização para acesso a ICUE.
26. Quem deixar de exercer funções que exijam acesso a ICUE será informado de que deverá continuar a salvaguardar as ICUE e, se necessário, confirmará por escrito essa sua obrigação.

IV. CIRCUNSTÂNCIAS EXCECIONAIS

27. Por motivos de urgência devidamente justificados pelo interesse do SEAE e enquanto se aguarda a conclusão de uma investigação de segurança exaustiva, a Autoridade de Segurança do SEAE, após consulta à ANS do Estado-Membro de nacionalidade do interessado e sob reserva dos resultados da verificação inicial de que não há conhecimento de informações desfavoráveis, pode conceder aos funcionários e outros agentes do SEAE uma autorização temporária de acesso a ICUE para uma função concreta. Deverá completar-se uma investigação de segurança completa assim que possível. Essas autorizações temporárias terão uma validade não superior a seis meses e não permitirão o acesso a informações com classificação TRÈS SECRET UE/EU TOP SECRET. Todas as pessoas a quem tenha sido concedida uma autorização temporária confirmarão por escrito que compreenderam as obrigações a que estão sujeitas no que respeita à proteção das ICUE e as consequências do comprometimento de ICUE. O SEAE conservará um registo dessas declarações escritas.
28. Quando devam ser atribuídas a alguém funções que exijam uma CSP de nível superior ao que a pessoa possui, a atribuição pode ser feita a título temporário, desde que:
- a) A necessidade urgente de acesso a ICUE de nível superior seja justificada, por escrito, pelo superior hierárquico da pessoa em causa;
 - b) O acesso seja limitado a ICUE específicas de apoio às funções exercidas;

- c) A pessoa em causa possua uma CSP válida;
 - d) Tenham sido iniciados os trâmites necessários para obter autorização para o nível de acesso exigido para essas funções;
 - e) A autoridade competente tenha feito verificações satisfatórias das quais se tenha concluído que a pessoa em causa não infringiu as regras de segurança de forma grave nem reiterada;
 - f) A atribuição de funções à pessoa em causa seja aprovada pela autoridade competente do SEAE; e
 - g) a ANS/ASD pertinente que emitiu a CSP da pessoa tenha sido consultada e não se tenha recebido qualquer objeção;
 - h) A exceção, incluindo uma descrição das informações para as quais tenha sido aprovado o acesso, seja averbada no registo responsável ou num registo que dele dependa
29. O procedimento acima descrito será utilizado para um único acesso a ICUE de nível superior àquele para o qual tenha sido concedida credenciação de segurança à pessoa em causa. Não se recorrerá repetidamente a este procedimento.
30. Em circunstâncias muito excecionais, como sejam as missões em ambiente hostil ou os períodos de crescente tensão internacional, quando as medidas de emergência o exijam, nomeadamente para salvar vidas humanas, a AR, o secretário-geral executivo ou o diretor operacional poderão conceder, por escrito, acesso a informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET a pessoas que não possuam a necessária CSP, desde que tal autorização seja absolutamente necessária e não haja dúvidas razoáveis quanto à lealdade, à idoneidade e à fiabilidade da pessoa em causa. Será conservado registo desta autorização, com a descrição das informações para as quais tenha sido aprovado acesso.
31. No caso de informações com classificação TRÈS SECRET UE/EU TOP SECRET, este acesso de emergência será limitado aos nacionais da UE que tenham sido autorizados a aceder ao equivalente nacional do nível TRÈS SECRET UE/EU TOP SECRET ou às informações com classificação SECRET UE/EU SECRET.
32. O Comité de Segurança do SEAE será informado dos casos em que se recorra ao procedimento descrito nos pontos 29 e 30.
33. Será anualmente apresentado ao Comité de Segurança do SEAE um relatório sobre o recurso aos procedimentos estabelecidos na presente secção.

V. PARTICIPAÇÃO EM REUNIÕES NA SEDE DO SEAE E NAS DELEGAÇÕES DA UNIÃO.

34. As pessoas que devam participar em reuniões na Sede do SEAE e nas delegações da União em que sejam discutidas informações com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior só poderão fazê-lo depois de confirmado o seu estatuto de CSP. No caso de representantes dos Estados-Membros, agentes do SGC e da Comissão, o CCSP, ou outra prova de CSP, será enviado pelas autoridades competentes à Direção da Segurança do SEAE, ao Coordenador de Segurança da delegação da União ou, a título excepcional, apresentado pela própria pessoa. Se necessário, poderá ser usada uma lista consolidada de nomes, com a indicação da prova de CSP relevante.
35. Se for retirada a CSP para efeitos de acesso a ICUE a alguém cuja presença seja necessária, em virtude das funções que exerce, em reuniões na Sede do SEAE ou numa delegação da União em que se debatem informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior, a autoridade competente informará do facto o SEAE.

VI. ACESSO POTENCIAL A ICUE

36. Quem for recrutado para trabalhar em circunstâncias em que possa ter acesso a informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior ficará sujeito aos procedimentos de credenciação de segurança adequados ou será permanentemente escoltado.
37. Os estafetas, guardas e escoltas devem possuir a credenciação de segurança para o nível adequado ou ser de outro modo sujeitos a uma investigação adequada nos termos das disposições legislativas e regulamentares nacionais, ser informados, em intervalos regulares, dos procedimentos de segurança aplicáveis à proteção das ICUE e do seu dever de proteção das informações que lhes forem confiadas ou a que possam ter acesso inadvertidamente.

ANEXO A II

SEGURANÇA FÍSICA DAS INFORMAÇÕES CLASSIFICADAS DA UE**I. INTRODUÇÃO**

1. O presente anexo estabelece as regras de execução do artigo 6.º do Anexo A. Nele se definem os requisitos mínimos para a proteção física de instalações, edifícios, gabinetes, salas e outras zonas em que sejam manuseadas e armazenadas ICUE, e, nomeadamente, zonas que alberguem SCI.
2. Serão concebidas medidas de segurança física para impedir o acesso não autorizado a ICUE:
 - a) Assegurando que as ICUE sejam devidamente manuseadas e armazenadas;
 - b) Permitindo a diferenciação do pessoal no que se refere ao acesso a ICUE com base na sua necessidade de tomar conhecimento de tais informações e, se for caso disso, na respetiva credenciação de segurança;
 - c) Dissuadindo, impedindo e detetando ações não autorizadas; e
 - d) Impedindo ou retardando a entrada sub-reptícia ou forçada de intrusos.

II REQUISITOS E MEDIDAS DE SEGURANÇA FÍSICA

3. O SEAE aplicará um processo de gestão de risco à proteção das ICUE nas suas instalações, por forma a assegurar que seja concedido um nível de proteção física proporcional ao risco avaliado. No processo de gestão de risco serão tidos em conta todos os fatores pertinentes, nomeadamente:
 - a) O nível de classificação das ICUE;
 - b) A forma e o volume das ICUE, tendo em conta que as grandes quantidades ou acervos de ICUE podem justificar a aplicação de medidas de proteção mais rigorosas;
 - c) A envolvente e a estrutura dos edifícios ou zonas que albergam as ICUE;
 - d) A avaliação de ameaças em países terceiros conforme desenvolvida pelo INTCEN com base em relatórios específicos das delegações da União, e
 - e) A avaliação da ameaça representada pelos serviços de informações que tenham por alvo a UE ou os Estados-Membros, pelos atos de sabotagem ou de terrorismo, bem como por outras atividades subversivas ou criminosas.
4. A autoridade de segurança do SEAE determinará, aplicando o conceito de defesa em profundidade, qual a combinação adequada de medidas de segurança física a implementar. Estas podem incluir uma ou mais das seguintes:
 - a) Um perímetro: uma barreira física que resguarda os limites de uma zona que precisa de ser protegida;
 - b) Sistemas de deteção de intrusos (IDS): podem ser utilizados IDS para aumentar o nível de segurança proporcionado pelo perímetro ou para substituir ou apoiar o pessoal de segurança em salas e edifícios;
 - c) Controlo do acesso: o controlo do acesso poderá ser exercido em relação a um local, a um edifício ou edifícios de determinado local, ou a zonas ou salas de um edifício. O controlo poderá ser exercido por processos eletrónicos ou eletromecânicos, efetuado pelo pessoal de segurança e/ou por um rececionista, ou por quaisquer outros meios físicos;
 - d) Pessoal de segurança: poderá nomeadamente recorrer-se a pessoal de segurança devidamente formado, supervisionado e, se necessário, com a devida credenciação de segurança para dissuadir todos aqueles que planeiem uma intrusão dissimulada;
 - e) Televisão em circuito fechado (CCTV): o pessoal de segurança poderá utilizar um sistema de CCTV para verificar incidentes e alarmes de IDS em locais de grandes dimensões ou nos perímetros;
 - f) Luzes de segurança: poderão ser utilizadas luzes de segurança para dissuadir os potenciais intrusos e proporcionar a iluminação necessária para uma vigilância efetiva, efetuada quer diretamente pelo pessoal de segurança, quer indiretamente através de um sistema de CCTV; e

- g) Quaisquer outras medidas físicas adequadas que sejam concebidas para dissuadir ou detetar o acesso não autorizado ou evitar que as ICUE se percam ou sejam danificadas.
5. A Direção da Segurança do SEAE pode efetuar buscas nas entradas e saídas, que funcionarão como elemento dissuasor da introdução não autorizada de material ou da saída não autorizada de ICUE das instalações ou edifícios.
6. Quando houver risco de olhares indiscretos sobre ICUE, mesmo que acidentalmente, serão tomadas as medidas necessárias para neutralizar esse risco.
7. Na fase de planeamento e conceção de novas instalações, deverão ser definidos os requisitos de segurança física e as respetivas especificações funcionais. Em instalações já existentes, os requisitos de segurança física serão aplicados em toda a medida do possível.

III. EQUIPAMENTO PARA A PROTEÇÃO FÍSICA DAS ICUE

8. Aquando da aquisição de equipamento (por exemplo, contentores de segurança, máquinas trituradoras, fechaduras de porta, sistemas eletrónicos de controlo de acesso, sistemas de deteção de intrusos, sistemas de alarme) para proteção física das ICUE, a autoridade de segurança do SEAE certificar-se-á de que o equipamento satisfaz as normas técnicas e os requisitos mínimos aprovados.
9. As especificações técnicas do equipamento a utilizar na proteção física das ICUE serão estabelecidas em diretrizes de segurança aprovadas pelo Comité de Segurança do SEAE.
10. Os sistemas de segurança serão regularmente sujeitos a inspeção e o equipamento será objeto de manutenção regular. Nos trabalhos de manutenção serão tidos em conta os resultados das inspeções, a fim de garantir que o equipamento continue a funcionar nas melhores condições.
11. Em cada inspeção será reavaliada a eficácia de cada medida de segurança e do sistema de segurança em geral.

IV. ZONAS FÍSICAMENTE PROTEGIDAS

12. Serão estabelecidos dois tipos de zonas fisicamente protegidas, ou os seus equivalentes nacionais, para assegurar a proteção física das ICUE:
- a) Zonas Administrativas e
- b) Zonas de Segurança (incluindo as Zonas Tecnicamente Seguras).
13. A autoridade de segurança do SEAE determinará que uma dada zona preenche os requisitos para ser designada Zona Administrativa, Zona de Segurança ou Zona Tecnicamente Segura.
14. No caso das Zonas Administrativas:
- a) Será estabelecido um perímetro visivelmente definido que permita o controlo de pessoas e, se possível, de veículos;
- b) Só poderão ter acesso sem escolta as pessoas devidamente autorizadas pela Direção da Segurança do SEAE; e
- c) Quaisquer outras pessoas serão permanentemente escoltadas ou sujeitas a controlos equivalentes.
15. No caso das Zonas de Segurança:
- a) Será estabelecido um perímetro visivelmente definido, em que qualquer entrada ou saída será controlada por meio de um sistema de livre-trânsito ou de reconhecimento de pessoas;
- b) Só poderão ter acesso sem escolta as pessoas com a devida credenciação de segurança para o nível em questão e especificamente autorizadas a entrar nessa zona por terem necessidade de tomar conhecimento das ICUE em causa;
- c) Quaisquer outras pessoas serão permanentemente escoltadas ou sujeitas a controlos equivalentes.
16. Nos casos em que a entrada numa Zona de Segurança represente, para todos os efeitos práticos, um acesso direto às informações classificadas que nela se encontrem, aplicam-se ainda os seguintes requisitos:
- a) Haverá uma indicação clara do nível de classificação de segurança mais elevado das informações normalmente conservadas nessa zona;

- b) Todos os visitantes deverão pedir autorização específica para entrar nessa zona, ser permanentemente escoltados e possuir a devida credenciação de segurança, a menos que sejam tomadas medidas para assegurar que não seja possível ter acesso às ICUE;
 - c) Os equipamentos eletrónicos deverão permanecer fora dessa zona.
17. As Zonas de Segurança a proteger contra escutas serão designadas Zonas Tecnicamente Seguras. A estas zonas aplicam-se ainda os seguintes requisitos:
- a) Serão equipadas com sistemas de deteção de intrusos (IDS), fechadas à chave quando não estiverem ocupadas e guardadas quando ocupadas. Todas as chaves serão controladas de acordo com a Secção VI do presente anexo;
 - b) Serão sujeitas a controlo todas as pessoas ou material que nelas penetrem;
 - c) Serão sujeitas a inspeção física e/ou técnica regular, consoante o que a autoridade de segurança do SEAE exigir. Essa inspeção será igualmente efetuada na sequência de qualquer entrada não autorizada ou de suspeitas dessa possibilidade; e
 - d) Serão desprovidas de dispositivos não autorizados como linhas de comunicação, telefones ou outros aparelhos de comunicação, bem como equipamento elétrico ou eletrónico;
18. Não obstante o disposto no ponto 17, alínea d) e em circunstâncias em que a ameaça seja considerada elevada, qualquer tipo de aparelho de comunicações e equipamento elétrico ou eletrónico será inspecionado pela autoridade de segurança do SEAE antes de ser utilizado em zonas onde decorram reuniões ou se trabalhe com informações com classificação SECRET UE/EU SECRET e superior, por forma a garantir que nenhuma informação inteligível seja transmitida por esse equipamento, ilícita ou inadvertidamente, para fora do perímetro da Zona de Segurança.
19. As Zonas de Segurança que não estejam ocupadas por pessoal em serviço 24 horas por dia serão, se necessário, inspecionadas no final das horas normais de serviço e a intervalos aleatórios fora dessas horas, a menos que esteja instalado um sistema de deteção de intrusos.
20. Poderão ser temporariamente criadas Zonas de Segurança e Zonas Tecnicamente Seguras no interior de determinada Zona Administrativa para a realização de uma reunião classificada ou para qualquer outro fim semelhante.
21. Para cada Zona de Segurança serão estabelecidos procedimentos operacionais de segurança que estipulem:
- a) O nível das ICUE que podem ser manuseadas ou armazenadas nessa zona;
 - b) As medidas de vigilância e de proteção a manter;
 - c) As pessoas autorizadas a aceder sem escolta à zona por terem necessidade de tomar conhecimento das ICUE em causa e possuírem a devida credenciação de segurança;
 - d) Se necessário, os procedimentos respeitantes a escoltas ou à proteção das ICUE quando se autorize o acesso de outras pessoas a essa zona;
 - e) Quaisquer outras medidas e procedimentos relevantes.
22. Serão construídas casas-fortes dentro das Zonas de Segurança. As paredes, o chão, os tetos, as janelas e as portas com sistema de fecho serão aprovados pela autoridade de segurança do SEAE e beneficiarão de proteção equivalente à de um contentor de segurança aprovado para armazenamento de ICUE com o mesmo nível de classificação.
- V. MEDIDAS DE PROTEÇÃO FÍSICA PARA O MANUSEAMENTO E ARMAZENAMENTO DE ICUE**
23. As ICUE com classificação RESTREINT UE/EU RESTRICTED podem ser manuseadas:
- a) Em Zonas de Segurança;
 - b) Em Zonas Administrativas, desde que as ICUE se encontrem protegidas do acesso por parte de pessoas não autorizadas; ou
 - c) Fora de Zonas de Segurança ou de Zonas Administrativas, desde que o detentor das informações classificadas as transporte nas condições estabelecidas nos pontos 30 a 42 do Anexo A III e se tenha comprometido a respeitar as medidas de compensação estabelecidas nas instruções emitidas pela autoridade de segurança do SEAE, a fim de assegurar que as ICUE fiquem protegidas do acesso por parte de pessoas não autorizadas.

24. As ICUE com classificação RESTREINT UE/EU RESTRICTED devem ser armazenadas em mobiliário de escritório apropriado e fechado à chave, numa Zona Administrativa ou Zona de Segurança. As referidas ICUE poderão ser temporariamente armazenadas fora de Zonas de Segurança ou de Zonas Administrativas, desde que o detentor das informações classificadas se tenha comprometido a respeitar as medidas de compensação estabelecidas nas instruções emitidas pela autoridade de segurança do SEAE.
25. As ICUE com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET podem ser manuseadas:
- Em Zonas de Segurança;
 - Em Zonas Administrativas, desde que as ICUE se encontrem protegidas do acesso por parte de pessoas não autorizadas; ou
 - Fora de Zonas de Segurança ou de Zonas Administrativas, desde que o detentor das informações classificadas:
 - as transporte nas condições estabelecidas nos pontos 30 a 42 do Anexo A III;
 - se tenha comprometido a respeitar as medidas de compensação estabelecidas nas instruções emitidas pela autoridade de segurança do SEAE, a fim de assegurar que as ICUE fiquem protegidas do acesso por parte de pessoas não autorizadas;
 - mantenha as ICUE permanentemente sob o seu controlo pessoal; e
 - no caso de documentos em suporte papel, tenha informado desse facto o registo competente.
26. As ICUE com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET serão armazenadas em Zonas de Segurança, dentro de um contentor de segurança ou de uma casa-forte.
27. As ICUE com classificação TRÈS SECRET UE/EU TOP SECRET serão manuseadas em Zonas de Segurança.
28. As ICUE com classificação TRÈS SECRET UE/EU TOP SECRET serão armazenadas em Zonas de Segurança na Sede, numa das seguintes condições:
- Num contentor de segurança, de acordo com o estabelecido no ponto 8, com um ou vários dos seguintes controlos suplementares:
 - proteção ou verificação permanente por pessoal de segurança ou de serviço com credenciação de segurança;
 - um IDS aprovado, conjugado com pessoal de segurança incumbido das situações de emergência;ou
 - Numa casa-forte com IDS, conjugada com pessoal de segurança incumbido das situações de emergência.
29. As regras a que deve obedecer o transporte de ICUE fora das zonas fisicamente protegidas são estabelecidas no Anexo A III.
- VI. CONTROLO DAS CHAVES E COMBINAÇÕES DE FECHADURAS DE SEGREDO UTILIZADAS PARA PROTEÇÃO DAS ICUE**
30. A autoridade de segurança do SEAE definirá procedimentos para a gestão das chaves e das combinações das fechaduras de segredo dos gabinetes, salas, casas-fortes e contentores de segurança. Tais procedimentos deverão assegurar a proteção contra o acesso não autorizado.
31. As combinações deverão ser memorizadas pelo menor número possível de pessoas que precisem de as conhecer. As combinações dos contentores de segurança e das casas-fortes em que sejam conservadas ICUE deverão ser mudadas:
- Após receção de novos contentores;
 - Sempre que mude o pessoal que conhece a combinação;
 - Sempre que haja conhecimento ou suspeita de comprometimento;
 - Sempre que uma fechadura tenha sido objeto de manutenção ou reparação; e
 - Pelo menos de 12 em 12 meses.

ANEXO A III

GESTÃO DAS INFORMAÇÕES CLASSIFICADAS**I. INTRODUÇÃO**

1. O presente anexo estabelece as regras de execução do artigo 7.º do Anexo A. Nele se definem as medidas administrativas de controlo das ICUE ao longo do seu ciclo de vida que visam contribuir para dissuadir e detetar a perda ou comprometimento deliberados ou acidentais de informações e para recuperar essas informações em caso de perda ou comprometimento.

II. GESTÃO DAS CLASSIFICAÇÕES**Classificações e marcas**

2. As informações serão classificadas se precisarem de proteção em virtude da sua confidencialidade.
3. A entidade de origem das ICUE será responsável pela determinação do nível de classificação de segurança, nos termos das diretrizes de classificação relevantes, e pela divulgação das informações.
4. O nível de classificação das ICUE será determinado nos termos do artigo 2.º, n.º 2 do Anexo A e mediante remissão para a política de segurança a aprovar nos termos do artigo 3.º, n.º 3 do Anexo A.
5. As informações classificadas dos Estados-Membros trocadas com o SEAE deverão receber o mesmo nível de proteção que as ICUE de classificação equivalente. A tabela de equivalências relativa às regras de segurança aplicáveis à proteção das informações classificadas da UE pode ser consultada no Apêndice B da Decisão 2011/292/UE do Conselho, de 31 de março de 2011.
6. A classificação de segurança e, se aplicável, a data ou o acontecimento específico após os quais pode ser desgraduada ou desclassificada, deverão ser clara e corretamente indicados, independentemente do suporte em que as ICUE sejam apresentadas: papel, oral, eletrónico ou outro.
7. Cada uma das partes de um determinado documento (páginas, parágrafos, secções, anexos, apêndices, adendas e elementos apensos) poderá exigir classificações diferentes, devendo ostentar a marca correspondente, inclusivamente quando for armazenado em suporte eletrónico.
8. Na medida do possível, os documentos que contenham partes com níveis de classificação diferentes serão estruturados de forma a que as partes com um nível de classificação diferente possam ser facilmente identificadas e, se necessário, destacadas.
9. A classificação geral de um documento ou dossiê deverá ser pelo menos tão elevada quanto a da parte desse documento classificada ao nível mais elevado. Quando forem coligidas informações provenientes de várias fontes, o produto final será analisado para determinar o seu nível geral de classificação de segurança, uma vez que poderá justificar uma classificação mais elevada que a das partes que o compõem.
10. A classificação de uma carta ou nota de envio deverá ser tão elevada quanto a mais alta classificação dos seus anexos. A entidade de origem deverá indicar claramente a que nível é classificada a carta ou nota quando destacada dos anexos, para o que deverá utilizar uma marca adequada, por exemplo:

CONFIDENTIEL UE/EU CONFIDENTIAL

Sem anexo(s) RESTREINT UE/EU RESTRICTED

Marcas

11. Para além de uma das marcas de classificação previstas no artigo 2.º, n.º 2 do Anexo A, as ICUE poderão ostentar outras marcas, tais como:
 - a) Um identificador para designar a entidade de origem;
 - b) Eventuais advertências, códigos ou acrónimos que especifiquem o domínio de atividade a que o documento diz respeito, uma distribuição especial baseada na necessidade de ter conhecimento ou restrições de utilização;
 - c) Marcas relativas à comunicabilidade;
12. Após a decisão de comunicação das ICUE a um Estado terceiro ou a uma Organização Internacional, a Direção da Segurança do SEAE procederá ao envio das informações classificadas em causa, que ostentarão uma marca relativa à comunicabilidade, indicando o Estado terceiro ou organização internacional a que as ICUE serão comunicadas.

13. Uma lista de marcas autorizadas será aprovada pela Autoridade de Segurança do SEAE.

Marcas de classificação abreviadas

14. Para indicar o nível de classificação de certos parágrafos de determinado texto, podem ser utilizadas marcas de classificação sob forma de abreviaturas normalizadas. As abreviaturas não substituem as marcas de classificação por extenso.
15. Nos documentos classificados da UE, podem ser utilizadas, para indicar o nível de classificação de secções ou blocos do texto com menos de uma página, as seguintes abreviaturas normalizadas:

TRES SECRET UE/EU TOP SECRET	TS-UE/EU-TS
SECRET UE/EU SECRET	S-UE/EU-S
CONFIDENTIEL UE/EU CONFIDENTIAL	C-UE/EU-C
RESTREINT UE/EU RESTRICTED	R-UE/EU-R

Produção de ICUE

16. Ao produzir um documento classificado da UE:
- Todas as páginas serão marcadas de forma clara com o nível de classificação;
 - Todas as páginas serão numeradas;
 - O documento ostentará um número de referência e o assunto, que não constituem por si só informação classificada, a menos que estejam marcados como tal;
 - O documento será datado;
 - Os documentos com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior que devam ser distribuídos em vários exemplares ostentarão um número de exemplar em todas as páginas.
17. Quando não for possível aplicar o disposto no ponto 15 às ICUE, deverão ser tomadas outras medidas adequadas nos termos das diretrizes de segurança a estabelecer ao abrigo da presente decisão.

Desgradação e desclassificação de ICUE

18. Aquando da produção de ICUE, a entidade de origem indicará, sempre que possível, especialmente se se tratar de informações com classificação RESTREINT UE/EU RESTRICTED, se estas podem ser desgraduadas ou desclassificadas em determinada data ou após um dado acontecimento.
19. O SEAE analisará regularmente as ICUE que se encontrem na sua posse, a fim de apurar se o respetivo nível de classificação continua a ser aplicável. O SEAE estabelecerá um sistema para proceder, pelo menos de cinco em cinco anos, à reanálise do nível de classificação das ICUE registadas que tiver produzido. Essa reanálise não será necessária se a entidade de origem tiver indicado à partida o momento específico em que as informações serão automaticamente desgraduadas ou desclassificadas e se nelas tiver sido aposta a marca correspondente.

III. REGISTO DE ICUE PARA EFEITOS DE SEGURANÇA

20. Será estabelecido um registo central na SEDE. Será estabelecido um registo responsável para cada entidade orgânica do SEAE em que sejam manuseadas ICUE, subordinado ao registo central, para assegurar que as informações classificadas da UE sejam manuseadas nos termos da presente decisão. Os registos serão considerados Zonas de Segurança, tal como definidas no Anexo A.

Cada delegação da União estabelece o próprio registo de ICUE.

A autoridade de segurança do SEAE designa um Chefe do Registo para estes registos.

21. Para efeitos da presente decisão, entende-se por «registo para efeitos de segurança» (a seguir designado por «registo») a aplicação de procedimentos que registem o ciclo de vida das informações, incluindo a sua divulgação e destruição. Os SCI podem executar os procedimentos de registo recorrendo aos seus próprios processos.

22. Todo o material com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e superior será registado à entrada e à saída de uma entidade orgânica incluindo as delegações da União. As informações com classificação TRÈS SECRET UE/EU TOP SECRET são inscritas em registos próprios.
23. O Registo Central é, na Sede do SEAE, o principal ponto de entrada e saída das informações classificadas que forem trocadas com Estados terceiros e organizações internacionais. Este manterá um registo de todos os intercâmbios.
24. A AR aprovará uma política de segurança aplicável ao registo de ICUE para efeitos de segurança, em conformidade com o artigo 14.º da presente decisão.

Registos de informações com classificação très secret UE/EU top secret

25. Será designado na Sede do SEAE o Registo Central que atuará como autoridade central de receção e envio de informações com classificação TRÈS SECRET UE/EU TOP SECRET. Se necessário, poderão ser designados registos dependentes do registo central, a fim de manusear essas informações para efeitos de registo.
26. Os registos dependentes não poderão enviar documentos com classificação TRÈS SECRET UE/EU TOP SECRET diretamente a outros registos dependentes adstritos ao mesmo registo central TRÈS SECRET/EU TOP SECRET nem ao exterior sem a aprovação expressa deste último, concedida por escrito.

IV. CÓPIA E TRADUÇÃO DE DOCUMENTOS CLASSIFICADOS DA UE

27. Os documentos com classificação TRÈS SECRET UE/EU TOP SECRET não serão copiados nem traduzidos sem o consentimento prévio da entidade de origem, dado por escrito.
28. Os documentos com classificação SECRET UE/EU SECRET ou inferior poderão ser copiados ou traduzidos por ordem do detentor se a respetiva entidade de origem não tiver imposto restrições à sua cópia ou tradução.
29. As medidas de segurança aplicáveis ao documento original serão igualmente aplicáveis às respetivas cópias e traduções. As cópias de informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior são produzidas apenas por um (sub)registo competente com uma fotocopiadora de segurança. As cópias são registadas.

V. TRANSPORTE DE ICUE

30. O transporte de ICUE fica sujeito às medidas de proteção estabelecidas nos pontos 31 a 41. Quando as ICUE forem transportadas por meios eletrónicos, e não obstante o artigo 7.º, n.º 4 do Anexo A, as medidas de proteção a seguir estabelecidas poderão ser complementadas pelas contramedidas técnicas adequadas que a autoridade de segurança do SEAE determinar, a fim de minimizar o risco de perda ou comprometimento.
31. A autoridade de segurança do SEAE emitirá instruções para o transporte de ICUE, nos termos da presente decisão.

No interior de um edifício ou bloco de edifícios

32. As ICUE transportadas dentro de um edifício ou bloco de edifícios deverão ser cobertas para evitar que o seu conteúdo possa ser visto.
33. No interior de um edifício ou bloco de edifícios, as informações com classificação TRÈS SECRET UE/EU TOP SECRET deverão ser transportadas, por pessoal com credenciação de segurança adequada, num envelope de segurança que ostente apenas o nome do destinatário.

Dentro do território da União Europeia

34. As ICUE transportadas entre edifícios ou instalações dentro do território da União Europeia devem ser acondicionadas de forma que as proteja da divulgação não autorizada.
35. O transporte de informações com classificação até SECRET UE/EU SECRET dentro do território da União Europeia será efetuado por um dos seguintes meios:
 - a) Estafeta militar, correio oficial ou mala diplomática, consoante o caso;
 - b) Transporte por mão própria, desde que:
 - i) as ICUE não saiam das mãos do portador, a menos que se encontrem armazenadas nos termos dos requisitos estabelecidos no Anexo A II,
 - ii) as ICUE não sejam abertas pelo caminho nem lidas em locais públicos,

- iii) as pessoas possuam a devida credenciação de segurança para o nível em questão e estejam informadas das suas responsabilidades em matéria de segurança,
 - iv) as pessoas em causa recebam, se necessário, um certificado de estafeta;
- c) Serviços postais ou serviços comerciais de estafeta, desde que:
- i) sejam aprovados pela ANS competente, nos termos das disposições legislativas e regulamentares nacionais,
 - ii) apliquem medidas de proteção adequadas nos termos dos requisitos mínimos a estabelecer nas diretrizes de segurança ao abrigo do artigo 20.º, n.º 1 da presente decisão.

Em caso de transporte de um Estado-Membro para outro, o disposto na alínea c) fica limitado a informações com classificação até CONFIDENTIEL UE/EU CONFIDENTIAL.

36. O material classificado CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET (por exemplo, equipamento ou maquinaria) que não possa ser transportado pelos meios a que se refere o ponto 34 será transportado como mercadoria por transportadoras comerciais nos termos do Anexo A V.
37. O transporte de informações com classificação TRÈS SECRET UE/EU TOP SECRET entre edifícios ou instalações dentro do território da União Europeia será efetuado por estafeta militar, correio oficial ou mala diplomática, consoante o caso.

Do território da UE para o território de um Estado terceiro, ou entre entidades da UE em Estados Terceiros

38. As ICUE transportadas do território da União Europeia para o território de um Estado terceiro, ou entre entidades da UE em Estados terceiros, deverão ser acondicionadas de forma que as proteja da divulgação não autorizada.
39. O transporte de informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET do território da UE para o território de um Estado terceiro, e o transporte de quaisquer informações com classificação até SECRET UE/EU SECRET entre entidades da UE em Estados terceiros será efetuado por um dos seguintes meios:
- a) Estafeta militar ou mala diplomática;
 - b) Transporte por mão própria, desde que:
 - i) O volume ostente um selo oficial ou esteja acondicionado de modo a indicar que se trata de remessa oficial que não deverá ser sujeita a inspeção aduaneira ou de segurança;
 - ii) As pessoas em causa possuam um certificado de estafeta que identifique o volume e as autorize a transportá-lo;
 - iii) as ICUE não saiam das mãos do portador, a menos que se encontrem armazenadas nos termos dos requisitos estabelecidos no Anexo A II;
 - iv) as ICUE não sejam abertas pelo caminho nem lidas em locais públicos; e
 - v) As pessoas possuam a devida credenciação de segurança para o nível em questão e estejam informadas das suas responsabilidades em matéria de segurança.
40. O transporte de informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET comunicadas pela UE a um Estado terceiro ou organização internacional deverá cumprir as disposições relevantes ao abrigo de um acordo de segurança das informações ou de um convénio administrativo nos termos do artigo 10.º, n.º 2 do Anexo A.

41. As informações com classificação RESTREINT UE/EU RESTRICTED podem também ser transportadas do território da União Europeia para o território de um Estado terceiro por serviços postais ou serviços comerciais de estafeta.
42. O transporte de informações com classificação TRÈS SECRET UE/EU TOP SECRET do território da União Europeia para o território de um Estado terceiro, ou entre entidades da UE em Estados terceiros, será efetuado por estafeta militar ou mala diplomática.

VI. DESTRUIÇÃO DE ICUE

43. Os documentos classificados da UE que deixem de ser necessários podem ser destruídos, sem prejuízo das regras e regulamentações pertinentes em matéria de arquivo.

44. Os documentos que devam ser registados nos termos do artigo 7.º, n.º 2 do Anexo A serão destruídos pelo registo responsável por ordem do detentor ou de uma autoridade competente. Os livros de registos e outras informações a registar serão atualizados em conformidade.
45. A destruição dos documentos com classificação SECRET UE/EU SECRET ou TRÈS SECRET UE/EU TOP SECRET será efetuada na presença de uma testemunha, que possuirá uma credenciação equivalente, pelo menos, ao nível de classificação dos documentos a destruir.
46. O funcionário do registo e a testemunha, sempre que a presença desta última seja exigida, assinarão um certificado de destruição, que será arquivado no registo. O registo conservará os certificados de destruição dos documentos TRÈS SECRET UE/EU TOP SECRET durante um período mínimo de dez anos e os dos documentos com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET durante um período mínimo de cinco anos.
47. Os documentos classificados, incluindo os documentos com classificação RESTREINT UE/EU RESTRICTED, serão destruídos por métodos que respeitem as normas UE relevantes ou normas equivalentes ou que tenham sido aprovados pelos Estados-Membros nos termos das normas técnicas nacionais, de modo a impedir a sua reconstituição total ou parcial.
48. A destruição dos suportes informáticos de ICUE será efetuada nos termos do ponto 36 do Anexo A IV.

VII. INSPEÇÕES DE SEGURANÇA

Inspeções de Segurança do SEAE

49. De acordo com o artigo 15.º da presente decisão, as inspeções de segurança do SEAE englobam:
 - a) Inspeções gerais de segurança, com o objetivo de avaliar o nível geral de segurança da Sede do SEAE, das delegações da União e de todas as instalações dependentes ou associadas, nomeadamente a fim de avaliar a eficácia das medidas de segurança implementadas para proteção dos interesses de segurança do SEAE;
 - b) Inspeções de segurança às ICUE, com o objetivo de avaliar, em geral com uma acreditação em vista, a eficácia das medidas implementadas para proteção das ICUE na Sede do SEAE e nas delegações da União.

Em particular, serão efetuadas inspeções para, nomeadamente:

- i) Garantir o respeito das normas mínimas aplicáveis à proteção de ICUE estabelecidas na presente decisão;
- ii) Realçar a importância da segurança e de uma gestão de risco eficaz nas entidades inspecionadas;
- iii) Recomendar contramedidas destinadas a atenuar as consequências específicas da perda de confidencialidade, integridade ou disponibilidade de informações classificadas; e
- iv) Reforçar os programas que as autoridades de segurança tenham em curso em matéria de educação e sensibilização para a segurança.

Realização de inspeções de segurança do SEAE e respetivos relatórios

50. As inspeções de segurança do SEAE são realizadas por uma equipa de inspeção da Direção da Segurança do SEAE e, se necessário, com o apoio de peritos em segurança de outras Instituições de UE ou Estados-Membros.

A equipa de inspeção terá acesso a todos os locais em que sejam manuseadas ICUE, designadamente registos e pontos de presença de SCI.
51. As inspeções de segurança do SEAE em delegações da União podem ser realizadas, sempre que necessário, com o apoio dos Oficiais de Segurança das embaixadas dos Estados-Membros localizadas nos países terceiros.
52. Antes do final de cada ano civil, a autoridade de segurança do SEAE aprova um programa de inspeção de segurança para o SEAE no ano seguinte.
53. Sempre que necessário, a Autoridade de Segurança do SEAE pode organizar inspeções de segurança não previstas no programa supramencionado.

54. No final da inspeção de segurança, serão apresentadas à entidade inspecionada as principais conclusões e recomendações. Em seguida, será elaborado um relatório de inspeção pela equipa de inspeção. Caso tenham sido propostas medidas corretivas e formuladas recomendações, devem constar do relatório os elementos necessários para corroborar as conclusões tiradas. O relatório será enviado à autoridade de segurança do SEAE e ao chefe da entidade inspecionada.

Será elaborado, sob a responsabilidade da Autoridade de Segurança do SEAE, um relatório periódico destacando os ensinamentos recolhidos das inspeções efetuadas durante um período determinado, relatório esse que será analisado pelo Comité de Segurança do SEAE.

Realização de inspeções de segurança em agências e órgãos da EU e respetivos relatórios ao abrigo do Capítulo 2 do Título 5 do TUE

55. A Direção da Segurança do SEAE pode, se adequado, destacar peritos contribuintes para participar em equipas conjuntas de inspeção da UE que realizem inspeções às agências e aos órgãos da UE ao abrigo do Capítulo 2 do Título V do TUE.

Lista de controlo para inspeções de segurança do SEAE

56. A Direção da Segurança do SEAE elaborará e atualizará uma lista de controlo dos pontos a verificar durante as inspeções de segurança do SEAE. A referida lista de controlo será remetida ao Comité de Segurança do SEAE.
57. As informações necessárias para completar a lista de controlo serão obtidas, nomeadamente durante a inspeção, junto dos serviços de gestão da segurança da entidade inspecionada. Uma vez completada com as respostas pormenorizadas, a lista de controlo será classificada por comum acordo com a entidade inspecionada. Esta lista não fará parte do relatório de inspeção.
-

ANEXO A IV

PROTEÇÃO DAS ICUE MANUSEADAS EM SCI**I. INTRODUÇÃO**

1. O presente anexo estabelece as regras de execução do artigo 8.º do Anexo A.
2. Para a segurança e o correto funcionamento das operações em Sistemas de Comunicação e Informação (SCI), são essenciais as seguintes propriedades e conceitos de Garantia da Informação (GI):

Autenticidade:	a garantia de que a informação é genuína e provém de fonte fidedigna;
Disponibilidade:	a propriedade de estar acessível e de poder ser utilizada a pedido de uma entidade autorizada;
Confidencialidade:	a propriedade de a informação não ser divulgada a pessoas ou entidades não autorizadas ou segundo processos não autorizados;
Integridade:	a propriedade de salvaguardar o carácter exato e completo da informação e dos ativos;
Não rejeição:	a capacidade de provar que um ato ou acontecimento teve lugar, de modo a que esse acontecimento ou ato não possa ser subsequentemente negado.

II. PRINCÍPIOS DA GARANTIA DA INFORMAÇÃO

3. As disposições adiante estabelecidas constituirão a base da segurança dos SCI em que sejam manuseadas ICUE. Serão definidos nas políticas e diretrizes de segurança em matéria de GI requisitos de pormenor para a execução das presentes disposições.

Gestão dos riscos de segurança

4. A gestão dos riscos de segurança constituirá parte integrante da definição, desenvolvimento, exploração e manutenção do SCI. A gestão de risco (avaliação, tratamento, aceitação e comunicação) será conduzida como um processo iterativo em que participem conjuntamente os representantes dos proprietários do sistema, as autoridades de projeto, as autoridades operacionais e as autoridades de aprovação de segurança, seguindo um processo de avaliação dos riscos comprovado, transparente e plenamente compreensível para todos. O alcance do SCI e os seus ativos serão claramente definidos logo no início do processo de gestão de risco.
5. As autoridades competentes do SEAE analisarão as potenciais ameaças ao SCI e farão avaliações rigorosas e atualizadas da ameaça que reflitam o ambiente operacional vigente. Atualizarão constantemente o seu conhecimento das questões relacionadas com as vulnerabilidades e procederão periodicamente à reanálise da avaliação das vulnerabilidades por forma a acompanhar a evolução do ambiente das tecnologias da informação (TI).
6. O objetivo da gestão dos riscos de segurança consistirá em aplicar um conjunto de medidas de segurança que resulte num compromisso satisfatório entre os requisitos do utilizador e o risco de segurança residual.
7. Os requisitos, a escala e o grau de pormenor específicos determinados pela Autoridade de Acreditação de Segurança (AAS) competente para proceder à acreditação de um SCI serão proporcionais ao risco avaliado, tendo em conta todos os fatores pertinentes, nomeadamente o nível de classificação das ICUE manuseadas no SCI. A acreditação incluirá uma declaração formal de risco residual e a aceitação do risco residual por uma autoridade responsável.

Segurança ao longo do ciclo de vida do SCI

8. Haverá que garantir a segurança ao longo de todo o ciclo de vida do SCI, desde o início até à retirada de serviço.
9. Para cada fase do ciclo de vida, será identificado o papel de cada um dos intervenientes no SCI e a interação entre eles em termos de segurança do sistema.
10. Os SCI, incluindo as medidas de segurança, de carácter técnico e outras, serão sujeitos a ensaios de segurança durante o processo de acreditação, a fim de assegurar o nível de garantia adequado das medidas de segurança implementadas e de verificar se os sistemas estão corretamente implementados, integrados e configurados.
11. Serão periodicamente efetuadas avaliações, inspeções e análises de segurança durante o funcionamento e a manutenção dos SCI, e quando ocorrerem circunstâncias excecionais.

12. A documentação de segurança do SCI evoluirá ao longo do seu ciclo de vida enquanto parte integrante do processo de gestão da mudança e da configuração.

Melhores práticas

13. O SEAE colabora com o SGC, a Comissão e os Estados-Membros no desenvolvimento das melhores práticas de proteção das ICUE manuseadas nos SCI. As orientações de melhores práticas apresentarão medidas de segurança de natureza técnica, material, organizativa e processual para os SCI, de comprovada eficácia na luta contra determinadas ameaças e vulnerabilidades.
14. A proteção das ICUE manuseadas nos SCI basear-se-á na experiência adquirida pelas entidades envolvidas na GI, tanto dentro como fora da UE.
15. A divulgação e a subsequente aplicação das melhores práticas ajudarão a atingir um nível de garantia equivalente nos vários SCI que são explorados pelo SEAE e em que são manuseadas ICUE.

Defesa em profundidade

16. Para atenuar os riscos que pesam sobre os SCI, será posta em prática uma série de medidas de segurança, de natureza técnica e não técnica, organizadas em múltiplos estratos de defesa. Estas incluirão:
- a) *Dissuasão*: medidas de segurança dissuasivas da concretização de planos hostis de ataque ao SCI;
 - b) *Prevenção*: medidas de segurança destinadas a impedir ou bloquear um ataque ao SCI;
 - c) *Deteção*: medidas de segurança destinadas a descobrir a ocorrência de um ataque ao SCI;
 - d) *Resistência*: medidas de segurança destinadas a limitar o impacto do ataque a um conjunto mínimo de informações ou ativos do SCI e a prevenir mais danos; e
 - e) *Recuperação*: medidas de segurança destinadas a restabelecer uma situação segura para o SCI.

O grau de rigor e de aplicação destas medidas de segurança será determinado após uma avaliação dos riscos.

17. As autoridades competentes do SEAE deverão ter capacidade de resposta a incidentes suscetíveis de ultrapassar as fronteiras de uma organização ou de um país, a fim de coordenar as respostas e de partilhar informações sobre esses incidentes e os riscos deles resultantes (capacidades de resposta a emergências informáticas).

Princípio da minimalidade e do menor privilégio

18. A fim de evitar riscos desnecessários, só serão ativadas as funcionalidades, os dispositivos e os serviços essenciais para satisfazer os requisitos operacionais.
19. Para limitar os danos que possam resultar de acidentes, de erros ou da utilização não autorizada dos recursos do SCI, os seus utilizadores e processos automatizados beneficiarão unicamente de acesso, privilégios ou autorizações que forem indispensáveis ao desempenho das suas funções.
20. Os procedimentos de registo cumpridos pelo SCI serão, sempre que necessário, verificados no âmbito do processo de acreditação.

Sensibilização para a Garantia da Informação

21. A sensibilização para os riscos e para as medidas de segurança disponíveis constitui a primeira linha de defesa da segurança dos sistemas de comunicação e informação. Mais concretamente, todos os elementos do pessoal envolvido no ciclo de vida dos SCI, incluindo os utilizadores, deverão compreender que:
- a) As falhas de segurança podem prejudicar significativamente os SCI e toda a organização;
 - b) A interconexão e a interdependência podem causar prejuízos a terceiros; e
 - c) Cada um tem a sua parte de responsabilidade e deverá prestar contas pela segurança do SCI, em função do papel que desempenha nos sistemas e processos.
22. A fim de assegurar uma boa perceção das responsabilidades em matéria de segurança, os cursos de formação e sensibilização para a GI serão obrigatórios para todo o pessoal envolvido, incluindo os funcionários que ocupem lugares de direção e os utilizadores dos SCI.

Avaliação e aprovação de produtos de segurança informática

23. O necessário grau de confiança nas medidas de segurança, definido como um nível de garantia, será determinado à luz dos resultados do processo de gestão de risco e de acordo com as políticas e diretrizes de segurança relevantes.
24. O nível de garantia será verificado mediante a utilização de metodologias e processos reconhecidos internacionalmente ou aprovados a nível nacional, entre os quais se destacam a avaliação, os controlos e as auditorias.
25. Os produtos criptográficos de proteção de ICUE serão avaliados e aprovados por uma Autoridade nacional de Aprovação Criptográfica (AAC) de um Estado-Membro.
26. Antes de a sua aprovação ser recomendada à AAC do SEAE, nos termos do artigo 7.º, n.º 5, os produtos criptográficos deverão ter sido submetidos com êxito a uma segunda avaliação por uma Autoridade de Avaliação Habilitada (AQUA) de um Estado-Membro que não esteja envolvido na conceção nem no fabrico do equipamento. O grau de pormenor exigido na segunda avaliação dependerá do nível de classificação máximo previsto para as ICUE a proteger pelos referidos produtos.
27. Quando tal se justifique por razões operacionais específicas, a AAC do SEAE pode, por recomendação do Comité de Segurança, dispensar os requisitos previstos nos pontos 25 ou 26 e conceder uma aprovação provisória por um período específico, nos termos do artigo 7.º, n.º 5, da presente decisão.
28. A AQUA é uma AAC de um Estado-Membro que tenha sido acreditada com base em critérios definidos pelo Conselho para realizar a segunda avaliação dos produtos criptográficos destinados a proteger as ICUE.
29. A Alta Representante aprovará uma política de segurança aplicável às qualificações e à aprovação de produtos não criptográficos de segurança informática.

Transmissão dentro de Zonas de Segurança

30. Não obstante o disposto na presente decisão, quando a transmissão de ICUE se realizar dentro de Zonas de Segurança, poderá ser utilizada a distribuição não cifrada ou a cifragem a um nível inferior, com base nos resultados de um processo de gestão de risco e sob reserva de aprovação da AAS.

Interconexão segura dos SCI

31. Para efeitos da presente decisão, entende-se por «interconexão» a conexão direta, unidirecional ou bidirecional, de dois ou mais sistemas informáticos para efeitos de partilha de dados e de outros recursos de informação (por exemplo, comunicação).
32. O SCI tratará qualquer sistema informático com ele interconetado como não fiável e tomará medidas de proteção para controlar o intercâmbio de informações classificadas.
33. Todas as interconexões de SCI com outro sistema informático obedecerão aos seguintes requisitos básicos:
 - a) Os requisitos operacionais ou de atividade dessas interconexões serão determinados e aprovados pelas autoridades competentes;
 - b) A interconexão será submetida a um processo de gestão de risco e de acreditação e deverá ser aprovado pelas AAS competentes; e
 - c) Serão instalados serviços de proteção periférica (Boundary Protection Services – BPS) no perímetro de todos os SCI.
34. Não pode haver interconexão entre um SCI acreditado e uma rede desprotegida ou pública, a não ser que o SCI tenha aprovado um BPS instalado para esse efeito entre o SCI e a rede desprotegida ou pública. As medidas de segurança aplicáveis a estas interconexões serão avaliadas pela Autoridade de Garantia da Informação (AGI) competente e aprovadas pela AAS competente.

Quando a rede desprotegida ou pública for exclusivamente utilizada como transmissora e os dados forem cifrados por um produto criptográfico aprovado nos termos do artigo 7.º, n.º 5, da presente decisão, não se considerará essa conexão como uma interconexão.

35. É proibida a interconexão direta ou em cascata entre SCI acreditados para manusear informações com classificação TRÈS SECRET UE/EU TOP SECRET e redes desprotegidas ou públicas.

Suportes informáticos

36. Os suportes informáticos deverão ser destruídos segundo procedimentos aprovados pela autoridade de segurança do SEAE.
37. Os suportes informáticos deverão ser reutilizados, desgraduados ou desclassificados segundo uma política de segurança a estabelecer ao abrigo do artigo 7.º, n.º 2, da presente decisão.

Circunstâncias de emergência

38. Não obstante o disposto na presente decisão, os procedimentos específicos a seguir descritos podem ser aplicados, durante um período de tempo limitado, numa emergência, nomeadamente em situações de crise iminente ou real, de conflito ou de guerra, ou em circunstâncias operacionais excecionais.
39. As ICUE poderão ser transmitidas por meio de produtos criptográficos aprovados para um nível de classificação inferior, ou sem cifragem, mediante o consentimento da autoridade competente, se o prejuízo causado por um atraso for claramente mais grave do que o decorrente da eventual divulgação do material classificado, e se:
- a) O remetente e o destinatário não dispuserem do dispositivo de cifragem necessário ou não possuírem nenhum dispositivo de cifragem; e
 - b) O material classificado não puder ser enviado a tempo por outros meios.
40. As informações classificadas transmitidas nas circunstâncias referidas no ponto 39 não ostentarão marcas nem indicações que as distingam de informações não classificadas ou de informações que possam ser protegidas por produtos de cifragem disponíveis. Os destinatários serão imediatamente notificados, por outros meios, do nível de classificação das informações.
41. Em caso de recurso ao disposto no ponto 39, será subsequentemente apresentado um relatório nessa matéria à Direção da Segurança do SEAE e, por esta, ao Comité de Segurança do SEAE. Este relatório indicará, pelo menos, o remetente, o destinatário e a entidade de origem de cada ICUE.

III. FUNÇÕES E AUTORIDADES DE GARANTIA DA INFORMAÇÃO

42. Serão criadas no SEAE as funções GI a seguir enunciadas. As funções em causa não implicam a existência de entidades orgânicas únicas. Terão mandatos independentes. Contudo, aquelas funções, e as responsabilidades que lhes estão associadas, podem ser combinadas ou integradas na mesma entidade orgânica ou divididas em diferentes entidades orgânicas, desde que sejam evitados quaisquer conflitos internos de interesses ou funções.

Autoridade de Garantia da Informação (AGI)

43. Cabe à AGI:
- a) Definir políticas e diretrizes de segurança em matéria de GI e controlar a sua eficácia e relevância;
 - b) Salvaguardar e administrar as informações técnicas relativas aos produtos criptográficos;
 - c) Garantir que as medidas em matéria de GI selecionadas para proteção das ICUE estejam em consonância com as políticas que regem as suas elegibilidade e seleção;
 - d) Garantir que os produtos criptográficos sejam selecionados em conformidade com as políticas que regem as suas elegibilidade e seleção;
 - e) Coordenar a formação e a sensibilização em matéria de GI;
 - f) Consultar o fornecedor do sistema, os intervenientes e os representantes dos utilizadores no domínio da segurança, a respeito das políticas e diretrizes de segurança em matéria de GI; e
 - g) Garantir que a subformação do Comité de Segurança do SEAE especializada para as questões de GI disponha das competências técnicas adequadas.

Autoridade TEMPEST

44. A Autoridade TEMPEST (AT) será responsável pela garantia de conformidade dos SCI com as políticas e diretrizes TEMPEST. A AT procederá à aprovação de contramedidas TEMPEST aplicáveis a instalações e produtos destinados a proteger as ICUE, no seu ambiente operacional, até um determinado nível de classificação.

Autoridade de Aprovação Criptográfica (AAC)

45. É da responsabilidade da AAC garantir a conformidade dos produtos criptográficos com a respetiva política em matéria de cifragem. A AAC aprovará um produto criptográfico destinado a proteger as ICUE, no seu ambiente operacional, até um determinado nível de classificação.

Autoridade de Distribuição Criptográfica (ADC)

46. Cabe à ADC:
- a) Gerir e prestar contas pelo material criptográfico da UE;
 - b) Garantir a aplicação dos procedimentos e a criação dos canais adequados para prestar contas por todo o material criptográfico da UE e proceder ao seu manuseamento, armazenamento e distribuição em condições de segurança; e
 - c) Assegurar as transferências de material criptográfico da UE para as pessoas singulares ou os serviços que o utilizem e as transferências deles provenientes.

Autoridade de Acreditação de Segurança (AAS)

47. Cabe à Autoridade de Acreditação de Segurança (AAS), relativamente a cada sistema:
- a) Garantir a conformidade dos SCI com as políticas e diretrizes de segurança pertinentes, emitir uma declaração de aprovação dos SCI para o manuseamento de ICUE até um determinado nível de classificação, no seu ambiente operacional, enunciando os termos e condições da acreditação e os critérios segundo os quais é exigida nova aprovação;
 - b) Definir um processo de acreditação de segurança, nos termos das políticas pertinentes, em que sejam claramente estabelecidas as condições de aprovação dos SCI sob a sua autoridade;
 - c) Definir uma estratégia de acreditação de segurança em que se estabeleça para o processo de acreditação um grau de pormenor proporcional ao nível de garantia exigido;
 - d) Analisar e aprovar documentação em matéria de segurança, nomeadamente as declarações de gestão de risco e de risco residual, os Requisitos de Segurança Específicos do Sistema (adiante designados por «RSES»), a documentação de verificação da implementação e os Procedimentos Operacionais de Segurança (adiante designados por «POS»), e garantir a conformidade desta documentação com as regras e políticas de segurança do SEAE;
 - e) Verificar a implementação das medidas de segurança relativamente aos SCI realizando ou promovendo avaliações, inspeções ou controlos de segurança;
 - f) Definir requisitos de segurança (por exemplo níveis de credenciação de segurança do pessoal) para cargos sensíveis relativamente aos SCI;
 - g) Subscrever a seleção dos produtos criptográficos e TEMPEST aprovados que são utilizados para conferir segurança aos SCI;
 - h) Aprovar a interconexão de um SCI com outro SCI, ou, se for caso disso, participar na aprovação conjunta dessa interconexão; e
 - i) Consultar o fornecedor do sistema, os intervenientes e os representantes dos utilizadores no domínio da segurança a respeito da gestão de risco, em especial do risco residual, e dos termos e condições da declaração de aprovação.
48. A AAS do SEAE será responsável pela acreditação de todos os SCI que operem no âmbito do mandato do SEAE.

Conselho de Acreditação de Segurança

49. Cabe a um Conselho Conjunto de Acreditação de Segurança proceder à acreditação dos SCI no âmbito dos mandatos respetivos da AAS do SEAE e das AAS dos Estados-Membros. O Conselho Conjunto será composto por um representante da AAS de cada Estado-Membro, nele participando um representante da AAS do SGC e da Comissão. Serão convidadas a participar nas reuniões outras entidades com nódulos num SCI quando for debatido o sistema em causa.

O Conselho de Acreditação de Segurança será presidido por um representante da AAS do SEAE. Deliberará por consenso dos representantes das AAS das instituições, dos Estados-Membros e de outras entidades com nódulos no SCI. Apresentará periodicamente um relatório de atividades ao Comité de Segurança do SEAE e notificará-lo-á de todas as declarações de acreditação.

Autoridade Operacional de Garantia da Informação

50. Cabe à Autoridade Operacional de GI, relativamente a cada sistema:

- a) Elaborar documentação em matéria de segurança de acordo com as políticas e diretrizes na matéria e em especial com os Requisitos de Segurança Específicos do Sistema (RSES), nomeadamente a declaração de risco residual, os Procedimentos Operacionais de Segurança (POS) e o plano criptográfico no processo de acreditação do SCI;
 - b) Tomar parte na seleção e no ensaio das medidas técnicas de segurança, dispositivos e programas informáticos específicos do sistema, a fim de supervisionar a sua implementação e garantir a segurança da sua instalação, configuração e manutenção, nos termos da documentação de segurança pertinente;
 - c) Participar na seleção de medidas e dispositivos de segurança TEMPEST se os RSES o exigirem e garantir a segurança da sua instalação e manutenção, em colaboração com a AT;
 - d) Acompanhar a implementação e aplicação dos POS e, se necessário, delegar no proprietário do sistema quaisquer responsabilidades em matéria de segurança operacional;
 - e) Gerir e manusear os produtos criptográficos, assegurar a guarda de elementos cifrados e controlados e, se necessário, assegurar a geração de variáveis criptográficas;
 - f) Proceder a revisões das análises de segurança e a ensaios, em especial para a elaboração dos relatórios de risco exigidos pela AAS;
 - g) Organizar ações de formação em matéria de GI específica do SCI;
 - h) Executar e pôr em prática medidas de segurança específicas do SCI.
-

ANEXO A V

SEGURANÇA INDUSTRIAL**I. INTRODUÇÃO**

1. O presente anexo estabelece as regras de execução do artigo 9.º do Anexo A. Estabelece as disposições gerais de segurança aplicáveis a entidades industriais ou outras no âmbito das negociações pré-contratuais e durante a vigência dos contratos classificados celebrados pelo SEAE.
2. A Alta Representante aprova uma política em matéria de segurança industrial que estabeleça, nomeadamente, os requisitos detalhados aplicáveis às Credenciações de Segurança de Empresa (CSE), às Cláusulas Adicionais de Segurança (CAS), às visitas, à transmissão e ao transporte de ICUE.

II. ELEMENTOS DE SEGURANÇA DOS CONTRATOS CLASSIFICADOS**Guia da Classificação de Segurança (GCS)**

3. Antes de abrir concursos públicos ou de celebrar contratos classificados, o SEAE determinará, enquanto entidade adjudicante, qual a classificação de segurança de todas as informações a fornecer aos proponentes e contratantes, bem como de todas as informações a produzir pelos contratantes. Para o efeito, o SEAE prepara um guia de classificação de segurança (GCS) para ser utilizado na execução do contrato.
4. Para determinar qual a classificação de segurança dos vários elementos de um contrato classificado, serão aplicáveis os seguintes princípios:
 - a) Na elaboração do GCS, o SEAE terá em consideração todos os aspetos de segurança relevantes, nomeadamente a classificação de segurança atribuída às informações fornecidas e aprovadas pela respetiva entidade de origem para utilização no âmbito do contrato;
 - b) O nível global de classificação do contrato não pode ser inferior à classificação mais elevada de qualquer das suas partes; e
 - c) Se necessário, o SEAE contacta as ANS/ASD ou quaisquer outras autoridades de segurança competentes dos Estados-Membros quando houver alguma alteração à classificação das informações produzidas pelos contratantes ou a estas fornecidas na execução de um contrato e quando pretender fazer alterações ao GCS.

Cláusula Adicional de Segurança (CAS)

5. Os requisitos de segurança específicos do contrato serão descritos numa CAS. Esta CAS compreenderá, sempre que necessário, o guia de classificação de segurança e fará parte integrante do contrato ou subcontrato.
6. A CAS exigirá que o contratante e/ou subcontratante cumpra as normas mínimas estabelecidas na presente decisão. O incumprimento dessas normas mínimas pode constituir motivo suficiente para a resolução do contrato.

Instruções de Segurança do Programa/Projeto (ISP)

7. Em função do âmbito dos programas ou projetos que impliquem acesso, manuseamento ou armazenamento de ICUE, a entidade adjudicante designada para efeitos da gestão do programa ou projeto pode elaborar Instruções específicas de Segurança do Programa/Projeto (ISP). As ISP deverão ser aprovadas pelas ANS/ASD ou por quaisquer outras autoridades de segurança competentes dos Estados-Membros que participem no programa/projeto e podem estabelecer requisitos de segurança adicionais.

III. CREDENCIAÇÃO DE SEGURANÇA DA EMPRESA (CSE)

8. A Direção da Segurança do SEAE solicitará a concessão de uma CSE à ANS ou ASD ou a qualquer outra autoridade de segurança competente de um Estado-Membro, a fim de atestar, nos termos das disposições legislativas e regulamentares nacionais, que determinada entidade industrial ou outra está em condições de proteger as ICUE ao nível de classificação adequado (CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET) dentro das respetivas instalações. O acesso de contratantes, subcontratantes, ou potenciais contratantes ou subcontratantes a ICUE só será concedido após confirmação da transmissão da CSE ao SEAE.
9. Se necessário, o SEAE, enquanto entidade adjudicante, informará a ANS/ASD competente, ou qualquer outra autoridade de segurança competente, de que é necessária uma CSE para a fase pré-contratual ou para a execução do contrato. Será exigida uma CSE ou uma CSP para a fase pré-contratual quando haja que fornecer ICUE com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET durante o processo de apresentação de propostas.

10. O SEAE, enquanto entidade adjudicante, não adjudicará nenhum contrato classificado ao proponente preferido antes de ter recebido, da ANS/ASD ou de qualquer outra autoridade de segurança competente do Estado-Membro em que o contratante ou subcontratante esteja registado, confirmação de que, sendo exigível, foi emitida a CSE adequada.
11. O SEAE, enquanto entidade adjudicante, solicitará à ANS ou ASD ou a qualquer outra autoridade de segurança competente emissora de uma CSE que o notifique de quaisquer informações adversas que afetem a CSE. No caso da subcontratação, será informada em conformidade a ANS/ASD ou qualquer outra autoridade de segurança competente.
12. A retirada da CSE por parte da ANS/ASD ou de qualquer outra autoridade de segurança competente constituirá motivo suficiente para que o SEAE, enquanto entidade adjudicante, ponha termo a um contrato classificado ou exclua um dos proponentes do concurso.

IV. CREDENCIAÇÃO DE SEGURANÇA DO PESSOAL (CSP) PARA FUNCIONÁRIOS DE CONTRATANTES

13. Os funcionários que trabalhem para contratantes que exijam acesso a ICUE com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior possuirão a devida credenciação de segurança e terão necessidade de tomar conhecimento das informações. Embora não seja necessária uma CSP para efeitos de acesso a ICUE ao nível da classificação RESTREINT UE/EU RESTRICTED, deverá existir necessidade de tomar conhecimento de tais informações.
14. As candidaturas para CSP para funcionários de contratantes devem ser submetidas à ANS/ASD responsável pela entidade.
15. O SEAE chamará a atenção dos contratantes que tencionem contratar cidadãos de um Estado terceiro para um cargo que exija o acesso a ICUE, para o facto de que cabe à ANS/ASD do Estado-Membro em que foi constituída e está sediada a entidade contratadora determinar se pode ser concedido acesso à pessoa em questão a tais informações, de acordo com a presente decisão e confirmar que houve consentimento por parte da entidade de origem antes de ser concedido o referido acesso.

V. CONTRATOS E SUBCONTRATOS CLASSIFICADOS

16. Quando forem fornecidas ICUE aos proponentes na fase pré-contratual, o aviso de concurso deverá compreender uma disposição que obrigue aqueles que não cheguem a apresentar proposta ou não sejam selecionados a devolver todos os documentos classificados num prazo determinado.
17. Uma vez adjudicado um contrato ou subcontrato classificado, o SEAE, enquanto entidade adjudicante, informará a ANS/ASD ou qualquer outra autoridade de segurança competente do contratante ou subcontratante acerca das disposições de segurança do contrato classificado.
18. Em caso de resolução ou do termo de contratos desta natureza, o SEAE, enquanto entidade adjudicante (e/ou a ANS/ASD ou qualquer outra autoridade de segurança competente, consoante o caso, quando se trate de um subcontrato), informará imediatamente desse facto a ANS/ASD ou qualquer outra autoridade de segurança competente do Estado-Membro em que o contratante ou subcontratante esteja registado.
19. No termo ou resolução do contrato classificado, o contratante ou subcontratante deverá, regra geral, restituir à entidade adjudicante quaisquer ICUE que se encontrem na sua posse.
20. Serão estabelecidas na CAS disposições específicas referentes à eliminação das ICUE durante a fase de execução ou após o termo ou resolução do contrato.
21. Quando o contratante ou subcontratante for autorizado a conservar ICUE após o termo ou resolução do contrato, as normas mínimas estabelecidas na presente decisão continuarão a ser cumpridas e a confidencialidade das ICUE protegida pelo contratante ou subcontratante.
22. As condições em que o contratante pode subcontratar serão definidas no concurso e no contrato.
23. Antes de procederem à subcontratação de quaisquer partes de contratos classificados, os contratantes deverão obter autorização do SEAE, enquanto entidade adjudicante. Nenhum subcontrato pode ser celebrado com entidades industriais ou outras registadas num Estado que não seja membro da União Europeia e com o qual a União não tenha celebrado nenhum acordo de segurança das informações.
24. É da responsabilidade do contratante garantir que todas as atividades de subcontratação respeitem as normas mínimas estabelecidas na presente decisão, não devendo fornecer ICUE a nenhum subcontratante sem o prévio consentimento escrito da entidade adjudicante.

25. Os direitos de entidade de origem das ICUE que o contratante ou subcontratante tenha produzido ou manuseado serão exercidos pela entidade adjudicante.

VI. VISITAS ASSOCIADAS A CONTRATOS CLASSIFICADOS

26. Quando o SEAE ou quaisquer contratantes ou subcontratantes precisem de aceder a informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET nas instalações uns dos outros para a execução de um contrato classificado, serão organizadas visitas através de ligação com as ANS/ASD ou quaisquer outras autoridades de segurança competentes a que o assunto diga respeito. Esta disposição aplica-se sem prejuízo da prerrogativa das ANS/ASD, no contexto de projetos específicos, para chegar a acordo sobre os procedimentos relativos à organização direta de tais visitas.
27. Para aceder às ICUE relacionadas com o contrato do SEAE, todos os visitantes devem possuir a devida CSP e ter «necessidade de tomar conhecimento» dessas informações.
28. Apenas será concedido aos visitantes acesso às ICUE relacionadas com a finalidade da visita.

VII. TRANSMISSÃO E TRANSPORTE DE ICUE

29. Para efeitos de transmissão de ICUE por meios eletrónicos são aplicáveis as disposições pertinentes do artigo 8.º do Anexo A e do Anexo A IV.
30. Para efeitos de transporte de ICUE, são aplicáveis as disposições pertinentes do Anexo A III, nos termos das disposições legislativas e regulamentares nacionais.
31. Para o transporte como mercadoria de material classificado, serão aplicados os seguintes princípios aquando da determinação dos mecanismos de segurança:
- a) É garantida a segurança em todas as fases do transporte desde o ponto de origem até ao destino final;
 - b) O grau de proteção atribuído a uma remessa é determinado pelo nível de classificação mais elevado do material nela contido;
 - c) É obtida uma CSE de nível adequado para as empresas que efetuam o transporte, se tal implicar que as informações classificadas sejam armazenadas nas instalações dos contratantes. Em todo o caso, o pessoal que manipula a remessa será sujeito a credenciação de segurança adequada, nos termos do Anexo A I;
 - d) Antes de qualquer transporte transfronteiras de material com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET, o expedidor elabora um plano de transporte, que é aprovado pela SEAE, sempre que adequado em ligação com as ANS/ASD em causa do expedidor e do destinatário ou por qualquer outra autoridade de segurança competente;
 - e) Na medida do possível, os transportes serão diretos, efetuando-se tão rapidamente quanto as circunstâncias o permitirem;
 - f) Sempre que possível, os itinerários apenas devem atravessar o território de Estados-Membros. Só deverão atravessar Estados que não sejam membros da União Europeia quando tal for autorizado pelo SEAE ou por quaisquer outras autoridades de segurança competentes dos Estados do expedidor e do destinatário.

VIII. TRANSFERÊNCIA DE ICUE PARA CONTRATANTES ESTABELECIDOS EM ESTADOS TERCEIROS

32. A transferência de ICUE para contratantes e subcontratantes estabelecidos em Estados terceiros que possuem um acordo de segurança válido com o SEAE far-se-á de acordo com as medidas de segurança acordadas entre o SEAE, enquanto entidade adjudicante, e a ANS/ASD do Estado terceiro em que o contratante se encontre registado.

IX. MANUSEAMENTO E ARMAZENAMENTO DE INFORMAÇÕES COM CLASSIFICAÇÃO RESTREINT UE/EU RESTRICTED

33. Enquanto entidade adjudicante e com base nas disposições contratuais, assiste ao SEAE, em ligação com a ANS/ASD do Estado-Membro, consoante o caso, o direito de efetuar visitas às instalações dos contratantes ou subcontratantes, para verificar se foram tomadas as medidas de segurança necessárias à proteção das ICUE de nível RESTREINT UE/EU RESTRICTED nos termos do contrato.

34. Na medida do necessário ao abrigo das disposições legislativas e regulamentares nacionais, as ANS/ASD ou quaisquer outras autoridades de segurança competentes serão informadas pelo SEAE, na qualidade de entidade adjudicante, dos contratos ou subcontratos que envolvam informações com classificação RESTREINT UE/EU RESTRICTED.
 35. Não será necessário que os contratantes ou subcontratantes e respetivo pessoal possuam CSE nem CSP para a execução de contratos celebrados pelo SEAE que envolvam informações com classificação RESTREINT UE/EU RESTRICTED.
 36. Não obstante as exigências de CSE ou CSP eventualmente previstas nas disposições legislativas e regulamentares nacionais, o SEAE, enquanto entidade adjudicante, analisará as candidaturas apresentadas em concursos para adjudicação de contratos que exijam acesso a informações com classificação RESTREINT UE/EU RESTRICTED.
 37. As condições em que o contratante pode recorrer à subcontratação deverão respeitar o disposto nos pontos 22 a 24.
 38. Quando um contrato implique o manuseamento de informações com classificação RESTREINT UE/EU RESTRICTED num SCI explorado por um contratante, o SEAE, enquanto entidade adjudicante, assegurará que o contrato ou eventual subcontrato especifique requisitos técnicos e administrativos necessários à acreditação do SCI que sejam proporcionais ao risco avaliado, tendo em conta todos os fatores pertinentes. O alcance da acreditação do SCI será acordado entre a entidade adjudicante e a ANS/ASD competente.
-

ANEXO A VI

INTERCÂMBIO DAS INFORMAÇÕES CLASSIFICADAS COM ESTADOS TERCEIROS E ORGANIZAÇÕES INTERNACIONAIS**I. INTRODUÇÃO**

1. O presente anexo estabelece as regras de execução do artigo 10.º do Anexo A.

II. QUADROS REGULAMENTARES PARA O INTERCÂMBIO DE INFORMAÇÕES CLASSIFICADAS

2. O SEAE pode trocar ICUE com Estado terceiros ou organizações internacionais de acordo com o artigo 10.º, n.º 1 do Anexo A.

A fim de apoiar a AR na execução das responsabilidades previstas no artigo 218.º do TFUE:

- a) O departamento geográfico ou temático competente do SEAE, em consulta com a Direção da Segurança do SEAE, identificará, sempre que adequado, a necessidade de um intercâmbio de ICUE a longo prazo com o Estado terceiro ou a organização internacional em questão;
 - b) a Direção da Segurança do SEAE, em consulta com o departamento geográfico competente do SEAE, apresentará à AR, se adequado, os projetos de texto a propor ao Conselho nos termos do artigo 218.º, n.º 3, n.º 5, e n.º 6 do TFUE;
 - c) a Direção da Segurança do SEAE apoiará a AR na condução de negociações, em coordenação com os serviços pertinentes da Comissão e do Secretariado-Geral do Conselho;
 - d) Relativamente a acordos ou convénios com Estados terceiros para a participação dos mesmos em operações PCSD de gestão de crises a que se refere o artigo 10.º, n.º 1, alínea c) do Anexo A, a Direção-Geral de Gestão de Crises e Planeamento, em consulta com os serviços competentes do SEAE, apresentará à AR, se adequado, os projetos de texto a propor ao Conselho nos termos do artigo 218.º, n.º 3, n.º 5 e n.º 6 do TFUE e apoiará a AR na condução de negociações em coordenação com os serviços pertinentes do SEAE e do Secretariado-Geral do Conselho;
3. Sempre que os acordos de segurança das informações prevejam modalidades técnicas de execução a acordar entre a Direção da Segurança do SEAE, em consulta com a Direção de Segurança da Direção-Geral dos Recursos Humanos e da Segurança da Comissão e o Gabinete de Segurança do Secretariado-Geral do Conselho e a autoridade de segurança competente do Estado terceiro ou organização internacional em questão, tais modalidades terão em conta o nível de proteção previsto nas regras, estruturas e procedimentos de segurança existentes no Estado terceiro ou organização internacional em causa.
 4. Quando o SEAE tenha, a longo prazo, necessidade de proceder ao intercâmbio de informações com uma classificação não superior a RESTREINT UE/EU RESTRICTED com um Estado terceiro ou organização internacional, e se tenha determinado que a outra parte interessada não dispõe de um sistema de segurança suficientemente desenvolvido para que seja possível celebrar um acordo de segurança das informações, a AR pode, após obtenção do parecer favorável por unanimidade do Comité de Segurança do SEAE de acordo com o artigo 14.º, n.º 5 da presente decisão, celebrar um convénio administrativo com as autoridades competentes do Estado terceiro ou organização internacional em questão.
 5. Não serão trocadas ICUE por meios eletrónicos com um Estado terceiro ou uma organização internacional, a não ser que tal se encontre expressamente previsto no acordo de segurança das informações ou no convénio administrativo.
 6. Ao abrigo de um convénio administrativo relativo ao intercâmbio de informações classificadas, o SEAE e o Estado terceiro ou a organização internacional designam um registo como principal ponto de entrada e saída das informações classificadas trocadas. Para o SEAE, este é o registo central do SEAE.
 7. Regra geral, os convénios administrativos assumirão a forma de troca de cartas.
- III VISITAS DE AVALIAÇÃO**
8. As visitas de avaliação a que se refere o artigo 16.º da presente decisão são realizadas por acordo mútuo com o Estado terceiro ou a organização internacional pertinente, e avaliam:
 - a) O quadro regulamentar aplicável à proteção das informações classificadas;

- b) Quaisquer características específicas dos regulamentos, procedimentos, leis ou políticas em matéria de segurança do Estado terceiro ou organização internacional que possam afetar o nível máximo de classificação das informações suscetíveis de intercâmbio;
 - c) Os procedimentos e as medidas de segurança em vigor à data para proteção das informações classificadas; e
 - d) Os procedimentos de credenciação de segurança para o nível de ICUE a comunicar.
9. Só haverá intercâmbio de ICUE após uma visita de avaliação e determinação do nível a que as informações classificadas deverão ser trocadas entre as partes, com base na equivalência do nível de proteção que lhes for atribuído.

Se, enquanto se aguarda uma visita de avaliação, a AR tomar conhecimento de razões excepcionais ou urgentes para o intercâmbio de informações classificadas, o SEAE deverá:

- a) Solicitar à entidade de origem que dê, por escrito, o consentimento prévio a fim de estabelecer que não existem objeções à comunicação das informações;
- b) Consultar a autoridade de segurança do SEAE, que pode decidir comunicar, desde que haja um parecer favorável por unanimidade dos Estados-Membros representados no Comité de Segurança do SEAE.

Se o SEAE não conseguir identificar a entidade de origem, a autoridade de segurança do SEAE assume esta responsabilidade em seu lugar, após obtenção do parecer favorável por unanimidade do Comité de Segurança do SEAE.

IV. AUTORIDADE PARA A COMUNICAÇÃO DE ICUE A ESTADOS TERCEIROS OU ORGANIZAÇÕES INTERNACIONAIS

10. Se existir um dos quadros referidos no artigo 10.º, n.º 1 do Anexo A para o intercâmbio de informações classificadas com um Estado terceiro ou uma organização internacional, a decisão de o SEAE comunicar ICUE a um Estado terceiro ou organização internacional será tomada pela autoridade de segurança do SEAE, que pode delegar esta autorização a altos funcionários do SEAE ou a outras pessoas sob a sua autoridade.
11. Se a entidade de origem das informações classificadas a comunicar, incluindo as entidades de origem do material de referência que possa conter, não for o SEAE, o SEAE solicitará à entidade de origem que dê, por escrito, o consentimento prévio a fim de estabelecer que não existem objeções à comunicação das informações. Se o SEAE não conseguir identificar a entidade de origem, a autoridade de segurança do SEAE assume esta responsabilidade em seu lugar, após obtenção do parecer favorável por unanimidade dos Estados-Membros representados no Comité de Segurança do SEAE.

V. COMUNICAÇÃO AD HOC DE ICUE A TÍTULO EXCEPCIONAL

12. Na ausência de um dos quadros a que se refere o artigo 10.º, n.º 1 do Anexo A, e sempre que os interesses da UE ou de um ou mais dos seus Estados-Membros exijam a comunicação de ICUE por razões políticas, operacionais ou urgentes, os ICUE podem ser excepcionalmente comunicados a um Estado terceiro ou a uma organização internacional após a aplicação das medidas seguintes.

Após assegurar que as condições referidas no n.º 11 são cumpridas, a Direção da Segurança do SEAE deverá:

- a) Na medida do possível, verificar junto das autoridades de segurança do Estado terceiro ou organização internacional em questão se as respetivas regras, estruturas e procedimentos de segurança são de molde a garantir que as ICUE que lhe sejam comunicadas serão protegidas segundo normas não menos rigorosas do que as estabelecidas na presente decisão;
 - b) Solicitar ao Comité de Segurança do SEAE que, com base nas informações disponíveis, formule uma recomendação sobre a confiança que pode ser depositada nas regras, estruturas e procedimentos de segurança do Estado terceiro ou organização internacional a que as ICUE deverão ser comunicadas;
 - c) Consultar a autoridade de segurança do SEAE, que pode decidir comunicar, desde que haja um parecer favorável por unanimidade dos Estados-Membros representados no Comité de Segurança do SEAE.
13. Na ausência de um dos quadros a que se refere o artigo 10.º, n.º 1 do Anexo A, a terceira parte em questão deverá assumir o compromisso, por escrito, de proteger devidamente as ICUE.

APÊNDICE A

DEFINIÇÕES

Para efeitos da presente decisão, entende-se por:

«Acreditação»: processo que conduz a uma declaração formal, emitida pela Autoridade de Acreditação de Segurança (AAS), segundo a qual um dado sistema está aprovado para funcionar com um determinado nível de classificação, num determinado modo de segurança no seu ambiente operacional e a um nível de risco aceitável, com base na premissa de que foi implementado um conjunto aprovado de medidas de segurança de carácter técnico, material, organizativo e processual;

«Ativo»: tudo o que é útil para uma organização, para as suas atividades e para a continuidade destas, nomeadamente os recursos de informação que a apoiam no desempenho das suas funções;

«Autorização para acesso a ICUE»: uma autorização da Autoridade de Segurança do SEAE emitida em conformidade com a presente decisão após emissão de uma CSP pelas autoridades competentes de um Estado-Membro e que atesta que uma pessoa pode, comprovada a sua necessidade de tomar conhecimento de tais informações, ser autorizada a aceder a ICUE até um determinado nível (CONFIDENTIEL UE/EU CONFIDENTIAL ou superior) até determinada data — ver artigo 2.º do Anexo A I;

«Quebra»: resulta de atos ou omissões de uma pessoa que são contrários às regras de segurança estabelecidas na presente decisão e/ou às políticas de segurança ou diretrizes que estabeleçam quaisquer medidas necessárias para a sua implementação;

«Ciclo de vida do SCI»: todo o período de existência do SCI, que compreende as fases da iniciativa, conceção, planeamento, análise dos requisitos, projeto, desenvolvimento, ensaio, implementação, exploração, manutenção e desativação;

«Contrato classificado»: contrato celebrado pelo SEAE com um contratante para o fornecimento de bens, a execução de obras ou a prestação de serviços cuja execução exija ou implique o acesso a ou a produção de ICUE;

«Subcontrato classificado»: contrato celebrado entre um contratante do SEAE e outro contratante (ou seja, o subcontratante) para o fornecimento de bens, a realização de obras ou a prestação de serviços cuja execução exija ou implique o acesso ou a produção de ICUE;

«Sistema de comunicação e informação» (SCI): um sistema que permita o manuseamento automatizado de informações. Um sistema de comunicação e informação compreende todos os ativos necessários ao seu funcionamento, designadamente infraestrutura, organização, pessoal e recursos em matéria de informação; — ver artigo 8.º, n.º 2 do Anexo A;

«Comprometimento de ICUE»: divulgação total ou parcial de ICUE a pessoas ou identidades não autorizadas — ver artigo 8.º, n.º 2;

«Contratante»: pessoa singular ou coletiva com capacidade jurídica para celebrar contratos;

«Produtos criptográficos (produtos cripto)»: algoritmos criptográficos, módulos criptográficos de *hardware* e *software*, e produtos que incluam detalhes de implementação e documentação conexa e material de cifragem;

«Operação PCSD»: operação de gestão militar ou civil de crises conduzida ao abrigo do Capítulo 2 do Título V do TUE;

«Desclassificação»: eliminação de qualquer classificação de segurança;

«Defesa em profundidade»: aplicação de uma série de medidas de segurança organizadas em múltiplos estratos de defesa;

«Autoridade de Segurança Designada» (ASD): autoridade responsável perante a Autoridade Nacional de Segurança (ANS) de um Estado-Membro que está encarregada de comunicar às entidades industriais ou outras a política nacional em todas as matérias de segurança industrial e de facultar orientação e prestar assistência na sua implementação. As funções de ASD podem ser desempenhadas pela ANS ou por qualquer outra autoridade competente;

«Documento»: quaisquer informações registadas, independentemente da sua forma ou características materiais;

«Desgradação»: redução do nível de classificação de segurança;

«Informações classificadas da UE» (ICUE): quaisquer informações ou material designado por uma classificação de segurança da UE cuja divulgação não autorizada possa causar prejuízos de vária ordem aos interesses da União Europeia ou de um ou mais Estados-Membros — ver artigo 2.º, alínea f);

«Credenciação de Segurança da Empresa» (CSE): certificação administrativa, emitida por uma ANS ou ASD, de que, do ponto de vista da segurança, determinada empresa está apta a garantir um nível adequado de proteção das ICUE com determinado nível de classificação de segurança e de que o seu pessoal que precise de aceder a ICUE foi sujeito ao processo de credenciação de segurança correspondente e informado dos requisitos de segurança necessários para aceder às ICUE e garantir a sua proteção;

«Manuseamento» de ICUE: todas as atividades a que as ICUE possam eventualmente ser sujeitas ao longo do seu ciclo de vida. Compreende a sua produção, tratamento, transporte, desgradação, desclassificação e destruição. Relativamente ao SCI, compreende ainda a sua recolha, visualização, transmissão e armazenamento;

«Detentor»: pessoa devidamente autorizada com necessidade comprovada de tomar conhecimento, que está na posse de ICUE e é consequentemente responsável pela sua proteção;

«Entidade industrial ou outra»: entidade envolvida no fornecimento de bens, execução de obras ou prestação de serviços. Pode tratar-se de uma entidade industrial, comercial, de serviços, científica, educativa, de investigação ou desenvolvimento, bem como de trabalhador por conta própria;

«Segurança industrial»: aplicação de medidas destinadas a garantir a proteção das ICUE pelos contratantes ou subcontratantes no âmbito das negociações pré-contratuais e durante a vigência dos contratos classificados. — ver artigo 9.º, n.º 1 do Anexo A;

A «garantia da informação» no domínio dos sistemas de comunicação e informação consiste na confiança com que esses sistemas protegem as informações neles manuseadas e funcionam como for necessário, quando for necessário, sob o controlo de utilizadores legítimos. Uma GI eficaz deve assegurar níveis adequados de confidencialidade, integridade, disponibilidade, não rejeição e autenticidade. A GI baseia-se num processo de gestão de risco — ver artigo 8.º, n.º 1 do Anexo A;

«Interconexão»: significa, para efeitos da presente decisão, a conexão direta, unidirecional ou multidirecional, de dois ou mais sistemas informáticos para efeitos de partilha de dados e de outros recursos de informação — ver Anexo A IV, ponto 31;

«Gestão das informações classificadas»: aplicação de medidas administrativas de controlo das ICUE ao longo do seu ciclo de vida que visam complementar as medidas previstas nos artigos 5.º, 6.º e 8.º e contribuir, deste modo, para dissuadir e detetar a perda ou o comprometimento deliberados ou acidentais de informações e para recuperar essas informações em caso de perda ou comprometimento. Estas medidas dizem respeito, nomeadamente, à produção, registo, cópia, tradução, transporte, manuseamento, armazenamento e destruição de ICUE — ver artigo 7.º, n.º 1 do Anexo A;

«Material»: qualquer documento ou peça de maquinaria ou equipamento, já fabricado ou em fase de fabrico;

«Entidade de origem»: instituição, agência ou organismo da UE, Estado-Membro, Estado terceiro ou organização internacional sob cuja autoridade tenham sido produzidas e/ou introduzidas nas estruturas da UE informações classificadas;

«Segurança do pessoal» consiste na aplicação de medidas que se destinam a garantir que o acesso às ICUE só seja concedido a quem:

— tenha necessidade de tomar conhecimento das informações,

— para efeitos de acesso a informação com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior, possua a credenciação de segurança para o nível adequado ou outra autorização devidamente emitida, em virtude das funções que exercem, nos termos das disposições legislativas e regulamentares nacionais, e

— tenha sido informado das responsabilidades que lhe cabem —

ver artigo 5.º, n.º 1 do Anexo A;

«Certificação de Segurança do Pessoal» (CSP) para acesso a ICUE: declaração de uma autoridade competente de um Estado-Membro feita depois de concluída uma investigação de segurança conduzida pelas autoridades competentes de um Estado-Membro, e pela qual se atesta que uma dada pessoa pode aceder a ICUE até determinado nível (CONFIDENTIEL UE/EU CONFIDENTIAL ou superior), e até determinada data, desde que tenha sido comprovada a sua «necessidade de tomar conhecimento»; diz-se da pessoa nestas condições que «possui credenciação de segurança»;

«Certificado de Credenciação de Segurança do Pessoal» (CCSP): certificado, emitido por uma autoridade competente, pelo qual se atesta que uma dada pessoa possui credenciação de segurança e é detentora de uma CSP nacional, e se indica o nível de ICUE a que a pessoa pode aceder (CONFIDENTIEL UE/EU CONFIDENTIAL ou superior), a data de validade da CSP em causa e a data de caducidade do próprio certificado;

«Segurança física»: aplicação de medidas físicas e técnicas de proteção destinadas a dissuadir o acesso não autorizado a ICUE — ver artigo 6.º do Anexo A;

«Instruções de Segurança do Programa/Projeto» (ISP): lista de procedimentos de segurança que são aplicados a um programa ou projeto específico a fim de normalizar os procedimentos de segurança. As Instruções podem ser revistas em qualquer fase do programa ou projeto;

«Registo»: aplicação de procedimentos que registem o ciclo de vida das informações, incluindo a sua divulgação e destruição. ver Anexo A III, ponto 21;

«Risco residual»: risco que permanece após terem sido aplicadas medidas de segurança, dado que não é possível neutralizar todas as ameaças nem eliminar todas as vulnerabilidades;

«Risco»: possibilidade de uma ameaça específica explorar as vulnerabilidades internas e externas de uma organização ou de um dos sistemas por ela utilizados, causando assim danos à organização e respetivos ativos corpóreos ou incorpóreos. Mede-se pela combinação entre a probabilidade de as ameaças ocorrerem e o respetivo impacto;

«Aceitação do risco»: decisão de aceitar a persistência de um risco residual após o tratamento do risco;

«Avaliação do risco»: identificação das ameaças e vulnerabilidades e realização da análise de risco conexa, ou seja, a análise da probabilidade e do impacto;

«Comunicação do risco»: consciencializar os grupos de utilizadores de SCI para os riscos, informar as autoridades de aprovação desses riscos e reportá-los às autoridades operacionais;

«Processo de gestão do risco»: todo o processo de identificação, controlo e minimização de acontecimentos indeterminados que possam afetar a segurança de determinada organização ou qualquer dos sistemas por ela utilizados. Este processo abarca todas as atividades relacionadas com o risco, designadamente avaliação, tratamento, aceitação e comunicação;

«Tratamento do risco»: atenuação, eliminação, redução (mediante uma combinação adequada de medidas técnicas, materiais, organizativas e processuais), transferência ou monitorização do risco;

«Cláusula Adicional de Segurança» (CAS): condições contratuais especiais emitidas pela entidade adjudicante que fazem parte integrante de um contrato classificado que implica o acesso a ICUE ou a sua produção, e nas quais são identificados os requisitos de segurança ou as partes do contrato que exigem proteção de segurança — ver Anexo A V, Secção II;

«Guia da Classificação de Segurança» (GCS): documento que descreve as partes do programa ou contrato que são classificadas, com especificação dos níveis de classificação de segurança aplicáveis. O GCS pode ser alargado durante a vigência do programa ou contrato e as informações podem ser reclassificadas ou desgraduadas; existindo um GCS, este fará parte integrante da CAS — ver Anexo A V, Secção II;

«Investigação de Segurança»: procedimentos de investigação conduzidos pela autoridade competente de um Estado-Membro, nos termos das respetivas disposições legislativas e regulamentares nacionais, a fim de se certificar que não há conhecimento de circunstâncias desfavoráveis que impeçam uma dada pessoa de obter uma CSP nacional ou CSP UE para acesso a ICUE até determinado nível (CONFIDENTIEL UE/EU CONFIDENTIAL ou superior);

«Procedimentos Operacionais de Segurança» (POS): uma descrição da implementação da política de segurança a adotar, dos procedimentos operacionais a seguir e das responsabilidades do pessoal;

«Requisitos de Segurança Específicos do Sistema» (RSES): conjunto de princípios de segurança vinculativos a observar e de requisitos de segurança vinculativos detalhados a implementar, subjacentes ao processo de certificação e acreditação dos SCI;

«TEMPEST»: investigação, estudo e controlo das emanações eletromagnéticas comprometedoras e medidas destinadas à sua eliminação;

«Ameaça»: causa potencial de incidente indesejável que pode resultar em danos para uma organização ou qualquer dos sistemas por ela utilizados. Estas ameaças podem ser acidentais ou deliberadas (com dolo) e caracterizam-se por elementos ameaçadores, alvos potenciais e métodos de ataque;

«Vulnerabilidade»: insuficiência, seja de que natureza for, que possa ser explorada por uma ou mais ameaças. A vulnerabilidade pode consistir numa omissão ou estar relacionada com uma insuficiência dos controlos no que se refere ao rigor, coerência ou exaustividade destes últimos, podendo ser de natureza técnica, processual, material, organizativa ou operacional.

INFORMAÇÕES DOS ESTADOS-MEMBROS

Informações comunicadas pelos Estados-Membros relativas a auxílios estatais concedidos nos termos do Regulamento (CE) n.º 800/2008 da Comissão, que declara certas categorias de auxílios compatíveis com o mercado comum, em aplicação dos artigos 87.º e 88.º do Tratado (Regulamento geral de isenção por categoria)

(Texto relevante para efeitos do EEE)

(2013/C 190/02)

Número de referência do auxílio estatal	SA.30208 (X 17/10)	
Estado-Membro	Países Baixos	
Número de referência do Estado-Membro	Verlenging O&Oprogramma SKB	
Designação da região (NUTS)	Regiões não assistidas	
Entidade que concede o auxílio	Ministerie VROM/BJZ Internationaal Postbus 20951 IPC 880 2500 EZ Den Haag e-mail: djz.internationaal@minvrom.nl www.minvrom.nl	
Título da medida de auxílio	Subsidie onderzoeks- en ontwikkelingsprogramma Stichting Kennisontwikkeling en Kennisoverdracht Bodem 2010-2014	
Base jurídica nacional (referência à publicação oficial nacional relevante)	Individueel subsidiebesluit op grond van de Algemene wet bestuursrecht en het Besluit Milieusubsidies	
Tipo de medida	auxílio ad hoc	
Alteração de uma medida de auxílio existente	Prolongation N 230/1999	
Data da atribuição	a partir de 8.12.2009	
Setor(es) económico(s) abrangido(s)	Todos os sectores económicos elegíveis para beneficiar de auxílios	
Tipo de beneficiário	PME, grande empresa	
Montante global do auxílio ad hoc concedido à empresa	EUR 10,00 (em milhões)	
Para garantias	EUR 10,00 (em milhões)	
Instrumentos de auxílio (artigo 5.º)	Subvenção directa	
Referência à decisão da Comissão	—	
Se for co-financiado por fundos comunitários	—	
Objetivos	Intensidade máxima de auxílios em % ou montante máximo do auxílio em moeda nacional	Majorações PME em %
Desenvolvimento experimental [n.º 2, alínea c), do artigo 31.º]	25 %	20 %
Auxílios para estudos de viabilidade técnica (artigo 32.º)	75 %	—
Investigação fundamental [n.º 2, alínea a), do artigo 31.º]	100 %	—
Investigação industrial [n.º 2, alínea b), do artigo 31.º]	50 %	20 %

Ligação Web ao texto integral da medida de auxílio

<http://www.rijksoverheid.nl/documenten-en-publicaties/brieven/2009/12/08/subsidieaanvraag-stichting-kennisontwikkeling-en-kennisoverdracht-bodem-skb-programma-2010-2014.html>

<http://www.rijksoverheid.nl/documenten-en-publicaties/brieven/2010/01/26/aanvullende-voorwaarden-groepsvrijstellingsverordening-bij-subsidieaanvraag-stichting-kennisontwikkeling-en-kennisoverdracht-bodem-skb-programma-2010-2014.html>

Número de referência do auxílio estatal	SA.36154 (13/X)	
Estado-Membro	Países Baixos	
Número de referência do Estado-Membro	—	
Designação da região (NUTS)	NEDERLAND N.º 3, alínea c), do artigo 107.º, Regiões não assistidas	
Entidade que concede o auxílio	Ministerie van Financiën Korte Voorhout 7 2511 CW Den Haag www.overheid.nl	
Título da medida de auxílio	Teruggaafregeling energiebelasting op elektriciteit voor energie-intensieve bedrijven	
Base jurídica nacional (referência à publicação oficial nacional relevante)	Artikel VIIC Belastingplan 2013 (Stb 2012, 668) en inwerkingtreding bij Koninklijk Besluit (Stb 2012, 672)	
Tipo de medida	Regime de auxílios	
Alteração de uma medida de auxílio existente	—	
Duração	1.1.2013-31.12.2020	
Setor(es) económico(s) abrangido(s)	Todos os sectores económicos elegíveis para beneficiar de auxílios	
Tipo de beneficiário	grande empresa	
Montante global anual do orçamento previsto no âmbito do regime	EUR 6,50 (em milhões)	
Para garantias	EUR 6,50 (em milhões)	
Instrumentos de auxílio (artigo 5.º)	Outra forma de benefício fiscal	
Referência à decisão da Comissão	—	
Se for co-financiado por fundos comunitários	—	
Objetivos	Intensidade máxima de auxílios em % ou montante máximo do auxílio em moeda nacional	Majorações PME em %
Auxílios sob a forma de reduções dos impostos ambientais (artigo 25.º)	110 000 EUR	—

Ligação Web ao texto integral da medida de auxílio

<https://zoek.officielebekendmakingen.nl/stb-2012-668.html?zoekcriteria=%3fzkt%3dUitgebreid%26pst%3dStaatsblad%26dpr%3dAlle%26spd%3d20130128%26epd%3d20130128%26jgp%3d2012%26nrp%3d668%26sdt%3dDatumUitgifte%26planId%3d%26pnr%3d1%26rpp%3d10&resultIndex=0&sorttype=1&sortorder=4>

<http://www.overheid.nl> -> Staatsblad -> jaargang 2012 + nummer 668

<https://zoek.officielebekendmakingen.nl/stb-2012-672.html?zoekcriteria=%3fzkt%3dUitgebreid%26pst%3dStaatsblad%26dpr%3dAlle%26spd%3d20130128%26epd%3d20130128%26jgp%3d2012%26nrp%3d672%26sdt%3dDatumUitgifte%26planId%3d%26pnr%3d1%26rpp%3d10&resultIndex=0&sorttype=1&sortorder=4>

<http://www.overheid.nl> -> Staatsblad -> jaargang 2012 + nummer 672

Número de referência do auxílio estatal	SA.36370 (13/X)	
Estado-Membro	Polónia	
Número de referência do Estado-Membro	PL	
Designação da região (NUTS)	Jeleniogórsko-walbrzyski N.º 3, alínea a), do artigo 107.º	
Entidade que concede o auxílio	Minister Gospodarki PL. Trzech Krzyży 3/5 www.mg.gov.pl	
Título da medida de auxílio	Mando Corporation Poland Sp. z o.o.	
Base jurídica nacional (referência à publicação oficial nacional relevante)	„Program wspierania inwestycji o istotnym znaczeniu dla gospodarki polskiej na lata 2011-2020”, przyjęty przez Radę Ministrów w dniu 5 lipca 2011 (Uchwała Rady Ministrów Nr 122/2011) na podstawie art. 19 ust. 2 ustawy z dnia 6 grudnia 2006 r. o zasadach prowadzenia polityki rozwoju (Dz. U. z 2009 r. Nr 84, poz. 712 i Nr 157, poz. 1241) zmieniony uchwałą Rady Ministrów z dnia 20 marca 2012 r. (Nr 39/2012).	
Tipo de medida	auxílio ad hoc	
Alteração de uma medida de auxílio existente	—	
Data da atribuição	a partir de 28.11.2012	
Setor(es) económico(s) abrangido(s)	Fabricação de outros componentes e acessórios para veículos automóveis	
Tipo de beneficiário	grande empresa — Mando Corporation Poland Sp. z o.o.	
Montante global do auxílio ad hoc concedido à empresa	PLN 15,11 (em milhões)	
Para garantias	PLN 15,11 (em milhões)	
Instrumentos de auxílio (artigo 5.º)	Subvenção directa	
Referência à decisão da Comissão	—	
Se for co-financiado por fundos comunitários	—	
Objetivos	Intensidade máxima de auxílios em % ou montante máximo do auxílio em moeda nacional	Majorações PME em %
Auxílio ad-hoc (n.º 1 do artigo 13.º)	3,9 %	0 %

Ligação Web ao texto integral da medida de auxílio

<http://www.mg.gov.pl/Wspieranie+przedsiebiorczosci/Wsparcie+finansowe+inwestycje/Pomoc+na+inwestycje+o+istotnym+znaczeniu+dla+gospodarki>

Número de referência do auxílio estatal	SA.36382 (13/X)	
Estado-Membro	Áustria	
Número de referência do Estado-Membro	—	
Designação da região (NUTS)	WIEN Regiões não assistidas	

Entidade que concede o auxílio	MA 5 der Stadt Wien Ebendorferstraße 2, 1082 Wien www.wien.gv.at	
Título da medida de auxílio	WIEN WORK — Integrativer Betrieb, Förderung Ausbildungs- und Produktionsstätte für behinderte Personen, Förderung gem. Art 42 AGVO	
Base jurídica nacional (referência à publicação oficial nacional relevante)	Beschluss des Wiener Gemeinderates vom 1.3.2013, siehe beigefügte Anlagen	
Tipo de medida	auxílio ad hoc	
Alteração de uma medida de auxílio existente	—	
Data da atribuição	a partir de 1.3.2013	
Setor(es) económico(s) abrangido(s)	Todos os sectores económicos elegíveis para beneficiar de auxílios	
Tipo de beneficiário	grande empresa — Wien Work — Integrative Betriebe und AusbildungsGmbH, Gemeinnützige GmbH., Unternehmensegegenstand:	
Montante global do auxílio ad hoc concedido à empresa	EUR 5,00 (em milhões)	
Para garantias	EUR 5,00 (em milhões)	
Instrumentos de auxílio (artigo 5.º)	Subvenção directa	
Referência à decisão da Comissão	—	
Se for co-financiado por fundos comunitários	—	
Objetivos	Intensidade máxima de auxílios em % ou montante máximo do auxílio em moeda nacional	Majorações PME em %
Auxílios sob forma de compensação pelos custos adicionais decorrentes do recrutamento de trabalhadores com deficiência (artigo 42.º)	81 %	—

Ligação Web ao texto integral da medida de auxílio

<https://www.wien.gv.at/infodat/ergdt?detvid=103242>

Número de referência do auxílio estatal	SA.36383 (13/X)
Estado-Membro	Reino Unido
Número de referência do Estado-Membro	N/A
Designação da região (NUTS)	NORTHERN IRELAND N.º 3, alínea c), do artigo 107.º
Entidade que concede o auxílio	Department of Agriculture and Rural Development (Northern Ireland) DARD Science, Evidence and Innovation Policy Division Room 359 Dundonald House Belfast BT4 3SB http://www.dardni.gov.uk/
Título da medida de auxílio	Agricultural Research and Development Scheme (Northern Ireland) 2013 — 2020
Base jurídica nacional (referência à publicação oficial nacional relevante)	Agriculture Act (Northern Ireland) 1949 Agriculture (Northern Ireland) Order 2004

Tipo de medida	Regime de auxílios	
Alteração de uma medida de auxílio existente	—	
Duração	1.4.2013-31.3.2020	
Setor(es) económico(s) abrangido(s)	Produção vegetal e animal, caça e actividades dos serviços relacionados	
Tipo de beneficiário	PME, grande empresa	
Montante global anual do orçamento previsto no âmbito do regime	GBP 1,00 (em milhões)	
Para garantias	GBP 1,00 (em milhões)	
Instrumentos de auxílio (artigo 5.º)	Subvenção directa	
Referência à decisão da Comissão	—	
Se for co-financiado por fundos comunitários	—	
Objetivos	Intensidade máxima de auxílios em % ou montante máximo do auxílio em moeda nacional	Majorações PME em %
Auxílios à investigação e desenvolvimento no sector agrícola e das pescas (artigo 34.º)	100 %	—

Ligação Web ao texto integral da medida de auxílio

<http://www.dardni.gov.uk/index/strategies-reports-accounts/dard-research-section/agriculture-research-and-development-scheme.htm>

Número de referência do auxílio estatal	SA.36496 (13/X)
Estado-Membro	Áustria
Número de referência do Estado-Membro	—
Designação da região (NUTS)	NIEDEROESTERREICH Regiões mistas
Entidade que concede o auxílio	Amt der NÖ Landesregierung Landhausplatz 1, 3109 St. Pölten www.noel.gv.at bzw. www.nafes.at
Título da medida de auxílio	Neufassung der NAFES-Förderungsrichtlinien
Base jurídica nacional (referência à publicação oficial nacional relevante)	NAFES Förderrichtlinien (Kennzeichen: RU2-N-133/077-2012 — Beschluß der Landesregierung)
Tipo de medida	Regime de auxílios
Alteração de uma medida de auxílio existente	—
Duração	26.2.2013-31.12.2017
Setor(es) económico(s) abrangido(s)	Todos os sectores económicos elegíveis para beneficiar de auxílios
Tipo de beneficiário	PME
Montante global anual do orçamento previsto no âmbito do regime	EUR 1,20 (em milhões)
Para garantias	EUR 1,20 (em milhões)

Instrumentos de auxílio (artigo 5.º)	Subvenção directa	
Referência à decisão da Comissão	—	
Se for co-financiado por fundos comunitários	—	
Objetivos	Intensidade máxima de auxílios em % ou montante máximo do auxílio em moeda nacional	Majorações PME em %
Regime de auxílios	20 %	0 %
Auxílios ao investimento e ao emprego a favor das PME (artigo 15.º)	20 %	—

Ligação Web ao texto integral da medida de auxílio

<http://www.nafes.at>

http://www.nafes.at/foerderung/formulare_und_leitfaeden — siehe „Förderrichtlinie“

Número de referência do auxílio estatal	SA.36505 (13/X)
Estado-Membro	Grécia
Número de referência do Estado-Membro	GR
Designação da região (NUTS)	KENTRIKI MAKEDONIA, DYTIKI ELLADA, ATTIKI N.º 3, alínea a), do artigo 107.º
Entidade que concede o auxílio	GENERAL SECRETARIAT FOR RESEARCH AND TECHNOLOGY 14-18 MESOGEION AV 115 10 ATHENS GREECE http://www.gsrt.gr
Título da medida de auxílio	Funding of Research Proposals Positively Evaluated under the 5th Call of ERC Grant Schemes
Base jurídica nacional (referência à publicação oficial nacional relevante)	Law 1514/1985 and its amendment, Law 3614/07 and its amendments, Ministerial Decision 14053/EIS 1749/27.3.2008 (FEK — Official Journal of Greek Government — 540/B/27.3.2008) and its amendments (43804/EYTHY 2041/7.9.2009 — FEK 1957/B/9.9.2009), 28020/EYTHI 1212/30.6.2010 — FEK 1088/B/19.7.2010), 5058/EYTHI 138/5-2-13 (FEK 292/B/13.2.2013)
Tipo de medida	Regime de auxílios
Alteração de uma medida de auxílio existente	—
Duração	20.3.2013-31.12.2015
Setor(es) económico(s) abrangido(s)	Investigação científica e desenvolvimento
Tipo de beneficiário	grande empresa
Montante global anual do orçamento previsto no âmbito do regime	EUR 0,83 (em milhões)
Para garantias	EUR 0,83 (em milhões)
Instrumentos de auxílio (artigo 5.º)	Subvenção directa
Referência à decisão da Comissão	—
Se for co-financiado por fundos comunitários	ESF — EUR 2,07 (em milhões)

Objetivos	Intensidade máxima de auxílios em % ou montante máximo do auxílio em moeda nacional	Majorações PME em %
Desenvolvimento experimental [n.º 2, alínea c), do artigo 31.º]	40 %	0 %
Investigação fundamental [n.º 2, alínea a), do artigo 31.º]	100 %	—
Investigação industrial [n.º 2, alínea b), do artigo 31.º]	65 %	0 %

Ligação Web ao texto integral da medida de auxílio

http://www.gsrt.gr/central.aspx?sid=10813341110616461444510&olID=671&neID=673&neTa=1_300_1&nclD=0&neHC=0&tbid=0&lrID=2&oldUIID=a16711011081334111061012&actionID=load&JScrip=1

Δράσεις Ενίσχυσης Ε&Τ › Τρέχουσες Εθνικές Δράσεις › Ενεργές προκηρύξεις ΕΣΠΑ

Número de referência do auxílio estatal	SA.36530 (13/X)	
Estado-Membro	Países Baixos	
Número de referência do Estado-Membro	NLD	
Designação da região (NUTS)	OVERIJSEL Regiões não assistidas	
Entidade que concede o auxílio	Provincie Overijssel Postbus 10078 8000 GB Zwolle www.overijssel.nl	
Título da medida de auxílio	Rijden op groen gas en electriciteit (aanschaf vrachtwagens)	
Base jurídica nacional (referência à publicação oficial nacional relevante)	Subsidieregeling Rijden op groen gas en electriciteit, in werking treding op 4 april 2013. Publicatie Provinciaal blad nr. 2013/0115269	
Tipo de medida	Regime de auxílios	
Alteração de uma medida de auxílio existente	—	
Duração	4.4.2013-31.12.2013	
Sector(es) económico(s) abrangido(s)	Todos os sectores económicos elegíveis para beneficiar de auxílios	
Tipo de beneficiário	PME	
Montante global anual do orçamento previsto no âmbito do regime	EUR 0,55 (em milhões)	
Para garantias	EUR 0,55 (em milhões)	
Instrumentos de auxílio (artigo 5.º)	Subvenção directa	
Referência à decisão da Comissão	—	
Se for co-financiado por fundos comunitários	—	
Objetivos	Intensidade máxima de auxílios em % ou montante máximo do auxílio em moeda nacional	Majorações PME em %
Auxílios à aquisição de novos veículos de transporte que superem as normas comunitárias ou, na sua ausência, que melhorem o nível de protecção do ambiente (artigo 19.º)	3 %	0 %

Ligação Web ao texto integral da medida de auxílio

http://www.overijssel.nl/loket/provinciale/uitvoeringsbesluit_subsidies_overijssel_2011

www.overijssel.nl, loket, provinciale regelingen, uitvoeringsbesluit subsidies Overijssel 2011, Hoofdstuk 8, paragraaf 8.11

Número de referência do auxílio estatal	SA.36540 (13/X)	
Estado-Membro	Alemanha	
Número de referência do Estado-Membro	—	
Designação da região (NUTS)	MERZIG-WADERN Regiões não assistidas	
Entidade que concede o auxílio	EVTZ Interreg IV A Großregion Préfecture de la Région Lorraine SGAR — Direction des Affaires Européennes GECT — Autorité de gestion Programme Interreg IV A Grande Région 36 place Saint Thiébault BP 71014 F-57034 METZ Cedex 1 www.interreg-4agr.eu	
Título da medida de auxílio	Initiative Précise: Initiative zur Optimierung der präzisen elektrochemischen Prozesse für industrielle Serienfertigung in der Großregion	
Base jurídica nacional (referência à publicação oficial nacional relevante)	Gesetz Nr. 938 betreffend Haushaltsordnung des Saarlandes (LHO) Vom 3. November 1971 in der Fassung der Bekanntmachung vom 5. November 1999 (Amtsbl. des Saarlandes 2000 S. 194), zuletzt geändert durch Art. 5 des Gesetzes vom 1. Dezember 2011 (Amtsbl. des Saarlandes I S. 556)	
Tipo de medida	auxílio ad hoc	
Alteração de uma medida de auxílio existente	—	
Data da atribuição	a partir de 22.11.2012	
Setor(es) económico(s) abrangido(s)	Fabricação de outras torneiras e válvulas	
Tipo de beneficiário	PME — MHA Zentgraf GmbH & Co.KG	
Montante global do auxílio ad hoc concedido à empresa	EUR 0,20 (em milhões)	
Para garantias	EUR 0,20 (em milhões)	
Instrumentos de auxílio (artigo 5.º)	Subvenção directa	
Referência à decisão da Comissão	—	
Se for co-financiado por fundos comunitários	103 GR 1 1 223 — EUR 0,20 (em milhões)	
Objetivos	Intensidade máxima de auxílios em % ou montante máximo do auxílio em moeda nacional	Majorações PME em %
Investigação industrial [n.º 2, alínea b), do artigo 31.º]	50 %	0 %

Ligação Web ao texto integral da medida de auxílio

<http://www.interreg-4agr.eu/de/projet-liste.php#>

Número de referência do auxílio estatal	SA.36551 (13/X)	
Estado-Membro	Itália	
Número de referência do Estado-Membro	ITD5	
Designação da região (NUTS)	EMILIA-ROMAGNA Regiões mistas	
Entidade que concede o auxílio	Direzione Attività Produttive, Commercio e Turismo della Regione Emilia-Romagna/Direzione Generale A Direzione Attività Produttive: Viale Aldo Moro, 44 — 40127 Bologna Direzione Ambiente: Viale Aldo Moro n. 8 — 40127 Bologna http://fesr.regione.emilia-romagna.it/che-cose-il-por-fesr/assi-pagine/asse-3-qualificazione-energetico-ambientale-e-sviluppo-sostenibile www.ermesambiente.it	
Título da medida de auxílio	POR FESR 2007-2013 — Asse III, Attività III 1.2 e Piano di Azione ambientale per un futuro sostenibile 2008-2010: Modalità e criteri per la concessione di contributi finalizzati alla rimozione dell'amianto dagli edifici, la coibentazione degli edifici e l'installazione di pannelli solari fotovoltaici	
Base jurídica nacional (referência à publicação oficial nacional relevante)	Delibera della Giunta Regionale del 10 gennaio 2011 n. 15 pubblicata sul BURER n. 14 del 27 gennaio 2011 (parte seconda)	
Tipo de medida	Regime de auxílios	
Alteração de uma medida de auxílio existente	—	
Duração	15.11.2012-30.9.2013	
Setor(es) económico(s) abrangido(s)	Todos os sectores económicos elegíveis para beneficiar de auxílios	
Tipo de beneficiário	PME	
Montante global anual do orçamento previsto no âmbito do regime	EUR 1,02 (em milhões)	
Para garantias	EUR 1,02 (em milhões)	
Instrumentos de auxílio (artigo 5.º)	Subvenção directa	
Referência à decisão da Comissão	—	
Se for co-financiado por fundos comunitários	POR FESR «Competitività regionale e occupazione» 2007-2013 regione Emilia-Romagna Decisione C(2007) 3875 — 7.8.2007 Codice CCI n. 2007 IT 16 2 PO 002 — EUR 0,33 (em milhões)	
Objetivos	Intensidade máxima de auxílios em % ou montante máximo do auxílio em moeda nacional	Majorações PME em %
Auxílios ao investimento no domínio do ambiente a favor da promoção da energia produzida a partir de fontes renováveis (artigo 23.º)	45 %	0 %
Auxílios ao investimento que permitem às empresas superar as normas comunitárias em matéria de protecção do ambiente ou, na sua ausência, aumentar o nível de protecção do ambiente (artigo 18.o)	45 %	0 %
Auxílios ao investimento no domínio do ambiente a favor de medidas de poupança de energia (artigo 21.º)	45 %	0 %

Ligação Web ao texto integral da medida de auxílio:

<http://fesr.regione.emilia-romagna.it/finanziamenti/bandi/bando-fotovoltaico-amianto>

Número de referência do auxílio estatal	SA.36555 (13/X)	
Estado-Membro	Países Baixos	
Número de referência do Estado-Membro	Subsidie Energiesprong Flevogebouw	
Designação da região (NUTS)	OVERIJSEL Regiões não assistidas	
Entidade que concede o auxílio	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Directie CZW Postbus 20011 2500 EA Den Haag email: angelique.herwijnen@minbzk.nl www.rijksoverheid.nl/ministeries/bzk	
Título da medida de auxílio	Subsidie energiesprong Consortium Flevogebouw Zwolle	
Base jurídica nacional (referência à publicação oficial nacional relevante)	Subsidiebesluit experimenten en kennisoverdracht wonen Geldend op 18.4.2013 http://wetten.overheid.nl/BWBR0020333/geldigheidsdatum_18-04-2013 Regeling Subsidiebesluit experimenten en kennisoverdracht wonen Geldend op 18.4.2013 http://wetten.overheid.nl/BWBR0020311/geldigheidsdatum_18-04-2013	
Tipo de medida	auxílio ad hoc	
Alteração de uma medida de auxílio existente	—	
Data da atribuição	a partir de 21.2.2013	
Setor(es) económico(s) abrangido(s)	Instalação de canalizações e de climatização, Desenvolvimento de projectos de edifícios, Construção de edifícios residenciais e não residenciais	
Tipo de beneficiário	PME, grande empresa — Bemog Projectontwikkeling; Nikkels Bouwbedrijf; Seinen Energy solutions; Brenorm Installatiegroep	
Montante global do auxílio ad hoc concedido à empresa	EUR 0,18 (em milhões)	
Para garantias	EUR 0,18 (em milhões)	
Instrumentos de auxílio (artigo 5.º)	Subvenção directa	
Referência à decisão da Comissão	—	
Se for co-financiado por fundos comunitários	—	
Objetivos	Intensidade máxima de auxílios em % ou montante máximo do auxílio em moeda nacional	Majorações PME em %
Auxílios ao investimento no domínio do ambiente a favor de medidas de poupança de energia (artigo 21.º)	40 %	0 %

Ligação Web ao texto integral da medida de auxílio

<http://www.rijksoverheid.nl/documenten-en-publicaties/bsluiten/2013/03/14/beschikking-subsidie-energiesprong-flevogebouw.html>

Número de referência do auxílio estatal	SA.36572 (13/X)	
Estado-Membro	Espanha	
Número de referência do Estado-Membro	ES51	
Designação da região (NUTS)	CATALUNA Regiões mistas	

Entidade que concede o auxílio	Departamento de Empresa y Ocupación; Dirección general de Economía Social y Cooperativa i Trabajo Au Sepúlveda, 148-150 08011 Barcelona http://www.gencat.cat/temes/cat/treball.htm	
Título da medida de auxílio	Acciones relativas a las unidades de apoyo a la actividad profesional en el marco de servicios de ayuda personal y social a las personas con discapacidad en los centros especiales de empleo.	
Base jurídica nacional (referência à publicação oficial nacional relevante)	Orden EMO/66/2012, de 21 de marzo, por la que se aprueban las bases reguladoras para la concesión de subvenciones destinadas a la realización de acciones relativas a las unidades de apoyo a la actividad profesional en el marco de los servicios de ajuste personal y social de las personas con discapacidad en los centros especiales de empleo, y se abre la convocatoria para el año 2012. RESOLUCIÓN EMO/577/2013, de 19 de marzo, de convocatoria para el año 2013	
Tipo de medida	Regime de auxílios	
Alteração de uma medida de auxílio existente	—	
Duração	1.1.2012-31.12.2013	
Setor(es) económico(s) abrangido(s)	Todos os sectores económicos elegíveis para beneficiar de auxílios	
Tipo de beneficiário	PME, grande empresa	
Montante global anual do orçamento previsto no âmbito do regime	EUR 41,00 (em milhões)	
Para garantias	EUR 41,00 (em milhões)	
Instrumentos de auxílio (artigo 5.º)	Subvenção directa	
Referência à decisão da Comissão	—	
Se for co-financiado por fundos comunitários	—	
Objetivos	Intensidade máxima de auxílios em % ou montante máximo do auxílio em moeda nacional	Majorações PME em %
Auxílios sob forma de compensação pelos custos adicionais decorrentes do recrutamento de trabalhadores com deficiência (artigo 42.º)	70 %	—

Ligação Web ao texto integral da medida de auxílio

<http://portaldogc.gencat.cat/utillsEADOP/PDF/6095/1232356.pdf>

<http://portaldogc.gencat.cat/utillsEADOP/PDF/6341/1291415.pdf>

Número de referência do auxílio estatal	SA.36583 (13/X)
Estado-Membro	Hungria
Número de referência do Estado-Membro	—
Designação da região (NUTS)	Hungary N.º 3, alínea a), do artigo 107.º, N.º 3, alínea c), do artigo 107.º
Entidade que concede o auxílio	Garantiqa Hitelgarancia Zrt. 1082 Budapest, Kisfaludy u. 32. www.garantiqa.hu
Título da medida de auxílio	A Garantiqa Hitelgarancia Zrt által kezességvállalási díj csökkentése formájában nyújtott beruházási támogatás

Base jurídica nacional (referência à publicação oficial nacional relevante)	2008. évi CII. törvény a Magyar Köztársaság 2009. évi költségvetéséről, 2012. évi CCIV törvény a Magyar Köztársaság 2013. évi költségvetéséről, 48/2002. (XII.28) PM rendelet a költségvetési vizontgaranciaállalásának és érvényesítésének részletes szabályairól	
Tipo de medida	Regime de auxílios	
Alteração de uma medida de auxílio existente	—	
Duração	13.5.2009-31.12.2013	
Setor(es) económico(s) abrangido(s)	Todos os sectores económicos elegíveis para beneficiar de auxílios	
Tipo de beneficiário	PME	
Montante global anual do orçamento previsto no âmbito do regime	HUF 6 000,00 (em milhões)	
Para garantias	HUF 6 000,00 (em milhões)	
Instrumentos de auxílio (artigo 5.º)	Garantia	
Referência à decisão da Comissão	—	
Se for co-financiado por fundos comunitários	—	
Objetivos	Intensidade máxima de auxílios em % ou montante máximo do auxílio em moeda nacional	Majorações PME em %
Auxílios à aquisição de novos veículos de transporte que superem as normas comunitárias ou, na sua ausência, que melhorem o nível de protecção do ambiente (artigo 19.º)	35 %	20 %
Auxílios ao investimento no domínio do ambiente a favor de medidas de poupança de energia (artigo 21.º)	60 %	20 %
Auxílios ao investimento no domínio do ambiente a favor da promoção da energia produzida a partir de fontes renováveis (artigo 23.º)	45 %	20 %
Investigação fundamental [n.º 2, alínea a), do artigo 31.º]	100 %	—
Investigação industrial [n.º 2, alínea b), do artigo 31.º]	50 %	20 %
Desenvolvimento experimental [n.º 2, alínea c), do artigo 31.º]	25 %	20 %
Regime de auxílios	50 %	20 %
Auxílios ao investimento que permitem às empresas superar as normas comunitárias em matéria de protecção do ambiente ou, na sua ausência, aumentar o nível de protecção do ambiente (artigo 18.º)	35 %	20 %

Ligação Web ao texto integral da medida de auxílio

http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0800102.TV

http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1200204.TV

http://www.njt.hu/cgi_bin/njt_doc.cgi?docid=65457.92922

<http://www.garantiqa.hu/hu/letoltheto-dokumentumok/uzletszabalyzataink>

http://www.njt.hu/cgi_bin/njt_doc.cgi?docid=65457.92920

Número de referência do auxílio estatal	SA.36607 (13/X)	
Estado-Membro	Espanha	
Número de referência do Estado-Membro	—	
Designação da região (NUTS)	GALICIA N.º 3, alínea a), do artigo 107.º	
Entidade que concede o auxílio	Instituto Enerxético de Galicia (Inega) C/ Avelino Pousa Antelo, núm. 5 15707 (San Lázaro) Santiago de Compostela (A Coruña) http://www.inega.es/?idioma=es	
Título da medida de auxílio	Ayudas del Inega para proyectos de energías renovables	
Base jurídica nacional (referência à publicação oficial nacional relevante)	Resolución de 9 de abril de 2013 [Diario Oficial de Galicia (DOG) núm.73, de 16 de abril] por la que se establecen las bases reguladoras y se anuncia la convocatoria de subvenciones para el año 2013 a proyectos de energías renovables, con financiación procedente de fondos comunitarios derivados del Programa Operativo Feder Galicia 2007-2013	
Tipo de medida	Regime de auxílios	
Alteração de uma medida de auxílio existente	—	
Duração	22.4.2013-31.10.2013	
Setor(es) económico(s) abrangido(s)	Todos os sectores económicos elegíveis para beneficiar de auxílios	
Tipo de beneficiário	PME, grande empresa	
Montante global anual do orçamento previsto no âmbito do regime	EUR 2,10 (em milhões)	
Para garantias	EUR 2,10 (em milhões)	
Instrumentos de auxílio (artigo 5.º)	Subvenção directa	
Referência à decisão da Comissão	—	
Se for co-financiado por fundos comunitários	Feder 2007-2013 — EUR 1,10 (em milhões)	
Objetivos	Intensidade máxima de auxílios em % ou montante máximo do auxílio em moeda nacional	Majorações PME em %
Auxílios ao investimento no domínio do ambiente a favor da promoção da energia produzida a partir de fontes renováveis (artigo 23.º)	45 %	20 %

Ligação Web ao texto integral da medida de auxílio

http://www.xunta.es/dog/Publicados/2013/20130416/AnuncioO3G1-090413-0001_es.pdf

Número de referência do auxílio estatal	SA.36611 (13/X)	
Estado-Membro	Alemanha	
Número de referência do Estado-Membro	612-40306-BY/0008	
Designação da região (NUTS)	BAYERN N.º 3, alínea c), do artigo 107.º	

Entidade que concede o auxílio	Technologie- und Förderzentrum im Kompetenzzentrum für Nachwachsende Rohstoffe Schulgasse 18, 94315 Straubing www.tfz.bayern.de	
Título da medida de auxílio	Bayern: Demonstrationsmaßnahmen zur Nutzung von Biomasse als regenerativer Energieträger (BioSol)	
Base jurídica nacional (referência à publicação oficial nacional relevante)	Richtlinie zur Förderung von Demonstrationsvorhaben zur Nutzung von Biomasse als regenerativer Energieträger (BioSol), Art. 23 und 44 der Bayerischen Haushaltsordnung und die Verwaltungsvorschriften hierzu.	
Tipo de medida	Regime de auxílios	
Alteração de uma medida de auxílio existente	—	
Duração	1.5.2013-30.6.2014	
Setor(es) económico(s) abrangido(s)	Todos os sectores económicos elegíveis para beneficiar de auxílios	
Tipo de beneficiário	PME, grande empresa	
Montante global anual do orçamento previsto no âmbito do regime	EUR 0,70 (em milhões)	
Para garantias	EUR 0,70 (em milhões)	
Instrumentos de auxílio (artigo 5.º)	Subvenção directa	
Referência à decisão da Comissão	—	
Se for co-financiado por fundos comunitários	—	
Objetivos	Intensidade máxima de auxílios em % ou montante máximo do auxílio em moeda nacional	Majorações PME em %
Auxílios ao investimento no domínio do ambiente a favor da promoção da energia produzida a partir de fontes renováveis (artigo 23.º)	30 %	10 %

Ligação Web ao texto integral da medida de auxílio

http://www.stmelf.bayern.de/mam/cms01/agrarpolitik/dateien/b_rili_biosol_2013.pdf

Número de referência do auxílio estatal	SA.36747 (13/X)
Estado-Membro	Reino Unido
Número de referência do Estado-Membro	—
Designação da região (NUTS)	UNITED KINGDOM N.º 3, alínea a), do artigo 107.º, N.º 3, alínea c), do artigo 107.º, Regiões não assistidas, Regiões mistas
Entidade que concede o auxílio	Department of Energy and Climate Change 3 Whitehall Place, London, SW1A 2AW https://www.gov.uk/renewable-heat-premium-payment-scheme#overview
Título da medida de auxílio	Amalgamation of all previous and future phases of Renewable Heat Premium Payment — Social Housing Competitions
Base jurídica nacional (referência à publicação oficial nacional relevante)	Section 153 of Environmental Protection Act 1990

Tipo de medida	Regime de auxílios	
Alteração de uma medida de auxílio existente	SA.36747 replaces SA.34995, SA.35310, SA.34994, SA.35312, SA.34795, SA.34996 and SA.35311.	
Duração	15.8.2011-30.6.2014	
Setor(es) económico(s) abrangido(s)	Instalação de canalizações e de climatização	
Tipo de beneficiário	PME, grande empresa	
Montante global anual do orçamento previsto no âmbito do regime	GBP 23,22 (em milhões)	
Para garantias	GBP 23,22 (em milhões)	
Instrumentos de auxílio (artigo 5.º)	Subvenção directa	
Referência à decisão da Comissão	—	
Se for co-financiado por fundos comunitários	—	
Objetivos	Intensidade máxima de auxílios em % ou montante máximo do auxílio em moeda nacional	Majorações PME em %
Auxílios ao investimento no domínio do ambiente a favor de medidas de poupança de energia (artigo 21.º)	60 %	20 %

Ligação Web ao texto integral da medida de auxílio

<https://www.gov.uk/renewable-heat-premium-payment-scheme#overview>

Informações comunicadas pelos Estados-Membros relativas a auxílios estatais concedidos em conformidade com o Regulamento (CE) n.º 1857/2006 da Comissão relativo à aplicação dos artigos 87.º e 88.º do Tratado aos auxílios estatais a favor das pequenas e médias empresas que se dedicam à produção de produtos agrícolas e que altera o Regulamento (CE) n.º 70/2001

(2013/C 190/03)

N.º do auxílio: SA.36717 (13/XA)

Estado-Membro: Espanha

Região: ASTURIAS

Denominação do regime de auxílios ou nome da empresa que recebe o auxílio individual concedido: Asociación de Criadores de Gochu Asturcelta (ACGA)

Base jurídica: Convenio de colaboración con la Asociación de Criadores de Gochu Asturcelta para el mantenimiento del libro genealógicoy el desarrollo del programa de conservación de dicha raza en 2013.

Despesas anuais previstas a título do regime ou montante total do auxílio individual concedido à empresa: Montante global do auxílio ad hoc concedido à empresa: EUR 0,01 (em milhões)

Intensidade máxima dos auxílios: 100,00 %

Duração do regime ou do auxílio individual: 18.6.2013-31.12.2013

Objetivo do auxílio: Assistência técnica (art. 15.º do Reg. (CE) n.º 1857/2006), Sector pecuário (art. 16.º do Reg. (CE) n.º 1857/2006)

Setor(es) em causa: Suinicultura

Nome e endereço da autoridade responsável pela concessão:

Consejería de Agroganadería y Recursos Autóctonos del Principado de Asturias
C/ Coronel Aranda, s/n, 3ª planta
33005 Oviedo — ASTURIAS

Endereço do sítio web:

http://www.asturias.es/Asturias/descargas/PDF_TEMAS/Ganaderia/ayudas/genetica/acga.pdf

Outras informações: —

N.º do auxílio: SA.36718 (13/XA)

Estado-Membro: Espanha

Região: ASTURIAS

Denominação do regime de auxílios ou nome da empresa que recebe o auxílio individual concedido: Asociación de Criadores de Cabra Bermeya (ACRIBER)

Base jurídica: Convenio de colaboración con la Asociación de Criadores de Cabra Bermeya para el mantenimiento del libro genealógico y el desarrollo del programa de conservación de dicha raza en 2013.

Despesas anuais previstas a título do regime ou montante total do auxílio individual concedido à empresa: Montante global do auxílio ad hoc concedido à empresa: EUR 0,01 (em milhões)

Intensidade máxima dos auxílios: 100,00 %

Duração do regime ou do auxílio individual: 18.6.2013-31.12.2013

Objetivo do auxílio: Assistência técnica (art. 15.º do Reg. (CE) n.º 1857/2006), Sector pecuário (art. 16.º do Reg. (CE) n.º 1857/2006)

Setor(es) em causa: Criação de ovinos e caprinos

Nome e endereço da autoridade responsável pela concessão:

Consejería de Agroganadería y Recursos Autóctonos del Principado de Asturias
C/ Coronel Aranda, s/n, 3ª planta
33005 Oviedo — ASTURIAS

Endereço do sítio web:

http://www.asturias.es/Asturias/descargas/PDF_TEMAS/Ganaderia/ayudas/genetica/acriber.pdf

Outras informações: —

N.º do auxílio: SA.36719 (13/XA)

Estado-Membro: Espanha

Região: ASTURIAS

Denominação do regime de auxílios ou nome da empresa que recebe o auxílio individual concedido: Ayudas al sector ganadero en forma de servicios prestados por Asturiana de Control Lechero, Cooperativa Limitada (ASCOL)

Base jurídica: Convenio de colaboración con la Cooperativa Asturiana de Control Lechero (ASCOL) para el desarrollo de un programa de mejora genética de la cabaña ganadera asturiana de raza firsona durante el año 2013.

Despesas anuais previstas a título do regime ou montante total do auxílio individual concedido à empresa: Montante global anual do orçamento previsto no âmbito do regime: EUR 0,44 (em milhões)

Intensidade máxima dos auxílios: 100,00 %

Duração do regime ou do auxílio individual: 14.6.2013-31.12.2013

Objetivo do auxílio: Assistência técnica (art. 15.º do Reg. (CE) n.º 1857/2006), Sector pecuário (art. 16.º do Reg. (CE) n.º 1857/2006)

Sector(es) em causa: Criação de bovinos para produção de leite

Nome e endereço da autoridade responsável pela concessão:

Consejería de Agroganadería y Recursos Autóctonos del Principado de Asturias
C/ Coronel Aranda, s/n, 3ª planta
33005 — Oviedo — ASTURIAS

Endereço do sítio web:

http://www.asturias.es/Asturias/descargas/PDF_TEMAS/Ganaderia/ayudas/genetica/ascol.pdf

Outras informações: —

N.º do auxílio: SA.36720 (13/XA)

Estado-Membro: Espanha

Região: ASTURIAS

Denominação do regime de auxílios ou nome da empresa que recebe o auxílio individual concedido: Asociación española de criadores de ganado vacuno selecto de raza Asturiana de los Valles (ASESAVA)

Base jurídica: Convenio de colaboración con la Asociación española de criadores de ganado vacuno selecto de raza Asturiana de los Valles para el mantenimiento del libro genealógico y el desarrollo del programa de mejora genética de dicha raza en 2013.

Despesas anuais previstas a título do regime ou montante total do auxílio individual concedido à empresa: Montante global anual do orçamento previsto no âmbito do regime: EUR 0,48 (em milhões)

Intensidade máxima dos auxílios: 100,00 %

Duração do regime ou do auxílio individual: 14.6.2013-31.12.2013

Objetivo do auxílio: Assistência técnica (art. 15.º do Reg. (CE) n.º 1857/2006), Sector pecuário (art. 16.º do Reg. (CE) n.º 1857/2006)

Sector(es) em causa: Criação de outros bovinos (excepto para a produção de leite) e búfalos

Nome e endereço da autoridade responsável pela concessão:

Consejería de Agroganadería y Recursos Autóctonos del Principado de Asturias
C/ Coronel Aranda, s/n, 3ª planta
33005 Oviedo — ASTURIAS

Endereço do sítio web:

http://www.asturias.es/Asturias/descargas/PDF_TEMAS/Ganaderia/ayudas/genetica/aseava.pdf

Outras informações: —

N.º do auxílio: SA.36721 (13/XA)

Estado-Membro: Espanha

Região: ASTURIAS

Denominação do regime de auxílios ou nome da empresa que recebe o auxílio individual concedido: Asociación Española de Criadores de Ganado Vacuno Selecto de raza Asturiana de la Montaña (ASEAMO)

Base jurídica: Convenio de colaboración con la Asociación Española de Criadores de Ganado Vacuno Selecto de raza Asturiana de la Montaña para el mantenimiento del libro genealógico y del desarrollo de un programa de conservación de dicha raza en 2013.

Despesas anuais previstas a título do regime ou montante total do auxílio individual concedido à empresa: Montante global anual do orçamento previsto no âmbito do regime: EUR 0,13 (em milhões)

Intensidade máxima dos auxílios: 100,00 %

Duração do regime ou do auxílio individual: 14.6.2013-31.12.2013

Objetivo do auxílio: Assistência técnica (art. 15.º do Reg. (CE) n.º 1857/2006), Sector pecuário (art. 16.º do Reg. (CE) n.º 1857/2006)

Sector(es) em causa: Criação de outros bovinos (excepto para a produção de leite) e búfalos

Nome e endereço da autoridade responsável pela concessão:

Consejería de Agroganadería y Recursos Autóctonos del Principado de Asturias
C/ Coronel Aranda, s/n, 3ª planta
33005 Oviedo — ASTURIAS

Endereço do sítio web:

http://www.asturias.es/Asturias/descargas/PDF_TEMAS/Ganaderia/ayudas/genetica/aseamo.pdf

Outras informações: —

N.º do auxílio: SA.36722 (13/XA)

Estado-Membro: Espanha

Região: ASTURIAS

Denominação do regime de auxílios ou nome da empresa que recebe o auxílio individual concedido: Asociación de Criadores de Oveya Xalda de Asturias (ACOXÁ)

Base jurídica: Convenio de colaboración con la Asociación de Criadores de Oveya Xalda de Asturias para el mantenimiento del libro genealógico y el desarrollo del programa de conservación de dicha raza durante 2013.

Despesas anuais previstas a título do regime ou montante total do auxílio individual concedido à empresa: Montante global do auxílio ad hoc concedido à empresa: EUR 0,03 (em milhões)

Intensidade máxima dos auxílios: 100,00 %

Duração do regime ou do auxílio individual: 18.6.2013-31.12.2013

Objetivo do auxílio: Assistência técnica (art. 15.º do Reg. (CE) n.º 1857/2006), Sector pecuário (art. 16.º do Reg. (CE) n.º 1857/2006)

Setor(es) em causa: Criação de ovinos e caprinos

Nome e endereço da autoridade responsável pela concessão:

Consejería de Agroganadería y Recursos Autóctonos del Principado de Asturias
C/ Coronel Aranda, s/n, 3ª planta
33005 — Oviedo — ASTURIAS

Endereço do sítio web:

http://www.asturias.es/Asturias/descargas/PDF_TEMAS/Ganaderia/ayudas/genetica/acoxa.pdf

Outras informações: —

N.º do auxílio: SA.36723 (13/XA)

Estado-Membro: Espanha

Região: ASTURIAS

Denominação do regime de auxílios ou nome da empresa que recebe o auxílio individual concedido: Asociación de Criadores de Pita Pinta Asturiana (ACPPA)

Base jurídica: Convenio de colaboración con la Asociación de Criadores de Pita Pinta Asturiana para el mantenimiento del libro genealógico y el desarrollo del programa de conservación de dicha raza en 2013.

Despesas anuais previstas a título do regime ou montante total do auxílio individual concedido à empresa: Montante global anual do orçamento previsto no âmbito do regime: EUR 0,01 (em milhões)

Intensidade máxima dos auxílios: 100,00 %

Duração do regime ou do auxílio individual: 14.6.2013-31.12.2013

Objetivo do auxílio: Assistência técnica (art. 15.º do Reg. (CE) n.º 1857/2006), Sector pecuário (art. 16.º do Reg. (CE) n.º 1857/2006)

Setor(es) em causa: Avicultura

Nome e endereço da autoridade responsável pela concessão:

Consejería de Agroganadería y Recursos Autóctonos del Principado de Asturias
C/ Coronel Aranda, s/n, 3ª planta
33005 Oviedo — ASTURIAS

Endereço do sítio web:

http://www.asturias.es/Asturias/descargas/PDF_TEMAS/Ganaderia/ayudas/genetica/acppa.pdf

Outras informações: —

N.º do auxílio: SA.36724 (13/XA)

Estado-Membro: Espanha

Região: ASTURIAS

Denominação do regime de auxílios ou nome da empresa que recebe o auxílio individual concedido: Asociación de Criadores de Ponis de Raza Asturcón (ACPRA)

Base jurídica: Convenio de colaboración con la Asociación de Criadores de Ponis de Raza Asturcón para el mantenimiento del libro genealógico y el desarrollo del programa de conservación de dicha raza en 2013.

Despesas anuais previstas a título do regime ou montante total do auxílio individual concedido à empresa: Montante global anual do orçamento previsto no âmbito do regime: EUR 0,13 (em milhões)

Intensidade máxima dos auxílios: 100,00 %

Duração do regime ou do auxílio individual: 14.6.2013-31.12.2013

Objetivo do auxílio: Assistência técnica (art. 15.º do Reg. (CE) n.º 1857/2006), Sector pecuário (art. 16.º do Reg. (CE) n.º 1857/2006)

Setor(es) em causa: Criação de equinos, asininos e muare

Nome e endereço da autoridade responsável pela concessão:

Consejería de Agroganadería y Recursos Autóctonos del Principado de Asturias
C/ Coronel Aranda, s/n, 3ª planta
33005 Oviedo — ASTURIAS

Endereço do sítio web:

http://www.asturias.es/Asturias/descargas/PDF_TEMAS/Ganaderia/ayudas/genetica/acpra.pdf

Outras informações: —

Informações comunicadas pelos Estados-Membros relativas a auxílios estatais concedidos nos termos do Regulamento (CE) n.º 800/2008 da Comissão, que declara certas categorias de auxílios compatíveis com o mercado comum, em aplicação dos artigos 87.º e 88.º do Tratado (Regulamento geral de isenção por categoria)

(Texto relevante para efeitos do EEE)

(2013/C 190/04)

Número de referência do auxílio estatal	SA.36385 (13/X)	
Estado-Membro	Letónia	
Número de referência do Estado-Membro	—	
Designação da região (NUTS)	Latvia N.º 3, alínea a), do artigo 107.º	
Entidade que concede o auxílio	valsts aģentūra "Latvijas Investīciju un attīstības aģentūra" Pērses iela 2, Rīga, Latvija, LV-1442 www.liaa.gov.lv	
Título da medida de auxílio	Atbalsts darba vietu radīšanai	
Base jurídica nacional (referência à publicação oficial nacional relevante)	2012.gada 13.marta Ministru kabineta noteikumi Nr.179 "Noteikumi par darbības programmas "Cilvēkresursi un nodarbinātība" papildinājuma 1.3.1.1.6.apakšaktivitāti "Atbalsts darba vietu radīšanai" " Darbības programma "Cilvēkresursi un nodarbinātība" (638. – 641. punkts) Darbības programmas "Cilvēkresursi un nodarbinātība" papildinājums (208.7. – 208.12. punkts)	
Tipo de medida	Regime de auxílios	
Alteração de uma medida de auxílio existente	—	
Duração	1.11.2012-31.12.2013	
Setor(es) económico(s) abrangido(s)	Todos os sectores económicos elegíveis para beneficiar de auxílios	
Tipo de beneficiário	PME, grande empresa	
Montante global anual do orçamento previsto no âmbito do regime	LVL 7,00 (em milhões)	
Para garantias	LVL 7,00 (em milhões)	
Instrumentos de auxílio (artigo 5.º)	Subvenção directa	
Referência à decisão da Comissão	—	
Se for co-financiado por fundos comunitários	Komisijas lēmums 18-XII-2007 ar ko pieņem darbības programmu Kопienas palīdzībai no Eiropas Sociālā fonda atbilstīgi konverģences mērķim Latvijas reģionos CCI 2007LV051PO001. – LVL 3,00 (em milhões)	
Objetivos	Intensidade máxima de auxílios em % ou montante máximo do auxílio em moeda nacional	Majorações PME em %
Formação geral (ponto 2 do artigo 38.º)	50 %	0 %
Regime de auxílios	50 %	0 %
Formação específica (ponto 1 do artigo 38.º)	25 %	0 %

Ligação Web ao texto integral da medida de auxílio:

<http://www.likumi.lv/doc.php?id=246032#top>

Número de referência do auxílio estatal	SA.36580 (13/X)	
Estado-Membro	Alemanha	
Número de referência do Estado-Membro	—	
Designação da região (NUTS)	DEUTSCHLAND N.º 3, alínea a), do artigo 107.º, N.º 3, alínea c), do artigo 107.º, Regiões não assistidas, Regiões mistas	
Entidade que concede o auxílio	KfW Bankengruppe Palmengartenstraße 5-9, 60325 Frankfurt www.kfw.de	
Título da medida de auxílio	KfW-Programm Erneuerbare Energien „Speicher“	
Base jurídica nacional (referência à publicação oficial nacional relevante)	KfW-Gesetz, BGBl. I S.2427, Programmmerkblatt „KfW-Programm Erneuerbare Energien “Speicher” ‘	
Tipo de medida	Regime de auxílios	
Alteração de uma medida de auxílio existente	—	
Duração	1.5.2013-31.12.2013	
Setor(es) económico(s) abrangido(s)	Todos os sectores económicos elegíveis para beneficiar de auxílios	
Tipo de beneficiário	PME, grande empresa	
Montante global anual do orçamento previsto no âmbito do regime	EUR 25,00 (em milhões)	
Para garantias	EUR 25,00 (em milhões)	
Instrumentos de auxílio (artigo 5.º)	Subvenção directa, Empréstimos em condições preferenciais	
Referência à decisão da Comissão	—	
Se for co-financiado por fundos comunitários	—	
Objetivos	Intensidade máxima de auxílios em % ou montante máximo do auxílio em moeda nacional	Majorações PME em %
Auxílios ao investimento e ao emprego a favor das PME (artigo 15.º)	20 %	—
Auxílios ao investimento no domínio do ambiente a favor da promoção da energia produzida a partir de fontes renováveis (artigo 23.º)	45 %	20 %

Ligação Web ao texto integral da medida de auxílio:

https://www.kfw.de/media/pdf/download_center/foerderprogramme__inlandsfoerderung_/pdf_dokumente_2/6000002700_M_275_Speicher.pdf

Número de referência do auxílio estatal	SA.36584 (13/X)	
Estado-Membro	Itália	
Número de referência do Estado-Membro	—	
Designação da região (NUTS)	ABRUZZO N.º 3, alínea c), do artigo 107.º, Regiões não assistidas	

Entidade que concede o auxílio	GIUNTA REGIONALE — DIREZIONE SVILUPPO ECONOMICO E TURISMO VIA PASSOLANCIANO N. 75 65127 PESCARA — ITALIA http://www.regione.abruzzo.it/portale/index.asp	
Título da medida de auxílio	BANDO PER LA PROMOZIONE SUL PROPRIO TERRITORIO REGIONALE DI INIZIATIVE DI LOCALIZZAZIONE, AMPLIAMENTO E AMODERNAMENTO DI UNITA INDUSTRIALI, ATTRAVERSO CONTRATTI DI SVILUPPO LOCALI — TITOLO IV PROGETTI DI RICERCA INDUSTRIALE E SVILUPPO SPERIMENTALE	
Base jurídica nacional (referência à publicação oficial nacional relevante)	PAR FA ABRUZZO 2007-2013 APPROVATO CON D.G.R. N. 458 DEL 4 LUGLIO 2011 E MODIFICATO CON D.G.R. N. 556 DELL'8 AGOSTO 2011 CON ALLEGATO A. PRESA D'ATTO DA PARTE DEL CIPE CON DELIBERAZIONE DEL 30.9.2011 G.U. SERIE GENERALE N. 47 DEL 25.2.2012.	
Tipo de medida	Regime de auxílios	
Alteração de uma medida de auxílio existente	—	
Duração	29.3.2013-30.6.2014	
Setor(es) económico(s) abrangido(s)	INDÚSTRIAS TRANSFORMADORAS	
Tipo de beneficiário	PME, grande empresa	
Montante global anual do orçamento previsto no âmbito do regime	EUR 10,00 (em milhões)	
Para garantias	EUR 10,00 (em milhões)	
Instrumentos de auxílio (artigo 5.º)	Subvenção directa	
Referência à decisão da Comissão	—	
Se for co-financiado por fundos comunitários	—	
Objetivos	Intensidade máxima de auxílios em % ou montante máximo do auxílio em moeda nacional	Majorações PME em %
Investigação industrial [n.o 2, alínea b), do artigo 31.o]	50 %	20 %
Desenvolvimento experimental [n.o 2, alínea c), do artigo 31.o]	25 %	20 %

Ligação Web ao texto integral da medida de auxílio:

<http://www.regione.abruzzo.it/portale/index.asp?modello=avvisoSing&servizio=le&stileDiv=sequence&template=default&tom=2497&b=avviso>

<http://bura.regione.abruzzo.it/bollettinoaccess.aspx?id=49993&tipo=Speciali&numero=35&data=29+Marzo+2013>

Número de referência do auxílio estatal	SA.36585 (13/X)
Estado-Membro	Itália
Número de referência do Estado-Membro	—
Designação da região (NUTS)	ABRUZZO Regiões não assistidas

Entidade que concede o auxílio	GIUNTA REGIONALE — DIREZIONE SVILUPPO ECONOMICO E TURISMO VIA PASSOLANCIANO N. 75 65127 PESCARA — ITALIA http://www.regione.abruzzo.it/portale/index.asp	
Título da medida de auxílio	BANDO PER LA PROMOZIONE SUL PROPRIO TERRITORIO REGIONALE DI INIZIATIVE DI LOCALIZZAZIONE, AMPLIAMENTO E AMODERNAMENTO DI UNITA INDUSTRIALI, ATTRAVERSO CONTRATTI DI SVILUPPO LOCALI — TITOLO III PROGETTI RELATIVI AD INVESTIMENTI IN AREE DIVERSE DA QUELLE DI CUI ALL'ART. 107 3, C) TFUE	
Base jurídica nacional (referência à publicação oficial nacional relevante)	PAR FAS ABRUZZO 2007-2013 APPROVATO CON D.G.R. N. 458 DEL 4 LUGLIO 2011 E MODIFICATO CON D.G.R. N. 556 DELL'8 AGOSTO 2011 CON ALLEGATO A. PRESA D'ATTO DA PARTE DEL CIPE CON DELIBERAZIONE 30.9.2011 G.U. SERIE GENERALE N. 47 DEL 25.2.2012	
Tipo de medida	Regime de auxílios	
Alteração de uma medida de auxílio existente	—	
Duração	29.3.2013-30.6.2014	
Setor(es) económico(s) abrangido(s)	INDÚSTRIAS TRANSFORMADORAS	
Tipo de beneficiário	PME	
Montante global anual do orçamento previsto no âmbito do regime	EUR 10,00 (em milhões)	
Para garantias	EUR 10,00 (em milhões)	
Instrumentos de auxílio (artigo 5.º)	Subvenção directa	
Referência à decisão da Comissão	—	
Se for co-financiado por fundos comunitários	—	
Objetivos	Intensidade máxima de auxílios em % ou montante máximo do auxílio em moeda nacional	Majorações PME em %
Auxílios ao investimento e ao emprego a favor das PME (artigo 15.º)	20 %	—

Ligação Web ao texto integral da medida de auxílio:

<http://www.regione.abruzzo.it/portale/index.asp?modello=avvisoSing&servizio=le&stileDiv=sequence&template=default&tom=2497&b=avviso>

<http://bura.regione.abruzzo.it/bollettinoaccess.aspx?id=49993&tipo=Speciali&numero=35&data=29+Marzo+2013>

Número de referência do auxílio estatal	SA.36586 (13/X)
Estado-Membro	Itália
Número de referência do Estado-Membro	—
Designação da região (NUTS)	ABRUZZO N.º 3, alínea c), do artigo 107.º

Entidade que concede o auxílio	GIUNTA REGIONALE — DIREZIONE SVILUPPO ECONOMICO E TURISMO VIA PASSOLANCIANO N. 75 65127 PESCARA — ITALIA http://www.regione.abruzzo.it/portale/index.asp	
Título da medida de auxílio	BANDO PER LA PROMOZIONE SUL PROPRIO TERRITORIO REGIONALE DI INIZIATIVE DI LOCALIZZAZIONE, AMPLIAMENTO E AMMODERNAMENTO DI UNITA INDUSTRIALI, ATTRAVERSO CONTRATTI DI SVILUPPO LOCALI — TITOLO II — PROGETTI RELATIVI AD INVESTIMENTI NELLE AREE 107 3, C) TFUE	
Base jurídica nacional (referência à publicação oficial nacional relevante)	PAR FAS ABRUZZO 2007-2013 APPROVATO CON D.G.R. n.458 del 4 luglio 2011 E MODIFICATO CON D.G.R. n.556 dell'8 Agosto 2011 con allegato A. PRESA D'ATTO DA PARTE DEL CIPE CON DELIBERAZIONE DEL 30.9.2011 G.U. SERIE GENERALE N. 47 DEL 25.2.2012	
Tipo de medida	Regime de auxílios	
Alteração de uma medida de auxílio existente	—	
Duração	29.3.2013-30.6.2014	
Setor(es) económico(s) abrangido(s)	INDÚSTRIAS TRANSFORMADORAS	
Tipo de beneficiário	PME, grande empresa	
Montante global anual do orçamento previsto no âmbito do regime	EUR 10,00 (em milhões)	
Para garantias	EUR 10,00 (em milhões)	
Instrumentos de auxílio (artigo 5.º)	Subvenção directa	
Referência à decisão da Comissão	—	
Se for co-financiado por fundos comunitários	—	
Objetivos	Intensidade máxima de auxílios em % ou montante máximo do auxílio em moeda nacional	Majorações PME em %
Regime de auxílios	15 %	20 %

Ligação Web ao texto integral da medida de auxílio:

<http://www.regione.abruzzo.it/portale/index.asp?modello=avvisoSing&servizio=le&stileDiv=sequence&template=default&tom=2497&b=avviso>

<http://bura.regione.abruzzo.it/bollettinoaccess.aspx?id=49993&tipo=Speciali&numero=35&data=29+Marzo+2013>

V

(Avisos)

PROCEDIMENTOS RELATIVOS À EXECUÇÃO DA POLÍTICA DE
CONCORRÊNCIA

COMISSÃO EUROPEIA

AUXÍLIO ESTATAL — REPÚBLICA HELÉNICA

Auxílio estatal SA.31155 (2013/C) (ex 2013/NN) (ex 2010/N) — Auxílios estatais a favor do Hellenic Postbank S.A. através da criação e da capitalização do banco de transição «New Hellenic Postbank S.A.»

Convite à apresentação de observações nos termos do artigo 108.º, n.º 2, do TFUE

(Texto relevante para efeitos do EEE)

(2013/C 190/05)

Por carta de 6 de maio de 2013, reproduzida na língua que faz fé a seguir ao presente resumo, a Comissão comunicou à República Helénica a sua decisão de dar início ao procedimento previsto no artigo 108.º, n.º 2, do TFUE relativamente ao auxílio acima mencionado.

As partes interessadas podem dar a conhecer as suas observações sobre a medida de auxílio, em relação à qual a Comissão deu início ao procedimento, no prazo de um mês a contar da data de publicação do presente resumo e da carta que se segue, enviando-as para o seguinte endereço:

Comissão Europeia
Direção-Geral da Concorrência
Registo dos Auxílios Estatais
1049 Bruxelles/Brussel
BELGIQUE/BELGIË

Fax +32 22961242

Essas observações serão comunicadas à República Helénica. Qualquer interessado que apresente observações pode solicitar por escrito o tratamento confidencial da sua identidade, devendo justificar o pedido.

TEXTO DO RESUMO

PROCEDIMENTOS

A 18 de janeiro de 2013, foi criada pelas autoridades gregas uma instituição de crédito temporária, o «New TT Hellenic Postbank S.A.» («New TT»). As atividades empresariais são do antigo TT Hellenic Postbank S.A. («TT») foram transferidas para o New TT. Nesse contexto, o New TT recebeu auxílios estatais no montante de 4 600 milhões de euros provenientes do Fundo de Estabilidade Financeira para a Grécia (FEFG).

Além disso, a 25 de maio de 2009, o TT recebeu uma injeção de capital num montante de 224,96 milhões de euros ao abrigo

do Regime Grego⁽¹⁾. Por decisão de 16 de maio de 2012⁽²⁾, relativa ao processo de auxílio estatal SA.34115 (2012/NN) sobre a resolução do T Bank S.A levada a cabo em dezembro de 2011, a Comissão autorizou, por um período de seis meses, um auxílio à resolução num montante próximo de 678 milhões de euros, considerando-o compatível com o mercado interno com base no artigo 107.º, n.º 3, alínea b), do Tratado sobre o Funcionamento da União Europeia («TFUE»).

⁽¹⁾ Ver Decisão da Comissão, de 19 de novembro de 2008, relativa ao auxílio estatal n.º 560/2008 «Support Measures for the Credit Institutions in Greece», JO C 125 de 5.6.2009, p. 6. O regime foi prorrogado várias vezes.

⁽²⁾ Decisão da Comissão de 16 de maio de 2012, relativa ao processo SA.34115 (2012/nn) «Resolution of T Bank», JO C 284 de, 20.9.2012, p. 9.

DESCRIÇÃO DAS MEDIDAS EM RELAÇÃO ÀS QUAIS A COMISSÃO DÁ INÍCIO AO PROCEDIMENTO

Em primeiro lugar, a 18 de janeiro de 2013, o FEFG proveu o New TT do seu capital inicial de 500 milhões de euros.

Em segundo lugar, como as atividades transferidas do TT para o New TT compreendiam menos 4 100 milhões de euros de ativos do que passivos, o FEFG cobriu o chamado «défice de financiamento», concedendo ao New TT obrigações do FEEF, no montante de 4 100 milhões de euros.

Em terceiro lugar, a 25 de maio de 2009, o TT recebeu uma injeção de capital num montante de 224,96 milhões de euros ao abrigo do Regime Grego.

Em quarto lugar, a 17 de dezembro de 2011, o Banco da Grécia procedeu à resolução do T Bank por meio de uma ordem de transferência dos seus ativos e passivos para o TT. Como o valor dos passivos transferidos era mais elevado do que o valor dos ativos transferidos, o conseqüente défice de financiamento de 676 956 514 euros foi coberto, nos termos das disposições pertinentes, pelo regime de resolução do Fundo de Garantia de Depósitos e Investimentos Grego (FGDIG).

APRECIÇÃO DAS MEDIDAS

Em primeiro lugar, no que diz respeito a i) injeção de capital no valor de 500 milhões de euros e ii) cobertura do défice de financiamento no montante de 4 100 milhões de euros pelo FEFG a favor do New TT, a Comissão considera que ambas as medidas de auxílio prefiguram auxílios estatais para efeitos do artigo 107.º, n.º 1, do TFUE. Em segundo lugar, no que diz respeito à recapitalização do TT em 2009, a Comissão já tinha concluído, na sua decisão de aprovação do regime ⁽³⁾, que a recapitalização concedida ao abrigo desse regime constituiria um auxílio estatal. Em terceiro lugar, no que diz respeito ao auxílio à resolução concedido ao T Bank, a Comissão estabeleceu, na sua decisão de 16 de maio de 2012 ⁽⁴⁾, que a intervenção pelo regime de resoluções do FGDIG constitui um auxílio estatal.

A base jurídica para a apreciação das medidas é o artigo 107.º, n.º 3, alínea b), do TFUE.

A compatibilidade das medidas acima referidas com o artigo 107.º, n.º 3, alínea b), do TFUE, é avaliada pela Comissão em relação à base jurídica da Comunicação relativa ao setor

bancário ⁽⁵⁾, da Comunicação relativa à recapitalização ⁽⁶⁾ e da Comunicação sobre a reestruturação ⁽⁷⁾.

No que respeita à compatibilidade das medidas, a Comissão considera a forma da injeção de capital e a cobertura do défice de financiamento no New TT adequada a título de auxílio de emergência a fim de concretizar o objetivo do restabelecimento da estabilidade financeira do sistema bancário grego e da economia em geral. Contudo, na presente fase, a Comissão tem dúvidas se o montante de 4 600 milhões de euros (500 milhões de euros de capital e 4 100 milhões de euros de cobertura de «défice de financiamento») se limita ao mínimo, pelo que convida as partes interessadas a apresentar as suas observações sobre esta questão. A Comissão considera ainda que ambas as medidas são proporcionadas enquanto auxílio de emergência de curto prazo, mas exige a adoção rápida de medidas para garantir que o auxílio não é utilizado para financiar o crescimento ou medidas não estritamente necessárias para restabelecer a viabilidade.

No que diz respeito ao restabelecimento da viabilidade a longo prazo ao abrigo da Comunicação relativa à reestruturação, a Comissão tem dúvidas de que o New TT seja capaz de restabelecer a sua viabilidade a longo prazo, de forma autónoma, tal como previsto no plano de reestruturação apresentado à Comissão a 29 de janeiro de 2013 e atualizado em março de 2013. As medidas propostas no plano de reestruturação com vista a gerar lucros no futuro parecem ser muito limitadas. Essas dúvidas residem sobretudo na redução limitada do pessoal e das sucursais, bem como na utilização limitada das possíveis sinergias, ou seja, a plena integração do T Bank. Neste contexto, a Comissão tem dúvidas se o New TT tem recursos para atingir os objetivos fixados no plano de reestruturação e, mais precisamente, para alcançar os almejados lucros futuros. Existe, portanto, o risco de o New TT acabar por ser um banco de transição, que recorre repetidamente aos auxílios estatais. Por conseguinte, a Comissão é de opinião, nesta fase, de que a reintegração do TT numa empresa financeira viável e de maior dimensão aumentará as perspetivas de viabilidade do New TT. A Comissão convida as partes interessadas a apresentar as suas observações sobre estas dúvidas.

No que se refere à repartição dos encargos e à limitação do auxílio ao mínimo necessário, a Comissão tem dúvidas de que assim seja de facto. Mais concretamente, a Comissão tem dúvidas de que os custos de reestruturação estejam limitados ao mínimo necessário, porquanto o New TT deve ser reestruturado de forma autónoma, o que inflaciona os custos de reestruturação. A Comissão convida as partes interessadas a apresentar as suas observações sobre esta questão.

⁽⁵⁾ Comunicação da Comissão — Aplicação das regras relativas aos auxílios estatais às medidas adotadas em relação às instituições financeiras no contexto da atual crise financeira global, JO C 270 de 25.10.2008, p. 8.

⁽⁶⁾ Comunicação da Comissão - A recapitalização das instituições financeiras na atual crise financeira: limitação do auxílio ao mínimo necessário e salvaguardas contra distorções indevidas da concorrência, JO C 10, 15.1.2009, p. 2.

⁽⁷⁾ Comunicação da Comissão intitulada «O regresso à viabilidade e avaliação, em conformidade com as regras em matéria de auxílios estatais, das medidas de reestruturação tomadas no setor financeiro no contexto da atual crise», JO C 195 de 19.8.2009, p. 9

⁽³⁾ Ver nota de rodapé 1.

⁽⁴⁾ Ver nota de rodapé 2.

Além disso, a Comissão observa que uma grande parte das perdas sofridas pelo TT nos últimos anos resulta de uma remissão de dívidas a favor do Estado, ou seja, através do ISP e através da venda de títulos de dívida pública grega ao Estado com um grande desconto face ao valor nominal no final de 2012. Essas medidas poderiam ser considerados equivalentes a um pagamento pelo TT ao Estado e, por conseguinte, justificar uma remuneração inferior do auxílio de recapitalização posteriormente concedido pelo Estado com o objetivo de cobrir as falhas de capital decorrentes da remissão de dívida a favor do Estado. As partes interessadas são convidadas a apresentar as suas observações sobre este parecer.

Quanto à distorção da concorrência, pode observar-se que o TT era o banco que, na Grécia, detinha de longe mais títulos de dívida pública grega em proporção à sua dimensão. Na presente fase, a Comissão considera que um investimento desta escala nesses títulos de dívida pública poderia consubstanciar uma assunção de riscos inapropriada. A Comissão convida as partes interessadas a apresentar as suas observações também sobre esta questão.

Em conformidade com o artigo 14.º do Regulamento (CE) n.º 659/1999 do Conselho, qualquer auxílio ilegal pode ser objeto de recuperação junto do beneficiário.

TEXTO DA CARTA

«The Commission wishes to inform the Hellenic Republic that, having examined the information supplied by your authorities on the aid measures referred to above, it has decided to initiate the procedure laid down in Article 108(2) of the Treaty on the Functioning of the European Union ("TFEU").

1. PROCEDURE

- (1) On 19 November 2008 ⁽⁸⁾, the Commission approved the Greek support measures for the credit institutions designed to ensure the stability of the Greek financial system (the "**Scheme**").
- (2) On 25 May 2009, TT Hellenic Postbank S.A. ("**TT**") received a capital injection of EUR 224.96 million under the Scheme.
- (3) The Greek authorities submitted information to the Commission on TT in February, March, May and June 2010.
- (4) By letter of 30 June 2010, the Commission's services requested the restructuring plan for TT to be submitted by 1 September 2010.
- (5) By letter of 22 July 2010, the Greek authorities requested an extension of the deadline for the submission of the restructuring plan until 30 September 2010. The Commission services agreed to the extension of the deadline on 23 August 2010.
- (6) On 1 October 2010, the Greek authorities submitted the initial restructuring plan for TT.
- (7) The restructuring plan was discussed between the Greek authorities and the Commission services in a series of meetings, teleconferences and other information exchanges between October 2010 and May 2011, in particular - amongst others - on 6 and 14 October 2010, 8 November 2010, 27 December 2010, 26 January 2011, 23 March 2011 and 13 April 2011.
- (8) On 17 December 2011, the Bank of Greece ("**BoG**") proceeded with the resolution of T Bank S.A. ("**T Bank**") by ordering a transfer of its good assets and liabilities to TT, which was already a shareholder of T Bank (holding around 32.9 % of its shares).
- (9) In March 2012, Greece and the EU/ECB/IMF updated the Memorandum of Economic and Financial Policies ("**MEFP**"). The MEFP sets out, among other economic and financial policies, that the Greek authorities have initiated an orderly resolution of TT through a Purchase and Assumption ("**P&A**") transaction. TT had been classified as non-viable in the framework of the viability assessment of all the Greek banks carried out by the BoG and its advisors, in consultation with the EU/ECB/IMF.
- (10) By decision of 16 May 2012 in State aid case SA.34115 (2012/NN) on the Resolution of T Bank ⁽⁹⁾, the Commission authorised an intervention by the Resolution scheme of the Hellenic Deposit and Investment Guarantee Fund ("**HDIGF**") for an amount of EUR 676 956 514 as compatible with the internal market on the basis of Article 107(3)(b) TFEU for a period of six months. In that decision, the Commission required the Greek authorities to submit an updated restructuring plan for TT within six months. That plan was to take into account the integration of T Bank's activities into TT. In the decision of 16 May 2012 the Commission could not definitively conclude on the compatibility of the resolution aid to T Bank since the buyer of the bank's activities – TT – was itself an aided bank on which the Commission had not yet taken a decision on its restructuring, as well as on the restoration of TT's long-term viability. The Commission could therefore not conclude on whether the transfer of T Bank to TT was an adequate way to restore the viability of the transferred entity.
- (11) Further correspondence took place between the Greek authorities and the Commission services between May and December 2012.
- (12) In January 2013, the Greek authorities submitted a draft restructuring plan for a bridge bank of TT. Due to the absence of buyers for TT, no P&A transaction (as envisaged in the MEFP) could take place and the creation of a bridge bank was considered as the only remaining solution for the resolution of TT. The bridge bank received aid from the Hellenic Financial Stability Fund ⁽¹⁰⁾ ("**HFSF**") which (a) covered the so-called "funding gap" of the transferred perimeter and (b) provided the bridge bank with initial share capital.
- (13) The establishment of the bridge bank and its restructuring plan were discussed by the Greek authorities and the Commission services in a series of meetings, teleconferences and other information exchanges between

⁽⁸⁾ See Commission decision of 19 November 2008 in State aid N 560/2008 "Support Measures for the Credit Institutions in Greece", OJ C 125, 05.06.2009, p. 6. The scheme has been prolonged several times. The last updated scheme is in place until 30 June 2013. See Commission decision of 22 January 2013 in State aid SA.35999 (2012/N) "Prolongation of the Guarantee Scheme and the Bond Loans Scheme for Credit Institutions in Greece", not yet published.

⁽⁹⁾ Commission decision of 16 May 2012 in case SA.34115 (2012/NN) "Resolution of T Bank", OJ C 284, 20.09.2012, p. 9.

⁽¹⁰⁾ The HFSF is a Fund originally established by Law 3864/2010 of the Greek Parliament. The Fund's resources stem from the financial support mechanism to Greece and its capital is gradually paid up by the Greek State. It is set up for a limited duration until 30 June 2017. For more details, see inter alia, Commission decision of 3 September 2010 in State Aid case N 328/2010 "Recapitalisation of credit institutions in Greece under the Financial Stability Fund (FSF)", OJ C 316, 20.11.2010, p. 7.

January and March 2013, in particular - amongst others - on 8, 11, 15, 22, 23 and 30 January and 12 March 2013.

- (14) For reasons of urgency, the Hellenic Republic exceptionally accepts that the present decision is adopted in the English language.

2. DESCRIPTION

2.1 TT Hellenic Postbank S.A.

- (15) TT was established in 1902 under the framework of the Hellenic Post Office Organisation. Until 2006, TT was a State-controlled special credit institution with activities limited to the granting of mortgages and consumer loans to public servants and publicly-owned companies. After having acquired a banking licence in 2006, TT expanded its activities to corporate finance and retail lending. In the same year, TT became listed on the Athens Stock Exchange through a public offering of 34.84 % of its existing shares. The Hellenic Republic remained its largest shareholder.

- (16) TT has a market share of 6 % in terms of deposits in Greece.

- (17) In 2009, when it received its first recapitalisation, TT had 146 own branches and 2 554 employees. TT had a balance sheet showing total assets of approximately EUR 16 billion and risk weighted assets ("**RWA**") of EUR 7.5 billion.

- (18) TT has a cooperation agreement with the Hellenic Post Office to market its products in approximately 800 branches of the latter. The contribution of that additional network to TT's services is 7 % of TT's total deposit base (which amounted to approximately EUR 12 billion in 2009).

- (19) Compared to its size, TT has a relatively large deposit base. TT had a loan-to-deposit ratio of less than 100 % in 2009.

- (20) On 25 May 2009, TT got a capital injection of EUR 224.96 million (corresponding to circa 2.9 % of its RWA at that time) under the Scheme⁽¹¹⁾ because its bank capital adequacy ratio ("**CAR**") was under the 10% minimum threshold set by the BoG for it.

- (21) On 3 July 2009, TT issued common shares in amount of EUR 526.3 million, which were then placed on the market. After the completion of the capital increases of May and July 2009, the bank's CAR amounted to approximately 17 %. TT's shareholding structure following the share capital increase of July 2009 was as follows: the Hellenic State with 44.04 % of which 10% was held through the Hellenic Post Office; individuals with 24.9 %; legal entities (domestic) owning 22.04 %; legal entities (international) owning 7.81 % and; own shares corresponding to 1.21 % ownership.

- (22) In April 2010, TT acquired 32.9 % of the share capital of Aspis Bank for an amount of EUR 28.56 million. After the acquisition, Aspis Bank was rebranded as T Bank. When that bank was acquired by TT, it was in a poor economic situation with the lowest capital adequacy among the Greek banks, insufficient liquidity and profitability.

- (23) Other participations held by TT are: (i) Post insurance (50 % shareholding), a company promoting and selling insurance and banc assurance products; and (ii) Attica Bank (22.4 % shareholding), one of the smallest banks (1.1 % market share in terms of total assets) in Greece.

- (24) On 17 December 2011, the BoG proceeded with the resolution of T Bank through a transfer order of its assets and liabilities to TT and at the same time, with the withdrawal of T Bank's license. T Bank was put into liquidation. TT acquired the package of assets and liabilities of T Bank as it had made the highest bid in the framework of an unconditional tender procedure open to other banks. The value of the net assets transferred from T Bank to TT at the resolution date amounted to EUR 1.5 billion⁽¹²⁾. TT took over 75 branches with 853 employees of T Bank.

- (25) As a result, TT's total assets increased by 16 % to EUR 18 billion and its deposits by 15 % to EUR 13.5 billion, compared to the standalone basis⁽¹³⁾. The acquisition of T Bank's assets had a negative impact on TT's capital adequacy due to the capital shortage of T Bank. However, TT's CAR stayed well above supervisory limit at the time as, on the consolidated basis, its CAR amounted to 15.7 %.

- (26) In March 2012, the BoG, based on an own 'viability framework' methodology applied to the entire Greek banking system, declared TT to be an unviable bank as it was highly unlikely that TT could remain viable under its current state. The situation of TT gave rise several concerns. Firstly, TT booked an exceptionally high loss in 2011, due to the Private Sector Involvement⁽¹⁴⁾ ("**PSI**"). TT had held a portfolio of Greek government bonds ("**GGB**") which, compared to its balance sheet size, was much higher than that of the other Greek banks. As a result of that very large loss, TT's capital became deeply negative. Secondly, TT faced a structural problem of a low profitability which had lasted since 2008.

⁽¹²⁾ Bain&Company assessment report regarding policies and procedures required to ensure effective liquidating bank asset management and recovery of February 2013.

⁽¹³⁾ Financial impact analysis of the proposed merger between TT and T Bank performed by BoG, 19 July 2011

⁽¹⁴⁾ Private Sector Involvement (PSI): negotiation between the Greek authorities and its private creditors which aimed to achieve a partial waiver of the Greek government debt by its private creditors on a voluntary basis. The PSI is extraordinary in nature and had a considerable impact on Greek banks. A series of banks made losses stemming from PSI. Those developments are described in more detail for instance in points 12 and 13 of the following document: "*The Second Economic Adjustment Programme for Greece - March 2012*", also available on http://ec.europa.eu/economy_finance/publications/occasional_paper/2012/op94_en.htm.

⁽¹¹⁾ See footnote 1.

- (27) The updated MEFP of March 2012 gives a preference to an orderly resolution of TT via a P&A transaction, implying that TT's good assets and liabilities would be put for sale to another existing bank. For that purpose, the BoG launched a call for an expression of interest to third parties for acquiring TT's good assets in December 2012. Three Greek banks expressed preliminary informal interest; however, by the deadline of 11 January 2013 for submitting binding offers, the Greek authorities had not received any such offers.
- (28) Therefore, in the absence of buyers, the Greek authorities considered that the creation of a bridge bank was the only remaining solution for the resolution of TT.

2.2. New TT Hellenic Postbank S.A.

- (29) On 18 January 2013, in the context of the Greek resolution framework⁽¹⁵⁾ and in line with the provisions in the MEFP regarding the resolution of TT by January 2013, the Greek authorities announced the immediate creation and capitalisation of a temporary credit institution (a bridge bank) "New TT Hellenic Postbank S.A." ("**New TT**"), following a decree adopted by the Ministry of Finance⁽¹⁶⁾ on a proposal by the BoG. In that context, the HFSF covered the so-called "funding gap" of the transferred perimeter *i.e.* the difference between the fair value of the assets transferred to New TT and the nominal value of the liabilities transferred to it. Since the former is lower than the latter, New TT had received a package having a negative value, which was compensated by a grant from the HFSF. In addition, the HFSF provided initial share capital to New TT amounting to EUR 500 million, fully and immediately paid up by the HFSF. As a consequence, HFSF is the sole shareholder of New TT. TT's bank licence was terminated.
- (30) TT's sound business activities were transferred to New TT, in accordance with the recommendation of the BoG⁽¹⁷⁾. Therefore, all the contractual relationships of TT with third parties were transferred to New TT. New TT received TT assets and liabilities such as cash, retail deposits and performing loans, central bank funding, GGB and T-Bills. Overall, EUR 10.8 billion assets ("**Transferred Assets**") were transferred to New TT.
- (31) A total amount of EUR 1.2 billion net assets were left into TT. In particular, non-performing loans, tax assets and liabilities of TT, and levies and duties of any kind were included in "non-transferred" items. Those residual assets remaining in TT will be resolved through liquidation.

⁽¹⁵⁾ See the Greek law 4021/2011 on Bank Restructuring and the Law 3864/2010 on the Hellenic Financial Stability Fund. The Law 4021 of October 2011 amends the existing Greek banking legislation by providing for recovery as well as for resolution measures for credit institutions seated in Greece.

⁽¹⁶⁾ Decree 2124/B.95 of the Hellenic Republic Ministry of Finance of 18 January 2013 establishing an interim credit institution by the name of "New TT Hellenic Postbank S.A."

⁽¹⁷⁾ See Bank of Greece Resolution Measures Committee Decision 7/2/18.01.2013 on the authorisation of the interim credit institution by the name of "New TT Hellenic Postbank S.A." and Resolution Measures Committee Decision 7/3/18/01.2013 on the withdrawal of the authorization of the credit institution by name of "TT Hellenic Postbank S.A." and placing thereof under liquidation.

- (32) New TT was only fully operational as from 21 January 2013 as the operations of New TT were suspended from 4 to 21 January due to a strike of its employees. After the trade unions approved the tentative deal as regards the employment contracts, the operations of New TT could be resumed.
- (33) On 30 January 2013, New TT signed new contracts with all the employees of TT. In that context, New TT reduced its annual personnel costs on average by 30% and started with 2 998 employees of TT as well as another 358 outsourced employees, resulting in a total bank staff of 3 356. New TT has a network of 217 branches and 300 automated teller machines ("ATM").

2.3 New TT's restructuring plan

- (34) On 29 January 2013, the Greek authorities submitted an initial restructuring plan for New TT. The draft was updated in March 2013. The plan foresees the restructuring to take place between 2013 and 2017 ("the restructuring period")
- (35) The main strategic objective of New TT is to improve the bank's investor attractiveness and financial results with the aim of selling it to a third party. For that purpose, New TT's restructuring plan foresees an employee cost reduction with the implementation of a Voluntary Retirement Scheme ("**VRS**"), as well as operating cost reductions assuming a steady amount of assets.
- (36) Firstly, the VRS targets between 520 and 900 exits at a cost of approximately EUR 39 - 45 million, depending on the take-up by employees. A fully subscribed VRS would allow for annual savings of EUR 22 million. However, it is currently not clear when the VRS will be implemented. Moreover, there is still no concrete plan on the table as regards the future of the 358 outsourced staff that New TT employs.
- (37) In a base scenario assuming the implementation of the VRS, the restructuring plan foresees a steady number of employees of 2 478 during the restructuring period. According to the plan, the number of branches will also remain steady, at 197 during the same period, resulting in 12.6 employees per branch as from 2013 until 2017. 20 branches have been closed since the creation of New TT.
- (38) Secondly, regarding the reduction of operating costs, an agreement with the Hellenic Post Office has been achieved in order to reduce the network usage cost. In addition, New TT has already simplified its organizational structure, reducing its seven main divisions to five, a 29 % reduction in the number of departments. The plan also foresees a reduction in marketing and promotional costs. Non-essential on-going projects will be, or already have been, stopped.
- (39) Furthermore, New TT intends to re-price its loans and deposits in order to achieve a significant increase in its net interest income. On that basis, the plan foresees that New TT would become profitable again in 2014-2015. In the base scenario, its net interest income would

increase from EUR 132 million in 2013 to EUR 325 million in 2017, while its total operating income would increase from EUR 156 million in 2013 to EUR 339 million in 2017. New TT's personal expenses would be reduced to EUR 80 million in 2017, against equivalent expenses of EUR 149 million in 2012 for TT. Other operating costs would decrease by approximately 15 % from EUR 95 million in 2012 (compared to TT) to an annual average of EUR 80 million in the period 2015-2017. New TT's profit after tax would amount to EUR 123 million in 2017, resulting in a return on equity ("RoE") of 15.2 % in 2017.

- (40) As regards assets, New TT aims to have a relatively steady amount of total assets, of around EUR 12.5 billion during the restructuring period. New TT intends to shift its assets mix from core lending activities of mortgages and consumer loans into corporate banking. New TT's corporate lending activities are expected to double in the restructuring period, i.e. from EUR 1 billion to EUR 2.1 billion.
- (41) As regards funding, the ECB's exposure will be totally eliminated and 100 % of emergency liquidity assistance ("ELA") funding dependence will be replaced with market funding. The bank's deposit base will, on the other hand, remain stable.

2.4. Aid measures

- (42) There are four aid measures which are relevant to the situation of TT, which will be described in chronological order. Firstly, on 25 May 2009, TT got a capital injection of EUR 224.96 million (corresponding to approximately 2.9 % of the bank's RWA at that time) in the form of preference shares under the Scheme⁽¹⁸⁾ ("measure C"). The injection was made because TT's CAR amounted to 8 %, which was below the minimum threshold of 10 % set by the BoG. The measure increased TT's CAR from 8.74 % (as of March 2009) to 10.96 %.
- (43) That capital injection took the form of the issuance by TT of 60 800 000 non-voting, non-listed, non-transferable, tax deductible, non-cumulative preference shares. The issue price of EUR 3.70 for each share was fully subscribed and paid by the Hellenic Republic with bonds of equivalent value⁽¹⁹⁾. Those preference shares pay a non-cumulative dividend of 10 %, subject to meeting the minimum CAR requirements set by the BoG and to the availability of after-tax net profits or distributable reserves in accordance with article 44a of C.L. 2190/1920. During the five years following the issuance of the preference shares, the Greek Ministry of Finance could either convert the preference shares into ordinary shares in case of insufficient regulatory capital, or redeem TT's preference shares.
- (44) Secondly, on 17 December 2011, the BoG proceeded with the resolution of T Bank by ordering the transfer of its assets and liabilities to TT and withdrawing T Bank's license, in accordance with the law on resolution (Law 4021/2011). T Bank was put into liquidation. In that context, the fair value of the liabilities transferred

from T Bank to TT amounted to EUR 2 160 182 164 and the fair value of the transferred assets amounted to EUR 1 483 225 650. The difference was a so-called "funding gap" of EUR 676 956 514, which was covered by the Resolution Scheme of the HDIGF ("measure D").⁽²⁰⁾

- (45) Thirdly, on 18 January 2013, the HFSF provided New TT with its initial capital of EUR 500 million, in exchange for which the HFSF received common shares with a nominal value of EUR 1 each ("measure A").
- (46) Finally, the Transferred Activities from TT to New TT contained a funding gap of EUR 4.1 billion resulting from the difference between assets and liabilities. As a result, the HFSF, by taking over the obligations of the HDIGF (in line with the provisions of L. 4051/2012 which clarify that, as from February 2012, the HFSF will take over HDIGF's obligation), made up for that funding gap by granting EFSF bonds worth EUR 4.1 billion to New TT ("measure B"). The measure was granted on 18 January 2013.
- (47) Table 1 summarizes those four aid measures.

Table 1: Overview of the aid measures

	Nature of aid	Legal entity which formally received the aid measure	Aid amount (in EUR million)
Measure A	Recapitalisation	New TT (bridge bank)	500
Measure B	Funding gap	New TT (bridge bank)	4 100
Aid to the other entities			
Measure C	Recapitalisation	TT	224.96
Measure D	Funding gap	TT	678

3. ASSESSMENT

3.1 Existence of State aid within the meaning of Article 107(1) TFEU and quantity of State aid

- (48) The Commission has to first assess whether measures A, B, C and D constitute State aid within the meaning of Article 107 (1) TFEU. According to that provision, State aid is any aid granted by a Member State or through State resources in any form whatsoever which distorts, or threatens to distort, competition by favouring certain undertakings or the production of certain goods, in so far as it affects trade between Member States.

⁽¹⁸⁾ See footnote 1.

⁽¹⁹⁾ Under Law 3723/2008.

⁽²⁰⁾ In 2011, a resolution branch was created in the HDIGF with the adoption of the Resolution Framework in Greece. According to law 4021/2011, in the case of a transfer order: 'In case the value of the liabilities transferred to the transferee-credit institution exceeds the value of the assets transferred, the Bank of Greece shall determine the difference, to be covered as follows: a) the Depositors Branch of the HDIGF shall pay an amount equal to the value of the guaranteed deposits after deduction of the value of the transferred assets and b) the Resolution Branch of HDIGF shall pay the surplus.'

Measure A

- (49) The Commission notes that the capital injection by the HFSF into New TT, amounting to EUR 500 million (Measure A), was provided by the HFSF, an entity set up and financed by the Greek State. In the Commission decision approving the recapitalisations under the HFSF as compatible State aid ⁽²¹⁾, the Commission notes that the HFSF receives its resources from the State and its activities are considered imputable to the State. It will stay in place until 2017 and after that its profits or losses will be borne by the State. ⁽²²⁾ In the present case, the Commission similarly concludes that measure A was financed by the State or through State resources.
- (50) The Commission further notes that the capital injection provided a selective advantage to New TT, since it was a measure concerning New TT alone which enabled it to obtain capital it could not have found on the market. Given TT's precarious financial situation and the challenging economic situation in Greece which directly affects the banking sector, it is highly doubtful that any private investor would have injected capital into New TT under those conditions.
- (51) Furthermore, New TT, although a bridge bank, competes with other banks amongst which are subsidiaries and branches of foreign banks. Even if there has been a general withdrawal of foreign banks from the Greek market (e.g. sale of their Greek banking activities by Credit Agricole, Société Générale and BCP), any selective advantage may affect the timing and condition of a return of some foreign banks to the Greek market. Therefore, the capital injection may have an effect on trade and may also distort competition between the Member States.
- (52) The Commission concludes therefore that the capital injection by the HFSF into New TT constitutes State aid for the purposes of Article 107(1) TFEU.

Measure B

- (53) As regards measure B, the Commission notes that it was also granted by the HFSF. Therefore, on the basis of the above argument for measure A as described in the recital 49, the Commission considers that measure B contains State resources and is imputable to the State.

⁽²¹⁾ Commission decision of 3 September 2010 in State Aid case N 328/2010 "Recapitalisation of credit institutions in Greece under the Financial Stability Fund (FSF)", OJ C 316, 20.11.2010, p. 7.

⁽²²⁾ More specifically, recital 46 of the Commission decision of 3 September 2010 in State Aid case N 328/2010 states that: 'The qualification of a measure as State aid first of all presupposes that the aid must be imputable to the State and financed by a Member State or through State resources. Neither imputability nor the presence of State resources are put into question by the fact that the Fund is independent. It is true that according to settled case-law regarding public undertakings it is not sufficient that the State is in a position to control a public undertaking and to exercise a dominant influence over its operations, but an actual exercise of that control must exist. However, in the present case the Fund is not acting as a public undertaking and its activities cannot be considered as falling into the sphere of a commercial market operator. Instead, the Fund is solely executing a public task. In addition it can be noted that the capital of the Fund is fully and solely paid by the Greek State, all seven members of the Fund's Board shall be appointed by a decision of the Minister of Finance and the Fund shall enjoy all the administrative, financial and judicial immunities applicable to the State.'

- (54) As regards the existence of a selective advantage, it should be recalled that measure B is a grant by the HFSF to New TT that covers a funding gap between the fair value of the assets transferred from TT and the nominal value of the transferred liabilities. Because that package of assets and liabilities had a negative value of more than EUR 4 billion, if measure B had not been granted to New TT, it would not have been possible to transfer TT's activities to another legal entity. They would then have been left in the liquidated TT and hence discontinued. Measure B thus allows the continuation within New TT of the economic activities previously carried out within TT. As measure concerns the transferred activities of TT and no other market operator it is by definition selective. The Commission considers New TT to be the economic beneficiary of the measure as it harbours TT's economic activities which continue to exist thanks to measure B.
- (55) In its earlier decisions ⁽²³⁾ on resolution supported by State measures, the Commission already observed that all the key productive banking assets (employees, branches, deposits, part of the loans, as well as central services and infrastructure) were transferred to the bridge bank or to the buying bank. No private investor would have made such an investment if the funding gap was not covered.
- (56) Measure B distorts competition and affects trade for the reasons already developed in respect of measure A at recital 51. That selective advantage distorts competition by keeping the transferred activities alive and allowing them to continue competing on the market ⁽²⁴⁾, when the BoG declared TT to be unviable.
- (57) The Commission concludes therefore that the capital injection into New TT by the HFSF aimed at covering the funding gap constitutes State aid falling for the purposes of Article 107(1) TFEU.

Measure C

- (58) As regards the recapitalisation of TT in 2009 (Measure C), that capital injection was granted under the Scheme ⁽²⁵⁾. In the decision approving the Scheme, the Commission already concluded that recapitalisations granted under that Scheme would constitute State aid.

Measure D

- (59) The Commission recalls that it has already established in its decision of 16 May 2012 ⁽²⁶⁾ that measure D, the intervention by the Resolution scheme of the HDIGF in the amount of approximately EUR 0.68 billion in favour of T Bank's assets which were transferred to TT, constitutes State aid.

⁽²³⁾ See footnotes 14 and 15.

⁽²⁴⁾ See by analogy Commission decision of 25.01.2010 in the State aid case NN 19/2009 – Restructuring aid to Dunfermline Building Society, recital 51; Commission decision of 25.10.2010 in State aid case N 560/2009 – Aid for the liquidation of Fionia bank, recital 56; Commission decision of 8.11.2010 in State aid case N 392/2010 – Restructuring of CajaSur, recital 52.

⁽²⁵⁾ See footnote 1.

⁽²⁶⁾ See footnote 2.

3.2 Compatibility of the aid

3.2.1. Legal basis for the compatibility assessment

(60) Article 107(3)(b) TFEU provides the legal basis for the Commission to declare aid compatible with the internal market if it is intended “to remedy a serious disturbance in the economy of a Member State”. The Commission has acknowledged in several recent Greek State aid cases in the banking sector that there is a threat of serious disturbance in the Greek economy and that State support of banks is suitable to remedy that disturbance.⁽²⁷⁾ Despite a slow global economic recovery that has taken hold since the beginning of 2010, the Commission still considers that the requirements for State aid to be approved pursuant to Article 107(3)(b) TFEU are fulfilled in view of the reappearance of stress in financial markets. In December 2011 the Commission confirmed that view by adopting the Communication⁽²⁸⁾ on the application, from 1 January 2012, of State aid rules to support measures in favour of banks in the context of the financial crisis which prolongs the application of those State aid rules.

(61) In the light of the foregoing considerations, the Commission accepts that the capital injections by the HFSF (measure A) and the grant by the HFSF to cover the funding gap (measure B) can be analysed as State aid measures taken to avoid a serious disturbance in the economy of Hellenic Republic. In its decisions on the Scheme and on the resolution of T Bank, respectively, the Commission had already accepted that Article 107(3)(b) TFEU was the appropriate legal instrument to assess the recapitalisation of TT (measure C) and the resolution aid to T Bank (measure D).

3.2.2. Compatibility assessment

(62) The compatibility of the measures A, B, C and D with Article 107(3)(b) TFEU are assessed by the Commission in light of the Banking Communication⁽²⁹⁾, the Recapitalisation Communication⁽³⁰⁾ and the Restructuring Communication⁽³¹⁾.

(63) In line with the general principles underlying the State aid rules of the Treaty and taking into account the global financial crisis and the systemic risk associated with it, the Banking Communication (point 15) requires that all measures have to be:

- a. *Appropriate*: The aid has to be well-targeted in order to be able to achieve effectively the objective of remedying a serious disturbance in the economy;
- b. *Necessary*: The aid measure must, in its amount and form, be necessary to achieve its legitimate purpose of remedying a serious disturbance in the economy and must, therefore, not exceed the necessary minimum amount to attain that effect;
- c. *Proportionate to the challenge faced*: The distortions of competition resulting from the aid granted must be avoided or minimized as far as possible. Therefore, the aid measures must be designed in such a way as to minimize negative spill-over effects on competitors, other sectors and other Member States.

(64) The Recapitalisation Communication further details the level of remuneration required for State capital injections.

(65) Finally, the Commission should assess the measures under the Restructuring Communication, according to which a restructuring plan needs to: (i) demonstrate how the bank will restore long-term viability without State aid as soon as possible; (ii) address moral hazard by imposing appropriate own contribution (“burden-sharing”) by the aid beneficiary to the restructuring costs; as well as (iii) ensure a competitive banking sector by limiting distortions of competition resulting from the aid granted, to the minimum necessary.

3.2.3. Compatibility with the Banking and Recapitalisation Communications

(66) The Commission will first assess whether measures A and B can be temporarily approved as rescue aid. It will then review the situation as regards the compatibility of measures C and D.

a. Appropriateness of measures A and B

(67) As regards the measure A, the capital injection from the HFSF was needed in order to have capital in New TT and to enable New TT to adhere to the minimum capital adequacy ratio set by the BoG.

(68) The Commission considers that the capital injection of EUR 500 million is appropriate as rescue aid since it enabled the transfer of the economic activities of TT to New TT. Hence, the economic activities have not been wound-up. An immediate winding-up of TT’s activities could have led to a bank run and could have triggered a serious disturbance on the Greek financial markets. A serious disturbance on the Greek financial markets could be avoided through the creation of New TT and the transfer of TT’s economic activities into New TT.

(69) On that basis, the Commission finds that the measure A is appropriate as rescue aid.

(70) As regards measure B, the intervention by HFSF was needed in order to fill the gap between the fair value of TT’s assets and the nominal value of its liabilities which were transferred to New TT.

⁽²⁷⁾ Commission decision of 22 January 2013 in State aid SA.35999 (2012/N) “Prolongation of the Guarantee Scheme and the Bond Loans Scheme for Credit Institutions in Greece”, not yet published, Commission decision of 16 May 2012 “Resolution of T Bank”,

⁽²⁸⁾ Commission communication on the application, from 1 January 2012, of State aid rules to support measures in favour of banks in the context of the financial crisis, OJ C 356, 6.12.2011, p. 7

⁽²⁹⁾ Communication from the Commission - The application of State aid rules to measures taken in relation to financial institutions in the context of the current global financial crisis, OJ C 270, 25.10.2008, p. 8.

⁽³⁰⁾ Communication from the Commission - The recapitalisation of financial institutions in the current financial crisis: limitation of aid to the minimum necessary and safeguards against undue distortions of competition, OJ C 10, 15.1.2009, p. 2.

⁽³¹⁾ Commission Communication - The return to viability and the assessment of restructuring measures in the financial sector in the current crisis under the State aid rules, OJ C 195, 19.8.2009, p. 9.

- (71) The Commission considers that measure B is appropriate as rescue aid because it helps keep alive TT's economic activities which were transferred to New TT. Without measure B, those activities would not have been able to continue, as TT was on the verge of bankruptcy and in current difficult market conditions no bank would have acquired a package having a negative value (i.e. with the fair value of the assets lower than the fair value of the liabilities). The measure thereby ensures that financial stability in Greece is maintained in the short-term. On that basis, the Commission finds that the measure B is appropriate as rescue aid.
- b. *Necessity of measures A and B – limitation of the aid to the minimum*
- (72) According to the Banking Communication, the aid measure must, in its amount and form, be necessary to achieve the objective. It implies that the capital injection must be of the minimum amount necessary to reach the objective.
- (73) As regards measure A, the Commission has doubts that the amount is limited to the minimum necessary because the Member State envisages as one possible option that New TT is to be restructured on a stand-alone basis. The Commission doubts that the bank can be viable on a stand-alone basis. Hence, the Commission is of the opinion that State aid may be used for an option which is not realistic in the long-term. The Commission is of the opinion that the Hellenic Republic should also assess other options, which might be less expensive than the stand-alone option. At this stage the Commission is of the preliminary view that the stand-alone option might not be the cheapest option available and therefore it doubts that the State aid is limited to the minimum necessary. The Commission invites interested parties to provide comments on that issue.
- (74) As regards measure B, the Commission doubts that the amount exactly covers the difference between the fair value of the transferred assets and the nominal value of the transferred liabilities. That amount may be excessive. Therefore, the Commission would ask for more detailed information regarding the exact amount of assets and liabilities that were and were not transferred to New TT, as well as additional information regarding the pricing model used.
- (75) Furthermore, regarding the remuneration of measures A and B, the Commission has doubts on whether New TT will be able to sufficiently remunerate the State for the aid it received. The Commission observes that, in line with the Recapitalisation Communication, any recapitalisation of banks should, in principle, reflect the risk profile of the beneficiary, i.e. not fundamentally sound banks or, unviable banks, should pay higher remuneration than those that are fundamentally sound. The Commission notes that capital assistance to a bank which is unable to sufficiently remunerate the State for the received recapitalisation may only be accepted upon condition that (i) either the bank is wound-up, or (ii) a far-reaching restructuring plan is set-up, including a change in management and corporate governance where appropriate. In the present case, the Commission has doubts on whether New TT is a fundamentally sound bank and observes that New TT is not able to remunerate the measure A, the recapitalisation. In addition, no remuneration is foreseen for measure B, in the sense that the State did not receive any ownership rights in exchange. The coverage of the funding gap is therefore a definitive cost for the State without offsetting future revenues.
- (76) In conclusion, on a preliminary basis, the Commission considers that the forms taken by measures A and B to be necessary as rescue aid to achieve the objective of restoring financial stability in the Greek banking system and economy as a whole.
- (77) However, at this stage, the Commission doubts whether the amount of EUR 4.6 billion (measures A and B) is limited to the minimum. The Commission underlines that the absence of remuneration triggers a need for in-depth restructuring.
- c. *Proportionality of measures A and B – measures limiting negative spill-over effects*
- (78) The Commission notes that the legal entity TT will be liquidated and will exit the market. However, thanks to measures A and B, the economic activities of TT continue to exist in New TT, thereby producing negative spill-over effects. New TT should be rapidly subject to measures that will limit negative spill-over effects.
- (79) The Commission considers that measures A and B are proportionate as rescue aid in the short-term, but require measures to be introduced rapidly to ensure aid is not used to fund growth or measures not strictly necessary to restore viability.
- d. *Compatibility of measures C and D*
- (80) For measure C, the Greek authorities submitted a restructuring plan for TT Bank on 1 October 2010 in line with the requirement of the Scheme. Because of the rapid and substantial changes in the Greek banking sector since then, while there have been extensive exchanges between the Greek authorities and the Commission services, it has not yet been possible to take a final view on that restructuring plan. In the meanwhile, the situation of TT Bank has altered so significantly that the restructuring plan which was submitted in 2010 is no longer pertinent. It is therefore necessary, in line with point 16 of the Restructuring Communication, to examine measure C in light of the updated restructuring plan presented in March 2013.
- (81) In its decision of 16 May 2012, the Commission temporarily approved measure D, the resolution aid of T Bank, as compatible rescue aid for six months as from the date of adoption of that decision on the basis that the Greek authorities would submit to the Commission, within that six-month period, an updated restructuring plan for TT which took into account the integration of T Bank's activities into TT. In that decision of 16 May 2012, the Commission could not conclude that the transfer of T Bank's activities into TT allowed the restoration of their viability since TT was itself an aided bank required to submit a restructuring plan. The Commission could therefore not give a definitive approval of the aid to T Bank's activities which were transferred to TT.

- (82) The decision of 16 May 2012 further concluded that the temporary authorisation of the aid would be automatically prolonged on submission of an updated restructuring until the Commission reached a final restructuring decision on TT's restructuring plan.⁽³²⁾
- (83) The Commission first notes that no standalone restructuring plan for TT was submitted by the Greek authorities by the end of the six-month period. While the Commission regrets that omission by the Greek authorities, it accepts that delayed submission was understandable since, as indicated previously, it has been required in the meantime in the MEFP that TT be resolved. Moreover, the Greek authorities submitted a restructuring plan for New TT in January 2013 which deals with the activities transferred from T Bank to TT. It is therefore necessary to examine the compatibility of measure D as restructuring aid in light of the compliance with the Restructuring Communication of the plan submitted by the Greek authorities in January 2013 and updated in March 2013. Until the Commission has taken a final decision on measures A, B, C and D as restructuring aid, the Commission considers that Measure D can be approved provisionally as rescue aid.
- 3.2.4. *Compatibility with the Restructuring Communication*
- (84) Because measures A, B, C and D all have the effect of allowing New TT to continue to operate on the market, the Commission must assess them individually and in combination in order to ensure that, as indicated in its Restructuring Communication, the restructuring plan will restore the viability of the company within a reasonable time span, that the aid granted by the measures is limited to the minimum necessary and ensures adequate burden-sharing, and that such aid is accompanied by measures which sufficiently limit distortions of competition.
- 3.2.4.1. *Restoration of long-term viability*
- (85) Under the HFSF law, the HFSF has the obligation to sell the shares it owns in any bridge bank after a number of years. Since the obligation is only to sell the shares, it can be a sale to any type of investor. Thus the sale does not necessarily entail the integration of New TT into a larger banking group; New TT could remain a standalone bank with only change being that it would have a new shareholder, for instance, a private equity group. Given the uncertainty about the type of the future owner, the notified restructuring plan is based on the continuation of the operations of the bank on a stand-alone basis, *i.e.* not merged into a larger bank.
- (86) As the Commission has indicated in its Restructuring Communication, the restructuring plan must restore the viability of the company within a reasonable time span. In that regard, the Commission notes positively that New TT reduced on average by 30 % annual personnel costs in January 2013.
- (87) However, the Commission has doubts that New TT will be able to restore its long-term viability on a stand-alone basis, as planned in the restructuring plan submitted to the Commission.
- (88) According to the restructuring plan, New TT plans to be profitable as of 2014. However, the proposed measures to generate profits in the future are very limited. Firstly, it is not clear whether New TT will manage to further reduce its personnel. Currently, the bank seems over-staffed compared to the services New TT offers. Moreover, the implementation of the VRS is uncertain as regards the timing and the acceptance rate by the employees. In that context, the VRS targets up to 900 potential persons and New TT plans to reduce headcount by approximately 520, as described in recital (36). No further steps are proposed in the restructuring plan to reduce personnel costs. For instance, no further indications are given as regards the future of 358 outsourced staff.
- (89) As regards branches, no further closure of branches is foreseen beyond the closing of 20 branches already implemented since the creation of the bridge bank. Additionally, the branches of TT are in the main cities, especially in the Attica region. TT took over T Bank in 2011, which had a similar concentration of branches presence in the Attica region. A rationalisation of the branch network did not take place after the acquisition of T Bank. T Bank seems to remain operating as a separate entity, on a separate IT-platform as well as having a different risk management system. Therefore, the Commission has doubts whether the potential to achieve synergies has been used. It doubts that viability can be restored by keeping T Bank separate, which was itself a non-viable bank.
- (90) Beside those limited cost-cutting measures, New TT's restructuring plan foresees re-pricing of loans and deposits. New TT aims at decreasing the deposit margins on existing deposits while, at the same time, increasing loan margins on new loan production. In that respect, the restructuring plan foresees that the interest margins paid by New TT on deposits will be decreased by 150 basis points ("**bp**") during 2013-2014 and a further 60 bp during 2015-2017. Loan margins will on the other hand increase by 70bp during 2013-2017. On that basis the interest income of New TT would significantly increase from EUR 433 million in 2013 to EUR 615 million in 2017. However, the Commission doubts that such ambitious re-pricing can be successfully implemented without losing a significant amount of customers and without making risky lending.
- (91) In that respect, the Commission observes that New TT intends to double its corporate loan book. However, it is not clear how New TT intends to achieve that significant increase. In the past the corporate segment was relatively small compared to the other activities of TT because TT entered that segment only in 2009. That loan portfolio has generated significant losses since then. It is therefore doubtful whether New TT has the expertise to grow in that segment on a viable and profitable basis.
- (92) Therefore it is questionable whether New TT has the resources to achieve the increase of income planned in the restructuring plan.

⁽³²⁾ See recitals (59)-(61) from Commission decision of 16 May 2012 "Resolution of T Bank".

- (93) Net interest income is an important income driver. If New TT does not manage to achieve the planned strong growth rate, it will not achieve the planned future profits or it will generate further losses in the future.
- (94) There is therefore a risk of New TT ending up as a bridge bank, repeatedly relying on State aid.
- (95) The Commission is at this stage of the opinion that the reintegration of TT into a larger viable financial company would increase the viability prospects of New TT. It would allow significant rationalisation of costs, would facilitate the re-pricing of deposits and of new loans, and would allow a wider range of products to be offered to customers, thereby achieving higher income through cross-selling.
- (96) The Restructuring Communication provides that if a bank cannot return to viability on a stand-alone basis, viability can be restored through a sale and integration into a larger entity. In that respect, point 17 of the Restructuring Communication clarifies that *the sale of an ailing bank to another financial institution can contribute to restoring long-term viability, if the purchaser is viable and capable of absorbing the transfer of the ailing bank and may help restoring market confidence.*
- (97) In conclusion, the Commission doubts that the restructuring plan submitted to the Commission on 29 January 2013 and updated in March 2013 will restore New TT's long-term viability. It therefore doubts that measures A and B can be found compatible with the Restructuring Communication.
- (98) Since the Commission has doubts about the restoration of the long-term viability of New TT which harbours the economic activities previously carried out within TT, including T Bank, the Commission has also to open a formal investigation procedure on whether measure D (coverage of the funding gap granted to the transferred activities of T Bank) and measure C (the recapitalisation of TT in 2009) offered a long-term solution for New TT's viability and hereby invites the Greek authorities to submit further information on that subject.
- 3.2.4.2 *Burden-sharing and limitation of the aid to the minimum necessary*
- (99) The Commission has doubts that the aid is limited to the minimum. In particular, the Commission doubts that the restructuring costs are limited to the minimum, because New TT is restructured on a stand-alone basis, which inflates the restructuring costs. The Commission doubts that New TT can be made viable on a stand-alone basis without incurring high costs, in particular to develop a sustainable personnel strategy, optimize the branch network, shift its assets mix to corporate lending and integrate T Bank, which includes developing a viable IT infrastructure and risk management structure. At this stage the Commission considers that the stand-alone option might not be the cheapest option and doubts that the State aid is limited to the minimum.
- (100) Concerning burden-sharing of shareholders and subordinated debt holders, the Commission notes that the shareholders and subordinated debt holders were not transferred to New TT but have remained in the entity in liquidation. Therefore, there is a high probability that they will lose their investments. That burden-sharing reduces the aid amount needed. Hence, the Commission considers that sufficient burden-sharing of shareholders and subordinated debt holders is achieved.
- (101) As regards the remuneration of the aid, the Greek State could expect to recover only part of the capital injections by the HFSF amounting to a total of EUR 500 million (Measure A). There will be no remuneration for the HFSF for covering the funding gap between assets and liabilities (Measure B). Further there is a very small likelihood of recovering much of the amount contributed by the HFSF. It is therefore highly probable that the EUR 4.1 billion granted is definitively lost.
- (102) Therefore the Commission considers that the burden-sharing, even if it probably represents the maximum of what is feasible for that distressed bank *i.e.* New TT, does not seem to meet the Communication's requirements. If that is the case, the absence of remuneration triggers the need for in-depth restructuring, both in terms of viability measures and in terms of measures to limit distortions of competition.
- (103) The Commission observes that a large part of the losses incurred in the last years stems from a waiver of debt in favour of the State *i.e.* through the PSI and through the sale of GGB to the State at a deep discount to par at the end of 2012. Those measures could be considered as equivalent to a payment by the bank to the State and therefore justify a lower remuneration on the subsequent recapitalisation aid granted by the State to cover the capital holes stemming from the debt waiver in favour of the State. The Member State authorities and interested parties are invited to comment on that view.
- 3.2.4.3 *Distortion of competition*
- (104) New TT has received EUR 4.6 billion of aid (EUR 0.5 billion in form of capital and 4.1 billion in form of "funding gap" coverage) which is a considerable amount of aid. That aid represents more than 70% of TT's RWA and more than 90% of New TT's RWA. Further the Commission notes that TT (which is the legal entity which previously performed the activities which are now harboured in New TT) had received aid in the past: TT received under the Scheme⁽³³⁾ a first capital injection of EUR 224.96 million in form of preference shares (measure C). Furthermore, on the resolution of T Bank, the transferred activities of T Bank, which were transferred to TT, received a resolution aid of approximately EUR 678 million (measure D). Such amounts of aid normally call for a deep restructuring and reduction of the market presence of the bank. Those requirements are even more acute if there is no remuneration of the aid, most of which will never be recovered. At the same time, a significant part of the losses which the bank incurred in recent years do not seem to stem from

⁽³³⁾ See footnote 1.

risk-taking activities but from the holding of government bonds. That factor may justify the view that the aid is creating fewer distortions of competition. However, it has also to be observed that TT was holding proportionally to its size far more GGBs than the other banks in Greece. At this stage, the Commission considers that apparently excessive investment in GGBs could reflect some inappropriate risk-taking. The authorities and interested parties are invited to comment on that view.

- (105) In terms of market presence, the Commission observes that the creation of the bridge bank is not a real resolution of TT as the restructuring plan of New TT foresees that New TT remains on the market nearly as TT was before.
- (106) TT was a medium-sized bank in Greece (approximately 6 % in terms of deposits). TT's assets and liabilities transferred into New TT are relatively small when compared with the size of the Greek banking system. Also, the bank has no foreign activities. Therefore, despite the exceptionally large aid amount, the distortions of competition caused by the aid to New TT could be considered to be rather limited.
- (107) However, to limit the risk that New TT would offer interest rates on deposits which are much higher than the interest rates on deposits of most of the competitors, a price leadership ban may be contemplated for New TT. Such a price leadership ban would decrease the probability that New TT uses the State aid to pay high interest rates and distorts competition on the market for deposits. Furthermore, to ensure that New TT does not expand its business and to limit the competition distortions, the Commission is of the view that some behavioural measures such as an acquisition ban and a ban on strong growth in lending would seem necessary.
- (108) At this stage, the Commission therefore doubts that sufficient measures are taken to limit undue distortions of competition.

3.3 Conclusion

- (109) In the light of the foregoing considerations, the Commission decides that measures A, B, C and D constitute State aid within the meaning of Article 107(1) TFEU and approves them provisionally as rescue aid. It doubts that those measures may be found compatible with the internal market pursuant to Article 107(3)(b) TFEU as restructuring aid, as they do not seem to comply with the requirements of the Restructuring Communication.

The Commission has accordingly decided to consider the aid to be temporarily compatible with the internal market within the meaning of Article 107(1) TFEU. Moreover, and in the light of the foregoing considerations, the Commission, acting under the procedure laid down in Article 108(2) of the TFEU, requests the Hellenic Republic to submit its comments and to provide all such information as may help to assess the restructuring aid, within one month of the date of receipt of this letter. In particular, it requests the Hellenic Republic to submit a new restructuring plan for New TT which addresses the Commission's doubts expressed in this decision. It requests your authorities to forward a copy of this letter to the potential recipient of the aid immediately.

The Commission wishes to draw the attention of the Hellenic Republic to Article 14 of Council Regulation (EC) No 659/1999, which provides that all unlawful aid may be recovered from the recipient.

Finally, the Commission warns the Hellenic Republic that it will inform interested parties by publishing this letter and a meaningful summary of it in the *Official Journal of the European Union*. It will also inform interested parties in the EFTA countries which are signatories to the EEA Agreement, by publication of a notice in the EEA Supplement to the *Official Journal of the European Union* and will inform the EFTA Surveillance Authority by sending a copy of this letter. All such interested parties will be invited to submit their comments within one month of the date of such publication.»

Preço das assinaturas 2013 (sem IVA, portes para expedição normal incluídos)

Jornal Oficial da União Europeia, séries L + C, só edição impressa	22 línguas oficiais da UE	1 300 EUR por ano
Jornal Oficial da União Europeia, séries L + C, edição impressa + DVD anual	22 línguas oficiais da UE	1 420 EUR por ano
Jornal Oficial da União Europeia, série L, só edição impressa	22 línguas oficiais da UE	910 EUR por ano
Jornal Oficial da União Europeia, séries L + C, DVD mensal (cumulativo)	22 línguas oficiais da UE	100 EUR por ano
Suplemento do Jornal Oficial (série S), Adjudicações e Contratos Públicos, DVD, uma edição por semana	Multilíngue: 23 línguas oficiais da UE	200 EUR por ano
Jornal Oficial da União Europeia, série C — Concursos	Língua(s) de acordo com o concurso	50 EUR por ano

O *Jornal Oficial da União Europeia*, publicado nas línguas oficiais da União Europeia, pode ser assinado em 22 versões linguísticas. Compreende as séries L (Legislação) e C (Comunicações e Informações).

Cada versão linguística constitui uma assinatura separada.

Por força do Regulamento (CE) n.º 920/2005 do Conselho, publicado no Jornal Oficial L 156 de 18 de junho de 2005, nos termos do qual as instituições da União Europeia não estão temporariamente vinculadas à obrigação de redigir todos os seus atos em irlandês nem a proceder à sua publicação nessa língua, os Jornais Oficiais publicados em irlandês são comercializados à parte.

A assinatura do Suplemento do Jornal Oficial (série S — Adjudicações e Contratos Públicos) reúne a totalidade das 23 versões linguísticas oficiais num DVD multilíngue único.

A pedido, a assinatura do *Jornal Oficial da União Europeia* dá direito à receção dos diversos anexos do Jornal Oficial. Os assinantes são avisados da publicação dos anexos através de um «Aviso ao leitor» inserido no *Jornal Oficial da União Europeia*.

Vendas e assinaturas

As subscrições de diversas publicações periódicas pagas, como a subscrição do *Jornal Oficial da União Europeia*, estão disponíveis através da nossa rede de distribuidores comerciais, cuja lista está disponível na Internet no seguinte endereço:

http://publications.europa.eu/others/agents/index_pt.htm

EUR-Lex (<http://eur-lex.europa.eu>) oferece acesso direto e gratuito ao direito da União Europeia. Este sítio permite consultar o *Jornal Oficial da União Europeia* e inclui igualmente os tratados, a legislação, a jurisprudência e os atos preparatórios da legislação.

Para mais informações sobre a União Europeia, consultar: <http://europa.eu>

