



OLIVEIRA, GAMBOA
& ASSOCIADOS

SOCIEDADE DE ADVOGADOS

Regulamento Geral de Proteção de Dados

Entrada em vigor a 25 de Maio de 2018.

por [Dra Ana Isa Couto]



NOVO ENQUADRAMENTO JURÍDICO

Este novo regime visa introduzir um enquadramento jurídico mais rigoroso no que diz respeito ao tratamento de dados pessoais, nomeadamente assegurando às pessoas singulares de todos os Estados-Membros que o tratamento dos seus dados pessoais será realizado ao mesmo nível de outros direitos suscetíveis de proteção judicial.

Introdução de Novos Conceitos

«**Definição de perfis**», qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações.

«**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.

«**Dados genéticos**», os dados pessoais relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular que deem informações únicas sobre a fisiologia ou a saúde dessa pessoa singular e que resulta designadamente de uma análise de uma amostra biológica proveniente da pessoa singular em causa.

«**Dados biométricos**», dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa

pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos.

«**Consentimento**»: uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento. Em especial, no contexto de uma declaração escrita relativa a outra matéria, deverão existir as devidas garantias de que o titular dos dados está plenamente ciente do consentimento dado e do seu alcance. Uma declaração de consentimento, previamente formulada pelo responsável pelo tratamento, deverá ser fornecida de uma forma inteligível e de fácil acesso, numa linguagem clara e simples e sem cláusulas abusivas

Reforço dos Direitos dos Titulares dos Dados

Direito à transparência das informações, das comunicações e das regras para o exercício dos direitos dos titulares dos dados - O princípio da transparência exige que qualquer informação destinada ao público ou ao titular dos dados seja concisa, de fácil acesso e compreensão, bem como formulada numa linguagem clara e simples, e que se recorra, adicionalmente, à visualização sempre que for adequado.

Direito à informação - cada titular de dados deverá ter o direito de conhecer e ser informado, nomeadamente, das finalidades para as quais os dados pessoais são tratados, quando possível do período durante o qual os dados são tratados, da identidade dos destinatários dos dados pessoais, da lógica subjacente ao eventual tratamento automático dos dados pessoais e, pelo menos quando tiver por base a definição de perfis, das suas consequências.

Direito de retificação - O titular tem direito de obter do responsável pelo tratamento a retificação dos dados pessoais inexatos que lhe digam respeito.

Direito ao apagamento - os titulares dos dados pessoais têm «direito a serem esquecidos» quando a conservação desses dados violar o presente regulamento ou o direito da União ou dos Estados-Membros aplicável ao responsável pelo tratamento. Em especial, os titulares de dados deverão ter direito a que os seus dados pessoais sejam apagados e deixem de ser objeto de tratamento se deixarem de ser necessários para a finalidade para a qual foram recolhidos ou tratados, se os titulares dos dados retirarem o seu consentimento ou se opuserem ao tratamento de dados pessoais que lhes digam respeito ou se o tratamento dos seus dados pessoais não respeitar o disposto no presente regulamento.

Direito de Acesso - Os titulares de dados deverão ter o direito de aceder aos dados pessoais recolhidos que lhes digam respeito e de exercer esse direito com facilidade e a intervalos razoáveis, a fim de conhecer e verificar a tomar conhecimento do tratamento e verificar a sua licitude.

Direito à limitação do tratamento - O titular dos dados tem o direito de obter do responsável pelo tratamento a limitação do tratamento.

Direito à portabilidade dos dados - O titular dos dados tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, e o direito de transmitir esses dados a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir.

Direito de oposição - O titular dos dados tem o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito.

Direito a não ficar sujeito a decisões tomadas exclusivamente em tratamento automatizado - O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base

no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar.

Data Protection Officer (DPO) - Encarregado de Proteção de dados

Trata-se um especialista em legislação e prática de proteção dados no controlo do cumprimento do presente regulamento a nível interno. É obrigatório nomear um Encarregado de Proteção de Dados sempre que o tratamento dos dados for efetuado por uma autoridade pública ou sempre que, no setor privado, o tratamento for efetuado por um responsável cujas atividades principais consistam em operações de tratamento que exijam o controlo regular e sistemático do titular dos dados em grande escala, ou sempre que as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados pessoais e de dados relacionados com condenações penais e infrações Funções:

- Avaliar e acompanhar as operações de tratamento de dados.
- Apoiar o responsável pelo tratamento ou subcontratante.



Regime das Transferências de dados para fora da União Europeia

Os responsáveis pelo tratamento ou subcontratantes só podem transferir os dados pessoais para um país terceiro se tiverem apresentado garantias adequadas, e na condição de os titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes.

Como proceder em caso de violação de normas de tratamento de dados pessoais:

- ➔ Nem todas as violações devem ser reportadas à autoridade de controlo, mas apenas aquelas que sejam suscetíveis de resultar num risco para os direitos dos titulares.
- ➔ No entanto todas as violações devem ser documentadas, descrevendo os factos relacionados com as mesmas, bem como os respetivos efeitos e a medida de reparação adotada.
- ➔ Notificar esse facto à autoridade de controlo competente sempre que possível até 72 horas após ter tido conhecimento da violação.
- ➔ Sempre que seja enviada depois de decorridas as 72 horas, a notificação à autoridade de controlo deve ser instruída dos motivos do atraso.
- ➔ A notificação deve descrever a natureza da violação dos dados, incluindo se possível, as categorias e o número aproximado de titulares afetados. Deverá ainda descrever as consequências da violação de dados pessoais e as medidas adotadas para reparar a violação.

Caso a violação seja suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, terá de ser comunicada ao titular dos dados.

Que medidas devo adotar?

Estabelecer políticas e procedimentos internos de reação a falhas de segurança à base de dados.

Rever o consentimento de forma a garantir que o mesmo respeita todas as novas exigências legais.

Rever políticas de privacidade de forma a garantir que a linguagem é clara e acessível, bem como que é fornecida toda o leque de informação obrigatória.

Nomear o encarregado de proteção de dados.

Estabelecer mecanismos de resposta ao exercício dos novos direitos dos titulares (direito ao apagamento e à portabilidade).

Rever os contratos de subcontratação de forma a garantir que os mesmos respeitam as novas exigências legais

Verificar se existe transferência de dados para fora da U.E.

Adotar códigos de conduta e políticas internas.

Privacy by Design and Privacy by Default

Para poder comprovar a conformidade com o presente regulamento, o responsável pelo tratamento deverá adotar orientações internas e aplicar medidas que respeitem, em especial, os princípios da proteção de dados desde a conceção e da proteção de dados por defeito. Tais medidas podem incluir a minimização do tratamento de dados pessoais, a pseudonimização de dados pessoais o mais cedo possível, a transparência no que toca às funções e ao tratamento de dados pessoais, a possibilidade de o titular dos dados controlar o tratamento de dados e a possibilidade de o responsável pelo tratamento criar e melhorar medidas de segurança.

Significa isto que o departamento de tecnologias da informação deve encarar com importância nuclear a privacidade durante todo o ciclo de vida do desenvolvimento ou processos de tratamento de dados pessoais, devendo as mesmas ser de aplicação imediata e automática aquando da aquisição de um novo produto ou serviço.

Privacy Impact Assessment (PIA) ou Avaliação de impacto sobre a proteção de dados

A fim de promover o cumprimento do presente regulamento nos casos em que as operações de tratamento de dados sejam suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo seu tratamento deverá encarregar-se da realização de uma avaliação de impacto da proteção de dados para determinação, nomeadamente, da origem, natureza, particularidade e gravidade desse risco. Os resultados dessa avaliação deverão ser tidos em conta na determinação das medidas que deverão ser tomadas a fim de comprovar que o tratamento de dados pessoais está em conformidade com o presente regulamento. Sempre que a avaliação de impacto sobre a proteção de dados indicar que o tratamento apresenta um elevado risco que o responsável pelo tratamento não poderá atenuar através de medidas adequadas, atendendo à

tecnologia disponível e aos custos de aplicação, será necessário consultar a autoridade de controlo antes de se proceder ao tratamento de dados pessoais.



PARA OBTER MAIS INFORMAÇÕES

Dra. Ana Isa Couto

Oliveira Gamboa & Associados

Estrada da Outurela, Edifício Strapex, 121, 1º Andar – 2794 – 051 Carnaxide.

Contactos: 214 161 829

e-mail: ana.couto@oga.pt

