POLÍTICA DE CONFORMIDADE COM A RGPD

Objetivo

A presente Política é um documento que regula a atividade da empresa Softline na área de conformidade com os requisitos atuais e específicos do Regulamento (UE) 2016/679 (Regulamento Geral de Proteção de Dados Pessoais, "RGPD").

O objetivo desta Política é assegurar a proteção dos direitos e interesses da pessoa que tem os dados, o que vai garantir a segurança da Empresa perante a responsabilidade definida pela lei e a integridade das operações comerciais.

Disposições gerais

A presente Política é aplicada em todos os escritórios de representação da Softline e a todos os funcionários.

Os funcionários da Softline são obrigados a:

· familiarizar-se com a presente Política e quaisquer outros documentos que visam a implementação desta Política, entendê-la e segui-la;

· fazer a formação exigida, incluindo treinamento e ensino;

· notificar os parceiros de negócio sobre os requisitos da presente Política.

Os diretores são obrigados a:

· garantir que os funcionários e parceiros de negócio sigam os requisitos e instruções desta Política.

O Serviço de Conformidade/Diretor de Conformidade são obrigados a:

·atualizar a presente Política e quaisquer outros documentos que visam a realização dela, caso for preciso;

· fornecer consultas e apoio aos funcionários e parceiros de negócios em relação ao cumprimento dos requisitos desta Política e legislação.

Esta Política não substitui as políticas de segurança existentes.

Termos e definições

Dados pessoais são qualquer informação relativa à identificação de uma pessoa singular (titular de dados); uma pessoa singular identificável é uma pessoa que pode ser identificada direta ou indiretamente, em particular, por meio de tais identificadores como nome, patronímico, apelido, número de identificação, dados de localização, identificador online, bem como por meio de uma ou mais características específicas relativas à identidade física, fisiológica, genética, mental, económica, cultural ou social desta pessoa singular.

O responsável pelo tratamento de dados é pessoa física ou jurídica, órgão estatal, agência ou outro organismo qualquer que, individualmente ou em conjunto com os outros, define os objetivos e os meios de tratamento de dados pessoais.

O responsável pelo processamento de dados é pessoa física ou jurídica, órgão estatal, agência ou outro organismo qualquer que trata os dados pessoais em nome e por pedido do responsável por tratamento dos dados.

Princípios de tratamento de dados pessoais

Legitimidade, justiça e transparência - os dados pessoais devem ser tratados de forma legal, justa e transparente. A melhor maneira de cumprir este requisito é avaliar as ações de tratamento dos dados do ponto de vista da pessoa em causa, titular dos dados, e das suas expectativas.

Objetivos de limitação - os dados pessoais devem ser recolhidos para fins específicos, explícitos e legítimos. A melhor abordagem para cumprir este requisito é evitar os objetivos gerais e definir os objetivos tão especificamente quanto possível.

Minimização dos dados - os dados pessoais a serem tratados devem ser adequados, atualizados e limitados de acordo com os fins específicos para os quais estão a ser tratados. Se for possível, os dados pessoais devem ser anónimos ou pseudónimos. Cada ativo de dados processado pela Empresa deve ser avaliado e reduzido no volume para ajustá-lo ao volume necessário para o fim específico do processamento. Quando os dados já não são necessários para os fins para os quais eles foram recolhidos e, se não houver uma razão legal para os guardar, os dados pessoais devem ser completamente eliminados ou despersonalizados.

Precisão - os dados pessoais a serem processados devem ser exatos e atualizados, caso for necessário. Quaisquer dados novos relativos ao titular dos dados devem ser registados de modo a definir claramente a sua precisão e relevância.

Integridade e confidencialidade - os dados pessoais devem ser tratados de forma a garantir uma segurança adequada dos dados pessoais, incluindo a proteção contra o processamento não autorizado ou ilegal e contra a perda, destruição ou danos causados acidentalmente, utilizando as medidas técnicas ou organizacionais adequadas.

Princípios de segurança dos dados

Abordagem sistémica. Todos os ativos da Empresa são considerados como os componentes inter-relacionados que dependem uns dos outros no sistema único. No caso da presença das ameaças à segurança de informação, o número máximo possível dos cenários do comportamento do sistema são tomados em consideração. O sistema de proteção é construído tendo em conta tanto todos os canais conhecidos de acesso não autorizado à informação, como levando em consideração a possibilidade de surgimento dos canais completamente novos para efetuar ameaças de segurança.

Abordagem integrada. Para garantir a segurança da informação, a ampla gama de medidas, métodos e meios de proteção da informação são implementada. O seu uso complexo pressupõe a coordenação de medidas diferentes na construção do sistema de proteção completo que possam bloquear todos os canais de ameaça existentes e não contenham os pontos fracos nas junções dos seus componentes individuais. A Empresa toma as medidas e procedimentos eficazes para verificar a segurança dos dados tanto no caso de comunicações eletrónicas como no caso de transações não automatizadas dos dados nas instalações físicas da Empresa.

Princípio da separação. Não se pode confiar apenas numa linha de defesa, por mais segura que pareça. O sistema de garantia de segurança da informação é projetado de maneira que a zona de segurança mais protegida esteja localizada dentro de outras zonas protegidas. Os dados são armazenados e processados de maneira a garantir a segurança de cada ativo de dados, caso a segurança de outros ativos de dados seja comprometida.

O princípio de resistência igual. A eficácia dos mecanismos de proteção não deve ser comprometida por causa de existência do elo fraco resultante da subestimação das ameaças reais ou da aplicação das medidas de proteção inadequadas.

O princípio de continuidade. A empresa garante que a segurança da informação é um processo contínuo e orientado pelo objetivo que envolve a tomada de medidas apropriadas em todas as etapas do ciclo de vida dos ativos dos dados.

O princípio da suficiência razoável. A empresa assume que é impossível criar uma proteção absoluta de todos os ativos de dados. Por isso, a escolha dos meios de proteção dos ativos corresponde às ameaças reais existentes e à sensibilidade de cada ativo de dados concreto.

Princípio da gestão. Todos os processos de gestão e segurança dos dados na Empresa são controlados, ou seja, os processos e seus componentes são monitorizados e medidos, as violações de segurança de informação são detetadas atempadamente e são tomadas as medidas apropriadas.

Princípio da responsabilidade pessoal. Cada funcionário é responsável pela segurança e proteção dos ativos de dados que estão à sua disposição.

Proteção dos dados por definição e por defeito

A implementação destes princípios é da responsabilidade do controlador. No entanto, o responsável pelo processamento está envolvido na implementação no âmbito das políticas e procedimentos de conformidade do controlador.

O requisito geral resultante destes princípios é ter em conta a proteção do titular dos dados em causa, os interesses e as expectativas do tratamento durante todo o ciclo de vida do tratamento. Os titulares dos dados são livres de tomar decisões sobre o tratamento dos seus dados. Estes princípios são implementados por defeito e não requerem quaisquer ações adicionais por parte do titular dos dados para serem implementados.

Em particular, as ações de tratamento de dados são organizadas de modo a evitar a divulgação pública deles, seja por defeito ou acidentalmente, sem intenção da pessoa a quem os dados dizem respeito.

A base de clientes da Empresa é armazenada de forma a impedir o acesso dos terceiros, os dados sobre os funcionários estão disponíveis apenas para o pessoal de Recursos Humanos, o software que contém dados pessoais é protegido por palavra-passe. A pessoa responsável pela proteção dos dados na Empresa tem em conta estes princípios ao efetuar auditoria das atividades específicas de processamento de dados.

Direitos dos sujeitos dos dados

O direito de retirar o consentimento

Se os dados pessoais forem tratados à base de consentimento do titular dos dados, este pode retirá-lo a qualquer momento sem afetar a legalidade do tratamento realizado à base de consentimento do titular dos dados antes de o retirar.

Direito de informação

Por pedido do titular dos dados em causa, o responsável pelo tratamento de dados deve fornecer as informações sobre os dados que lhe dizem respeito, incluindo os que foram tratados pelo processador dos dados em seu nome ou de acordo com a sua notificação, as fontes de onde os dados foram obtidos, a finalidade, os fundamentos e a duração do tratamento, o nome e o endereço do processador de dados, bem como as informações sobre as suas ações relacionadas com o tratamento

dos dados, e sobre as condições e consequências do incidente com os dados e as medidas tomadas para os eliminar e, em caso de transferência de dados, os fundamentos jurídicos e os destinatários.

O responsável pelo tratamento de dados deve executar sem demora os pedidos da pessoa que é titular dos dados pessoais, fornecendo as informações solicitadas de forma bem clara e por escrito no prazo máximo de vinte e cinco dias a contar da receção do respetivo pedido.

A informação é fornecida gratuitamente para qualquer categoria de dados uma vez por ano. A informação adicional relacionada com a mesma categoria de dados pode ser fornecida por pagamento de respetivas taxas. Se qualquer pagamento for efetuado em relação aos dados que tenham sido processados ilegalmente ou se o pedido causar as correções, tal pagamento será reembolsado.

Direito à correção

O titular dos dados pode solicitar a correção dos seus dados pessoais se estes estiverem incorretos, incompletos ou desatualizados. Se os dados pessoais não forem verdadeiros e os dados que são verdadeiros estiverem disponíveis para o Controlador de Dados, os dados pessoais serão corrigidos pelo Controlador de Dados.

Direito à correção

O titular dos dados pode solicitar eliminar os seus dados pessoais, se:

- os dados pessoais já não são necessários para fins de processamento de dados;
- o titular dos dados retirou o seu consentimento para o tratamento dos dados processados exclusivamente com base no seu consentimento;
- o titular dos dados manifestou o seu desacordo com o tratamento dos dados;
- o tratamento dos dados pessoais é ilegal;
- os dados pessoais devem ser eliminados a fim de cumprir as obrigações legais assumidas pela Empresa.

A Empresa tomará as medidas razoáveis para informar as outras pessoas para as quais os dados pessoais foram transferidos sobre o facto de eliminação dos dados pessoais.

Direito de restringir o processamento

O titular dos dados pode solicitar restringir o processamento da informação no caso de:

- a correção dos dados pessoais é contestada;
- o titular dos dados em causa quer restringir o acesso aos seus dados pessoais em vez de apagá-los, apesar de seu tratamento ser ilegal;
- o titular dos dados quer que a Empresa guarde os seus dados pessoais porque o titular dos dados precisa disso para o proteger no âmbito de quaisquer requisitos legais;
- se o titular dos dados estiver oposto ao tratamento de dados pessoais e a Empresa efetuar as verificações para determinar se existem os motivos legítimos suficientes para ignorar os direitos do próprio titular dos dados, dado que o tratamento de dados se baseia nos interesses legítimos da Empresa.

Direito de transferir os dados

O titular dos dados pode solicitar que os seus dados pessoais sejam transferidos, desde que o seu tratamento se baseie no seu consentimento ou na execução do contrato e seja efetuado por meios automáticos (ou seja, sem utilização dos documentos escritos (em papel)).

Direito de recusar o tratamento

Se o titular dos dados estiver contra o tratamento dos dados que lhe dizem respeito, o

responsável pelo tratamento de dados deve analisar a razão desta objeção o mais rapidamente possível no prazo de quinze dias, tomar uma respetiva decisão e notificar o titular dos dados em causa por escrito sobre a sua decisão.

Se o responsável pelo tratamento de dados chegar à conclusão que a objeção do titular dos dados em causa for justificada, o responsável pelo tratamento deve pôr termo a todas as operações de tratamento (incluindo a recolha e transmissão de dados), bloquear os dados em questão e notificar todos os destinatários que já tenham recebido estes dados sobre a objeção e as medidas subsequentes com base nas quais tais destinatários igualmente devem tomar as medidas relativas à objeção.

Se o titular dos dados não concordar com a decisão do responsável pelo tratamento de dados ou se o responsável pelo tratamento de dados não respeitar o prazo para tomar decisão, a pessoa em causa pode recorrer ao tribunal no prazo de 30 dias após a notificação sobre a decisão ou a partir do último dia do prazo limite.

Direito à indemnização e compensação

Se o responsável pelo tratamento de dados causar danos devido ao processamento ilegal dos dados pessoais ou violação dos requisitos de segurança de dados, ele deverá compensar os prejuízos.

Se o responsável pelo tratamento de dados violar o direito pessoal do titular dos dados como resultado do processamento ilegal dos seus dados pessoais ou violar os requisitos de segurança dos dados, o titular dos dados pode pedir indemnização de danos.

O responsável pelo tratamento de dados é também responsável perante o titular dos dados por danos causados pelo processador. O responsável pelo tratamento de dados está isento de responsabilidade por danos e perdas se provar que o dano ou violação do direito pessoal do titular dos dados é causado por uma razão inevitável que não esteja relacionada com o processamento de dados.

O titular de dados não pode reclamar os danos e pedir compensação quando os danos causados à pessoa lesada ou a violação do direito à privacidade foram causados pelo comportamento intencional ou por negligência grosseira do respetivo titular dos dados.

Direito à proteção jurídica

A pessoa interessada pode enviar uma demanda ao tribunal por violação dos seus direitos. O responsável pelo tratamento de dados deve demonstrar que o processamento de dados é efetuado em conformidade com a lei. Uma ação judicial pode ser proposta pela pessoa interessada, à sua escolha, e apresentada ao tribunal competente do local de residência ou habitação.

Se o tribunal satisfazer o pedido do titular dos dados, o responsável pelo tratamento de dados é obrigado a fornecer as informações, a corrigir, bloquear, apagar, decifrar o tratamento automatizado de dados, tendo em conta o direito de oposição da respetiva pessoa.

O direito de contactar a Autoridade de Proteção de Dados

Se existirem os problemas relacionados com as condições de tratamento dos dados pessoais, a pessoa em causa, titular dos dados, pode igualmente apresentar uma queixa à autoridade de controlo da proteção de dados.

Diretor Geral e Global
da Softline
S.V.Chernovolenko