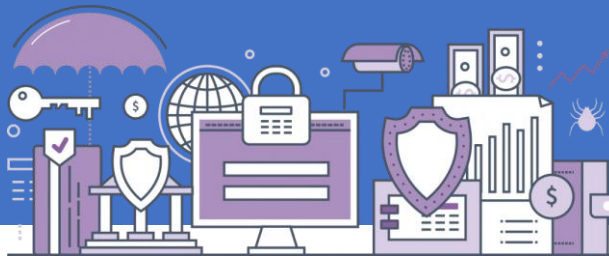




RGPD

Regulamento Geral
de Proteção de
Dados



NET
BIT

RGPD – Regulamento Geral de Proteção de Dados

Entra em vigor no próximo dia 25 de Maio o RGPD, ao abrigo do Regulamento (EU) 2016/679, que vem alterar profundamente o tratamento e proteção de dados pessoais, com o objectivo de proteger as pessoas singulares na sua vida privada e familiar, do seu domicílio e da sua correspondência. Como a classificação de dados pessoais é tão abrangente como por exemplo nome e apelido ou mesmo endereço de mail profissional, as empresas têm doravante uma responsabilidade acrescida quanto à posse e utilização dos mesmos.

Recomendamos, pois, que seja definido um processo de implementação do RGPD, em função da dimensão de cada organização, mas que fatalmente tem de abranger a análise de vários pontos chave para avaliar o cumprimento do novo regulamento.

O RGPD visa proteger direitos considerados fundamentais das pessoas, **de que destacamos:**

Direito à confidencialidade

Os dados pessoais têm de estar protegidos de acessos não autorizados.

Direito à portabilidade dos dados

Pode ser solicitada cópia ou transferência dos dados pessoais em formato eletrónico standard

Direito ao apagamento

Pode ser solicitado em qualquer momento, desde que não sejam dados que por lei não possam ser apagados

Direito ao consentimento

Os dados pessoais só podem ser utilizados por terceiros desde que com prévio consentimento do próprio, por declaração ou acto semelhante inequívoco, e definindo que tipo de utilização pode ser dado.

Em qualquer momento esse direito pode ser revogado pelo próprio (direito à rectificação dos dados e direito de oposição)

ALGUNS CONCEITOS DO RGPD

O que são dados pessoais

Nome e apelido, morada, nº do CC, NIF, SS, Composição do agregado familiar, idade, peso, altura, Email, Telef (incluindo o profissional), endereço ip, dados de localização, perfis de redes sociais, informação bancária e fiscal, etc

O que são dados sensíveis

Saúde, dados genéticos, raça ou etnia, orientação sexual, opinião política, filiação sindical, dados biométricos

Consentimento

Quem é a sua empresa, finalidade da utilização dos dados pessoais, durante quanto tempo serão conservados, quem mais poderá receber esses dados



IMPLEMENTAÇÃO DO RGPD NAS EMPRESAS

A implementação do RGPD nas empresas passa por uma auditoria interna e posterior aplicação de medidas administrativas e técnicas que garantam o cumprimento do regulamento:

PRÉ AUDITORIA INTERNA

Auditoria aos dados

Identificação dos dados pessoais que são processados na empresa e legitimidade para proceder ao seu tratamento. Que dados tenho? Para que fins os utilizo? Tenho consentimento?

Segurança dos dados

Proteção dos dados, através de controlos de segurança e rastreabilidade, quer através dos meios informáticos quer da segurança física dos mesmos. Onde estão armazenados? Quem tem acesso? Cópias de segurança? Encriptação? Sistemas de firewall? Software de anti vírus e ransomware? ERP certificado?

Auditoria aos processos internos

Verificar se a informação é apenas a estritamente necessária, se está autorizada e se cumpre com os direitos das pessoas

Facilitar o exercício dos direitos

De acesso, informação, consentimento, esquecimento, oposição, rectificação, portabilidade. Manter arquivo desses registos e das respostas aos pedidos

Contrato com outras entidades subcontratadas

Para garantir a segurança e confidencialidade da informação que tem de ser fornecida a terceiros
Ex: Gab. Contabilidade

Este conjunto de medidas visa

- ✓ Assegurar a integridade, confidencialidade e disponibilidade em segurança dos dados pessoais
- ✓ A pseudo denominação e cifragem dos dados
- ✓ Restabelecer o acesso aos dados pessoais em caso de incidente
- ✓ Regularmente testar e verificar a eficácia dos procedimentos e sistemas de proteção de dados.

AUDITORIA AOS SISTEMAS INFORMÁTICOS

Com vista à adaptação da empresa aos requisitos do RGPD, há que avaliar a estrutura informática da empresa e detectar potenciais falhas e insuficiências, devendo para o efeito ser elaborado um diagrama da sua rede informática e que avalie os seguintes pontos:

- ✓ Equipamentos e acessos: Discriminação dos equipamentos, acessos internos e externos
- ✓ Tipo de rede informática: Caracterização dos servidores, switch, router, firewall, repositórios de dados
- ✓ Acessos remotos e existência de Firewall: Proteção e controle de acesso, VPN
- ✓ Backups: Alertas, Logs, redundâncias
- ✓ Suporte Técnico: interno ou externo, nível de compromisso, tempo de resposta
- ✓ Políticas de segurança: Domain control, passwords, firewall, anti virus, anti ransomware, registo de Logs, políticas de arquivo e destruição de dados
- ✓ Sistemas operativos e software profissional: versões legais e actualizadas
- ✓ Software aplicacional: em conformidade com o RGPD?
- ✓ Postos de trabalho: autenticação, anti vírus, encriptação, firewall
- ✓ Dispositivos móveis: autenticações, protocolos, anti vírus, firewall
- ✓ Documentação da rede e aplicações

Os nossos serviços estão habilitados a todo o apoio necessário no domínio da auditoria aos sistemas informáticos.