Os 6 passos essenciais para a implementação do RGPD

O exercício de implementação do Regulamento Geral de Proteção de Dados ('RGPD') tem-se revelado de grande complexidade para as empresas e instituições públicas em Portugal.

Em vigor desde Maio de 2016, este Regulamento, de aplicação direta em todos os Estados Membros, exigirá que as organizações tenham implementadas medidas legais, técnicas e organizacionais que demonstrem o cumprimento efetivo das obrigações ali previstas a partir de Maio de 2018, sob pena de se sujeitarem a avultadas coimas e danos reputacionais de difícil reparação.

Tendo conhecimento das dificuldades inerentes a um projeto desta dimensão e complexidade, a Autoridade de Proteção de Dados Francesa ('CNIL') publicou um comunicado com uma metodologia de preparação para o RGPD com 6 passos essenciais, sublinhando a responsabilidade e a transparência como princípios estruturantes deste diploma comunitário.

"A Autoridade de Proteção de Dados Francesa publicou um comunicado com uma metodologia de preparação para o RGPD com 6 passos essenciais, sublinhando a responsabilidade e a transparência como princípios estruturantes"

De acordo com a CNIL, os 6 passos essenciais para a correta implementação do RGPD são os seguintes:

Passo #1: Nomeie um Encarregado de Proteção de Dados ('Data Protection Officer') para "pilotar" o Programa de Compliance que será implementado na sua organização.

Nos termos do disposto no Artigo 37 do Regulamento Geral de Proteção de Dados, a nomeação de um Data Protection Officer será obrigatória se a organização for uma entidade pública; ou se as atividades principais da organização requererem uma monitorização regular e sistemática dos titulares dos dados numa grande escala, ou se tais atividades consistirem no processamento de dados sensíveis em grande escala. A CNIL recomenda a nomeação de um Data Protection Officer antes da aplicação do RGPD em Maio de 2018.

O Data Protection Officer será responsável pela monitorização e cumprimento integral das obrigações previstas no Regulamento pelo responsável do tratamento de dados pessoais e será a pessoa de contacto para qualquer assunto com a autoridade de supervisão competente.

Passo #2: Prepare um mapeamento dos tratamentos de dados pessoais.

O Artigo 30 do Regulamento Geral de Proteção de Dados estabelece que os responsáveis pelo tratamento e os subcontratantes serão obrigados a manter um registo de todos os tratamentos de dados que executam. De forma a calcular o impacto que o Regulamento terá nos tratamentos de dados que as organizações atualmente desenvolvem, a CNIL aconselha a identificação de cada tratamento de dados pessoais, designadamente, as categorias de dados tratados, as finalidades de cada tratamento, as pessoas/entidades que tratam os dados (incluindo subcontratantes) e os fluxos de dados, com especial destaque para as transferências para fora da União Europeia.

Para este efeito, a CNIL aconselha a resposta às seguintes questões:

- Quem trata os dados?
- Que tipo de dados trata?
- Para que finalidades?
- Onde armazena os dados?
- Qual o período de conservação de cada tratamento?
- Que medidas de segurança implementou?

Passo #3: Com base nos resultados do mapeamento de tratamento de dados pessoais, identifique as principais ações a tomar.

De forma a priorizar as ações a serem tomadas, a CNIL recomenda que as organizações:

- Assegurem que são apenas recolhidos e tratados dados pessoais necessários a uma finalidade específica e identificada;
- Identifiquem a base legal para o tratamento de dados;
- Revejam as políticas de privacidade, de forma a garantir que estão conformes ao Regulamento Geral de Proteção de Dados;
- Assegurem que os subcontratantes conhecem as suas novas obrigações e responsabilidades e que os acordos e relações contratuais contêm cláusulas relativas a segurança, confidencialidade e proteção de dados pessoais;
- Saibam como irão os titulares dos dados aceder aos seus dados e exercer os seus direitos;
- Verifiquem as medidas de segurança implementadas.

A CNIL recomenda ainda uma especial atenção ao tratamento de dados pessoais sensíveis e dados pessoais de menores, sobretudo, quando haja um tratamento massivo destas categorias de dados e/ou quando estes são transferidos para um país localizado fora da União Europeia.

Passo #4: Efetue uma avaliação de impacto de risco (‘Privacy Impact Assessment’) para os tratamentos que apresentem riscos de violação de privacidade face à sua natureza ou âmbito das atividades desenvolvidas.

Efetuar uma avaliação de impacto de risco é essencial para calcular o nível de risco de violação de privacidade e proteção de dados pessoais e certificar que os princípios fundamentais do Regulamento estão a ser cumpridos.

A CNIL recomenda a realização desta avaliação de impacto de risco previamente a um processo de recolha dos dados e ao início do tratamento e sempre que haja riscos elevados na privacidade dos titulares dos dados.

Passo #5: Implemente medidas internas que garantam um nível elevado na proteção de dados pessoais.

De acordo com a CNIL, a implementação de procedimentos internos implica a adoção de medidas de 'privacy by design', realização de ações de formação e capacitação interna nesta matéria, divulgação de informação e comunicação dentro da organização, resposta aos pedidos e reclamações de titulares dos dados pessoais e antecipação de violação de dados pessoais.

Passo #6: Documente tudo o que possa evidenciar o cumprimento integral do Regulamento Geral de Proteção de Dados

De forma a possibilitar/facilitar a demonstração do cumprimento efetivo do Regulamento Geral de Proteção de Dados, a CNIL recomenda que as organizações conservem todos os documentos relativos ao tratamento de dados, tais como: documentos referentes às atividades de tratamento, resultados de avaliação de impacto de risco e documentos relativos a transferências de dados para países localizados fora da União Europeia, políticas de privacidade, formulários de consentimento, procedimentos para exercício dos direitos dos titulares dos dados, contratos com subcontratantes e evidência do consentimento quando o tratamento de dados se baseia nesta condição de legitimidade.

Para mais informações sobre o tema, por favor contacte:

Joana Mota Agostinho I jmagostinho@ctsu.pt

www.ctsu.pt