Articolo 18

Denuncia

1 — Ciascuno Stato Contraente ha il diritto di denunciare l'Accordo. A tal fine, una comunicazione scritta di denuncia dovrà essere consegnata all'altro Stato Contraente e che avrà effetto sei mesi dopo la data del rispettivo ricevimento.

2 — Nonostante la denuncia del presente Accordo, tutte le informazioni classificate fornite sulla base del presente Accordo dovranno continuare ad essere protette in conformità alle disposizioni qui definite. Inoltre, speciali categorie di informazioni o materiali classificate, determinate di concerto tra le Autorità Nazionali per la Sicurezza degli Stati Contraenti e conformemente designate come tali, saranno restituite allo Stato Contraente originatore, su richiesta di quest'ultimo.

Articolo 19

Modifiche

1 — Ciascuno Stato Contraente dovrà prontamente notificare all'altro Stato Contraente qualsiasi cambiamento alle sue Leggi e ai suoi regolamenti che possa avere effetti sulla tutela delle informazioni classificate in base al presente Accordo. In tal caso, gli Stati Contraenti dovranno consultarsi per prendere in considerazione eventuali modifiche all'Accordo. Nel frattempo, le informazioni classificate continueranno ad essere protette come qui descritto, a meno che non sia diversamente richiesto per iscritto dallo Stato Contraente che le ha cedute.

2 — Modifiche od emendamenti al presente Accordo verranno apportate in base alle procedure previste per la firma e l'entrata in vigore del presente Accordo.

In fede di che i sottoscritti Rappresentanti, debitamente autorizzati dai rispettivi Governi, hanno firmato il presente Accordo.

Fatto a Roma il 17 ottobre 2007, in duplice esemplare, nelle lingue portoghese e italiana, entrambe facenti egualmente fede.

Per la Repubblica Portoghese:

Vasco Valente, ambasciatore straordinario e plenipotenziario del Portogallo a Roma.

Per la Repubblica Italiana:

General C. A. *Giuseppe Cucchi,* Autorità Nazionale per la Sicurezza.

Decreto n.º 42/2008

de 10 de Outubro

Considerando que o presente Acordo permitirá garantir a segurança de toda a informação que tenha sido classificada pela autoridade competente de cada Parte, ou por solicitação desta, e que tenha sido transmitida para a outra Parte através das autoridades ou organismos expressamente autorizados para esse efeito, quer para o cumprimento das atribuições da Administração Pública, quer no quadro de outros instrumentos contratuais envolvendo entidades públicas ou privadas de ambos os países;

Considerando que o presente Acordo visa estabelecer padrões mínimos, comuns, de medidas de segurança, aplicáveis a todas as negociações, acordos de cooperação ou outros instrumentos contratuais que impliquem troca de informação classificada;

Atendendo que a vigência do presente Acordo permitirá às empresas portuguesas credenciadas pela Autoridade Nacional de Segurança habilitar-se a participar em concursos públicos que envolvam informação classificada, na Estónia;

Assim:

Nos termos da alínea *c*) do n.º 1 do artigo 197.º da Constituição, o Governo aprova o Acordo para a Protecção de Informação Classificada entre a República Portuguesa e a República da Estónia, assinado em Lisboa em 29 de Novembro de 2005, cujo texto, nas versões autenticadas nas línguas portuguesa, estoniana e inglesa, se publica em anexo.

Visto e aprovado em Conselho de Ministros de 7 de Agosto de 2008. — *José Sócrates Carvalho Pinto de Sousa — Luís Filipe Marques Amado — Manuel Pedro Cunha da Silva Pereira.*

Assinado em 15 de Setembro de 2008.

Publique-se.

O Presidente da República, Aníbal Cavaco Silva.

Referendado em 16 de Setembro de 2008.

O Primeiro-Ministro, *José Sócrates Carvalho Pinto de Sousa.*

ACORDO PARA A PROTECÇÃO DE INFORMAÇÃO CLASSIFICADA ENTRE A REPÚBLICA PORTUGUESA E A REPÚBLICA DA ESTÓNIA

A República Portuguesa e a República da Estónia, doravante designadas por Partes:

Reconhecendo a necessidade das Partes em garantir a protecção de informação classificada trocada entre as Partes, pessoas singulares ou colectivas, no âmbito de acordos de cooperação ou contratos celebrados ou a celebrar;

Desejando estabelecer um conjunto de regras sobre a protecção mútua da informação classificada trocada entre as Partes;

acordam o seguinte:

Artigo 1.º

Objecto

O presente Acordo estabelece as regras de segurança aplicáveis a todos os acordos de cooperação ou contratos que prevejam a transmissão de informação classificada, celebrados ou a celebrar pelas autoridades nacionais competentes das Partes ou por pessoas singulares ou colectivas autorizadas para esse efeito.

Artigo 2.º

Âmbito de aplicação

1 — O presente Acordo estabelece os procedimentos a adoptar para a protecção de informação classificada trocada entre as Partes.

2 — O presente Acordo não é aplicável à cooperação directa entre os serviços de informações.

Artigo 3.º

Definições

Para os efeitos do presente Acordo:

a) «Informação classificada» designa a informação, os documentos e materiais, independentemente da sua forma, natureza e meios de transmissão, aos quais tenha sido atribuído um grau de classificação de segurança e que requeiram protecção contra divulgação não autorizada;

b) «Autoridade nacional de segurança» designa a autoridade designada por cada Parte como responsável pela aplicação e supervisão do presente Acordo;

c) «Parte transmissora» designa a Parte que entrega ou transmite informação classificada à outra Parte;

d) «Parte destinatária» designa a Parte à qual é entregue ou transmitida informação classificada pela Parte transmissora;

e) «Terceira Parte» designa qualquer organização internacional ou Estado, incluindo os seus cidadãos e pessoas colectivas, e que não é Parte no presente Acordo;

f) «Contratante» designa uma pessoa singular ou colectiva possuidora de capacidade legal para celebrar contratos;

g) «Contrato classificado» designa qualquer acordo entre dois ou mais contratantes que estabelece e define direitos e obrigações entre eles e que contém ou envolve informação classificada;

h) «Credenciação de segurança do pessoal» designa a determinação feita pela autoridade nacional de segurança ou outra entidade competente de que um indivíduo está habilitado para ter acesso a informação classificada, de acordo com o direito interno;

i) «Credenciação de segurança industrial» designa a determinação feita pela autoridade nacional de segurança ou outra entidade competente de que, sob o ponto de vista da segurança, uma entidade tem capacidade física e organizacional para manusear e guardar informação classificada, de acordo com o respectivo direito interno;

j) «Necessidade de conhecer» designa que o acesso à informação classificada que só pode ser concedido à pessoa que tenha comprovada necessidade de a conhecer, ou de a possuir, para cumprimento das suas funções oficiais e profissionais, de acordo com o propósito para o qual a informação foi entregue ou transmitida à Parte destinatária;

k) «Instrução de segurança do projecto» designa uma compilação de requisitos de segurança, que são aplicados a um determinado projecto para garantir a uniformização nos procedimentos de segurança;

l) «Guia de classificação de segurança do projecto» designa a parte da instrução de segurança do projecto que identifica os elementos do projecto que são classificados, especificando os respectivos níveis de classificação de segurança.

Artigo 4.º

Autoridades nacionais de segurança

1 — As Autoridades Nacionais de Segurança são:

Pela República Portuguesa — Autoridade Nacional de Segurança, Presidência do Conselho de Ministros, Avenida da Ilha da Madeira, 1, 1400-204 Lisboa, Portugal;

Pela República da Estónia — Departamento de Segurança, Ministério da Defesa, Rua Sakala, 1, 15094 Tallinn, Estónia.

2 — As Partes informar-se-ão mutuamente, por via diplomática, de qualquer alteração relativa às suas autoridades nacionais de segurança.

Artigo 5.º

Princípios de segurança

1 — A protecção e utilização de informação classificada trocada entre as Partes rege-se pelos seguintes princípios:

a) As Partes atribuirão a toda a informação classificada transmitida, produzida ou desenvolvida o mesmo grau de segurança atribuído à sua própria informação classificada de grau equivalente;

b) O acesso à informação classificada é limitado às pessoas que tenham necessidade de conhecer e que, no caso de informação classificada como Confidencial/Konfidentsiaalne ou superior, estejam habilitadas com uma credenciação de segurança do pessoal emitida pelas autoridades competentes.

2 — Com o objectivo de se obterem e manterem padrões de segurança comparáveis, as autoridades nacionais de segurança deverão, sempre que solicitado, disponibilizar mutuamente informação sobre os seus padrões de segurança, procedimentos e práticas para a protecção de informação classificada.

Artigo 6.º

Classificação de segurança

1 — As Partes acordam que os graus de classificação de segurança seguintes são equivalentes e correspondem aos graus de classificação segurança especificados no respectivo direito interno de cada uma das Partes:

República Portuguesa	República da Estónia	Equivalente em inglês
Muito secreto	Täiesti salajane	Top secret.
Secreto	Salajane	Secret.
Confidencial	Konfidentsiaalne	Confidential.
Reservado	Piiratud	Restricted.

2 — A Parte destinatária marcará a informação classificada recebida com as suas próprias marcas de classificação de segurança equivalentes, em conformidade com as equivalências referidas no n.º 1 do presente artigo.

3 — As Partes informar-se-ão mutuamente sobre as alterações ulteriores dos graus de classificação da informação classificada transmitida.

4 — A Parte destinatária não poderá baixar o grau de classificação de segurança ou desclassificar a informação classificada recebida, sem prévia autorização escrita da Parte transmissora.

Artigo 7.º

Credenciação de segurança

1 — Se solicitado, as Partes, através das suas autoridades nacionais de segurança, tendo em conta o respectivo direito interno, colaborará com a outra no decurso dos procedimentos para a credenciação de segurança das suas pessoas singulares ou colectivas que residam ou estejam localizadas no território da outra Parte, precedendo a emissão

da credenciação de segurança do pessoal e da credenciação de segurança industrial.

2 — Cada Parte reconhecerá a credenciação de segurança do pessoal e a credenciação de segurança industrial emitidas de acordo com o direito interno da outra Parte. A equivalência dos graus de classificação de segurança será feita em conformidade com o artigo 6.º do presente Acordo.

3 — As autoridades nacionais de segurança informar-se-ão mutuamente sobre quaisquer alterações relativas à credenciação de segurança do pessoal e à credenciação de segurança industrial, designadamente no caso de cancelamento ou abaixamento do grau de classificação de segurança atribuído.

Artigo 8.º

Tradução, reprodução e destruição

1 — A informação classificada marcada como Secreto/Salajane ou superior só poderá ser reproduzida ou traduzida após autorização escrita da autoridade nacional de segurança da Parte transmissora.

2 — As traduções e as reproduções de informação classificada deverão obedecer aos seguintes procedimentos:

a) As pessoas envolvidas deverão ser titulares de credenciação de segurança do pessoal de acordo com o artigo 5.º;

b) As traduções e reproduções serão marcadas e protegidas da mesma forma que a informação original;

c) As traduções e o número de cópias a efectuar deverão ser limitadas às requeridas para uso oficial;

d) As traduções deverão ter a indicação, na língua para que foram traduzidas, de que contêm informação classificada recebida da Parte transmissora.

3 — A informação classificada marcada como Muito secreto/Täiesti salajane não poderá ser destruída, devendo ser devolvida à autoridade nacional de segurança da Parte transmissora.

4 — A destruição de informação classificada marcada como Secreto/Salajane será notificada à autoridade nacional de segurança da Parte transmissora.

5 — A informação classificada marcada até Confidencial/Konfidentsiaalne, inclusive, deverá ser destruída de acordo com o respectivo direito interno.

6 — No caso de uma situação de crise que torne impossível proteger ou devolver informação classificada criada ou transferida de acordo com o presente Acordo, esta deverá ser destruída imediatamente. A Parte destinatária deverá notificar a autoridade nacional de segurança da Parte transmissora acerca da destruição da informação classificada com a maior brevidade possível.

Artigo 9.º

Transmissão de informação classificada

1 — A informação classificada será transmitida entre as Partes através de canais aprovados conjuntamente pelas autoridades nacionais de segurança.

2 — As Partes podem transmitir informação classificada por meios electrónicos, de acordo com os procedimentos de segurança aprovados conjuntamente pelas autoridades nacionais de segurança.

3 — A transmissão de informação classificada volumosa ou em grande quantidade será aprovada em cada caso por ambas as autoridades nacionais de segurança.

4 — A Parte destinatária confirmará, por escrito, a recepção de informação classificada e transmiti-la-á aos utilizadores.

Artigo 10.º

Uso e cumprimento

1 — A informação classificada transmitida só poderá ser utilizada para os fins que foi transmitida.

2 — Cada Parte informará as suas pessoas singulares e colectivas da existência do presente Acordo, sempre que esteja envolvida informação classificada.

3 — Cada Parte assegurará que todas as pessoas singulares e colectivas, que recebam informação classificada, respeitem as obrigações do presente Acordo.

4 — A Parte destinatária não transmitirá informação classificada a uma terceira Parte sem autorização prévia escrita da Parte transmissora.

Artigo 11.º

Medidas de segurança para contratos classificados

1 — Uma Parte que pretenda celebrar um contrato classificado com um contratante da outra Parte, ou que pretenda autorizar um dos seus contratantes a efectuar um contrato classificado no território da outra Parte, no âmbito de um projecto classificado, obterá, através da respectiva autoridade nacional de segurança, garantia escrita prévia da autoridade nacional de segurança da outra Parte, em como o contratante é detentor de uma credenciação de segurança industrial com o grau de classificação de segurança adequado.

2 — O contratante obriga-se a:

a) Assegurar que as suas instalações estão em condições de proteger correctamente a informação classificada;

b) Estar habilitado com a classificação de segurança apropriada;

c) Garantir o grau de classificação de segurança do pessoal adequado às pessoas que necessitem ter acesso a uma dada informação classificada;

d) Assegurar que todas as pessoas que tenham acesso a informação classificada estejam informadas das suas responsabilidades sobre protecção de informação classificada, em conformidade com o direito interno;

e) Permitir inspecções de segurança às suas instalações.

3 — Qualquer subcontratante deverá cumprir as mesmas obrigações de segurança que o contratante.

4 — A autoridade nacional de segurança detém a competência para assegurar o cumprimento pelo contratante das disposições previstas no n.º 2 do presente artigo.

5 — Logo que sejam desencadeadas negociações pré-contratuais entre pessoas singulares ou colectivas que residam ou estejam situadas no território de uma das Partes e outras pessoas singulares ou colectivas que residam ou estejam situadas no território da outra Parte para a celebração de actos contratuais classificados, a autoridade nacional de segurança em cujo território será cumprido o contrato informará a outra Parte sobre a classificação de segurança atribuída à informação classificada relacionada com o contrato em negociação.

6 — Qualquer contrato classificado celebrado entre pessoas singulares ou colectivas das Partes, nos termos do presente Acordo, deverá incluir uma instrução de segurança do projecto identificando os seguintes aspectos:

a) Guia de classificação de segurança do projecto e lista da informação classificada;
b) Procedimentos para a comunicação de alterações à classificação de segurança;
c) Canais de comunicação e meios de transmissão electrónica;
d) Procedimento para o transporte de informação classificada;
e) Autoridades responsáveis pela coordenação e salvaguarda de informação classificada relacionada com o contrato classificado;
f) Obrigatoriedade de notificação de qualquer comprometimento ou suspeita de comprometimento de informação classificada.

7 — Deverá ser enviada cópia da instrução de segurança do projecto de qualquer contrato classificado à autoridade nacional de segurança da Parte em cujo território o contrato classificado será cumprido, por forma a garantir adequada supervisão de segurança e controlo.
8 — Os representantes das autoridades nacionais de segurança podem efectuar visitas mútuas a fim de verificarem a eficácia das medidas adoptadas pelo contratante na protecção de informação classificada relativa ao contrato classificado. O aviso da visita deverá ser efectuado com uma antecedência mínima de 30 dias.

Artigo 12.º

Visitas

1 — As visitas que envolvam acesso a informação classificada por cidadãos de uma Parte à outra Parte estão sujeitas a autorização prévia escrita conferida pela autoridade nacional de segurança da Parte anfitriã.
2 — As visitas que envolvam acesso a informação classificada serão autorizadas por uma Parte aos visitantes da outra Parte, apenas se estes:

a) Possuírem credenciação de segurança do pessoal apropriada concedida pela autoridade nacional de segurança ou outra autoridade relevante da Parte visitante; e
b) Estiverem autorizados a receber ou a ter acesso a informação classificada fundamentado na necessidade de conhecer, de acordo com o direito interno.

3 — A autoridade nacional de segurança da Parte visitante notificará a visita planeada à autoridade competente da Parte anfitriã, endereçando um pedido de visita com uma antecedência mínima de 30 dias anterior à data prevista para a visita.
4 — Em casos urgentes, o pedido de visita poderá ser efectuado com uma antecedência mínima de sete dias.
5 — O pedido de visita deverá incluir:

a) O nome e o apelido do visitante, a data e o local de nascimento, nacionalidade e o número do passaporte ou bilhete de identidade;
b) O nome da entidade que o visitante representa ou a que pertence;
c) Nome e morada da entidade a visitar;
d) Certificação da credenciação de segurança do pessoal do visitante e a respectiva validade;
e) Objecto e propósito da visita ou visitas;
f) A data prevista para a visita ou visitas e respectiva duração, e, em caso de visitas recorrentes, deverá ser referido o período total das visitas;
g) Nome e número de telefone do contacto da instituição ou instalação a visitar, os contactos prévios e qualquer outra informação que seja útil para justificar a visita ou visitas;
h) A data, a assinatura e a aposição do selo oficial da autoridade nacional de segurança.

6 — A autoridade nacional de segurança da Parte que recebe o pedido de visita examina e decide sobre o pedido e informa da sua decisão a autoridade nacional de segurança da Parte requerente.
7 — As vistas de pessoas de uma terceira Parte que impliquem acesso a informação classificada da Parte transmissora apenas serão autorizadas mediante consentimento escrito da autoridade nacional de segurança da Parte transmissora.
8 — Uma vez aprovada a visita, a autoridade nacional de segurança da Parte anfitriã fornecerá cópia do pedido de visita ao encarregado de segurança da entidade a ser visitada.
9 — A validade da autorização da visita não deverá exceder os 12 meses.
10 — Para qualquer projecto ou contrato, as autoridades nacionais de segurança podem acordar em elaborar listas de pessoas autorizadas a efectuar visitas recorrentes. Essas listas são válidas por um período inicial de 12 meses.
11 — Após aprovação das listas pelas autoridades nacionais de segurança, os termos das visitas específicas serão directamente acordados com os representantes das entidades a serem visitadas, nos termos do presente Acordo.

Artigo 13.º

Comprometimento da informação classificada

1 — Em caso de quebra de segurança que resulte em comprometimento ou suspeita de comprometimento de informação classificada com origem ou recebida da outra Parte, a autoridade nacional de segurança da Parte onde ocorra a quebra de segurança ou comprometimento de informação classificada informará prontamente a autoridade nacional de segurança da outra Parte e instaurará a correspondente investigação.
2 — Se a quebra de segurança ou comprometimento de informação classificada ocorrer num outro Estado que não o das Partes, a autoridade nacional de segurança da Parte transmissora actuará em conformidade com o n.º 1 do presente artigo.
3 — A outra Parte, se necessário, colaborará na investigação.
4 — Em qualquer caso, a outra Parte será informada, por escrito, dos resultados da investigação, incluindo a indicação das razões da quebra e comprometimento de segurança, a extensão dos danos e as conclusões da investigação.

Artigo 14.º

Encargos

Cada Parte assumirá os encargos que para si advenham da aplicação e supervisão do presente Acordo.

Artigo 15.º

Solução de controvérsias

Qualquer diferendo sobre a interpretação ou a aplicação das medidas previstas no presente Acordo será resolvido por via diplomática.

Artigo 16.º

Revisão

1 — O presente Acordo pode ser objecto de revisão a pedido de qualquer das Partes.

2 — As emendas entrarão em vigor nos termos previstos no artigo 18.º do presente Acordo.

Artigo 17.º

Vigência e denúncia

1 — O presente Acordo permanecerá em vigor por um período indeterminado.

2 — Qualquer das Partes poderá, a qualquer momento, denunciar o presente Acordo.

3 — A denúncia deverá ser notificada, por escrito e por via diplomática, produzindo efeitos seis meses após a data da recepção da respectiva notificação.

4 — Em caso de denúncia, a informação classificada trocada na vigência do presente Acordo continuará a ser tratada em conformidade com as disposições do mesmo, até que a Parte transmissora dispense a Parte destinatária dessa obrigação.

Artigo 18.º

Entrada em vigor

1 — Cada uma das Partes notificará a outra, por escrito e por via diplomática, que todos os procedimentos internos necessários para a entrada em vigor do presente Acordo foram cumpridos.

2 — O presente Acordo entrará em vigor no 30.º dia após a recepção da última das notificações referidas no n.º 1 do presente artigo.

Em fé do que, os signatários, devidamente autorizados para o efeito, assinam o presente Acordo.

Feito em Lisboa, aos 29 de Novembro de 2005, em dois originais, em português, estónio e inglês, fazendo qualquer dos textos igualmente fé. Em caso de divergência de interpretação, o texto em inglês prevalecerá.

Pela República Portuguesa:

Fernando Manuel de Mendonça d'Oliveira Neves, Secretário de Estado dos Assuntos Europeus.

Pela República da Estónia:

Heiki Loot, Secretário de Estado.

PORTUGALI VABARIIGI JA EESTI VABARIIGI SALASTATUD TEABE KAITSE KOKKULEPE

Portugali Vabariik ja Eesti Vabariik, edaspidi «pooled»:

tunnistades, et nad peavad tagama poolte ja nende füüsiliste või juriidiliste isikute vahel sõlmitud või sõlmitavate koostöökokkulepete või lepingute alusel vahetatava salastatud teabe kaitse;

soovides sätestada poolte vahetatava salastatud teabe vastastikuse kaitsmise korra;

on kokku leppinud järgmises:

Artikkel 1

Eesmärk

Kokkuleppega kehtestatakse salastatud teabe kaitse kord, mida kohaldatakse poolte pädevate asutuste või füüsiliste või juriidiliste isikute vahel sõlmitud või sõlmitavate koostöökokkulepete või lepingute suhtes, millega nähakse ette salastatud teabe vahetamine.

Artikkel 2

Kohaldamisala

1 — Kokkuleppega sätestatakse poolte vahetatava salastatud teabe kaitse kord.

2 — Kokkulepet ei kohaldata poolte julgeolekuasutuste otsekoostöö suhtes.

Artikkel 3

Mõisted

Kokkuleppes kasutatakse järgmisi mõisteid:

a) salastatud teave — teave, dokument või materjal, mida selle vormist, laadist ja edastamisviisist olenemata on vaja kaitsta loata avalikustamise eest ja millele on määratud salastatuse tase;

b) riigi julgeoleku volitatud esindaja — asutus, mille kumbki pool on määranud vastutavaks käesoleva kokkuleppe täitmise ja selle järelevalve eest;

c) päritolupool — pool, kes annab või edastab salastatud teavet teisele poolele;

d) vastuvõttev pool — pool, kellele päritolupool annab või edastab salastatud teavet;

e) kolmas isik — rahvusvaheline organisatsioon või riik, sealhulgas selle kodanikud ja juriidilised isikud, kes ei ole käesoleva kokkuleppe pool;

f) lepinglane — füüsiline või juriidiline isik, kellel on õigus sõlmida lepinguid;

g) salastatud leping — kahe või enama lepinglase kokkulepe, millega nähakse ette nende õigused ja kohustused ning mis sisaldab salastatud teavet või on sellega seotud;

h) füüsilise isiku juurdepääsuluba — riigi julgeoleku volitatud esindaja või muu pädeva asutuse poolt tehtud otsus, et füüsilisel isikul on salastatud teabele juurdepääsu õigus kooskõlas riigisiseste õigusaktidega;

i) juriidilise isiku juurdepääsuluba — riigi julgeoleku volitatud esindaja või muu pädeva asutuse otsus, et juriidiline isik on julgeolekust lähtudes reaalselt ja organisatsioooniliselt võimeline kasutama ja hoidma salastatud teavet kooskõlas riigisiseste õigusaktidega;

j) põhjendatud teadmisvajadus — salastatud teabele juurdepääsu võimaldamine üksnes isikule, kellel on tõestatud vajadus saada sellist teavet oma teenistus- ja ametikohustuste täitmiseks, milleks teave vastuvõtvale poolele anti või edastati;

k) projekti julgeolekueeskiri — julgeolekunõuded, mida kohaldatakse konkreetse projekti suhtes julgeolekukorra standardimiseks;

l) projekti salastamisjuhend — projekti julgeolekueeskirja see osa, milles määratakse projekti salastatud osad ja nende salastatuse tasemed.

Artikkel 4

Riigi julgeoleku volitatud esindaja

1 — Riikide julgeoleku volitatud esindajad on järgmised:

Portugali Vabariigis:
Riigi julgeoleku volitatud esindaja
Ministrite nõukogu eesistuja
Av. Ilha da Madeira, 1
1400-204 Lisbon
Portugal;
Eesti Vabariigis:
Julgeolekuosakond
Kaitseministeerium
Sakala 1
15094 Tallinn
Eesti.

2 — Pooled teatavad teineteisele diplomaatiliste kanalite kaudu oma julgeoleku volitatud esindajaid puudutavatest muudatustest.

Artikkel 5

Julgeolekupõhimõtted

1 — Poolte vahetatava salastatud teabe kaitsmisel ja kasutamisel kehtivad järgmised põhimõtted:

a) pooled tagavad kogu edastatud, koostatud või väljatöötatud salastatud teabele samasuguse kaitse nagu oma samaväärsel tasemel salastatud teabele;
b) juurdepääs salastatud teabele võimaldatakse üksnes isikutele, kellel on põhjendatud teadmisvajadus; teabe puhul, mille salastatuse tase on Confidencial/Konfidentsiaalne või kõrgem, isikutele, kellel on pädevate asutuste väljastatud kehtiv juurdepääsuluba.

2 — Võrreldaval tasemel kaitstuse saavutamiseks ja säilitamiseks annavad riikide julgeoleku volitatud esindajad asjakohase taotluse korral teineteisele teavet oma salastatud teabe kaitsmise õigusaktide, menetluskorra ja tavade kohta.

Artikkel 6

Salastatuse tasemed

1 — Poolte kokkuleppel on järgmised salastatuse tasemed võrdväärsed ning vastavad nende riigisiseste õigusaktidega määratud salastatuse tasemetele:

Portugali Vabariik	Eesti Vabariik	Ingliskeelne vaste
Muito secreto	Täiesti salajane.	Top secret.
Secreto	Salajane	Secret.
Confidencial.	Konfidentsiaalne . . .	Confidential.
Reservado.	Piiratud.	Restricted.

2 — Vastuvõttev pool märgistab saadud salastatud teabe lõike 1 kohaselt salastatuse taseme omakeelse vastega.
Pooled teatavad teineteisele kõigist edastatud teabe salastatuse taseme muudatustest.

3 — Vastuvõttev pool ei alanda saadud teabe salastatuse taset ega kustuta teabe salastatust ilma päritolupoole eelneva kirjaliku nõusolekuta.

Artikkel 7

Juurdepääsuload

1 — Pooled aitavad oma julgeoleku volitatud esindajate kaudu asjakohase taotluse korral ja oma õigusaktidest lähtudes enne füüsiliste ja juriidiliste isikute juurdepääsulubade väljastamist teineteisel kontrollida oma riigi füüsilisi ja juriidilisi isikuid, kes elavad või asuvad teise poole territooriumil.
2 — Pooled tunnustavad teise poole õigusaktide kohaselt väljastatud füüsiliste ja juriidiliste isikute juurdepääsulube. Juurdepääsulubade tasemed peavad olema kooskõlas artikliga 6.
3 — Riikide julgeoleku volitatud esindajad teatavad teineteisele kõigist muudatustest seoses asjaomaste füüsiliste ja juriidiliste isikute juurdepääsulubadega, eeskätt nende tühistamisest või nende taseme alandamisest.

Artikkel 8

Tõlkimine, paljundamine ja hävitamine

1 — Teavet, mille salastatuse tase on Secreto/Salajane või kõrgem, paljundatakse ja tõlgitakse ainult päritolupoole julgeoleku volitatud esindaja kirjalikul loal.
2 — Salastatud teavet tõlgitakse ja paljundatakse järgmise korra kohaselt:

a) asjaomastel isikutel peab olema artikli 5 nõuete kohane füüsilise isiku juurdepääsuluba;
b) tõlked ja paljundused märgistatakse ja kaitstakse võrdselt originaaliga;
c) tõlkeid ja paljundusi tehakse üksnes ametlike ülesannete täitmiseks vajalikus mahus;
d) tõlgetele lisatakse märge selles keeles, millesse ta on tõlgitud, selle kohta, et tõlge sisaldab päritolupoolelt saadud salastatud teavet.

3 — Tasemel Muito secreto/Täiesti salajane salastatud teavet ei hävitata, vaid tagastatakse päritolupoole julgeoleku volitatud esindajale.
4 — Tasemel Secreto/salajane salastatud teabe hävitamisest teatatakse päritolupoole julgeoleku volitatud esindajale.
5 — Tasemel kuni Confidencial/Konfidentsiaalne (k.a) salastatud teave hävitatakse kooskõlas riigisiseste õigusaktidega.
6 — Kriisiolukorras, kui käesoleva kokkuleppe alusel koostatud või edastatud salastatud teavet ei ole võimalik kaitsta ega tagastada, hävitatakse see kohe. Vastuvõttev pool teatab salastatud teabe hävitamisest päritolupoole julgeoleku volitatud esindajale võimalikult kiiresti.

Artikkel 9

Salastatud teabe edastamine

1 — Pooled kasutavad salastatud teabe edastamiseks teineteisele oma julgeoleku volitatud esindajate poolt vastastikku heaks kiidetud kanaleid.
2 — Pooled võivad salastatud teavet edastada elektrooniliselt, pidades kinni oma julgeoleku volitatud esindajate vahel kokkulepitud julgeolekunõuetest.

3 — Suurte esemete ja mahuka salastatud teabe vahetamiseks annavad mõlema poole julgeoleku volitatud esindajad iga kord eraldi loa.

4 — Vastuvõttev pool kinnitab salastatud teabe kättesaamist kirjalikult ning edastab selle kasutajatele.

Artikkel 10

Salastatud teabe kasutamine ja sellekohaste nõuete täitmine

1 — Saadud salastatud teavet kasutatakse üksnes otstarbel, milleks see edastati.

2 — Kumbki pool teatab salastatud teabega seotud olukordades oma füüsilistele ja juriidilistele isikutele käesoleva kokkuleppe olemasolust.

3 — Pooled tagavad, et nende füüsilised ja juriidilised isikud, kes saavad salastatud teavet, täidavad käesolevast kokkuleppest tulenevaid kohustusi.

4 — Vastuvõttev pool tohib saadud salastatud teavet edastada kolmandatele isikutele ainult päritolupoole eelneval kirjalikul loal.

Artikkel 11

Salastatud lepingutega seotud nõuded

1 — Pool, kes soovib sõlmida salastatud lepingut teise poole lepinglasega või volitada oma lepinglast sõlmima teise poole territooriumil salastatud projekti põhjal salastatud lepingut, hangib oma riigi julgeoleku volitatud esindaja kaudu teise poole julgeoleku volitatud esindajalt eelneva kirjaliku kinnituse selle kohta, et asjaomasel lepinglasel on nõuetekohase tasemega juriidilise isiku juurdepääsuluba.

2 — Lepinglane kohustub:

a) tagama, et tema ruumid vastavad salastatud teabe käitlemise nõuetele;

b) omama asjakohast juurdepääsuluba;

c) tagama nõuetekohase füüsilise isiku juurdepääsuloa väljastamise isikutele, kellel on seoses oma tööülesannetega vaja juurdepääsu salastatud teabele;

d) tagama, et kõikidele isikutele, kellel on juurdepääs salastatud teabele, tutvustatakse nende salastatud teabe kaitsmise kohustusi riigisiseste õigusaktide kohaselt;

e) lubama julgeolekuinspektsiooni oma ruumides.

3 — Alltöövõtja peab täitma samu julgeolekukohustusi kui lepinglane.

4 — Riigi julgeoleku volitatud esindaja on pädev tagama, et lepinglane täidab lõikes 2 sätestatud kohustusi.

5 — Kui füüsilised või juriidilised isikud, kelle elu- või asukoht on ühe poole territooriumil, ning füüsilised või juriidilised isikud, kelle elu- või asukoht on teise poole territooriumil, alustavad läbirääkimisi salastatud lepingu sõlmimise üle, teatab selle poole julgeoleku volitatud esindaja, kelle territooriumil kõnealust salastatud lepingut täitma hakatakse, teisele poolele selle lepinguga seotud salastatud teabe kõrgeima salastatuse taseme.

6 — Poolte füüsiliste või juriidiliste isikute vahel käesoleva kokkuleppe kohaselt sõlmitud salastatud lepingud peavad sisaldama projekti julgeolekueeskirja, milles määratakse:

a) projekti salastamisjuhend ja salastatud teabe loend;

b) teabe salastatuse muutmisest teatamise kord;

c) sidekanalid ja elektroonilised sidevahendid;

d) salastatud materjali vedamise kord;

e) salastatud lepinguga seotud salastatud teabe kaitse kooskõlastamise eest vastutavad asutused;

f) kohustus teatada salastatud teabe ohtusattumisest või sellekohasest kahtlusest.

7 — Salastatud lepingu julgeolekueeskirja koopia edastatakse selle poole julgeoleku volitatud esindajale, kelle territooriumil salastatud lepingut täidetakse, et tal oleks võimalik jälgida ja kontrollida julgeolekunõuete täitmist.

8 — Poolte julgeoleku volitatud esindajad võivad vastastikuste külastuste põhjal analüüsida lepinglase poolt salastatud lepinguga seotud salastatud teabe kaitseks võetud meetmete tõhusust. Külastusest teatatakse vähemalt kolmkümmend päeva ette.

Artikkel 12

Külastused

1 — Poolte kodanike vastastikused külastused, millega kaasneb juurdepääsuvajadus salastatud teabele, võivad toimuda vastuvõtva poole julgeoleku volitatud esindaja eelneval kirjalikul loal.

2 — Üks pool lubab teise poole külastusi, millega kaasneb juurdepääsuvajadus salastatud teabele, üksnes juhul, kui:

a) lähetava poole julgeoleku volitatud esindaja või muu pädev asutus on nendele külastajatele väljastanud nõuetekohase füüsilise isiku juurdepääsuloa ning;

b) külastajatel on oma riigisiseste õigusaktide kohaselt õigus saada põhjendatud teadmisvajaduse tõttu salastatud teavet või omada sellele juurdepääsu.

3 — Lähetava poole julgeoleku volitatud esindaja teatab kavandatavast külastusest vastuvõtva poole julgeoleku volitatud esindajale külastustaotluses, mis peab laekuma vähemalt kolmkümmend päeva enne külastust.

4 — Kiireloomulistel juhtudel tuleb külastustaotlus edastada vähemalt seitse päeva varem.

5 — Külastustaotlus peab sisaldama järgmist:

a) külastaja ees- ja perekonnanimi, sünniaeg ja -koht, kodakondsus, passi või isikutunnistuse number;

b) selle asutuse nimi, mida külastaja esindab või kus ta töötab;

c) külastatava asutuse nimi ja aadress;

d) tõend külastaja füüsilise isiku juurdepääsuloa olemasolu ja kehtivuse kohta;

e) visiidi või visiitide eesmärk ja otstarve;

f) visiidi või visiitide eeldatav toimumisaeg ja kestus ning kordusvisiitide puhul kogu ajavahemik, mida need hõlmavad;

g) külastatava asutuse kontaktisiku nimi ja telefoninumber, varasemad kontaktid ja muu teave, mis aitab otsustada visiidi või visiitide põhjendatuse üle;

h) kuupäev, allkiri ja riigi julgeoleku volitatud esindaja ametlik pitser.

6 — Külastustaotluse adressaadist poole julgeoleku volitatud esindaja vaatab taotluse läbi ja teeb selle rahuldamise kohta otsuse ning teatab otsusest taotluse saatnud poole julgeoleku volitatud esindajale.

7 — Kolmandate isikute esindajate külastused, millega kaasneb juurdepääsuvajadus päritolupoole salastatud teabele, on lubatud üksnes päritolupoole julgeoleku volitatud esindaja kirjalikul nõusolekul.

8 — Kui külastus on kinnitatud, edastab vastuvõtva poole julgeoleku volitatud esindaja külastustaotluse koopia külastatava asutuse julgeolekutöötajatele.

9 — Külastusloa kehtivus ei tohi ületada 12 kuud.

10 — Riikide julgeoleku volitatud esindajad võivad iga projekti või lepingu puhul koostada isikute nimekirjad, kellele on lubatud korduskülastused. Nimekirjade esialgne kehtivusaeg on 12 kuud.

11 — Kui riikide julgeoleku volitatud esindajad on nimekirjad kinnitanud, kooskõlastatakse konkreetsete külastuste tingimused otse külastatavate asutuste esindajatega, lähtudes käesolevast kokkuleppest.

Artikkel 13

Salastatud teabe ohtusattumine

1 — Salastatud teabe kaitse nõuete rikkumise korral, mille tulemusel teise poole koostatud või temalt saadud salastatud teave satub ohtu või on kahtlus, et see on ohtu sattunud, teatab selle poole julgeoleku volitatud esindaja, kelle territooriumil julgeolekunõuete rikkumine toimus või salastatud teave ohtu sattus, teise poole julgeoleku volitatud esindajale juhtunust võimalikult kiiresti ning viib läbi nõuetekohase uurimise.

2 — Kui salastatud teabe kaitse nõudeid rikutakse või salastatud teave satub ohtu muudes riikides, võtab salastatud teabe edastanud poole julgeoleku volitatud esindaja lõikes 1 ettenähtud meetmeid.

3 — Teine pool võtab vajaduse korral uurimisest osa.

4 — Igal juhul teatatakse teisele poolele kirjalikult uurimise tulemustest, sealhulgas salastatud teabe kaitse nõuete rikkumise või salastatud teabe ohtusattumise põhjustest, tekitatud kahju ulatusest ning uurimise järeldustest.

Artikkel 14

Kulud

Kumbki pool kannab oma kokkuleppe täitmisega ja selle järelevalvega seotud kulud.

Artikkel 15

Vaidluste lahendamine

Vaidlused kokkuleppes ettenähtud meetmete tõlgendamise ja kohaldamise üle lahendatakse diplomaatiliste kanalite kaudu.

Artikkel 16

Muudatused

1 — Käesolevat kokkulepet võib muuta kummagi poole taotlusel.

2 — Muudatused jõustuvad artikli 18 tingimuste kohaselt.

Artikkel 17

Kehtivusaeg ja lõpetamine

1 — Kokkulepe sõlmitakse määramata ajaks.

2 — Kumbki pool võib kokkuleppe igal ajal lõpetada.

3 — Lõpetamisest tuleb teisele poolele teatada kirjalikult diplomaatiliste kanalite kaudu ning leping lõpeb kuus kuud pärast teate kättesaamist.

4 — Kokkuleppe lõpetamisest olenemata kaitstakse kokkuleppe alusel saadud teavet edasi selle sätete kohaselt, kuni päritolupool vastuvõtva poole sellest kohustusest vabastab.

Artikkel 18

Jõustumine

1 — Pooled teatavad teineteisele kirjalikult diplomaatiliste kanalite kaudu kokkuleppe jõustumiseks vajaliku riigisisese menetluse lõpetamisest.

2 — Kokkulepe jõustub kolmekümnendal päeval pärast seda, kui saabub viimane lõikes 1 osutatud teade.

Selle kinnituseks on poolte täievoloiloised esindajad kokkuleppele alla kirjutanud.

Koostatud Lisbon, 29.novembril 2005, kahes originaaleksemplaris portugali, eesti ja inglise keeles; kõik on võrdselt autentsed. Kokkuleppe erineva tõlgendamise korral lähtutakse ingliskeelsest variandist.

Portugali Vabariigi nimel:

Fernando Manuel de Mendonça d'Oliveira Neves, Euroopa asjade riigisekretär.

Eesti Vabariigi nimel:

Heiki Loot, Riigisekretär.

AGREEMENT ON THE PROTECTION OF CLASSIFIED INFORMATION BETWEEN THE PORTUGUESE REPUBLIC AND THE REPUBLIC OF ESTONIA

The Portuguese Republic and the Republic of Estonia, hereinafter referred to as the «Parties»:

Recognising the need of the Parties to guarantee the protection of the classified information exchanged between the Parties, their individuals or legal entities, under cooperation agreements or contracts concluded or to be concluded;

Desiring to create a set of rules on the mutual protection of classified information exchanged between the Parties;

agree as follows:

Article 1

Object

The present Agreement establishes the security rules applicable to all cooperation agreements or contracts, which envisage the transmission of classified information, concluded or to be concluded between the competent national authorities of both Parties or by individuals or legal entities duly authorized to that purpose.

Article 2

Scope of application

1 — The present Agreement sets out security rules for the protection of classified information exchanged between the Parties.

2 — The present Agreement is not applicable to direct co-operation between the intelligence services.

Article 3

Definitions

For the purposes of the present Agreement:

a) «Classified information» designates the information, documents and materials, regardless of their form, nature,

and means of transmission, determined to require protection against unauthorised disclosure, which has been so designated by security classification;

b) «National security authority» designates the authority designated by a Party as being responsible for the implementation and supervision of the present Agreement;

c) «The originating Party» designates the Party, which gives or transmits classified information to the other Party;

d) «The receiving Party» designates the Party to which classified information is given or transmitted to by the originating Party;

e) «Third Party» designates any international organisation or state, including its citizens and legal entities, that is not a Party to the present Agreement;

f) «Contractor» designates an individual or a legal entity possessing the legal capacity to conclude contracts;

g) «Classified contract» designates an arrangement between two or more contractors creating and defining enforceable rights and obligations between them, which contains or involves classified information;

h) «Personnel security clearance» designates the determination by the national security authority or other competent authority, that an individual is eligible to have access to classified information, in accordance with the national law;

i) «Facility security clearance» designates the determination by the national security authority or other competent authority that, from a security point of view, a legal entity has the physical and organisational capability to use and deposit classified information, in accordance with the national law;

j) «Need-to-know» designates that access to classified information may only be granted to a person who has a verified requirement for knowledge or possession of such information in order to perform official and professional duties, in accordance with the purpose for which the information was given or transmitted to the receiving Party;

k) «Project security instruction» designates a compilation of security requirements, which are applied to a specific project in order to standardize security procedures;

l) «Project security classification guide» designates the part of the project security instruction, which identifies the elements of the project that are classified and specifies their security classification levels.

Article 4

National security authorities

1 — The National Security Authorities are:

For the Portuguese Republic — National Security Authority, Presidency of the Council of Ministers, Avenida da Ilha da Madeira, 1, 1400-204 Lisbon, Portugal;

For the Republic of Estonia — Security Department, Ministry of Defence, Sakala Street 1, 15094 Tallinn, Estonia.

2 — The Parties shall inform each other, through diplomatic channels, of modifications concerning their national security authorities.

Article 5

Security principles

1 — The protection and use of the classified information exchanged between the Parties is ruled by the following principles:

a) The Parties shall afford all transmitted, produced or developed classified information the same degree of security protection as is provided for their own classified information of the equivalent level;

b) Access to classified information is allowed only to persons who have a need-to-know and, in case of information classified Confidencial/Konfidentsiaalne and above, hold a valid personnel security clearance issued by the competent authorities.

2 — In order to achieve and maintain comparable standards of security, the national security authorities shall, on request, provide each other with information about their security standards, procedures and practices for protection of classified information.

Article 6

Security classification

1 — The Parties agree that the following security classification levels are equivalent and correspond to the security classification levels specified in the national law of each Party:

Portuguese Republic	Republic of Estonia	Equivalent in english
Muito secreto	Täiesti salajane	Top secret.
Secreto	Salajane	Secret.
Confidencial	Konfidentsiaalne	Confidential.
Reservado	Piiratud	Restricted.

2 — The receiving Party shall mark the received classified information with its own equivalent security classification level marking, in accordance with the equivalences referred to in paragraph 1 of the present article.

3 — The Parties shall inform each other about all subsequent classification level alterations to the classified information transmitted.

4 — The receiving Party shall neither downgrade nor declassify the received classified information without the prior written consent of the originating Party.

Article 7

Security clearance

1 — On request, the Parties, through their national security authorities, preceding the issue of the personnel security clearance and the facility security clearance, shall assist each other during the clearance procedures of their individuals or legal entities living or located in the territory of the other Party, taking into account their national law.

2 — The Parties shall recognise the personnel security clearance and facility security clearance issued in accordance with the national law of the other Party. The equivalence of the security clearance levels shall be in compliance with article 6 of the present Agreement.

3 — The national security authorities shall communicate to each other any information with respect to changes of the related personnel security clearances and facility security clearances, particularly in cases of withdrawal or downgrading of their level.

Article 8

Translation, reproduction and destruction

1 — Classified Information marked as Secreto/Salajane or above shall be reproduced and translated only upon the written permission of the national security authority of the originating Party.

2 — Translations and reproductions of classified information shall be made in accordance with the following procedures:

a) The individuals shall hold the appropriate personnel security clearance as required in article 5;

b) The translations and the reproductions shall be marked and placed under the same protection as the original information;

c) The translations and the number of reproductions shall be limited to that required for official purposes;

d) The translations shall bear an appropriate note in the language into which it is translated indicating that it contains classified information received from the originating Party.

3 — Classified Information marked as Muito secreto/Täiesti salajane shall not be destroyed and it shall be returned to the national security authority of the originating Party.

4 — Destruction of classified information marked as Secreto/Salajane shall be notified to the national security authority of the originating Party.

5 — Information classified up to, and including, Confidencial/Konfidentsiaalne, shall be destroyed in accordance with the national law.

6 — In case of crisis situation, which makes it impossible to protect and return classified information generated or transferred according to the present Agreement the classified information shall be destroyed immediately. The receiving Party shall notify the national security authority of the originating Party about the destruction of the classified information as soon as possible.

Article 9

Transmission of classified information

1 — The classified information shall be transmitted between the Parties through channels mutually approved by the national security authorities.

2 — The Parties may transmit classified information by electronic means in accordance with security procedures mutually approved by the national security authorities.

3 — Delivery of large items or quantities of classified information shall be approved by both national security authorities on a case-by-case basis.

4 — The receiving Party shall confirm in writing the reception of the classified information and transmits it to the users.

Article 10

Use and compliance

1 — The transmitted classified information shall be used only for the purpose that it was transmitted for.

2 — Each Party shall inform its individuals and legal entities of the existence of the present Agreement, whenever classified information is involved.

3 — Each Party shall ensure that all individuals and legal entities, which receive classified information, duly comply with the obligations of the present Agreement.

4 — The receiving Party shall not transmit the classified information to a third Party, without prior written authorization of the originating Party.

Article 11

Requirements for classified contracts

1 — One Party, wishing to place a classified contract with a Contractor of the other Party or wishing to authorise one of its own contractors to place a classified contract in the territory of the other Party, within a classified project, shall obtain, through its national security authority, prior written assurance from the national security authority of the other Party that the proposed contractor holds a facility security clearance of an appropriate level.

2 — The contractor commits itself to:

a) Ensure that its premises have adequate conditions for processing classified information;

b) Hold an appropriate security clearance;

c) Have an appropriate personnel security clearance granted to persons who perform functions that require access to classified information;

d) Ensure that all persons with access to classified information are informed of their responsibility towards the protection of Classified Information in accordance with the national law;

e) Allow security inspections of their premises.

3 — Any subcontractor must fulfil the same security obligations as the contractor.

4 — The national security authority holds the competence to assure the compliance of the contractor with the commitments set in paragraph 2 of the present article.

5 — As soon as pre-contractual negotiations begin between individuals living, or legal entities located in the territory of one of the Parties and other individuals living, or legal entities located in the other Party's territory, aiming at the signing of classified contracts, the national security authority of the Party in whose territory the classified contract will be performed shall inform the other Party of the highest security classification level given to the classified information related to the contract which is being negotiated.

6 — Every classified contract signed by individuals or legal entities of the Parties under the present Agreement shall include a project security instruction identifying the following aspects:

a) Project security classification guide and list of classified information;

b) Procedure for the communication of changes in the classification of information;

c) Communication channels and means for electronic transmission;

d) Procedure for the transportation of classified information;

e) The authorities responsible for the co-ordination of the safeguarding of classified information related to the classified contract;

f) An obligation to notify any actual or suspected compromise of classified information.

7 — Copy of the project security instruction of any classified contract shall be forwarded to the national security authority of the Party in whose territory the classified contract is to be performed, in order to allow adequate security supervision and control.

8 — Representatives of the national security authorities may visit each other in order to analyse the efficiency of the measures adopted by a contractor for the protection of classified information involved in a classified contract. Notice of the visit shall be provided, at least, 30 days in advance.

Article 12

Visits

1 — Visits entailing access to classified information by citizens from one Party to the other Party are subject to prior written authorisation given by the national security authority of the host Party.

2 — Visits entailing access to classified information shall be allowed by one Party to visitors from the other Party, only if they have been:

a) Granted appropriate personnel security clearance by the national security authority or other competent authority of the requesting Party; and

b) Authorised to receive or to have access to classified information on a need-to- know basis, in accordance with the national law.

3 — The national security authority of the requesting Party shall notify the national security authority of the host Party of the planned visit through a request for visit, which has to be received at least 30 days before the visit takes place.

4 — In urgent cases, the request for visit shall be transmitted at least seven days in advance.

5 — The request for visit shall include:

a) Visitor's first and last name, place and date of birth, citizenship, passport or identity card number;

b) Name of the entity, which the visitor represents or to which the visitor belongs;

c) Name and address of the entity to be visited;

d) Certification of the visitor's personnel security clearance and its validity;

e) Objective and purpose of the visit or visits;

f) Expected date and duration of the requested visit or visits, and, in case of recurring visits, the total period covered by the visits;

g) Name and phone number of the point of contact at the entity to be visited, previous contacts and any other information useful to determine the justification of the visit or visits;

h) The date, signature and the official seal of the national security authority.

6 — The national security authority of the Party that receives a request for visit examines and decides on the request and shall inform of its decision the national security authority of the requesting Party.

7 — Visits of individuals from a third Party, entailing access to classified information of the originating Party shall only be authorized by a written consent of the national security authority of the originating Party.

8 — Once the visit has been approved, the national security authority of the host Party shall provide a copy of the request for visit to the security officers of the entity to be visited.

9 — The validity of visit authorisation shall not exceed 12 months.

10 — For any project or contract the national security authorities may agree to establish lists of authorized persons to make recurring visits. Those lists are valid for an initial period of 12 months.

11 — Once those lists have been approved by the national security authorities, the terms of the specific visits shall be directly arranged with the representatives of the entities to be visited, in accordance with the present Agreement.

Article 13

Compromise of classified information

1 — In case of breach of security that results in a certain or suspected compromise of classified information originated by or received from the other Party, the national security authority of the Party where the breach of security or compromise of classified information occurs shall inform the national security authority of the other Party, as soon as possible, and carry out the appropriate investigation.

2 — If a breach of security or compromise of classified information occurs in a state other than the Parties, the national security authority of the transmitting Party shall take the actions prescribed in paragraph 1 of the present article.

3 — The other Party shall, if required, co-operate in the investigation.

4 — In any case, the other Party shall be informed of the results of the investigation, in writing, including the reasons for the breach of security or compromise of classified information, the extent of the damage and the conclusions of the investigation.

Article 14

Expenses

Each Party shall bear its own expenses incurred in connection with the application and supervision of the present Agreement.

Article 15

Settlement of disputes

Any dispute concerning the interpretation or application of the measures prescribed in the present Agreement shall be settled through diplomatic channels.

Article 16

Amendments

1 — The present Agreement may be amended on request of one of the Parties.

2 — The amendments shall enter into force in accordance with the terms specified in article 18 of the present Agreement.

Article 17

Duration and termination

1 — The present Agreement shall remain in force for an indeterminate period of time.

2 — Each Party may at any time terminate the present Agreement.

3 — The termination shall be notified to the other Party, in writing and through diplomatic channels, producing its effects six months after the date of reception of the notification.

4 — Notwithstanding the termination, all classified information transferred pursuant to the present Agreement shall continue to be protected in accordance with the provisions set forth herein, until the originating Party dispenses the receiving Party from this obligation.

Article 18

Entry into force

1 — The Parties shall notify each other, in writing and through diplomatic channels, that all internal procedures necessary for bringing the Agreement into force have been fulfilled.

2 — The present Agreement shall enter into force on the thirtieth day following the receipt of the last of the notifications referred to in paragraph 1 of the present article.

In witness thereof, the undersigned, duly authorized, have signed the present Agreement.

Done at Lisbon, on 29 November 2005, in two originals, each one in the portuguese, estonian and english languages, each text being equally authentic. In case of any divergence of interpretation the english text shall prevail.

For the Portuguese Republic:

Fernando Manuel de Mendonça d'Oliveira Neves, Secretary of State for European Affaires.

For the Republic of Estonia:

Heiki Loot, Secretary of State.

MINISTÉRIO DA AGRICULTURA, DO DESENVOLVIMENTO RURAL E DAS PESCAS

Portaria n.º 1138/2008

de 10 de Outubro

O Decreto-Lei n.º 148/2008, de 29 de Julho, transpõe para a ordem jurídica interna a Directiva n.º 2004/28/CE, do Parlamento Europeu e do Conselho, de 31 de Março, e parcialmente a Directiva n.º 2001/82/CE, do Parlamento Europeu e do Conselho, de 6 de Novembro, que estabelece o código comunitário relativo aos medicamentos veterinários, e a Directiva n.º 2006/130/CE, da Comissão, de 11 de Dezembro, que determina os critérios de isenção da receita veterinária para determinados medicamentos veterinários aplicáveis a animais produtores de alimentos, e revoga os Decretos-Leis n.os 146/97, de 11 de Junho, 184/97, de 26 de Julho, 232/99, de 24 de Junho, 245/2000, de 29 de Setembro, 185/2004, de 29 de Julho, e 175/2005, de 25 de Outubro.

Este diploma revogou o Decreto-Lei n.º 175/2005, de 25 de Outubro, que estabelece o regime jurídico da receita médico-veterinária, da requisição médico-veterinária normalizada, da vinheta médico-veterinária normalizada e do livro de registos de medicamentos utilizados em animais de exploração.

Pretende o Decreto-Lei n.º 148/2008, de 29 de Julho, melhorar quer a informação ao consumidor quer a sua protecção através do controlo racional da utilização de medicamentos e medicamentos veterinários em animais produtores de alimentos para consumo humano.

Importa, para o efeito, aprovar os modelos de receita e vinheta.

Assim:

Nos termos do n.º 1 do artigo 119.º do Decreto-Lei n.º 148/2008, de 29 de Julho, manda o Governo, pelo Ministro da Agricultura, do Desenvolvimento Rural e das Pescas, o seguinte:

Artigo 1.º

Receita médico-veterinária normalizada

1 — Para a prescrição de medicamentos e medicamentos veterinários sujeitos a prescrição obrigatória, bem como de preparações medicamentosas, magistrais ou oficinais, os médicos veterinários devem utilizar a receita médico-veterinária normalizada, cujo modelo consta do anexo I à presente portaria, da qual faz parte integrante.

2 — A receita médico-veterinária normalizada é editada em triplicado.

Artigo 2.º

Vinheta

1 — É aprovado o modelo de vinheta para validação da receita médico-veterinária normalizada, cujo modelo consta do anexo II à presente portaria, da qual faz parte integrante, e que inclui as seguintes informações:

a) Nome profissional do médico veterinário adoptado na Ordem dos Médicos Veterinários;

b) Código de identificação do médico veterinário, composto pelos seguintes caracteres:

i) Cinco dígitos de identificação do número da cédula profissional do médico veterinário;

ii) Um dígito de verificação ou controlo;

c) Código de barras, que inclui a informação respeitante ao controlo das vinhetas e aos dados pessoais e profissionais do médico veterinário, a estabelecer pela Ordem dos Médicos Veterinários;

d) Os elementos referidos nas alíneas anteriores são apostos sobre o logótipo da Ordem dos Médicos Veterinários, em marca de água ou holograma, que faz parte integrante da vinheta.

2 — A cor da tinta a utilizar na vinheta deve ser diferente da utilizada na impressão da receita.

O Ministro da Agricultura, do Desenvolvimento Rural e das Pescas, *Jaime de Jesus Lopes Silva,* em 25 de Setembro de 2008.