POLÍTICA GERAL DE PROTEÇÃO DE DADOS PESSOAIS

INDÍCE

1. FINALIDADE, ÂMBITO E DESTINATÁRIOS

A RISI, doravante referida como a "Empresa", esforça-se para cumprir as leis e regulamentos aplicáveis relacionados à proteção de dados pessoais nos países onde a Empresa opera. Esta Política estabelece os princípios básicos pelos quais a Empresa processa os dados pessoais de consumidores, clientes, fornecedores, parceiros de negócios, funcionários e outros indivíduos, e indica as responsabilidades dos seus departamentos comerciais e funcionários durante o processamento de dados pessoais.

Esta Política aplica-se à Empresa e suas subsidiárias integrais, controlada direta ou indiretamente, que conduzem negócios dentro da Área Econômica Europeia (EEA) ou processam os dados pessoais de sujeitos de dados dentro da EEA.

Os utilizadores deste documento são todos funcionários, permanentes ou temporários, e todos os contratados que trabalham em nome da Empresa.

2. DOCUMENTOS DE REFERÊNCIA

- EU GDPR 2016/679 (REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados))
- Retificação do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016
- 10 Medidas para preparar a aplicação do Regulamento Europeu de Proteção de Dados (CNPD)
- Política de Proteção de Dados do Funcionário (02.2)
- Política de Retenção de Dados (02.6)
- Descrição do cargo de Encarregado da Proteção de Dados (02.8)
- Diretrizes do Inventário de Dados e Mapeamento de Atividades de Processamento (03.1)
- Procedimento de Acesso aos Dados pelo Titular dos Dados (04.5)
- Metodologia de Avaliação do Impacto da Proteção de Dados (AIPD) (05.1)
- Política de segurança de TI (08.1)
- Política de Controle de Acessos (08.2)
- Procedimentos de Segurança para o Departamento de TI (08.3)
- Política BYOD (Traga seu próprio dispositivo) (08.4)
- Política de Dispositivos Móveis e Trabalho Remoto (08.5)
- Política de Ecrã e Mesa Limpa (08.6)
- Política de Classificação de Informação (08.7)
- Política de Anonimização e Pseudonimização (08.8)
- Politica sobre o uso da Encriptação (08.9)
- Plano de Disaster Recovery (08.10)
- Procedimentos de Auditoria Interna (08.11)
- Lista de Verificação de Auditoria Interna da ISO 27001 (Anexo A) (08.12)
- Procedimento de Resposta e Notificação de Violação de Dados (09.1)

3. DEFINIÇÕES

As seguintes definições de termos usados neste documento foram retiradas do Artigo 4 do Regulamento Geral de Proteção de Dados da União Europeia:

Dados Pessoais: Qualquer 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.

Dados Pessoais Sensíveis: Os dados pessoais que são, pela sua natureza, particularmente sensíveis em relação aos direitos e liberdades fundamentais merecem proteção específica, dado que o contexto do seu processamento pode criar riscos significativos para os direitos e liberdades fundamentais. Esses dados pessoais incluem dados pessoais revelando origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas, ou associação a sindicatos, dados genéticos, dados biométricos para identificar unicamente uma pessoa singular, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa singular.

Responsável pelo Tratamento: A 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.

Subcontratante: uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes.

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.

Anonimização: Desidentificar de forma irreversível os dados pessoais de forma que a pessoa não possa ser identificada usando tempo, custo e tecnologia razoáveis, seja pelo responsável pelo tratamento ou por qualquer outra pessoa, para identificar esse indivíduo. Os princípios de processamento de dados pessoais não se aplicam a dados anônimos, pois não são mais dados pessoais.

Pseudonimização: O tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável. Pseudonimização reduz, mas não elimina completamente, a capacidade de vincular dados pessoais a um assunto de dados. Como os dados sob pseudónimo ainda são dados pessoais, o processamento de dados sob pseudónimo deve obedecer aos princípios do Processamento de Dados Pessoais.

Tratamento Transfronteiriço: O tratamento de dados pessoais que ocorre no contexto das atividades de estabelecimentos em mais do que um Estado-Membro de um responsável pelo tratamento ou um subcontratante na União, caso o responsável pelo tratamento ou o subcontratante esteja estabelecido em mais do que um Estado-Membro; ou tratamento de dados pessoais que ocorre no contexto das atividades de um único estabelecimento de um responsável pelo tratamento ou de um subcontratante, mas que afeta substancialmente, ou é suscetível de afetar substancialmente, titulares de dados em mais do que um Estados-Membro.

Autoridade de Controlo: uma autoridade pública independente criada por um Estado-Membro nos termos do artigo 51 do RGPD da UE.

A **autoridade de controlo principal** é o organismo que tem como responsabilidade principal gerir uma atividade de tratamento transfronteiriço, por exemplo, quando está a ser investigada uma empresa que exerça atividades de tratamento em vários Estados-Membros. A autoridade principal coordena as operações que impliquem as autoridades de controlo interessadas, em conformidade com os artigos 60.º a 62.º do regulamento (p.ex., balcão único, assistência mútua e operações conjuntas). Apresenta qualquer projeto de decisão às autoridades de controlo com interesse na matéria.

Cada "**Autoridade de Controlo Local**" continuará a manter no seu próprio território e monitorizará qualquer processamento de dados local que afete os titulares de dados ou que seja realizado por um Responsável pelo Tratamento ou subcontratante da UE ou não UE quando o seu processamento atingir os titulares de dados residentes no seu território. Suas tarefas e poderes incluem conduzir investigações e aplicar medidas administrativas e multas, promovendo a conscientização pública sobre os riscos, regras, segurança e direitos em relação ao processamento de dados pessoais, bem como obter acesso a quaisquer instalações do responsável pelo tratamento e do subcontratante, incluindo qualquer equipamento e meios de processamento de dados.

"**Estabelecimento principal no que diz respeito a um responsável pelo tratamento**": Quando uma organização tem vários estabelecimentos na UE, o princípio a seguir é que o estabelecimento principal é o local da administração central dessa organização. No entanto, se outro estabelecimento tomar as decisões sobre as finalidades e os meios de tratamento – e tiver competência para mandar executar tais decisões –, passa a constituir o estabelecimento principal. Cabe aos responsáveis pelo tratamento de dados estabelecer claramente onde são tomadas as decisões sobre as finalidades e os meios das atividades de tratamento de dados pessoais.

O **estabelecimento principal do subcontratante** é o local da sua administração central na União, ou, caso não tenha administração central na União, o local onde são exercidas as principais atividades de tratamento de dados na União. Nos casos que impliquem tanto o responsável pelo tratamento como o subcontratante, a autoridade de controlo principal deverá continuar a ser a autoridade de controlo do Estado-Membro onde o responsável pelo tratamento tem o estabelecimento principal, mas a autoridade de controlo do subcontratante deverá ser considerada uma autoridade de controlo interessada e deverá participar no processo de cooperação previsto pelo presente regulamento.

Grupo de Empresas: Qualquer holding em conjunto com as sua(s) subsidiária(s).

4. PRINCÍPIOS BÁSICOS RELATIVOS AO PROCESSAMENTO DE DADOS PESSOAIS

Os princípios de proteção de dados descrevem as responsabilidades básicas das organizações que lidam com dados pessoais. O Artigo 5(2) do RGPD estipula que "*o Responsável pelo Tratamento deve ser responsável e demonstrar o cumprimento dos princípios*".

4.1. LICITUDE, LEALDADE E TRANSPARÊNCIA

Os dados pessoais devem ser objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados.

4.2. LIMITAÇÃO DAS FINALIDADES

Os dados pessoais devem ser recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades.

4.3. MINIMIZAÇÃO DOS DADOS

Os dados pessoais devem ser adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados. A Empresa deve aplicar a anonimização ou pseudonimização aos dados pessoais, se possível, para reduzir os riscos para os titulares de dados em causa.

4.4. EXATIDÃO

Os dados pessoais devem ser exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora.

4.5. LIMITAÇÃO DA CONSERVAÇÃO

Os dados pessoais devem ser conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados.

4.6. INTEGRIDADE E CONFIDENCIALIDADE

Levando em conta o estado da tecnologia e outras medidas de segurança disponíveis, o custo de implementação e a probabilidade e gravidade dos riscos de dados pessoais, a Empresa deve usar medidas técnicas ou organizacionais apropriadas para processar Dados Pessoais de uma maneira que garanta a segurança apropriada dos dados pessoais, incluindo proteção contra destruição acidental ou ilegal, perda, alternância, acesso não autorizado ou divulgação.

4.7. RESPONSABILIDADE

O responsável pelo tratamento é responsável pela demonstração da conformidade com os princípios acima descritos.

5. PROTEÇÃO DE DADOS NAS ATIVIDADES DO NEGÓCIO

Para demonstrar a conformidade com os princípios da proteção de dados, uma organização deve criar proteção de dados em todas as suas atividades de negócios.

5.1. NOTIFICAÇÃO DO TITULAR DOS DADOS

A RISI possui um **formulário de notificação do Titular dos dados**. Formulário esse que caso exista uma violação de dados pessoais podendo causar danos físicos, materiais ou imateriais às pessoas singulares, como a perda de controlo sobre os seus dados pessoais, a limitação dos seus direitos, a discriminação, o roubo ou usurpação da identidade, perdas financeiras, a inversão não autorizada da pseudonimização, danos para a reputação, a perda de confidencialidade de dados pessoais protegidos por sigilo profissional ou qualquer outra desvantagem económica ou social significativa das pessoas 4.5.2016 L 119/16 Jornal Oficial da União Europeia PT singulares. Por conseguinte, logo que a RISI tenha conhecimento de uma violação de dados pessoais, **notifica a Autoridade de Controlo (CNPD)** assim como o(s) **Titular(es) dos Dados** em causa, sem demora injustificada e, sempre que possível, no prazo de **72 horas** após ter tido conhecimento do ocorrido, a menos que seja capaz de demonstrar em conformidade com o princípio da responsabilidade, que essa violação não é suscetível de implicar um risco para os direitos e liberdades das pessoas singulares.

5.2. CONSENTIMENTO DO TITULAR DOS DADOS

A Empresa possui vários formulários do Titular dos dados. Formulários esses que são os seguintes:

- Formulário de Consentimento do Titular dos Dados (04.1)
- Formulário de Eliminação do Consentimento do Titular dos Dados (04.2)
- Formulário de Consentimento dos Pais (04.3)
- Formulário de Eliminação de Consentimento dos Pais (04.4)

5.3. RECOLHA

A A empresa deve-se esforçar para recolher a menor quantidade possível de dados pessoais. Se os dados pessoais forem recolhidos por terceiros, o **Departamento de Proteção de Dados** deve garantir que os dados pessoais são recolhidos legalmente.

5.4. USO, RETENÇÃO E DESTRUIÇÃO

Os propósitos, métodos, limitação de armazenamento e período de retenção de dados pessoais devem ser consistentes com as informações contidas na Política de Privacidade. A Empresa deve manter a precisão, integridade, confidencialidade e relevância dos dados pessoais com base no propósito do processamento. Mecanismos de segurança adequados, projetados para proteger os dados pessoais, devem ser usados para evitar que dados pessoais sejam roubados, mal utilizados ou violados, além de evitar violações de dados pessoais. O **Departamento de Proteção de Dados** é responsável pela conformidade com os requisitos listados nesta seção

5.5. DIREITO AO ACESSO PELO TITULAR DOS DADOS

Ao atuar como um responsável pelo tratamento, o Encarregado de Proteção de Dados é responsável por fornecer aos titulares dos dados um mecanismo de acesso razoável para permitir que eles acedam aos seus dados pessoais e permitir que eles atualizem, corrijam, apaguem ou transmitam seus Dados Pessoais, se apropriado ou exigido por lei. O mecanismo de acesso será detalhado no **Procedimento de Acesso aos Dados pelo Titular dos Dados** (04.5).

5.6. PORTABILIDADE DOS DADOS

Os titulares de dados têm o direito de receber, mediante solicitação, uma cópia dos dados que nos forneceram num formato estruturado e de transmitir esses dados para outro responsável pelo tratamento, gratuitamente. O **Departamento de Proteção de Dados** é responsável por garantir que tais solicitações sejam processadas dentro de um mês, que os pedidos não sejam excessivos e não afetem os direitos de dados pessoais de outros indivíduos.

5.7. DIREITO AO APAGAMENTO

Mediante solicitação, os Titulares dos Dados têm o direito de obter da Empresa o apagamento dos seus dados pessoais. Quando a Empresa está atuando como responsável pelo tratamento, Departamento de Proteção de Dados deve tomar as medidas necessárias (incluindo medidas técnicas) para informar os terceiros que usam ou processam esses dados para atender à solicitação.

6. DIRETRIZES DE PROCESSAMENTO

Os dados pessoais só devem ser processados quando explicitamente autorizados pelo **Departamento de Proteção de Dados**.

A Empresa deve decidir se executa a Avaliação de Impacto de Proteção de Dados para cada atividade de processamento de dados de acordo com as **Diretrizes da Avaliação de Impacto de Proteção de Dados**.

6.1. AVISOS AOS TITULARES DOS DADOS

No momento da recolha ou antes de recolher dados pessoais para qualquer tipo de atividades de processamento, incluindo, mas não limitado a, venda de produtos, serviços ou atividades de marketing, o **Departamento de Proteção de Dados** é responsável por informar adequadamente os titulares dos dados: os tipos de dados pessoais recolhidos, as finalidades do processamento, métodos de processamento, direitos dos titulares dos dados com relação aos seus dados pessoais, período de retenção, possíveis transferências internacionais de dados, e se os dados serão partilhados com terceiros e medidas de segurança da Empresa para proteger esses dados pessoais. Esta informação é fornecida através da **Política de Privacidade**.

Quando os dados pessoais confidenciais estiverem a ser recolhidos, o **Departamento de Proteção de Dados** deve certificar-se de que a política de privacidade declara explicitamente a finalidade para a qual esses dados pessoais confidenciais são recolhidos.

6.2. OBTENDO CONSENTIMENTO

Sempre que o processamento de dados pessoais for baseado no consentimento do titular dos dados ou em outros motivos legais, o **Departamento de Proteção de Dados** é responsável por manter um registo de tal consentimento. O **Departamento de Proteção de Dados** é responsável por fornecer aos titulares de dados opções para fornecer o consentimento e deve informar e garantir que o seu consentimento possa ser retirado a qualquer momento.

Quando a recolha de dados pessoais for relativa a uma criança menor de 13 anos, o **Departamento de Proteção de Dados** deve garantir que o consentimento dos pais seja dado antes da recolha, usando o Formulário de Consentimento dos Pais (04.3).

Quando surgem solicitações para corrigir, alterar ou destruir registos de dados pessoais, o **Departamento de Proteção de Dados** deve garantir que essas solicitações sejam tratadas dentro de um prazo razoável. O **Departamento de Proteção de Dados** também deve registar as solicitações e manter um registo das mesmas.

Os dados pessoais só devem ser processados para o propósito para o qual foram originalmente recolhidos. No caso em que a Empresa deseja processar dados pessoais recolhidos para outra finalidade, a Empresa deve obter o consentimento dos seus titulares de dados numa redação clara e concisa. Qualquer solicitação desse tipo deve incluir a finalidade original para a qual os dados foram recolhidos e também a(s) finalidade(s) nova(s) ou adicional(ais). A solicitação também deve incluir o motivo da mudança na(s) finalidade(s). O encarregado de proteção de dados é responsável pelo cumprimento das regras deste parágrafo.

Agora e no futuro, o **Departamento de Proteção de Dados** deve garantir que os métodos de recolha estejam em conformidade com as leis relevantes, boas práticas e padrões do setor.

O **Departamento de Proteção de Dados** é responsável por criar e manter um registo das Politicas de Privacidade.

7. ORGANIZAÇÃO E RESPONSABILIDADES

A responsabilidade de garantir o processamento adequado de dados pessoais é de todos que trabalham para ou com a Empresa e que têm acesso a dados pessoais processados pela Empresa.

As principais áreas de responsabilidades para o processamento de dados pessoais estão nas seguintes funções organizacionais:

A Gerência toma decisões e aprova as estratégias gerais da Empresa sobre a proteção de dados pessoais.

O **Encarregado de Proteção de Dados** é responsável pela gestão do programa de proteção de dados pessoais e é responsável pelo desenvolvimento e promoção de políticas de proteção de dados pessoais end-to-end, conforme definido na Descrição do Cargo de Encarregado da Proteção de Dados (02.8)

O **Advogado da Empresa em conjunto com o Encarregado de Proteção de Dados**, monitoriza e analisa as leis de dados pessoais e mudanças nos regulamentos, desenvolve requisitos de conformidade e auxilia os departamentos de negócios a atingir suas metas de dados pessoais.

O **Responsável pelo DRD,** é responsável por:

- Garantir que todos os sistemas, serviços e equipamentos usados para armazenar dados atendam a padrões de segurança aceitáveis.
- Realizar verificações regulares para garantir que o hardware e o software de segurança estejam a funcionar

adequadamente.

O **Responsável pelo DRH**, é responsável por:

- Melhorar a consciencialização de todos os funcionários no papel de utilizadores sobre a proteção de dados pessoais do usuário.
- Organizar formações de proteção de dados pessoais para os funcionários que trabalham com dados pessoais.
- Proteção dos dados pessoais dos funcionários. Deve-se garantir que os dados pessoais dos funcionários sejam processados com base nos objetivos e necessidades comerciais legítimos da entidade empregadora.

O **EPD** é responsável por passar as responsabilidades de proteção de dados pessoais aos fornecedores e melhorar os níveis de consciencialização dos fornecedores quanto à proteção de dados pessoais, bem como reduzir os requisitos de dados pessoais que os terceiros estejam a usar. O **Departamento de Proteção de Dados** deve garantir que a Empresa se reserva ao direito de auditar fornecedores.

8. RESPOSTA A INCIDENTES DE VIOLAÇÃO DE DADOS PESSOAIS

Quando a Empresa verifica uma violação de dados pessoais suspeita ou real, Departamento de Redes e Dados deve realizar uma investigação interna e tomar medidas corretivas adequadas em tempo hábil, de acordo com a **Política de Violação de Dados**. Caso exista qualquer risco para os direitos e liberdades dos titulares dos dados, a Empresa deve notificar as autoridades competentes em matéria de proteção de dados sem demora injustificada e, quando possível, no prazo de 72 horas.

9. AUDITORIA E RESPONSABILIZAÇÃO

O **Departamento de Proteção de Dados** é responsável por auditar como os departamentos de negócios implementam esta Política.

Qualquer funcionário que violar esta Política estará sujeito a ação disciplinar podendo também estar sujeito a responsabilidades civis ou criminais se sua conduta violar leis ou regulamentos.

10. CONFLITOS DAS LEIS

Esta Política destina-se a cumprir as leis e regulamentos no lugar do estabelecimento e dos países nos quais a RISI opera. **No caso de qualquer conflito entre esta Política e as leis e regulamentos aplicáveis, estes últimos prevalecerão.**