

ANEXO I

Medidas preventivas**Artigo 1.º****Âmbito territorial**

Ficam sujeitas a medidas preventivas as áreas assinaladas na planta anexa.

Artigo 2.º**Âmbito material**

Naquelas áreas, as medidas preventivas consistem na sujeição a prévio parecer vinculativo do Instituto de Gestão do Património Arquitectónico e Arqueológico (IGESPAR, I. P.) das seguintes acções, sem prejuízo de quaisquer outros condicionalismos legalmente exigidos:

a) Obras de construção civil, ampliação, alteração e reconstrução, com excepção das que estejam isentas de procedimento de licenciamento ou comunicação prévia;

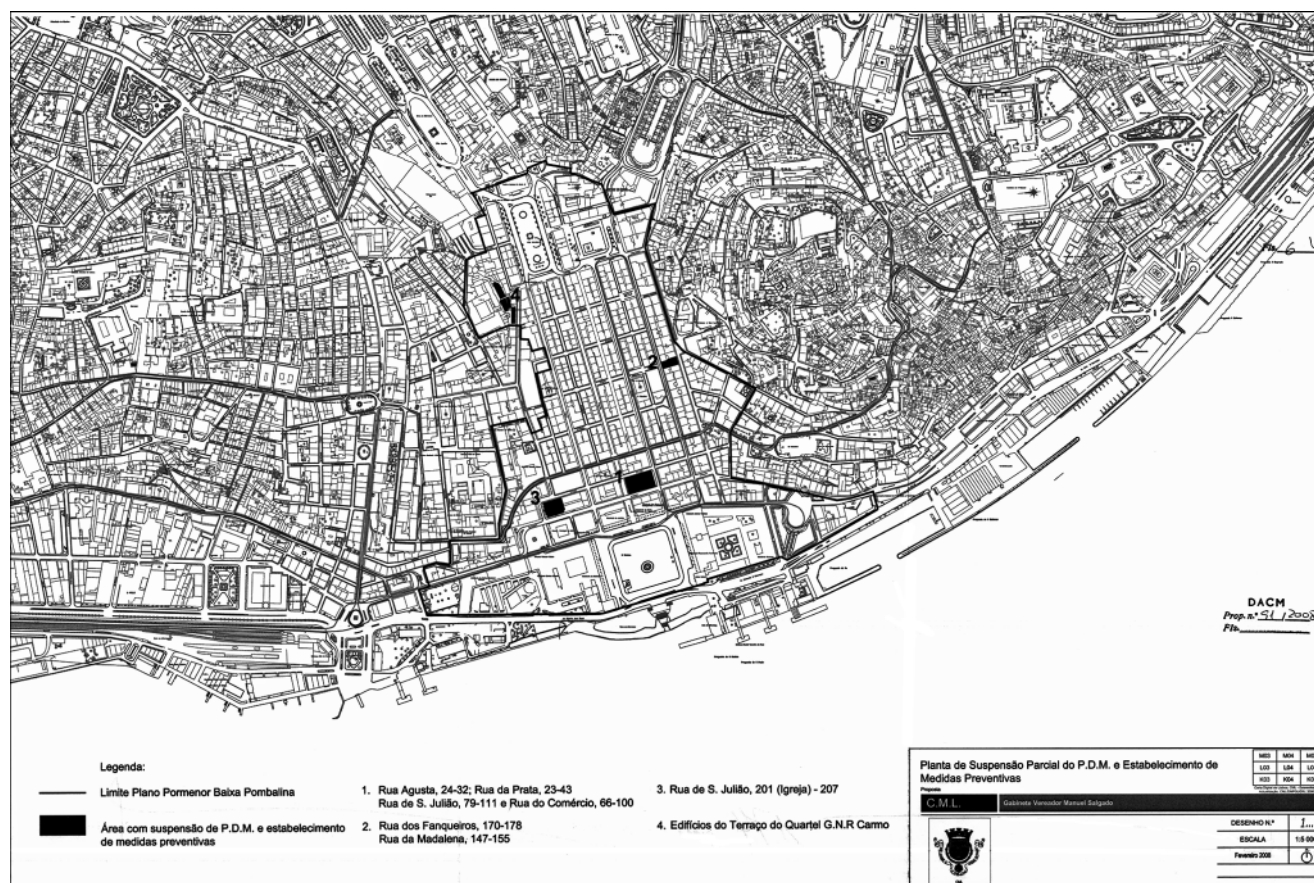
b) Trabalhos de remodelação de terrenos;
c) Obras de demolição de edificações existentes, excepto as que, por regulamento municipal, possam ser dispensadas de licença ou autorização.

Artigo 3.º**Âmbito temporal**

O prazo de vigência das medidas preventivas é de dois anos a contar da data da respectiva entrada em vigor, prorrogável por mais um, quando tal se mostre necessário, caducando com a conclusão da execução dos projectos para as áreas mencionadas no artigo 1.º ou com a entrada em vigor do Plano de Pormenor da Baixa Pombalina, se esta ocorrer primeiro.

Artigo 4.º**Entrada em vigor**

As medidas preventivas entram em vigor no dia seguinte ao da sua publicação no *Diário da República*.

**MINISTÉRIO DOS NEGÓCIOS ESTRANGEIROS****Decreto n.º 46/2008**

de 14 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 Letónia:

Assim:

Nos termos da alínea c) do n.º 1 do artigo 197.º da Constituição, o Governo aprova o Acordo para a Protecção Mútua de Informação Classificada entre a República Portuguesa e a República da Letónia, assinado em Lisboa em 24 de Janeiro de 2007, cujo texto, nas versões autenticadas nas línguas portuguesa, letã 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 MÚTUA DE INFORMAÇÃO CLASSIFICADA ENTRE A REPÚBLICA PORTUGUESA E A REPÚBLICA DA LETÓNIA

A República Portuguesa e a República da Letónia, doravante designadas por Partes;

Reconhecendo a necessidade das Partes em garantir a protecção de informação classificada trocada entre ambas, no âmbito de negociações e de acordos de cooperação, concluídos ou a concluir, bem como de outros instrumentos contratuais de entidades públicas ou privadas das Partes;

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

acordam no seguinte:

Artigo 1.º

Objecto

O presente Acordo estabelece as regras de segurança aplicáveis a todos os instrumentos contratuais que prevejam a transmissão de informação classificada celebrados ou a celebrar pelas autoridades nacionais competentes das Partes ou pelos organismos ou empresas autorizadas para esse efeito.

Artigo 2.º

Âmbito de aplicação

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

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 meio de transmissão, aos quais tenha sido atribuído um grau de classificação de segurança e que requeiram protecção contra divulgação não autorizada, de acordo com o direito interno em vigor na parte transmissora;

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 que não é Parte no presente Acordo;

f) «Contracto 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;

g) «Contratante» designa uma pessoa singular ou colectiva possuidora de capacidade legal para celebrar contractos classificados;

h) «Credenciação de segurança do pessoal» designa a determinação feita pela Autoridade Nacional de Segurança ou outra autoridade estatal relevante de que um indivíduo está habilitado para ter acesso a informação classificada, de acordo com o respectivo direito interno em vigor;

i) «Credenciação de segurança industrial» designa a determinação feita pela Autoridade Nacional de Segurança ou outra autoridade estatal relevante de que, sob o ponto de vista de segurança, a entidade tem a capacidade física e organizacional para manusear e guardar informação classificada, de acordo com o respectivo direito interno em vigor;

j) «Necessidade de conhecer» designa o princípio segundo o qual o acesso à informação classificada só pode ser concedido à pessoa que tenha comprovada necessidade de a conhecer, ou de a possuir, para cumprimento das suas funções e tarefas oficiais, nos termos em que a matéria foi disponibilizada à parte destinatária;

k) «Guia de classificação de segurança do projecto» designa as instruções sobre segurança do projecto que identifica os elementos classificados, especificando os níveis de classificação de segurança.

Artigo 4.º

Autoridades nacionais de segurança

1 — As Autoridades Nacionais de Segurança responsáveis pela aplicação do presente Acordo 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 Letónia:

Constitution Protection Bureau, Miera Street 85 a Riga, LV 1013, Letónia.

2 — Cada uma das Partes informará a outra, através dos canais diplomáticos, de qualquer alteração relativa às suas autoridades nacionais de segurança.

3 — As autoridades nacionais de segurança, sem alterar qualquer obrigação ora acordada, poderão celebrar protocolos para a implementação técnica do presente Acordo.

Artigo 5.º

Princípios de segurança

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

a) A parte destinatária atribuirá à informação classificada recebida um grau de protecção equivalente à marca que foi expressamente atribuída a essa informação classificada pela parte transmissora;

b) O acesso à informação classificada, bem como aos locais e instalações onde se realizem actividades classificadas ou onde seja armazenada informação classificada, é limitado às pessoas que estejam habilitadas com uma credenciação de segurança do pessoal para acesso a informação classificada como «confidencial/konfidenciāli», ou superior, e que para o desempenho das suas funções ou emprego, tenham necessidade de conhecer.

2 — Com o objectivo de se obterem e manterem padrões de segurança comparáveis, qualquer autoridade nacional de segurança deverá, sempre que solicitado pela outra, disponibilizar informação sobre os seus padrões de segurança, procedimentos e práticas para a protecção de informação classificada.

Artigo 6.º

Classificações de segurança e equivalências

As Partes acordam que os seguintes graus de classificação de segurança são equivalentes e correspondem aos graus de classificação de segurança especificados no respectivo direito interno em vigor:

República Portuguesa	República da Letónia	Língua inglesa
Muito secreto	<i>Sevišķi slepeni</i>	<i>Top secret.</i>
Secreto	<i>Slepeni</i>	<i>Secret.</i>
Confidencial	<i>Konfidenciāli</i>	<i>Confidential.</i>
Reservado	<i>Dienesta vajadzībām</i>	<i>Restricted.</i>

Artigo 7.º

Classificação, recepção e alterações

1 — A parte destinatária marcará a informação classificada recebida com as suas próprias marcas nacionais de classificação de segurança, em conformidade com as equivalências referidas no artigo 6.º do presente Acordo.

2 — As Partes informar-se-ão mutuamente sobre todas as alterações ulteriores de classificação de informação classificada transmitida.

3 — A parte destinatária e ou as suas entidades não poderão baixar o grau de classificação de segurança ou desclassificar a informação classificada recebida sem prévia autorização da parte transmissora.

Artigo 8.º

Tradução, reprodução e destruição

1 — A informação classificada marcada como «muito secreto/*sevišķi slepeni*» só poderá ser traduzida e repro-

duzida após autorização escrita da autoridade nacional de segurança da parte transmissora.

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

a) As pessoas envolvidas deverão ser titulares de credenciação de segurança do pessoal;

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 limitados às requeridas para uso oficial;

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

3 — A informação classificada será destruída ou modificada de forma a prevenir a reconstrução da informação classificada no todo ou em parte.

4 — A informação classificada marcada como «muito secreto/*sevišķi slepeni*» não poderá ser destruída mas sim devolvida à autoridade nacional de segurança da parte transmissora a menos que se verifique um caso de perigo imediato, no qual tal informação poderá ser destruída sem o consentimento prévio por escrito da autoridade nacional de segurança da parte transmissora, a qual será prontamente notificada de tal ocorrência.

5 — A destruição de informação classificada marcada como «secreto/*slepeni*» será efectuada após notificação prévia à parte transmissora.

6 — A informação classificada marcada até «confidencial/*konfidenciāli*», inclusive, deverá ser destruída de acordo com o respectivo direito interno em vigor.

Artigo 9.º

Transmissão entre as Partes

1 — A informação classificada será normalmente transmitida entre as Partes utilizando canais diplomáticos.

2 — Caso o uso dos canais diplomáticos se revele impraticável ou excessivamente moroso para a recepção de informação classificada, as transmissões poderão ser efectuadas por pessoal devidamente credenciado e detentor de um certificado de correio emitido pela Parte que transmite a informação classificada.

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

4 — A transmissão de informação classificada volumosa ou em grande quantidade, acordada pontualmente, será aprovada por ambas as autoridades nacionais de segurança.

5 — 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, ao abrigo de acordos ou quaisquer outros instrumentos contratuais celebrados entre as Partes.

2 — Cada Parte dará conhecimento às suas entidades da existência do presente Acordo sempre que esteja envolvida informação classificada.

3 — Cada Parte assegurará que todas as entidades que recebam informação classificada respeitem as obrigações do presente Acordo.

4 — A parte destinatária não transmitirá informação classificada a uma terceira parte, pessoa singular ou colectiva da nacionalidade de um terceiro Estado, sem autorização prévia escrita da parte transmissora.

Artigo 11.º

Credenciações de segurança

1 — Se solicitado, a autoridade nacional de segurança de qualquer das Partes, tendo em conta o respectivo direito interno em vigor, colaborará com a outra no decurso dos procedimentos para a credenciação de segurança dos seus cidadãos que residam ou das instalações que 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 em vigor na outra Parte. A equivalência dos graus 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 12.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 um certificado de 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) Garantir o grau de classificação de segurança adequado a essas instalações;
- c) Garantir o grau de classificação de segurança do pessoal adequado às pessoas que necessitem de 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 em vigor;
- e) Efectuar 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 uma entidade situada no território de uma das Partes e outra situada no território da outra Parte para

a celebração de instrumentos 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 essas negociações pré-contratuais.

6 — Qualquer contrato classificado celebrado entre entidades das Partes, nos termos do presente Acordo, deverá incluir uma secção de segurança apropriada, 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 de informação classificada;
- 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;
- f) Obrigatoriedade de notificação de perda ou suspeita de perda, extravio ou comprometimento de informação classificada.

7 — A cópia da secção de segurança de qualquer contrato classificado deverá ser enviada à autoridade nacional de segurança da Parte em cujo território o contrato classificado será cumprido, por forma a garantir adequada supervisão e controlo de segurança.

8 — Os representantes das autoridades nacionais de segurança podem efectuar visitas mútuas a fim de verificar 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 13.º

Visitas

1 — As visitas que envolvam acesso a informação classificada por nacionais 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 estatal relevante da Parte visitante; e
- b) Estiverem autorizados a receber ou ter acesso a informação classificada fundamentado na necessidade de conhecer, de acordo com o respectivo direito interno em vigor.

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, a nacionalidade e o número do passaporte ou bilhete de identidade;

b) O nome da instituição, empresa ou organismo que o visitante representa ou a que pertence;

c) Nome e endereço da instituição, empresa ou organismo a visitar;

d) Certificação da credenciação de segurança do pessoal do visitante e respectiva validade;

e) Objecto e propósito da visita ou visitas;

f) A data prevista para a visita ou visitas e respectiva duração. No caso de visitas recorrentes, deverá ser indicado o período total coberto pelas visitas;

g) Nome e número de telefone de contacto da instituição ou instalação a visitar, 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 de segurança competente.

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 visitas de pessoas de um terceiro Estado que impliquem acesso a informação classificada apenas serão autorizadas mediante acordo entre as Partes.

8 — Uma vez aprovada a visita, a autoridade nacional de segurança da Parte anfitriã fornecerá cópia do pedido de visita ao funcionário de segurança da instituição, empresa ou organismo a ser visitado.

9 — A validade da autorização da visita não deverá exceder 12 meses.

Artigo 14.º

Visitas recorrentes

1 — Para qualquer projecto, programa ou contrato, as Partes podem acordar em elaborar listas de pessoas autorizadas a efectuar visitas recorrentes. Essas listas são válidas por um período inicial de 12 meses.

2 — Após aprovação das listas pelas Partes, os termos das visitas específicas podem ser directamente acordados com as autoridades competentes dos organismos a visitar pelas pessoas que constam daquelas listas, segundo os termos e condições acordados.

Artigo 15.º

Quebra e comprometimento de segurança

1 — Em caso de quebra ou comprometimento 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 ocorre a quebra ou comprometimento informará prontamente a autoridade nacional de segurança da outra Parte e instaurará a correspondente investigação.

2 — Se a quebra ou comprometimento de segurança ocorrer num outro Estado que não o das Partes, a autoridade nacional de segurança da Parte despachante actua 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 da segurança, a extensão dos danos e as conclusões da investigação.

Artigo 16.º

Encargos

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

Artigo 17.º

Solução de controvérsias

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

Artigo 18.º

Revisão

1 — O presente Acordo pode ser objecto de revisão por acordo mútuo por escrito de ambas as Partes.

2 — As emendas entrarão em vigor nos termos previstos no artigo 20.º do presente Acordo.

Artigo 19.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 através dos canais diplomáticos, produzindo efeito 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 20.º

Entrada em vigor

O presente Acordo entrará em vigor no 30.º dia após a recepção da última notificação, por escrito e por via diplomática, de que foram cumpridos os requisitos do direito interno das Partes necessários para o efeito.

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

Feito em Lisboa, aos 24 de Janeiro de 2007, em dois originais, em português, letão e inglês, fazendo qualquer dos textos igualmente fé. Em caso de divergência na interpretação, o texto em inglês prevalecerá.

Pela República Portuguesa, *Manuel Lobo Antunes*, Secretário de Estado Adjunto e dos Assuntos Europeus.

Pela República da Letónia, *Ints Upmacis*, Embaixador da Letónia em Portugal.

PORTUGÁLES REPUBLIKAS UN LATVIJAS REPUBLIKAS LĪGUMS PAR SAVSTARPĒJU KLASIFICĒTĀS INFORMĀCIJAS AIZSARDZĪBU

Portugāles Republika un Latvijas Republika Turpmāk sauktas Puses,

Apzinoties abu Pušu nepieciešamību nodrošināt klasificētās informācijas aizsardzību, ar kuru Puses ir apmainījušās pārrunu un noslēgto vai plānoto sadarbības

līgumu ietvaros, kā arī citu līgumsaistību ietvaros starp Pušu publiskām vai privātām personām,

Vēloties nostiprināt klasificētās informācijas, ar ko Puses ir apmainījušās, savstarpējas aizsardzības noteikumus;

ir vienojušās par sekojošo:

1. Pants

Mērķis

Šis Līgums nosaka drošības noteikumus, kas attiecas uz visām līgumsaistībām, kas paredz klasificētās informācijas nodošanu un kas ir parakstītas vai kuras ir plānots parakstīt starp abu Pušu attiecīgajām nacionālajām institūcijām, organizācijām vai uzņēmumiem, kas ir pilnvaroti to darīt.

2. Pants

Piemērošana

Šis Līgums nosaka klasificētās informācijas, ar kuru Puses ir apmainījušās, aizsardzības pasākumus.

3. Pants

Definīcijas

Šī Līguma mērķiem:

a) "Klasificētā informācija" nozīmē informāciju, dokumentus un materiālus, neatkarīgi no to fiziskās formas, veida vai nodošanas līdzekļiem, kuriem ir nepieciešama aizsardzība pret nesankcionētu izpaušanu un kuriem ir noteikta klasifikācijas pakāpe saskaņā ar izcelsmes Puses nacionālajiem normatīvajiem aktiem;

b) "Nacionālā drošības iestāde" nozīmē institūciju, kuru Puse ir nozīmējusi par atbildīgo institūciju šī Līguma ieviešanai un pārraudzībai;

c) "Izcelsmes Puse" nozīmē Pusi, kura nodod vai nosūta klasificēto informāciju otrai Pusei;

d) "Saņēmēja Puse" nozīmē Pusi, kurai izcelsmes Puse nodod vai nosūta klasificēto informāciju;

e) "Trešā puse" nozīmē jebkuru starptautisku organizāciju vai valsti, kas nav šī Līguma puse;

f) "Klasificēts līgums" nozīmē līgumu starp diviem vai vairākiem līgumslēdzējiem, kas rada un nosaka izpildāmas tiesības un pienākumus starp tiem un satur vai ietver klasificēto informāciju;

g) "Līgumslēdzējs" nozīmē fizisku vai juridisku personu, kas ir tiesīga uzņemties klasificētu līgumu izpildi;

h) "Speciālā atļauja" nozīmē Nacionālās drošības iestādes vai citas valsts institūcijas lēmumu personai piešķirt pieeju klasificētajai informācijai saskaņā ar nacionālajiem normatīvajiem aktiem;

i) "Industriālās drošības sertifikāts" nozīmē Nacionālās drošības iestādes vai citas valsts institūcijas lēmumu, ka no drošības viedokļa uzņēmumam ir fiziskās un organizatoriskās spējas izmantot un glabāt klasificēto informāciju saskaņā ar nacionālajiem normatīvajiem aktiem;

j) "Nepieciešamība zināt" nozīmē principu, ka pieeja klasificētai informācijai var tikt piešķirta vienīgi personai, kurai ir pārbaudīta nepieciešamība to zināt vai saņemt saistībā ar oficiālajiem un profesionālajiem pienākumiem, kuru ietvaros informācija ir tikusi nodota saņēmējai Pusei;

k) "Projekta klasifikācijas pakāpju rādītājs" nozīmē daļu no projekta drošības noteikumiem, kas nosaka tās projekta daļas, kas ir klasificētas un to klasifikācijas pakāpes.

4. Pants

Nacionālās drošības iestādes

1. Nacionālās drošības iestādes, kas ir atbildīgas par šī Līguma piemērošanu, ir:

- Portugāles Republikā:

Nacionālā drošības iestāde, Ministru Padomes Prezidentūra, Av. Ilha da Madeira, 1, 1400-204 Lisabona, Portugāle.

- Latvijas Republikā:

Satversmes aizsardzības birojs, Miera iela 85 a Rīga, LV 1013, Latvija.

2. Puses informē viena otru caur diplomātiskajiem kanāliem par jebkādam izmaiņām saistībā ar to Nacionālām drošības iestādēm.

3. Nacionālās drošības iestādes, nemainot šajā Līgumā noteiktos pienākumus, var vienoties par šī Līguma tehniskās īstenošanas pasākumiem.

5. Pants

Drošības pamatprincipi

1. Klasificētās informācijas, ar kuru Puses ir apmainījušās, aizsardzību un izmantošanu, nosaka sekojoši pamatprincipi:

a) Saņēmēja Puse piešķir saņemtajai klasificētajai informācijai aizsardzības pakāpi atbilstoši apzīmējumiem, kādus klasificētajai informācijai ir noteikusi Izcelsmes Puse;

b) Pieeja klasificētai informācijai un vietām un objektiem, kur tiek veiktas darbības ar klasificēto informāciju vai kur tā tiek glabāta, tiek nodrošināta tikai tām personām, kurām ir speciālā atļauja pieejai informācijai, kas klasificēta KONFIDENCIĀLI / CONFIDENCIAL vai augstāk un kurām ir "nepieciešamība zināt" saistībā ar viņu funkcijām vai darba pienākumiem.

2. Lai sasniegtu un ievērotu līdzīgus drošības standartus, Nacionālās drošības iestādes pēc pieprasījuma iesniedz viena otrai informāciju par to drošības standartiem, procedūrām un praksi klasificētās informācijas aizsardzībai.

6. Pants

Klasifikācijas pakāpes un to ekvivalenti

Puses vienojas, ka sekojošas klasifikācijas pakāpes ir ekvivalentas un atbilst klasifikācijas pakāpēm, kādas ir noteiktas attiecīgās Puses nacionālajos normatīvajos aktos:

Portugāles Republika	Latvijas Republika	Angļu valoda
MUITO SE- CRETO. SE- CRETO CONFIDENCIAL RESERVADO ...	SEVIŠKI SLEPENI SLEPENI KONFIDENCIĀLI DIENESTA VAJADZĪBĀM	TOP SECRET. SECRET. CONFIDENTIAL RESTRICTED.

7. Pants

Klasificēšana, saņemšana un izmaiņas

1. Saņēmēja Puse apzīmē saņemto klasificēto informāciju ar tās ekvivalento klasifikācijas pakāpi, saskaņā ar šī Līguma 6.pantā noteiktajiem ekvivalentiem.

2. Puses savstarpēji informē viena otru par visām izmaiņām nodotās klasificētās informācijas klasifikācijas pakāpēs.

3. Saņēmēja puse un/vai tās valsts institūcijas nedrīkst pazemināt saņemtas klasificētās informācijas klasifikācijas pakāpi vai deklasificēt šo informāciju bez iepriekšējas rakstiskas izcelsmes Puses piekrišanas.

8. Pants

Tulkošana, pavairošana un iznīcināšana

1. Klasificēto informāciju, kas klasificēta kā SEVIŠĶI SLEPENI / MUITO SECRETO, var tulkot un pavairot tikai pēc izcelsmes Puses Nacionālās drošības iestādes rakstiskas atļaujas saņemšanas.

2. Klasificētās informācijas tulkošana un pavairošana tiek veikta saskaņā ar sekojošām procedūrām:

- a) Personām ir jābūt atbilstoši speciālajai atļaujai;
- b) Uz tulkojumiem un kopijām tiek izdarīti tādi paši apzīmējumi, kā uz oriģināliem, un tie tiek aizsargāti kā oriģināli;
- c) Tulkojumu un kopiju skaits tiek ierobežots tā, lai nepārsniegtu oficiāliem nolūkiem nepieciešamo skaitu;
- d) Uz tulkojuma tiek izdarīts apzīmējums valodā, uz kuru tulkojums ir veikts, kas norāda, ka tulkojums satur izcelsmes Puses klasificēto informāciju.

3. Klasificētā informācija tiek iznīcināta vai pārveidota tā, lai novērstu tās pilnīgu vai daļēju rekonstruēšanu.

4. Informācija, kas klasificēta kā SEVIŠĶI SLEPENI/ MUITO SECRETO, netiek iznīcināta. Tā tiek nosūtīta atpakaļ izcelsmes Puses Nacionālajai drošības iestādei. Gadījumā, ja pastāv tieši draudi, tāda informācija var tikt iznīcināta bez iepriekšējas izcelsmes Puses Nacionālās drošības iestādes rakstiskas atļaujas, par ko pēdējā tiek nekavējoties informēta.

5. Par informācijas, kas klasificēta kā SLEPENI / SECRETO, iznīcināšanu ir jāinformē izcelsmes Puse.

6. Informācija, kas klasificēta līdz pakāpei KONFIDENCIĀLI / CONFIDENCIAL, ieskaitot, tiek iznīcināta saskaņā ar nacionālajiem normatīvajiem aktiem.

9. Pants

Nodošana starp Pusēm

1. Klasificētā informācija parasti tiek nodota starp Pusēm pa diplomātiskajiem kanāliem.

2. Ja šādu kanālu izmantošana ir nepraktiska vai kavē klasificētās informācijas saņemšanu, informācijas nodošanu var veikt personas ar atbilstošu speciālo atļauju un kurjera sertifikātu, kuru ir izsniegusi Puse, kura nodod klasificēto informāciju.

3. Puses var nodot klasificēto informāciju elektroniski saskaņā ar drošības procedūrām, par kurām savstarpēji ir vienojušās Nacionālās drošības iestādes.

4. Par lielu klasificētās informācijas objektu vai daudzumu nosūtīšanu abas Nacionālās drošības iestādes vienojas katrā gadījumā atsevišķi.

5. Saņēmēja Puse apstiprina klasificētās informācijas saņemšanu rakstiski un nodod to lietotājiem.

10. Pants

Izmantošana un prasību ievērošana

1. Nodotā klasificētā informācija tiek izmantota tikai tādām mērķim, kādam tā ir nodota saskaņā ar līgumiem vai citām līgumsaistībām, kas ir noslēgtas starp Pusēm.

2. Katra Puse informē savas institūcijas par šī Līguma esamību gadījumos, kad ir iesaistīta klasificētā informācija.

3. Katra Puse nodrošina, ka visas institūcijas, kas saņem klasificēto informāciju, ievēro šī Līguma nosacījumus.

4. Saņēmēja Puse nenodod klasificēto informāciju Trešajai pusei, fiziskai vai juridiskai personai, kam ir citas valsts pavalstniecība, bez iepriekšējas izcelsmes Puses rakstiskas atļaujas.

11. Pants

Speciālās atļaujas un industriālās drošības sertifikāti

1. Pēc pieprasījuma un saskaņā ar to nacionālajiem normatīvajiem aktiem, Pušu Nacionālās drošības iestādes palīdz viena otrai veikt pārbaudi personām, kas dzīvo, vai objektiem, kas atrodas otras Puses teritorijā, pirms tiek izsniegtas speciālās atļaujas un industriālās drošības sertifikāti.

2. Puses savstarpēji atzīst speciālās atļaujas un industriālās drošības sertifikātus, kas ir izsniegti saskaņā ar otras Puses attiecīgajiem nacionālajiem normatīvajiem aktiem. Speciālo atļauju un industriālās drošības sertifikātu ekvivalence ir saskaņā ar šī Līguma 6. pantu.

3. Nacionālās drošības iestādes informē viena otru par jebkurām izmaiņām attiecībā uz izsniegtajām speciālajām atļaujām un industriālās drošības sertifikātiem, īpaši to anulēšanas vai klasifikācijas pakāpes samazināšanas gadījumiem.

12. Pants

Prasības klasificētiem līgumiem

1. Ja kādai no Pusēm ir nepieciešams slēgt klasificētu līgumu ar otras Puses līgumslēdzēju vai ja tai ir nepieciešams pilnvarot tās līgumslēdzēju slēgt klasificētu līgumu otras Puses teritorijā klasificēta līguma ietvaros, tad iepriekš ar tās Nacionālās drošības iestādes starpniecību tiek saņemts rakstisks apliecinājums no otras Puses Nacionālās drošības iestādes, ka attiecīgajam līgumslēdzējam ir atbilstošas pakāpes industriālās drošības sertifikāts.

2. Līgumslēdzējs apņemas sekojošo:

- a) Nodrošināt, ka tā telpas ir atbilstošas attiecīgās klasificētās informācijas glabāšanai;
- b) Nodrošināt, ka telpām ir izsniegts atbilstošs drošības prasību ievērošanas apstiprinājums;
- c) Nodrošināt, ka personām, kuras veic funkcijas, kurām ir nepieciešama pieeja klasificētai informācijai, ir izsniegtas atbilstošas speciālās atļaujas;
- d) Nodrošināt, ka visas personas ar pieeju klasificētai informācijai, ir informētas par saviem pienākumiem klasificētās informācijas aizsardzībai saskaņā ar nacionālajiem normatīvajiem aktiem;
- e) Atļaut veikt savu telpu drošības pārbaudes.

3. Jebkuram līgumslēdzējam, kas slēdz apakšlīgumu, ir jāievēro tādas pašas drošības prasības, kā līgumslēdzējam.

4. Nacionālās drošības iestādes kompetencē ir pārliecināties, ka līgumslēdzējs ievēro saistības, kas ir noteiktas šī panta 2.daļā.

5. Tiklīdz tiek uzsāktas pārrunas par līguma slēgšanu starp uzņēmumu, kas atrodas vienas Puses teritorijā un otru uzņēmumu, kas atrodas otras Puses teritorijā, tās Puses Nacionālā drošības iestāde, kuras teritorijā klasificētais līgums tiks izpildīts, informē otru Pusi par tās klasificētās informācijas klasifikācijas pakāpēm, kas ir saistīta ar šīm pārrunām.

6. Katram klasificētam līgumam, kas tiek noslēgts starp Pušu institūcijām šī Līguma ietvaros, ir jāsaturs atbilstoša drošības sadaļa, kurā ir noteikti sekojoši aspekti:

a) Projekta klasifikācijas pakāpju rādītājs un klasificētās informācijas saraksts;

b) Informācijas klasifikācijas pakāpju izmaiņu paziņošanas procedūra;

c) Saziņas kanāli un elektromagnētiskās nosūtīšanas līdzekļi;

d) Klasificētās informācijas transportēšanas procedūra;

e) Atbildīgās institūcijas par klasificētās informācijas, kas ir saistīta ar līgumu, aizsardzības koordinēšanu;

f) Pienākums informēt par jebkuru notikušu vai iespējamu klasificētās informācijas pazaudēšanu, izpaušanu vai kompromitēšanu.

7. Jebkura klasificēta līguma drošības sadaļas kopija tiek nosūtīta tās Puses Nacionālajai drošības iestādei, kurā klasificētais līgums tiks izpildīts, lai nodrošinātu atbilstošu drošības pārraudzību un kontroli.

8. Nacionālo drošības iestāžu pārstāvji var apmeklēt viens otru, lai analizētu līgumslēdzēja noteikto pasākumu efektivitāti klasificētā līguma izpildē iesaistītās klasificētās informācijas aizsardzībai. Šādas vizītes tiek pieteiktas vismaz trīsdesmit dienas iepriekš.

13. Pants

Vizītes

1. Vizīšu veikšanai, kuru laikā vienas Puses pārstāvjiem pie otras Puses ir nepieciešama pieeja klasificētajai informācijai, ir jāsaņem iepriekšēja rakstiska atļauja no uzņēmējas Puses Nacionālās drošības iestādes.

2. Viena puse atļauj veikt vizītes, kuru laikā ir nepieciešama pieeja klasificētai informācijai, otras Puses apmeklētājiem tikai tādā gadījumā, ja viņi ir:

a) Saņēmuši atbilstošas speciālās atļaujās, ko ir izsniegusi vizītes prasītājas Puses Nacionālā drošības iestāde vai cita atbildīgā valsts institūcija;

b) Pilnvaroti saņemt vai piekļūt klasificētajai informācijai uz „nepieciešamība zināt” pamata saskaņā ar nacionālajiem normatīvajiem aktiem.

3. Vizītes prasītājas Puses Nacionālā drošības iestāde nosūta uzņēmējas Puses Nacionālajai drošības iestādei pieprasījumu par plānoto vizīti, kas ir jāsaņem vismaz trīsdesmit dienas pirms vizītes vai vizīšu sākuma.

4. Steidzamos gadījumos vizītes pieprasījums jānosūta vismaz septiņas dienas iepriekš.

5. Vizītes pieprasījumā iekļauj šādu informāciju:

a) Apmeklētāja vārds un uzvārds, dzimšanas vieta un datums, pilsonība, pases vai personību apliecināša dokumenta numurs;

b) Iestādes, uzņēmuma vai organizācijas nosaukums, kuru apmeklētājs pārstāv vai kurai apmeklētājs pieder;

c) Iestādes, uzņēmuma vai organizācijas, kas tiks apmeklēta, nosaukums un adrese;

d) Apmeklētāja speciālās atļaujas apstiprinājums un tās derīguma termiņš;

e) Vizītes vai vizīšu mērķis un nolūks;

f) Pieprasītās vizītes vai vizīšu plānotais datums un ilgums. Atkārtotu vizīšu gadījumā jānorāda kopējais vizīšu periods;

g) Apmeklējamās iestādes vai objekta kontaktpersonas vārds un telefona numurs, iepriekšēji kontakti un cita informācija, kas ļauj noteikt vizītes vai vizīšu pamatojumu;

h) Datums, paraksts un atbilstošās drošības iestādes oficiālais zīmogs.

6. Tās Puses Nacionālā drošības iestāde, kas saņem vizītes pieprasījumu, izskata to, pieņem lēmumu un informē par to vizītes prasītājas Puses Nacionālo drošības iestādi.

7. Vizītes, kuru veikšanai citas valsts pavalstniekiem ir nepieciešama pieeja klasificētajai informācijai, atļauj tikai pēc abpusējas Pušu piekrišanas.

8. Tiklīdz vizīte tiek apstiprināta, uzņēmējas Puses Nacionālā drošības iestāde iesniedz vizītes pieprasījuma kopiju apmeklējamās iestādes, objekta vai organizācijas atbildīgajiem par drošību.

9. Vizītes atļaujas derīguma termiņš nepārsniedz divpadsmit mēnešus.

14. Pants

Atkārtotas vizītes

1. Jebkura projekta, programmas vai līguma ietvaros Puses var vienoties par tādu personu saraksta izveidošanu, kas var veikt atkārtotas vizītes. Šādi saraksti ir derīgi divpadsmit mēnešus.

2. Tiklīdz Puses šos sarakstus apstiprina, konkrēto vizīšu nosacījumus saskaņo tieši ar apmeklējamo organizāciju atbildīgajām personām saskaņā ar noteiktajiem nosacījumiem.

15. Pants

Drošības pārkāpums un kompromitēšana

1. Ja drošības pārkāpuma vai kompromitēšanas rezultātā ir notikusi vai ir iespējama klasificētās informācijas, kura ir izcēlusies vai saņemta no otras Puses, nesankcionēta izpaušana, tās Puses Nacionālā drošības iestāde, kur drošības pārkāpums vai kompromitēšana ir notikusi, nekavējoties informē otras Puses Nacionālo drošības iestādi un veic nepieciešamo izmeklēšanu.

2. Ja drošības pārkāpums vai kompromitēšana notiek valstī, kas nav šī Līguma puse, tās Puses Nacionālā drošības iestāde, kura ir nosūtījusi informāciju, veic pasākumus saskaņā ar šī panta 1. daļu.

3. Ja nepieciešams, otra Puse piedalās izmeklēšanā.

4. Jebkurā gadījumā otra Puse tiek rakstiski informēta par izmeklēšanas rezultātiem, tai skaitā par drošības pārkāpuma vai kompromitēšanas iemesliem, zaudējuma apmēru un izmeklēšanas secinājumiem.

16. Pants

Izdevumi

Katra Puse sedz savus izdevumus saistībā ar visiem šī Līguma piemērošanas un pārraudzības aspektiem.

17. Pants

Strīdu izšķiršana

Jebkuri strīdi, kas saistīti ar šī Līguma nosacījumu interpretāciju vai piemērošanu, tiek risināti caur diplomātiskiem kanāliem.

18. Pants

Grozījumi

1. Šis Līgumu var tikt grozīts pamatojoties uz abu Pušu savstarpēju rakstisku vienošanos.

2. Grozījumi stājas spēkā saskaņā ar nosacījumiem, kas noteikti šī Līguma 20. pantā.

19. Pants

Terminš un izbeigšana

1. Šis Līgums ir noslēgts uz nenoteiktu laiku.
2. Katra Puse var jebkurā laikā izbeigt šī Līguma darbību.

3. Par Līguma darbības izbeigšanu ir jāinformē rakstiski pa diplomātiskajiem kanāliem. Līgums zaudē spēku pēc sešiem mēnešiem, skaitot no datuma, kurā ir saņemts šāds paziņojums.

4. Neskatoties uz Līguma darbības izbeigšanu, visa klasificētā informācija, kas ir nodota saskaņā ar šo Līgumu, tiek aizsargāta, kā noteikts šajā Līgumā, kamēr izcelsmes Puse neatbrīvo saņēmēju Pusi no šī pienākuma.

20. Pants

Stāšanās spēkā

Šis Līgums stājas spēkā trīsdesmitajā dienā pēc pēdējā rakstiskā paziņojuma saņemšanas pa diplomātiskajiem kanāliem, ar kuru informē, ka Puses ir izpildījušas visas iekšējās procedūras.

To apliecinot, šo Līgumu ir parakstījuši pilnvaroti šī Līguma parakstītāji.

Līgums noslēgts Lissabonā, 2007. gada 24. janvārī, divos oriģinālos eksemplāros portugāļu, latviešu un angļu valodās, un visi teksti ir vienlīdz autentiski. Dažādu interpretāciju gadījumā noteicošais ir teksts angļu valodā.

Portugāles Republikas vārdā, *Manuel Lobo Antunes*, Valsts sekretārs – ministra biedrs un Eiropas lietās.

Latvijas Republikas vārdā, *Ints Upmacis*, Latvijas vēstnieks Portugālē.

AGREEMENT FOR THE MUTUAL PROTECTION OF CLASSIFIED INFORMATION BETWEEN THE PORTUGUESE REPUBLIC AND THE REPUBLIC OF LATVIA

The Portuguese Republic and the Republic of Latvia, hereinafter referred to as the Parties;

Recognising the need of both Parties to guarantee the protection of the classified information exchanged between them within the scope of the negotiations and cooperation agreements concluded, or to be concluded, as well as other contractual instruments from both, public or private entities of the Parties;

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 contractual instruments, which envisage the transmission of classified information, signed or to be signed between the adequate national authorities of both Parties or by organizations or companies duly authorized to that purpose.

Article 2

Scope of application

The present Agreement sets out procedures for the protection of classified information exchanged between the Parties.

Article 3

Definitions

For the purposes of the present Agreement:

a) «Classified information» means 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, in accordance with the national law in force of the originating party;

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

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

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

e) «Third party» means any international organisation or state that is not a Party to the present Agreement;

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

g) «Contractor» means an individual or a legal entity possessing the legal capacity to conclude classified contracts;

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

i) «Facility security clearance» means the determination by the national security authority or other relevant state authority that, from a security point of view, a facility has the physical and organisational capability to use and deposit classified information, in accordance with the respective national law in force;

j) «Need-to-know» means a principle that the access to classified information that may only be granted to a person who has a verified requirement for knowledge of, or possession of such information in order to perform official and professional duties, within the framework of which the information was released to the receiving party;

k) «Project security classification guide» means the part of the project security instructions, which identifies the elements of the project that are classified, specifying the security classification levels.

Article 4

National security authorities

1 — The responsible national security authorities for the application of the present Agreement are:

For the Portuguese Republic:

National security authority, Presidency of the Council of Ministers, Av. Ilha da Madeira, 1, 1400-204 Lisbon, Portugal;

For the Republic of Latvia:

Constitution Protection Bureau, Miera street 85 a Riga, LV 1013, Latvia.

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

3 — The national security authorities, without altering any obligations hereby agreed, may conclude arrangements for the technical implementation of the present Agreement.

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 receiving party shall grant to the received classified information a level of protection equivalent to the markings expressly given to the classified information by the originating party;

b) Access to classified information and to locations and facilities where classified activities are performed or where classified information is stored, is limited to persons who have been granted a personnel security clearance for access to information classified «confidencial/konfidenciāli» or above, and who, due to their functions or employment, have a need-to-know.

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 the protection of classified information.

Article 6

Security classifications and equivalences

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

Portuguese Republic	Republic of Latvia	English
Muito secreto	Sevišķi slepeni	Top secret.
Secreto	Slepeni	Secret.
Confidencial	Konfidenciāli	Confidential.
Reservado	Dienesta vajadzībām	Restricted.

Article 7

Classification, reception, and alterations

1 — The receiving party shall mark the received classified information with its own equivalent security clas-

sification, in accordance with the equivalences referred in article 6 of the present Agreement.

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

3 — The receiving party and/or entities from its State shall neither downgrade nor declassify the received classified information without the prior written consent of the originating party.

Article 8

Translation, reproduction and destruction

1 — Classified information marked as «muito secreto/sevišķi slepeni» shall be translated and reproduced 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;

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 shall be destroyed or modified in such a manner so as to prevent reconstruction of the classified information in whole or in Part.

4 — Classified information marked as «muito secreto/sevišķi slepeni» shall not be destroyed and it shall be returned to the national security authority of the originating party, unless there is a case of immediate danger, in which such information may be destroyed without the prior written permission of the national security authority of the originating party, who shall be promptly notified of that event.

5 — Destruction of classified information marked as «secreto/slepeni» shall be notified to the originating party.

6 — Classified information marked up to «confidencial/konfidenciāli», including, shall be destroyed in accordance with the respective national law in force.

Article 9

Transmission between the Parties

1 — The classified information shall normally be transmitted between the Parties through diplomatic channels.

2 — If the use of such channels would be impractical or unduly delay receipt of the classified information, transmissions may be undertaken by appropriately security cleared personnel empowered with a courier certificate issued by the Party, which transmits the classified information.

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

4 — Both national security authorities shall approve delivering of large items or quantities of classified information, arranged on a case-by-case basis.

5 — The receiving party shall confirm the reception, in writing, of the classified information and shall transmit 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, under the agreements or any other contractual instruments signed between the Parties.

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

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

4 — The receiving party will not transmit the classified information to a third party, any individual or legal entity, which holds the nationality of a third State, without prior written authorization from the originating party.

Article 11

Security clearances

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

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

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

Article 12

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 duly classified information;

b) Have a proper level of security clearance granted to those premises;

c) Have a proper level of 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, according to the national law in force;

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 an entity located in the territory of one of the Parties and another entity located in the other Party's territory, aiming at the signing of classified contractual instruments, the national security authority of the Party in whose territory the classified contract will be performed shall inform the other Party of the security classification given to the classified information related to those pre-contractual negotiations.

6 — Every classified contract concluded between entities of the Parties, under the provisions of the present Agreement, shall include an appropriate security section 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 electromagnetic transmission;

d) Procedure for the transportation of classified information;

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

f) An obligation to notify any actual or suspected loss, leak or compromise of the classified information.

7 — Copy of the security section of any classified contract shall be forwarded to the national security authority of the Party where the classified contract is to be performed, 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, thirty days in advance.

Article 13

Visits

1 — Visits entailing access to classified information by nationals 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 relevant state 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 in force.

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 thirty days before the visit or visits take place.

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

5 — The request for visit shall include:

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

b) Name of the establishment, company or organisation the visitor represents or to which the visitor belongs;

c) Name and address of the establishment, company or organisation 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. In case of recurring visits the total period covered by the visits should be stated;

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

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

6 — The national security authority of the Party that receives the 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 entailing access to classified information by nationals from a third State shall only be authorized by a common agreement between the Parties.

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 establishment, facility or organisation to be visited.

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

Article 14

Recurring visits

1 — For any project, program or contract the Parties may agree to establish lists of authorized persons to make recurring visits. Those lists are valid for an initial period of twelve months.

2 — Once those lists have been approved by the Parties, the terms of the specific visits shall be directly arranged with the appropriate authorities of the organizations to be visited by those persons, in accordance with the terms and conditions agreed upon.

Article 15

Breach and compromise of security

1 — In case of breach or compromise 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 or compromise 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 or compromise of security occurs in a State other than the Parties, the national security authority of the despatching 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 or the compromise of security, the extent of the damage and the conclusions of the investigation.

Article 16

Expenses

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

Article 17

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 18

Amendments

1 — The present Agreement may be amended on the basis of a mutual written consent of both Parties.

2 — The amendments shall enter into force in accordance with the terms specified in article 20 of the present Agreement.

Article 19

Duration and termination

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

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

3 — The termination shall be notified, in writing and through diplomatic channels, producing its effects six months after the date of reception of the respective 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 20

Entry into force

The present Agreement shall enter into force on the thirtieth day following the receipt of the last written notification through diplomatic channels, stating that all the internal procedures of both Parties have been fulfilled.

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

Done at Lisbon, on 24 January 2007, in two originals, each one in the portuguese, latvian and english languages, each text being equally authentic. In case of any divergence of interpretation, the english text shall prevail.

For the Portuguese Republic, *Manuel Lobo Antunes*, Secretary of State Assistant to the Minister and for European Affairs.

For the Republic of Latvia, *Ints Upmacis*, Ambassador of Latvia in Portugal.