ASSEMBLEIA DA REPÚBLICA

ADMINISTRAÇÃO DE SEGURANÇA DA INFORMAÇÃO

Ajuste Direto n.º

005/ASI/2021

CADERNO DE ENCARGOS

Licenciamento da plataforma de formação e sensibilização em cibersegurança da Cybeready (módulos: BLAST - Phishing Simulation Training, CAB - Continuous Awareness Bites e AuditReady)

Índice

1 ENQUADRAMENTO 1
2 OBJETO 1
3 CARACTERIZAÇÃO DO LICENCIAMENTO 1
4 ALOJAMENTO DO LICENCIAMETO 2
5 VIGÊNCIA CONTRATUAL 2
6 PREÇO, CONDIÇÕES DE PAGAMENTO E FATURAÇÃO 3
7 SIGILO E CONFIDENCIALIDADE 3
8 REQUISITOS DE PROTEÇÃO DE DADOS 4
9 REQUISITOS DE SEGURANÇA DA INFORMAÇÃO 5
10 CASOS FORTUITOS OU DE FORÇA MAIOR 6
11 PATENTES LICENÇAS E MARCAS 7
12 CESSÃO DA POSIÇÃO CONTRATUAL E SUBCONTRATAÇÃO 7
13 RESOLUÇÃO DO CONTRATO 7
14 GARANTIA 8
15 GESTOR DO CONTRATO 8
16 LEGISLAÇÃO APLICÁVEL 8
ANEXO I 9
ACORDO DE TRATAMENTO DE DADOS PESSOAIS EM SUBCONTRATAÇÃO 9

ASSEMBLEIA DA REPÚBLICA

ADMINISTRAÇÃO DE SEGURANÇA DA INFORMAÇÃO

1 ENQUADRAMENTO

No âmbito do processo de implementação do Sistema de Gestão da Segurança da Informação da Assembleia da República (SGSI-AR), em conformidade com as recomendações da norma ISO 27001, em janeiro de 2021, a Administração de Segurança da Informação deu início a uma campanha de simulação de ataques de *phishing,* com o objetivo de promover uma ação de formação e sensibilização em cibersegurança e simultaneamente aferir o nível de resiliência dos utilizadores da rede informática da AR a ataques cibernéticos.

No primeiro trimestre de 2021, foram realizadas 4 Campanhas que proporcionaram os seguintes resultados:

- Cerca de 50% dos utilizadores da rede informática da AR participaram na ação de formação e sensibilização em cibersegurança;
- Registou-se uma redução significativa do número de utilizadores que clicaram nos links apresentados nas mensagens de e-mails de simulação de *phishing* (cerca de 20%);
- Os Assistentes Operacionais Parlamentares (AOPs) representaram o perfil de utilizadores com maior percentagem de *clicks* a mensagens de simulação de *phishing* (cerca de 30%).

Nos meses de abril, maio, junho e julho, foram realizadas 5 campanhas que permitiram concluir o seguinte:

- É cada vez maior o número de utilizadores da rede informática da AR resilientes a ataques de phishing;
- O grupo de utilizadores de baixo risco, aqueles que raramente clicam em mensagens de phishing, é de aproximadamente 60%;
- O grupo de utilizadores de alto risco, aqueles que sempre clicam em mensagens de phishing, é de apenas 4%;
- O grupo de utilizadores de médio risco, aqueles que frequentemente clicam em mensagens de phishing, representa aproximadamente 36% dos utilizadores da rede AR;
- O registo de cerca de 50 novos utilizadores na rede informática da AR, entre abril e maio de 2021, provocou um aumento na percentagem de clicks de aproximadamente 20%.

2 OBJETO

O presente procedimento pré-contratual tem por objeto a aquisição do licenciamento da plataforma de formação e sensibilização em cibersegurança da Cybeready (módulos: BLAST - Phishing Simulation Training, CAB - Continuous Awareness Bites e AuditReady), pelo período de um ano.

3 CARACTERIZAÇÃO DO LICENCIAMENTO

O licenciamento da plataforma de formação e sensibilização em cibersegurança da Cybeready, tem como objetivo melhorar o nível de prontidão e conhecimento dos utilizadores da rede informática da AR para lidarem com a ameaça de ataques de *phishing* através de mensagens de correio eletrónico

O âmbito desta aquisição compreende o licenciamento dos seguintes módulos da plataforma de formação e sensibilização em cibersegurança da Cybeready:

Módulo BLAST

O modulo BLAST consiste de simulações contínuas de phishing cujo objetivo é treinar utilizadores da rede informática da AR para detetar e evitar ataques. O resultado esperado desta ação é aumentar a curva de experiência dos utilizadores de modo a alterar o comportamento dos mesmos perante ataques de phishing.

Módulo CAB

O módulo CAB consiste no envio de campanhas de "quizzes" para o e-mail dos utilizadores, com o objetivo de avaliação de conhecimentos sobre cibersegurança. A formação contempla todos os tópicos exigidos pelo NIST *National Institute of Standars and Technology*)[1] incluindo Passwords, Utilização da Web, Segurança Física, Políticas de Clean Desk, Dispositivos Amovíveis, Segurança de Telemóveis, Privacidade e Partilha de Informação, Redes Sociais, Phishing entre outros.

Módulo AuditReady

O módulo AuditReady, consiste numa plataforma de formação periódica, em complemento da formação contínua dos módulos BLAST e CAB. O AuditReady envia aos utilizadores ações de formação em matéria de sensibilização para a cibersegurança, acompanha a sua execução e gera relatórios em conformidade com a aptidão do utilizador, nos domínios de trabalho remoto, segurança física, clean desk, clean desktop, credenciais e autenticação, classificação e partilha de dados, videoconferências, confidencialidade e monitorização e registo

4 ALOJAMENTO DO LICENCIAMETO

O Licenciamento é prestado de forma centralizada na plataforma cloud do fabricante.

5 VIGÊNCIA CONTRATUAL

O licenciamento estará em vigor pelo período de 12 meses.

[1] https://www.nist.gov/

6 PREÇO, CONDIÇÕES DE PAGAMENTO E FATURAÇÃO

a) Pelo licenciamento dos módulos BLAST - Phishing Simulation Training, CAB - Continuous Awareness Bites e AuditReady da plataforma da Cybeready, a Assembleia da República pagará o preço total constante da proposta que não deverá exceder os 19.999,00 € (dezanove mil novecentos e noventa e nove euros), acrescido de IVA à taxa legal em vigor.

b) O pagamento do preço referido no número anterior será efetuado de uma só vez, após a disponibilização do licenciamento do pacote de software.

c) O pagamento será realizado no prazo de **trinta dias** após a apresentação da fatura correspondente pelo Contratante, desde que apresentada nos termos adequados à sua liquidação.

d) Em caso de discordância por parte da Assembleia da República quanto aos valores indicados na fatura, deve esta comunicar ao Contratante, por escrito, os respetivos fundamentos, ficando este obrigado a prestar os esclarecimentos necessários ou proceder à emissão de nova fatura corrigida.

7 SIGILO E CONFIDENCIALIDADE

a) Contratante obriga-se a garantir o sigilo quanto a informações, factos e ocorrências de que venha a ter conhecimento por força da execução do contrato, relacionadas com a atividade da entidade adjudicante ou com pessoas que nela exerçam funções, abrangendo esta obrigação os seus agentes, funcionários, colaboradores ou terceiros que se encontrem envolvidos no fornecimento ou no procedimento ao qual o mesmo deu origem.

b) Para além das ações penais e processos disciplinares que ao caso couber, o Contratante pagará à Assembleia da República uma compensação pela divulgação, seja por que meio for, de factos relativos à Assembleia da Republica, aos deputados, funcionários ou outros agentes vinculados à entidade pública contratante, num montante calculado pela seguinte fórmula: C = RMMG x 50, em que “C” corresponde ao montante da compensação (em euros) e “RMMG” corresponde ao valor da remuneração mínima mensal garantida em vigor.

c) O disposto no número anterior não é aplicável em caso de imposição legal ou judicial de comunicação de factos sigilosos, desde que sejam cumpridos os estritos termos e objetivos inerentes à obrigação de comunicação.

d) A aplicação pela Assembleia da República da compensação prevista no n.º 2 da presente cláusula, obedece às regras previstas no presente caderno de encargos para a aplicação de penalidades.

8 REQUISITOS DE PROTEÇÃO DE DADOS

O adjudicatário compromete-se a assegurar cumprimento das obrigações decorrentes da legislação de proteção de dados (vd. anexo I) aplicável, em particular, o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27/4 de 2016, (adiante, RGPD), bem como, a Lei de Execução Nacional aprovada pela Lei n.º 58/2019, de 8 de agosto, no decurso do procedimento concursal, bem como durante a vigência do contrato, nomeadamente as seguintes:

a) Garantir a confidencialidade dos dados pessoais a que tenha ou venha a ter acesso por via do presente procedimento ou do contrato, ou qualquer ato relacionado direta ou indiretamente a decorrer deste, nomeadamente, assegurando que as pessoas autorizadas a tratar os dados pessoais assumiram um compromisso de confidencialidade ou estão sujeitas a adequadas obrigações legais de confidencialidade;

b) Tratar os dados pessoais a que tenha acesso por via do presente, apenas para as finalidades previstas no presente Caderno de Encargos e no respetivo contrato e segundo as instruções da Assembleia da República

c) Informar a Assembleia da República, caso considere que alguma das instruções por esta providenciada possa dar origem ao incumprimento da legislação aplicável em matéria de proteção de dados pessoais;

d) Implementar as medidas técnicas e organizativas de segurança, adequadas a assegurar a confidencialidade, a integridade e a disponibilidade dos dados pessoais, bem como a resiliência dos sistemas e serviços de tratamento, designadamente as previstas no artigo 32.º do RGPD, a fim de impedir a destruição, acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizados, bem como qualquer outra forma de tratamento ilícito dos dados pessoais;

e) Não subcontratar o tratamento de dados pessoais da entidade adjudicante, sem a sua prévia autorização escrita;

f) Em caso de autorização de subcontratação, impor ao subcontratado as obrigações em matéria de proteção de dados estabelecidas no presente Caderno de Encargos;

g) Notificar a Assembleia da República de quaisquer transferências de dados pessoais para país fora do Espaço Económico Europeu e que não apresente um nível adequado de proteção;

h) Informar a Assembleia da República, com a maior brevidade possível, em caso de efetivo ou potencial incidente de violação de dados pessoais;

i) Prestar assistência à Assembleia da República no sentido de permitir que esta cumpra a obrigação de dar resposta aos pedidos dos titulares dos dados, tendo em vista o exercício dos direitos previstos no RGPD, bem como as obrigações estabelecidas nos artigos 32.º a 36.º do RGPD;

j) Disponibilizar à Assembleia da República todas as informações necessárias para que sejam cumpridas todas as obrigações a que o adjudicatário esteja sujeito, contribuindo para auditorias,

inspeções e demais fiscalizações conduzidas pelo Responsável pelo Tratamento, quando necessário e aplicável.

k) Sensibilizar o pessoal autorizado no âmbito do tratamento dos dados para as questões relacionadas com privacidade, proteção de dados e segurança da informação, garantindo ainda, a necessária formação ao correto manuseamento dos mesmos;

l) Finda a prestação de serviços, apagar ou devolver, segundo o critério da Assembleia da República, todos os dados pessoais tratados por sua conta, apagando as cópias existentes, sem prejuízo de conservação posterior que seja legalmente exigida.

9 REQUISITOS DE SEGURANÇA DA INFORMAÇÃO

No âmbito desta prestação de serviços, o adjudicatário obriga-se a cumprir os seguintes requisitos de segurança da informação:

a) A descrição da informação a ser fornecida/acedida e os métodos para fornecer/aceder a informação;

b) A classificação da informação fornecida/acedida tem de ser efetuada de acordo com os critérios de classificação de informação estabelecidos na AR;

c) Os requisitos legais e regulamentares aplicáveis, incluindo a proteção de dados, os direitos de propriedade intelectual, os direitos de autor (copyright) e uma descrição de como vai ser garantido o seu cumprimento;

d) A obrigação de cada parte contratual de implementar os controlos acordados, incluindo controlos de acesso, avaliação do desempenho, monitorização, gestão de incidentes, e realização de auditorias;

e) A lista de funcionários do fornecedor autorizados para aceder ou receber informação da AR ou, em alternativa, os procedimentos/condições estabelecidos para autorizar e remover os privilégios de acesso ou receção de informação da AR;

f) As políticas operacionais de segurança da informação relevantes para o contrato em causa;

g) Os requisitos do Processo de Gestão de Incidentes e Pedidos de Serviço da AR e do Processo de Gestão de Incidentes de Segurança da Informação, com destaque para as responsabilidades de notificação e colaboração durante a resolução de incidentes;

h) Os requisitos de formação e sensibilização necessários para determinados procedimentos e requisitos de segurança da informação (por exemplo, resposta a incidentes ou procedimentos de autorização);

i) Os regulamentos relevantes para a subcontratação, incluindo os controlos necessários a implementar;

j) Os acordos com parceiros relevantes, incluindo a pessoa de contacto para questões relacionadas com segurança da informação;

k) Os requisitos de rastreio, quando considerado necessário, dos funcionários dos fornecedores, tais como a verificação da sua identidade, a informação pessoal e o registo criminal. Estes requisitos incluem ainda as responsabilidades para conduzir os procedimentos de rastreio e notificação, no caso de o rastreio não ser concluído ou se os resultados levantarem dúvidas ou preocupações;

l) O direito de auditar os processos e controlos do fornecedor;

m) Os processos a seguir em caso de disputas contratuais;

n) A obrigação do fornecedor em providenciar informação sobre incidentes de segurança da informação para revisão da AR;

o) A obrigação do fornecedor em assegurar a monitorização e revisão dos aspetos de segurança da informação relativos às relações com os seus próprios fornecedores (quando aplicável);

p) A obrigação do fornecedor em assegurar a continuidade de serviço adequada, através de planos de recuperação de desastres que assegurem os níveis de continuidade dos serviços acordados com a AR, no caso de ocorrência de falhas ou desastres;

q) A obrigação do fornecedor em apresentar periodicamente relatórios sobre a eficiência dos controlos e as medidas estabelecidas para a correção atempada de questões relevantes suscitadas no relatório;

r) A obrigação do fornecedor em cumprir com os requisitos de segurança da informação da AR (e.g. proteção contra software malicioso; salvaguarda de dados; procedimentos de recuperação de desastres; controlos criptográficos; gestão de vulnerabilidade; gestão de incidentes de segurança da informação; recolha, manutenção e proteção de evidências, incluindo logs e audit trails; autenticação e controlo de acessos).

10 CASOS FORTUITOS OU DE FORÇA MAIOR

a) Nenhuma das partes pode ser responsável pelo incumprimento ou pelo cumprimento defeituoso das obrigações emergentes do contrato, na estrita medida em que se verifiquem em casos de força maior, sendo considerados casos de força maior as circunstâncias que impossibilitam o cumprimento das obrigações emergentes do contrato, alheias à vontade da parte afetada, que ela não pudesse conhecer ou prever à data da celebração do contrato e cujos efeitos não lhe fosse razoavelmente exigível contornar ou evitar.

b) A parte que invocar casos fortuitos ou de força maior deverá comunicar e justificar tais situações à outra parte, bem como informar o prazo previsível para restabelecer a situação.

c) Quando uma das partes não aceite por escrito que certa ocorrência invocada pela outra constitua força maior, cabe a esta fazer prova do mesmo.

d) A verificação de uma situação de força maior determina a prorrogação dos prazos de cumprimento das obrigações contratuais afetadas, pelo período de tempo comprovadamente correspondente ao impedimento resultante de força maior.

e) Caso a impossibilidade de execução do contrato, em resultado de força maior, se prolongue por um período continuo superior a um mês, qualquer das partes pode proceder à respetiva resolução, mediante comunicação enviada à outra parte, com pelo menos 5 (cinco) dias de antecedência.

11 PATENTES LICENÇAS E MARCAS

a) São da responsabilidade do adjudicatário quaisquer encargos decorrentes da utilização, de marcas registadas, patentes registadas ou licenças.

b) Caso a entidade adjudicante venha a ser demandada por ter infringido, na execução do contrato, qualquer dos direitos mencionados no ponto anterior, o adjudicatário indemniza-a de todas as despesas que, em consequência haja lugar e de todas as quantias que tenha que pagar, seja a que titulo for.

12 CESSÃO DA POSIÇÃO CONTRATUAL E SUBCONTRATAÇÃO

a) O adjudicatário não pode ceder a terceiros, total ou parcialmente, a sua posição contratual, ou qualquer dos direitos e obrigações decorrentes do contrato, nomeadamente subcontratar, sem autorização prévia da entidade adjudicante.

b) Para efeitos de obtenção da *suprarreferida* autorização, deverá o adjudicatário observar o previsto sobre esta matéria no artigo 318.º do Código dos Contratos Públicos.

13 RESOLUÇÃO DO CONTRATO

a) A entidade adjudicante reserva-se ao direito de resolver o contrato em caso de incumprimento definitivo pelo adjudicatário das suas obrigações contratuais, nos termos do disposto na parte final do n.º 1 do artigo 325.º e ainda do disposto nos artigos 334.º, 335.º e 448.º do Código dos Contratos Públicos.

b) Em tais circunstâncias a entidade adjudicante comunicará por escrito ao adjudicatário as deficiências do serviço, fixando um prazo para a sua regularização, findo o qual, se as anomalias não tiverem sido totalmente corrigidas, terá lugar a resolução do contrato que será comunicada ao adjudicatário mediante carta registada com aviso de receção, na qual serão indicadas as razões que a entidade adjudicante considera justificativas da resolução.

c) Sem prejuízo da resolução do contrato nos termos previstos nos pontos anteriores, a entidade adjudicante mantém o direito ao pagamento das indemnizações e penalidades aplicáveis nos termos do presente caderno de encargos ou de qualquer disposição legal vigente.

14 GARANTIA

O adjudicatário garantirá, sem qualquer encargo para a entidade adjudicante, a plena utilização da licença, pelo prazo indicado na sua proposta, que não pode ser inferior a 1 (um) ano a contar da data efetiva de início da prestação do serviço.

15 GESTOR DO CONTRATO

A entidade adjudicante, dando cumprimentos ao previsto no artigo 290.º-A do CCP, designará um gestor do contrato, com a função de acompanhar permanentemente a execução deste último.

16 LEGISLAÇÃO APLICÁVEL

Em tudo o que o presente caderno de encargos for omisso observar-se-á o disposto no C.C.P., aprovado pelo Decreto-Lei n.º 18/2008, de 29 de janeiro, na sua redação atual e demais legislação aplicável e, em qualquer caso, sempre a Lei portuguesa.

ANEXO I

ACORDO DE TRATAMENTO DE DADOS PESSOAIS EM SUBCONTRATAÇÃO

Nos termos e para os efeitos do disposto no artigo 28.º do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 (Regulamento Geral sobre Proteção de Dados, adiante designado RGPD), e considerada, ainda, a Lei 58/2019, de 8 de agosto, que o executa na ordem jurídica portuguesa, o presente acordo rege-se pelas cláusulas seguintes:

Definições:

Dados Pessoais: informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular.

Tratamento: uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição.

Responsável pelo Tratamento: pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro.

Contratante: Pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes, definida no RGPD como *Subcontratante*.

Subcontratado: Pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo, designada no RGPD como *Outro Subcontratante*, que trate os dados pessoais por conta do Responsável do Tratamento, subcontratado pelo Contratante.

Cláusula 1.ª

Objeto e âmbito de aplicação

O presente acordo vincula o Contratante à Assembleia da República e regula o tratamento de dados a realizar pelo Contratante, por conta da Responsável pelo Tratamento, nos termos do artigo 28.º do RGPD.

O presente acordo complementa e faz parte integrante do contrato de prestação de serviços celebrado entre as partes e que tem por objeto a aquisição licenciamento da plataforma de formação e sensibilização em cibersegurança da Cybeready (módulos: BLAST - Phishing Simulation Training, CAB - Continuous Awareness Bites e AuditReady).

No âmbito do contrato acima identificado, o Contratante tratará dados pessoais por conta da Assembleia da República para as seguintes finalidades: promover ações de sensibilização continua online - Continuous Awareness Bites (CAB).

Para efeitos do presente, o Contratante tratará*:* dados de contacto pertencentes às seguintes categorias de titulares de dados: funcionários da AR e deputados.

Cláusula 2.ª

Duração do presente acordo

O presente acordo de tratamento de dados pessoais em regime de subcontratação vigorará enquanto se mantiver em vigor o contrato de prestação de serviços entre a Assembleia da República e o Contratante ou até tais dados serem apagados ou devolvidos, por instrução daquela.

O acordo de tratamento de dados em apreço terminará com efeitos imediatos caso cesse o contrato de prestação de serviços celebrado entre as partes, por qualquer forma de cessação dos contratos, seja por resolução, caducidade, revogação ou denúncia, exceto se existirem instruções em contrário da Assembleia da República.

Cláusula 3.ª

Da relação entre a Assembleia da República e o Contratante

Compete à Assembleia da República determinar o âmbito, finalidades e forma pela qual o Contratante poderá aceder ou proceder ao tratamento dos dados pessoais.

O Contratante tratará os dados pessoais somente em conformidade com as instruções documentadas que lhe forem fornecidas pela Assembleia da República.

O Contratante notificará por escrito a Assembleia da República, e fundamentará, caso entenda que uma instrução que receba infringe o RGPD ou outra legislação nacional ou da União relativa à proteção de dados.

Cláusula 4.ª

Da contratação de outro subcontratado

O Contratante apenas contrata outro subcontratado quando a Assembleia da República tenha dado, previamente e por escrito, autorização específica para esse efeito.

Em caso de autorização por escrito, o Contratante informa a Assembleia da República de quaisquer alterações pretendidas quanto ao aumento do número ou à substituição de outros subcontratados, dando assim à Assembleia da República a oportunidade de se opor a tais alterações.

Caso o Contratante contrate outro subcontratado para a realização de operações específicas de tratamento de dados por conta da Assembleia da República, são impostas a esse outro subcontratado, por contrato ou outro ato normativo ao abrigo do direito da União ou da legislação nacional, as mesmas obrigações em matéria de proteção de dados que as estabelecidas neste acordo.

Caso esse outro subcontratado não cumpra as suas obrigações em matéria de proteção de dados, o Contratante que é parte neste contrato continua a ser plenamente responsável, perante a Assembleia da República, pelo cumprimento das obrigações desse outro subcontratado.

Em caso de autorização para subcontratação pela Assembleia da República o Contratante deverá preencher o ANEXO I.

Cláusula 5.ª

Das garantias de segurança do tratamento

As partes assumiram o presente vínculo jurídico reconhecendo a Assembleia da República as competências técnicas e de segurança do Contratante e este a possibilidade de delas dispor e poder implementar, a fim de ser levado a cabo o tratamento de dados pessoais para as finalidades definidas pela Assembleia da República.

Nos termos do artigo 32.º do RGPD, as partes devem aplicar as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, sem excluir outras que o tratamento exija ou venha a exigir, nomeadamente, a capacidade de garantir a confidencialidade, integridade e disponibilidade da informação e a resiliência dos sistemas de tratamento.

A Assembleia da República e o Contratante implementaram medidas que garantem que qualquer pessoa singular que tenha acesso a dados pessoais e agindo sob a autoridade da Assembleia da República ou do Contratante, só procede ao seu tratamento mediante instruções daquela, exceto se tal lhe for exigido pelo direito da União ou pela legislação nacional.

Cláusula 6.ª

Da confidencialidade

O Contratante deve assegurar que as pessoas autorizadas a tratar os dados pessoais assumiram um compromisso de confidencialidade ou estão sujeitas a adequadas obrigações legais de confidencialidade.

O fim do presente acordo de tratamento de dados pessoais em subcontratação não exonera o Contratante ou outros subcontratados do seu dever de confidencialidade, o qual se mantém sem limite temporal.

Cláusula 7.ª

Transferências de dados

O Contratante deverá imediatamente notificar a Assembleia da República de quaisquer transferências temporárias ou permanentes de dados pessoais para país fora do E.E.E.- Espaço Económico Europeu - que não apresente um nível adequado de proteção.

Essa transferência deverá ser apenas efetuada após a obtenção de autorização da Assembleia da República, que poderá recusá-la na medida do seu critério que entender adotar.

Cláusula 8.ª

Da assistência à Assembleia da República

O Contratante, na medida do possível e tomando em conta a natureza do tratamento, presta assistência à Assembleia da República através de medidas técnicas e organizativas adequadas, permitindo que esta cumpra a sua obrigação de dar resposta aos pedidos dos titulares dos dados tendo em vista o exercício dos seus direitos previstos RGPD, bem como as obrigações estabelecidas nos artigos 32.º a 36.º do RGPD.

O Contratante deve facilitar e contribuir para as auditorias, inclusive as inspeções, conduzidas pela Assembleia da República ou por outro auditor por este mandatado para o efeito.

Cláusula 9.ª

Do destino dos dados finda a prestação de serviços

De harmonia com o critério ou escolha da Assembleia da República, o Contratante apaga ou devolve-lhe todos os dados pessoais depois de concluída a prestação de serviços relacionados com o tratamento, apagando as cópias existentes, a menos que a conservação dos dados seja exigida ao abrigo do direito da União ou dos Estados-Membros.

Cláusula 10.ª

Gestão de incidentes

No caso de o Contratante tomar conhecimento de incidente que afete o tratamento de dados pessoais deverá prontamente notificar a Assembleia da República desse facto, com ela cooperar e seguir as suas instruções relativas a tais incidentes, de modo a permitir-lhe executar uma investigação aprofundada do incidente e responder-lhe corretivamente tomando as medidas adequadas.

Cláusula 11.ª

Da responsabilidade do Contratante

O Contratante deverá indemnizar a Assembleia da República e assumir a responsabilidade em relação a qualquer queixas, procedimentos, queixas de terceiros, perdas, danos e encargos em que a Assembleia da República incorra e que decorram, direta ou indiretamente de violações do presente contrato e/ou legislação de proteção de dados aplicável imputáveis ao Contratado.

Cláusula 12.ª

Entrada em vigor

O presente acordo de tratamento de dados pessoais em subcontratação entre a Assembleia da República e o Contratante vigorará a partir da data da outorga do contrato subjacente a este procedimento pré-contratual.

Cláusula 13.ª

Lei do contrato e Conflitos

O presente acordo rege-se pela lei portuguesa e pelas normas europeias diretamente aplicáveis.

Na eventualidade de existir um conflito entre o contrato de prestação de serviços e este acordo de tratamento de dados pessoais em subcontratação entre a Assembleia da República e o Contratante, este deverá prevalecer sobre o primeiro.