REGULAMENTO GERAL DE PROTEÇÃO DE DADOS

como um dos pilares fundamentais (modelo jurídico) na proteção dos dados pessoais

Medidas para implementação do RGPD

→ **Designação de um EPD -** O EPD reporta ao mais alto nível e a sua designação deve ser realizada em função das competências profissionais, em especial dos conhecimentos avançados de proteção de dados e que seja capaz de cumprir as funções atribuídas no Artigo 39º do regulamento[1]. O EPD deve ainda contribuir para dar cumprimento aos elementos essenciais do RGPD, tais como os princípios do tratamento de dados, os direitos dos titulares de dados, a proteção de dados desde a conceção e por defeito, os registos das atividades de tratamento, a segurança do tratamento e a notificação e comunicação de violações de dados. Das suas tarefas, destaca-se:

- Sensibilizar e informar todos os que tratem dados pessoais;
- Assegurar o cumprimento das políticas de privacidade e proteção de dados;
- Controlar e regular a conformidade do RGPD;
- Recolher informação para identificar atividades de tratamento;
- Controlar e acompanhar a produção da Avaliação de Impacto sobre Proteção de Dados;
- Promover as abordagens de Privacidade por Desenho e por Padrão;
- Realizar a avaliação na exposição aos riscos de violações de privacidade;
- Manter actualizados os registos das atividades de tratamento de dados;
- Controlar o cumprimento de contratos escritos com o subcontratante[2];
- Promover formações de boas práticas para a proteção de dados;
- Ser o ponto de contacto com os titulares de dados de forma a esclarecer questões relacionadas com o tratamento dos dados;
- Ser o ponto de contacto com as autoridades de controlo.

→ **Perceber o impacto do RGPD -** O Regulamento terá impacto em toda a organização, pelo que é importante consciencializar e comprometer a gestão de topo para a sua aplicabilidade e transversalidade. Deve ser também avaliada a natureza e contexto do tratamento de dados futuros, de modo a analisar os potenciais riscos que possam comportar para os titulares dos dados e assim aplicar com eficácia os princípios da proteção de dados.

→ **Preparar um plano de comunicação -** Deverá ser elaborado um plano de comunicação sobre o tema. No plano interno, deverão explicar-se os procedimentos a adotar para cumprir o RGPD. No plano externo o objetivo é gerar confiança nos interlocutores sobre a utilização adequada dos seus dados.

→ **Listar os processos que podem sofrer impacto do RGPD -** Deverá ser feito um levantamento de necessidades de adaptação de processos ao RGPD em toda a instituição.

---

[1] "a) Informa e aconselha o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações;
b) Controla a conformidade com o regulamento, com outras disposições de proteção de dados da União ou dos Estados-Membros e com as políticas do responsável pelo tratamento ou do subcontratante relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados, e as auditorias correspondentes;
c) Presta aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados e controla a sua realização;
d) Coopera com a autoridade de controlo;
e) Ponto de contato para a autoridade de controlo sobre questões relacionadas com o tratamento, incluindo a consulta prévia a que se refere o artigo 36.º, e consulta, sendo caso disso, esta autoridade sobre qualquer outro assunto.
No desempenho das suas funções, o EPD tem em devida consideração os riscos associados às operações de tratamento, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento."

[2] Uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes;

→ **Definir um plano de implementação -** Estruturar um plano de implementação das ações identificadas e operacionalizar a sua implementação nas diferentes áreas da organização, de forma a assegurar que respeita todas as diretrizes do Regulamento.

→ **Formação -** Deve ser proporcionada formação sobre segurança e privacidade de dados pessoais a todos os colaboradores que têm contato direto com dados pessoais.

→ **Atualizar as políticas de segurança e privacidade -** As políticas e práticas da instituição à luz do regulamento devem ser revistas, e devem ser adotadas as medidas técnicas e organizativas adequadas e necessárias para assegurar e poder comprovar que todos os tratamentos de dados efetuados estão em conformidade com o RGPD, como a política de privacidade, a política de utilização de cookies no website ou adaptação dos contratos e outros documentos às novas exigências do RGPD.

→ **Adaptar processos de recolha e tratamento de dados -** Implementar os conceitos de "Privacy by design"[3] e "Privacy by default"[4] (Proteção da privacidade desde a conceção e por defeito), levando-os à prática nos vários processos da organização que envolvam recolha e tratamento de dados pessoais. Estes conceitos remetem para a necessidade de obtenção de consentimento prévio à utilização dos dados. Deve ser verificada, nos termos exigidos pelo regulamento, a forma e circunstâncias em que foi obtido o consentimento dos titulares, quando este serve de base legal para o tratamento de dados pessoais. Assim, caso não respeite as novas exigências é imprescindível obter novo consentimento dos titulares dos dados em conformidade com as disposições do RGPD.

→ **Identificar os dados pessoais que estão na posse da organização -** Deve ser feito o inventário e catalogação dos dados pessoais recolhidos e/ou guardados pela instituição, com a menção aos dados pessoais existentes; aos tipos de dados; à finalidades de tratamento; ao local onde são guardados; ao período em que serão utilizados; à pessoa que os forneceu; e as pessoas que têm acesso aos dados. Deve ser feita a avaliação da natureza do tratamento de dados efetuados, a fim de apurar quais os que se podem enquadrar no conceito de dados sensíveis, e consequentemente se aplicarem condições específicas para o seu tratamento, relativas à licitude do tratamento, aos direitos ou às decisões automatizadas.

→ **Listar procedimentos de recolha e tratamento de dados pessoais -** Devem estar identificadas, documentadas e de fácil acesso, as formas de recolha e de tratamento de dados pessoais, assim como o fundamento para o seu tratamento (consentimento, execução de contratos, interesses vitais do titular, etc.). É importante que este registo permita demonstrar o cumprimento de todas as obrigações decorrentes do RGPD.

→ **Implementar medidas de proteção e privacidade -** Devem ser adotadas ou revistas as medidas técnicas e organizativas destinadas à proteção e privacidade de dados pessoais (ex. política de secretária limpa, implementação de cifragem de dados, etc.).

→ **Detetar incidentes de violação de dados -** Devem ser criados mecanismos processuais que permitam detetar incidentes de violação de dados pessoais, bem como a respetiva comunicação à entidade reguladora e aos titulares (quando sejam suscetíveis de resultar num risco para os direitos dos titulares). Todas as violações devem ser devidamente documentadas conforme preceituado no regulamento.

→ **Preparar workflows de resposta aos direitos dos titulares -** Devem ser desenhados processos e procedimentos internos que permitam responder às solicitações dos titulares dos

---

[3] Privacy by Design (Privacidade desde a conceção) - Significa levar o risco de privacidade em conta em todo o processo de conceção de um novo produto ou serviço, em vez de considerar as questões de privacidade apenas posteriormente. Tal significa avaliar cuidadosamente e implementar medidas e procedimentos técnicos e organizacionais adequados desde o início para garantir que o tratamento está em conformidade com o RGPD e protege os direitos dos titulares dos dados em causa.

[4] Privacy By Default (privacidade por defeito) - Significa assegurar que são colocados em prática, dentro de uma organização, mecanismos para garantir que, por defeito, apenas será recolhida, utilizada e conservada para cada tarefa, a quantidade necessária de dados pessoais.

dados, no âmbito dos direitos que estão consagrados no RGPD, como o direito à limitação do tratamento, o direito à portabilidade, o direito à eliminação dos dados e quanto à notificação de terceiros[5] sobre retificação ou apagamento ou limitação de tratamento solicitados pelos titulares. No âmbito da recolha de dados (impressos), a informação fornecida aos titulares dos dados deve ser revista, seja esta realizada diretamente junto do titular ou não, devendo passar a respeitar as políticas de privacidade e a fornecer a informação exigida por lei.

→ **Validar conformidade dos sistemas com o RGPD -** Conferir se as aplicações informáticas utilizadas na instituição para o processamento de dados pessoais estão em conformidade com o RGPD.

→ **Salvaguardar conformidade das entidades subcontratantes -** Quando se recorre a subcontratantes para realizar atividades que envolvem dados pessoais, é fundamental garantir que essa relação consta de um contrato escrito, pelo que é provável que os contratos existentes necessitem de ser modificados para respeitar os termos do regulamento. É ainda importante que nesse documento estejam patentes instruções sobre a forma como o tratamento dos dados deve ser efetuado.

→ **Avaliação de Impacto de Proteção de dados (Privacy Impact Assessment - PIA[6]) -** Devem ser incluídas nas metodologias de trabalho, a realização de PIA's nas situações em que as mesmas são obrigatórias ou úteis.

→ **Monitorização -** A aplicação do plano definido deve ser continuamente monitorizado e devem ainda ser implementadas medidas de controlo nas diversas estruturas da organização.

→ **Auditoria -** Deve ser realizada uma Auditoria externa, que ateste o cumprimento de todas as normas previstas no Regulamento.

→ **Solicitar certificação -** Submeter um pedido de certificação à Comissão Nacional de Proteção de Dados (CNPD) ou outro organismo avalizado para o efeito.

→ **Divulgar certificação -** Divulgar a conformidade com o RGPD, com o objetivo de contribuir para aumentar a confiança dos seus interlocutores, posicionando-se como uma organização que respeita na íntegra os direitos dos titulares dos dados.

Fontes:
"Regulamento (EU) 2016/679", do Parlamento Europeu e do Conselho de 27 de abril de 2016;
"Orientações sobre os Encarregados da Proteção de Dados (EPD)", do grupo do artigo 29.º para a proteção de dados;
"10 medidas para preparar a aplicação do Regulamento Europeu da proteção de dados", do CNPD;
21 passos para adaptar a sua empresa ao RGPD, da Primavera;
Como devem as empresas tratar os dados pessoais que têm na sua posse?, da Quickaid

Sites:
Comissão Nacional de Proteção de Dados – www.cnpd.pt
Instituto das Tecnologias da Informação na Justiça – www.dgsi.pt
União Europeia - http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679
Centro de Computação Gráfica - http://www.ccg.pt
ACEPI – Associação da Economia Digital - http://www.acepi.pt

[5] A pessoa singular ou coletiva, a autoridade pública, o serviço ou organismo que não seja o titular dos dados, o responsável pelo tratamento, o subcontratante e as pessoas que, sob a autoridade direta do responsável pelo tratamento ou do subcontratante, estão autorizadas a tratar os dados pessoais;

[6] Privacy Impact Assessments (avaliação do impacto da privacidade) - É um processo destinado a descrever o processamento de dados privados, a avaliar a necessidade e a proporcionalidade de um processamento de dados e a ajudar a gerir os riscos aos direitos e liberdades das pessoas, resultantes do processamento de dados pessoais. Trata-se de uma avaliação de risco, na medida em que se avalia o ato da concretização de ameaças da privacidade de dados e a probabilidade de ocorrerem.