RGPD – REGULAMENTO GERAL PROTEÇÃO DE DADOS.

Regulamento EU2 016/679 do Parlamento Europeu e do Conselho, de 27.04.2016;

Será diretamente aplicável a todos os Estados Membros da União Europeia a partir de 25 de Maio de 2018

Wincode
WINCODE | SOFTWARE | CONTABILIDADE | INTERNET

RGPD - REGULAMENTO GERAL PROTEÇÃO DE DADOS

- Considerações gerais sobre o regulamento
- Direitos dos cidadãos sobre os seus dados pessoais
- Regulamento e obrigatoriedades legais
- Processos e formação interna
- Tecnologia e proteção dos dados

RGPD - REGULAMENTO GERAL PROTEÇÃO DE DADOS

• Considerações gerais sobre o regulamento

Regulamento Geral de Proteção de Dados (RGPD) passará a ser aplicado diretamente a partir de **25 de maio de 2018,** e vem substituir a atual diretiva e lei de proteção de dados pessoais. O novo quadro legal traz algumas mudanças significativas que **terão diferente impacto** na vida das organizações, consoante a sua natureza, área de atividade, dimensão e tipo de tratamentos de dados pessoais que realizem.

Assim, empresas e entidades públicas devem começar desde já a **preparar internamente a sua organização** para a aplicação do RGPD. É essencial conhecer **as novas regras**, analisar **as novas obrigações**, verificar o **nível atual de cumprimento** e adotar as medidas necessárias durante este período de transição para assegurar que tudo está pronto atempadamente. A CNPD identifica dez áreas principais de atuação, a analisar em documento anexo.

1. Informação aos titulares dos dados
2. Exercício dos direitos dos titulares dos dados
3. Consentimento dos titulares dos dados
4. Dados sensíveis
5. Documentação e Registo de atividades de tratamento (*)
6. Informação aos titulares dos dados

6. Contratos de subcontratação
7. Encarregado de proteção de dados
8. Medidas técnicas e organizativas e segurança do tratamento
9. Proteção de dados desde a conceção e avaliação de impacto
10. Notificação de violações de segurança

(*) – o registo de atividades poderá não ser obrigatório para empresas com menos de 250 trabalhadores.

- Considerações gerais sobre o regulamento

Definição do plano de implementação do RGPD
A Gestão de Topo deve começar por definir um plano de ação estratégico para implementar o RGPD, que envolva todas as áreas de negócio da empresa. No plano de ação deve constar a identificação, avaliação e categorização de todos os dados pessoais que as organizações têm armazenados.

Envolvimento de toda a organização
Deve ser criado um programa interno de comunicação mobilizador, que envolva transversalmente toda a organização, informando e sensibilizando os colaboradores sobre a privacidade, as alterações ao RGPD e os riscos inerentes ao incumprimento.

Aconselhamento jurídico
O aconselhamento jurídico é uma peça fundamental para a implementação do RGPD sem sobressaltos. O consultor jurídico deve identificar os passos já implementados e os que estão em falta para que se cumpra o novo Regulamento Geral para a Proteção de Dados e não incorra em coimas. Este levantamento de necessidades é extremamente útil se necessitar de recorrer a um parceiro para implementar as alterações necessárias.

Avaliação
Levantamento inicial, recolha de informação e documentação, check-List, Inventários de dados e de sistemas.

Diagnóstico
Analise legal, processual e tecnológica. Analise da conformidade versus requisitos do RGPD. Analise documental, analise de processos e arquitetura do sistema de informação.

Implementação
Desenho da organização. Politicas e procedimentos. Gestão do Risco. Controlo de Segurança. Formação. Atividades técnicas, apoio jurídico e transferência de conhecimento.

• Direitos dos cidadãos sobre os seus dados pessoais

- **Informação** e acesso aos seus dados pessoais (artigo 13º,14º e 15º);
- Correção e **retificação** de erros nas suas informações pessoais (artigo 16º)
- Eliminação dos seus dados pessoais (direito a ser **esquecido** *) (artigo 17º)
- **Oposição**, impedimento e limitação ao processamento (artigo 18º e 21º)
- **Portabilidade** ** dos dados pessoais (artigo 20.º) .
- O **consentimento** do titular deverá ser conferido mediante um ato positivo claro, que indique uma manifestação de vontade livre, específica, informada e inequívoca de que consente no tratamento de dados pessoais que lhe digam respeito;

Em caso de violação de dados pessoais, o responsável pelo tratamento de dados pessoais deverá notificar a entidade competente (CNPD), sem demora injustificada e, sempre que possível, até 72 horas do conhecimento da mesma.

(*) Deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento;
O titular retira o consentimento em que se baseia o tratamento dos dados;
O titular opõe-se ao tratamento;
Os dados pessoais foram tratados ilicitamente;
Cumprimento de uma obrigação jurídica decorrente do direito da União ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito;
(**) Direito à portabilidade inclui apenas dados fornecidos pelo titular

Dados pessoais - Informação relativa a uma pessoa singular identificada ou identificável. (Art.4.º do RGPD);
Categorias específicas de informação: Genética (art.4.º,n.13); Biométrica (art.4.º,n.14); Médica (art.4.º,n.14 e 15); Política e social (artigo 9.º); Penal (artigo 10º)

*É considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um **nome**, um **número de identificação**, dados de **localização**, identificadores por via **eletrónica** ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular, Exemplos:* número de cartão de cidadão, NIF, IBAN, nº telemóvel, IP, grupo sanguíneo, etc.

• Regulamento e obrigatoriedades legais

- **Condições para a LICITUDE do tratamento de dados pessoais (artigo 7º):**
  - O titular tiver dado **consentimento*** explicito e demonstrável;
  - O tratamento for necessário para a execução de um contrato ou para efeitos de diligências pré-contratuais a pedido do titular;
  - O tratamento for necessário para o cumprimento de uma obrigação jurídica;
  - O tratamento for necessário para efeito de interesses legítimos prosseguidos pelo responsável pelo tratamento.

- **Obrigações da Entidade Responsável e/ou Subcontratante**
  - Obter previamente e provar o consentimento do titular;
  - Tratamento desenvolvido na *pseudonimização*;
  - Garantir o direito a ser esquecido;
  - Garantir o direito à portabilidade dos dados;
  - Garantir "privacy by design";
  - Garantir "privacy by default";
  - Efetuar avaliações de impacto sobre proteção de dados ("*PIA*");
  - Ter encarregado de proteção de dados ("DPO");
  - Notificar e registar as violações de dados pessoais ("data breach").

(*) Consentimento pode ser dado por menores a partir dos 13 anos

• Regulamento e obrigatoriedades legais

- **Confidencialidade**
  - Todos os dados pessoais devem estar convenientemente protegidos quanto ao seu acesso ou exposição não autorizada.
- **Integridade**
  - Todos os dados pessoais devem conservar todas as características definidas pelo seu titular, desde o seu fornecimento à sua destruição.
- **Disponibilidade**
  - Todos os dados pessoais deverão estar apenas disponíveis mediante validação de perfis, permissões e condições previamente estabelecidas.
- **Conformidade legal normativa**
  - Todas as ações de recolha e tratamento de dados pessoais devem respeitar as regras do RGPD e restante legislação conexa.

Regime Sancionatório

€10M ou 2% do volume de negócios anual (faturação) a nível mundial, consoante aquele que for mais elevado em caso de **violação** dos requisitos para o **tratamento lícito** de dados;
€20M ou 4% do volume de negócios anual (faturação) a nível mundial, consoante aquele que for mais elevado em cado de **violação** de **direitos dos titulares**.

Regime Indemnizatório

O RGDP reconhece o direito do titular: a) Apresentar queixa à autoridade de controlo (CNPD); b) Ação judicial contra autoridades de controlo; c) Ação judicial contra o responsável pelo tratamento e/ou subcontratantes; d) Direito de reclamar indemnização e responsabilidade ao responsável pelo tratamento e/ou subcontratantes pelos danos sofridos.

• Processos e formação interna

- **Códigos de Conduta e Certificações**
  - Definição e redação de politicas internas de privacidade, manuais de politicas e procedimentos, códigos de ação, estatutos e outros. As empresas representantes de categorias de responsáveis pelo tratamento ou subcontratantes devem elaborar códigos de conduta;

- ***(Privacy by design & Privacy by default)***
  - Implementação de medidas técnicas e organizacionais para demonstrar que foram consideradas e integradas as exigências do **RGPD** nas atividades de tratamento de dados (pseudonimização, PIA's *).

- **Accountability**
  - Os responsáveis terão de estar em condições de demonstrar o cumprimento dos princípios do **RGPD**.

• Processos e formação interna

ENCARREGADO DE PROTEÇÃO DE DADOS (DPO - Data Protection Officer), **obrigatório se**:

- O tratamento for efetuado por uma autoridade ou um organismo público, excetuando os tribunais no exercício da sua função jurisdicional;
- As atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento que, devido à sua natureza, âmbito /ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala;
- As atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados nos termos do artigo 9º e de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10º

- **Funções do Encarregado de Proteção de Dados**
  - Informa e aconselha em matéria de proteção de dados pessoais;
  - Controla a conformidade do tratamento de dados pessoais com o RGPD e com outras disposições de proteção de dados da UE;
  - Presta aconselhamento no que respeita à avaliação de impacto sobre proteção de dados e controla a sua realização;
  - Coopera e funciona como ponto de ligação com a autoridade de controlo.

- **Quando há necessidade de recorrer a um subcontratante para efetuar o tratamento de dados pessoais há que ter em conta as seguintes regras:**
  - O recurso a serviços de tratamento de dados pessoais deve ser assegurado por garantias de execução de medidas técnicas e organizativas adequadas ao RGPD;
  - O subcontratado não pode recorrer a outro subcontratante sem autorização prévia e específica por escrito do representante de proteção de dados;
  - Um contrato de subcontratação terá de incluir o objeto e duração do tratamento de dados, natureza e finalidade, tipo de dados e categorias dos titulares assim como as obrigações e direitos do responsável.

Nota – É aconselhável, mesmo não sendo obrigatório, a nomeação de um **E**ncarregado da **P**roteção de **D**ados (EPD), essa pessoal ou subcontratante desempenharia as funções do DPO dentro da empresa ou organização.

- Tecnologia e proteção dos dados

Criação de **procedimentos de certificação** em matéria de proteção de dados bem como selos e marcas de proteção de dados para demonstrar o cumprimento e as melhores práticas.

Implementar medidas técnicas e organizativas a fim de **garantir um nível de segurança adaptado ao risco** é essencial para estar em conformidade com o GDPR.

Estas medidas devem incluir:

- A capacidade de **recuperar a disponibilidade e acesso aos dados pessoais em tempo útil** na eventualidade de um acidente físico ou técnico;
- Um método para **testar regularmente, aceder e avaliar a eficácia das medidas técnicas** e organizativas para garantir a segurança do processamento. Ver artigo 32º 1 – RPGD.
- **Monitorização** e a **análise comportamental** da rede e analisar a deteção de ataques, com a execução sistemática de **antivírus** e **anti-malware** para deteção código malicioso fazendo o respetivo isolamento e protegendo a entrada e as vulnerabilidades.

Software Anti-Vírus	Firewall	Servidores e sistemas Backups e Armazenamento	WIFI	VPN	Acessos c/Password	Sistemas NAS

RGPD - REGULAMENTO GERAL PROTEÇÃO DE DADOS

O que deve analisar neste tempo que falta?

- Onde estão os dados pessoais? Sistemas? Papel? Estão atualizados? Temos registo organizados?
- Temos consentimento do titular? Estamos preparados para dar resposta aos direitos do titular?
- Os sistemas garantem a confidencialidade, integridade e disponibilidade dos dados?
- Conseguimos comunicar violações em 72 Horas?
- Temos procedimentos para avaliar e gerir os riscos?
- Conseguimos criar evidencias e demonstrar que cumprimos o RGPD?
- Já nomeamos o Encarregado de Proteção de dados (DPO)?
- Os Sistemas e equipamentos estão atualizados?
- Os Backups e sistemas de seguranças estão em conformidade com o RGPD?
- Os antivírus estão atualizados e em conformidade.
- As firewalls e sistemas anti-intrusão estão atualizadas.

O que precisa fazer?

- **Inventariação** dos dados pessoais existentes (quais, onde estão, para onde são transmitidos, quem tem acesso, por quanto tempo) e estabelecer políticas e procedimentos que permitam gerir os dados em conformidade e reagir a qualquer falha de segurança e **notificar** à CNPD e ao titular dos dados, no prazo máximo de 72 horas, de quaisquer perdas ou acessos indevidos.
- Rever impressos, formulários, politicas de privacidade. Verificar se a linguagem utilizada é clara, acessível e se são fornecidos aos titulares dos dados, toda a informação a que o RGPD obriga: o direito à **Consulta/Alteração**, Direito ao **Esquecimento**; Direito à **Portabilidade** de Dados.
- Analisar com que fundamento legal está a processar dados. Caso seja com base no **consentimento**, terá de rever o consentimento dado, para apurar se respeita todas as novas exigências, ou se será necessário **obter novo consentimento**.
- Rever os contratos de **subcontratação** de serviços realizados no âmbito de tratamento de dados pessoais, para verificar se cumprem com os requisitos exigidos pelo RGPD.
- Garantir que tem regras especificas para **provar e evidenciar** que todos os requisitos legais são cumpridos. Realizar uma auditoria/*Assessment* para verificar o que tem de fazer para cumprir com o RGPD **(*Accountability*)**.
- Preparar a designação e funções do **Encarregado de Proteção de Dados** (se aplicável). Deve documentar de forma detalhada todas as atividades relacionadas com tratamento de dados pessoais (se aplicável).
- Verificar a efetividade do sistema de **gestão da segurança da informação**.
- Delinear rapidamente um cronograma de ação, de procedimentos a executar, plano de investimento do reforço da segurança dos sistemas e software.

A avaliação do impacto sobre a proteção de dados (PIA), deverá incluir:

- A descrição de todas as operações de tratamento a que os dados estarão sujeitos;
- Qual a finalidade das ações de tratamento de dados pessoais, e caso seja necessário qual o interesse legítimo do responsável pelo tratamento;
- A avaliação das necessidades e proporcionalidade das operações de tratamento em relação aos seus objetivos;
- A avaliação dos riscos para os direitos e liberdades dos titulares dos dados;
- Medidas previstas e garantias para fazer face aos riscos;
- Medidas e procedimentos de segurança em conformidade com o regulamento e que assegurem a proteção dos dados pessoais;
- O parecer do DPO.

FIM

Este documento é um documento de trabalho de carácter geral e abstrato, deve servir apenas para esclarecimento e analise da temática do **RGPD**. Não aborda qualquer caso concreto.

Abril de 2018

WINCODE I SOFTWARE I CONTABILIDADE I INTERNET