

PERCEBER O IMPACTO GLOBAL DO RGPD

Informar a gestão de topo da importância e do possível impacto.

PREPARAR UM PLANO DE COMUNICAÇÃO INTERNO

Elaborar um plano de comunicação interno, explicando aos trabalhadores os procedimentos a adotar para cumprir o RGPD.

AVALIAR A NECESSIDADE DE DESIGNAÇÃO DE UM ENCARREGADO DE PROTEÇÃO DE DADOS (DPO)

Não é obrigatório, mas é recomendado a todas as organizações que tratem dados pessoais. A designação do perfil deve ser realizada em função das competências profissionais em especial dos conhecimentos avançados de proteção de dados.

DEFINIR UM PLANO DE IMPLEMENTAÇÃO

Estruturar um plano de implementação com ações operacionais envolvendo todas as áreas de negócio.

AVALIAÇÃO DE IMPACTO SOBRE PROTEÇÃO DE DADOS (PIA)

Elaborar um documento que descreva as operações de tratamento e auxilie a gestão dos riscos com determinadas medidas para o tratamento dos dados pessoais.

LISTAR PROCESSOS QUE CONTACTEM COM DADOS PESSOAIS

Efetuar um levantamento de processos operacionais de cada departamento que contactem com dados pessoais.

IDENTIFICAR TODOS OS DADOS PESSOAIS

Elaborar um documento com o inventário de todos os dados guardados e categorizá-los por:

- Dados pessoais existentes;
- Tipos de dados;
- Finalidades de tratamento;
- Local onde são guardados;
- Período em que serão utilizados;
- Pessoa ou Entidade que os forneceu;
- Quem tem acesso aos dados;

ATUALIZAR POLÍTICAS DE PROTEÇÃO E PRIVACIDADE

Rever as políticas relativas à proteção de dados pessoais, de privacidade, de cookies e termos de utilização.

VALIDAR CONFORMIDADE DOS SISTEMAS

Conferir se os sistemas informáticos utilizados estão em conformidade com o RGPD, se não adaptá-los.

IMPLEMENTAR MEDIDAS TÉCNICAS DE SEGURANÇA

Adotar medidas técnicas de proteção em redes e sistemas de informação que possuam dados pessoais: passwords, cifragens e backups.

SALVAGUARDAR CONFORMIDADE DOS SUBCONTRATANTES

Estabelecer contratos escritos com medidas técnicas de segurança, sempre que sejam realizadas atividades que envolvem dados pessoais.

FORMAÇÃO

Proporcionar aos colaboradores que têm contacto direto com dados pessoais, formação sobre segurança da informação e privacidade de dados.

ADAPTAR PROCESSOS DE PRIVACIDADE DE DADOS

Implementar os conceitos de “Privacy by Design” e “Privacy by Default” sempre que envolva dados pessoais e que sejam tratados para cada finalidade.

PREPARAR O PROCESSO DE RESPOSTA AOS DIREITOS DOS TITULARES

Desenhar processos que permitam responder às solicitações de pedidos dos titulares dos dados: acesso, limitação, retificação, apagamento, portabilidade e oposição de processamento de dados.

DETETAR INCIDENTES DE VIOLAÇÃO DE DADOS

Garantir a existência de processos que permitam detetar incidentes de violação de dados pessoais e respetiva comunicação à entidade reguladora e aos titulares quando aplicável.

MONITORIZAÇÃO

Monitorizar todo o plano, aplicando em diversos processos ações e controlos de melhoria.

AUDITORIAS PERIÓDICAS

Realização de auditorias de conformidade, por forma a garantir o cumprimento do RGPD.