



**RGPD**  
Regulamento Geral  
de Proteção de Dados

Valença  
julho de 2018  
FEDERAÇÃO MINHA TERRA  
Projeto REDE LEADER2020  
Joaquim Amado

# SUMARIO

- \* **1.Regulamento Geral de Protecção de Dados (RGPD)**
- \* **2.Âmbito de Aplicação**
- \* **3.Conceitos e Princípios Relevantes**
- \* **4.Direitos dos Titulares dos Dados**
- \* **5.Obrigações do Responsável pelo Tratamento de Dados**
- \* **6.Avaliação de Impacto**
- \* **7.Encarregado de Protecção de Dados**
- \* **8.Notificação de Incidentes de Violação**
- \* **9.Quadro Sancionatório**
- \* **10.Como fazer a preparação para a conformidade com o Regulamento**

# 1. Regulamento Geral de Proteção de Dados (RGPD)

- O Regulamento Geral da Proteção de Dados (RGPD) é o regulamento da UE 2016/679 do Parlamento Europeu e do Conselho de 27/04/2016 relativo à proteção de dados pessoais e à livre circulação de dados.
- Aplicável desde o dia 25 de Maio de 2018, simultaneamente nos 28 Estados-Membros.
- Revogou a legislação europeia sobre a proteção de dados pessoais, publicada em 1995, ou seja, revogou a legislação que foi aprovada em momento anterior à utilização generalizada da internet e ao surgimento da economia digital.

# 1. Regulamento Geral de Protecção de Dados (RGPD)

No entanto, os princípios subjacentes a este normativo são exatamente os mesmos:

- \* Proteger a privacidade dos cidadãos;
- \* Garantir a livre circulação de dados pessoais dentro da União Europeia;

# 1. Regulamento Geral de Protecção de Dados (RGPD)

## \* Principais alterações deste novo Regulamento:

- Desaparece a obrigação de notificar e obter autorização, por parte da Comissão Nacional de Protecção de Dados, previamente ao início do tratamento.
- Surge a necessidade de as entidades se auto regularem com vista á conformidade com o RGPD.
- Aumenta o valor das sanções aplicáveis: a coima máxima é de 20 milhões de euros ou até 4% do volume de negócios anual da empresa a nível mundial e correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado.
- Os titulares dos dados adquirem novos direitos.

## 2. Âmbito de Aplicação do RGPD

Art.º 2º e 3º

Aplica-se a todas as pessoas singulares e coletivas que efetuem tratamento de dados pessoais de pessoas que estejam na UE.

Não se aplica a dados de pessoas coletivas, apenas e exclusivamente a dados pessoais de pessoas singulares.

O RGPD também se aplica aos subcontratantes que tratam dos dados pessoais por conta do responsável pelo tratamento.

Estão excluídos os tratamentos de dados efetuados por pessoas singulares no exercício de atividades exclusivamente pessoais ou domésticas, sem qualquer conexão à atividade comercial.

## 2. Âmbito de Aplicação do RGPD

Art. 4º nº2

### O que é o tratamento de dados?

- \* Visualização;
- \* Recolha de dados;
- \* Registo de dados;
- \* Organização de dados;
- \* Conservação de dados;
- \* Adaptação e alteração:

## 2. Âmbito de Aplicação do RGPD

Artº 4º nº 2 (continuação)

### O que é o tratamento de dados?

- \* Recuperação;
- \* Consulta;
- \* Utilização;
- \* Divulgação por qualquer forma;
- \* Destruição ou Apagamento;

## 3. Definições e Princípios Relevantes

Art. 4º nº1

### 3.1 Dados pessoais, o que são?

Não existe uma lista taxativa do que são considerados dados pessoais, mas são dados pessoais todos aqueles que possam identificar a pessoa singular, tais como: nome, morada, nº de telemóvel, correio eletrónico, idade, estado civil, dados de localização, dados genéticos, fisiológicos, económicos, sociais ou culturais.

# 3. Definições e Princípios Relevantes

Art. 4º nº2

## 3.2 Tratamento, o que é?

Operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como:

**a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição.**

# 3. Definições e Princípios Relevantes

Art. 4º nº 7

## 3.3 Responsável pelo tratamento, quem é?

Pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras:

**determina as finalidades e os meios de tratamento de dados pessoais.**

## 3. Definições e Princípios Relevantes

Art. 4º nº 8

### **3.4 Subcontratante, quem é?**

Pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes.

## 3. Definições e Princípios Relevantes

Art. ° 4 n° 11

### 3.5 Consentimento do titular dos dados

Manifestação de vontade,

-livre, específica, informada e explícita,

-pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco,

-que os dados pessoais que lhe dizem respeito sejam objeto de tratamento

Formulários eletrónicos deverão conter toda a informação para que se possa obter o consentimento formal.

## 3. Definições e Princípios Relevantes

Art. 4º nº 12

### 3.6 Violação de dados pessoais, o que é?

Considera-se uma violação da segurança que provoque, de modo acidental ou ilícito:

- a destruição, perda, alteração ou a divulgação ou o acesso, não autorizados,
- a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

## 3. Definições e Princípios Relevantes

### \* 3.7 Que princípios são aplicáveis?

- \* **Livre circulação** - artº 1º nº1
- \* **Licitude, lealdade e transparência** – artº 5 nº 1 a)
- \* **Limitação das finalidades** – artº 5 nº 1 b)
- \* **Minimização** – artº 5 nº 1 c)
- \* **Exatidão** – artº 5 nº 1 d)
- \* **Limitação da conservação** – artº 5 nº 1 e)
- \* **Integridade e confidencialidade** – artº 5 nº1 f)
- \* **Responsabilidade** – artº 5 nº 2

## 3. Definições e Princípios Relevantes

- \* Art. 6º nº1

- \* **3.8 A licitude do tratamento**

- \* **Consentimento**

- \* **Execução de um contrato**

- \* **Cumprimento de uma obrigação jurídica**

- \* **Defesa de interesses vitais do titular**

- \* **Exercício de funções de interesse público ou de autoridade pública**

- \* **Interesse legítimos do responsável pelo tratamento**

# 4. Direitos dos Titulares de Dados

O RGPD confere aos titulares dos dados um conjunto de direitos que têm de ser salvaguardados pelo responsável pelo tratamento, são eles:

- \* 4.1 Direito de acesso – art. 15 ;
- \* 4.2 Direito de retificação – art. 16 ;
- \* **4.3 Direito ao apagamento** - art. 17 ;
- \* **4.4 Direito à limitação do tratamento** – art. 18 ;
- \* **4.5 Direito de portabilidade dos dados** – art. 20 ;
- \* 4.6 Direito de oposição – art. 21 ;
- \* 4.7 Direito a não ficar sujeito a decisões individuais automatizadas – art. 22 ;

# 4. Direitos dos Titulares de Dados

## 4.1 Direito de acesso - art 15

É garantido aos titulares dos dados o direito a saber se estão, ou não, a ser tratados dados pessoais que lhe digam respeito, garantindo-se ainda o direito ao titular dos dados de aceder aos mesmos.

Esse direito de acesso deve ser tendencialmente gratuito, não obstante possa ser criada uma taxa para permitir tal acesso no caso de pedidos infundados ou excessivos.

# 4. Direitos dos Titulares de Dados

## \* Pedido de informação

Ao abrigo do art. 15º do Regulamento de Proteção de Dados, EU 2016/679

Exmos. Senhores,

Eu, ....., portador do cartão de cidadão....., venho por este meio solicitar que me facultem:

- \* 1- Os dados pessoais (dados identificativos e dados conexos) que têm sobre mim,
- \* 2- Os tratamentos que realizam sobre esses dados ,
- \* 3- A base legal de cada tratamento realizado,

# 4. Direitos dos Titulares de Dados

- \* 4- A origem dos dados cuja fonte não sou eu,
- \* 5- Se quaisquer dados pessoais são comunicados a terceiros e nesse(s) caso(s) quais dados, a qual entidade terceira e qual a respetiva base legal.
- \* 6- As evidências de consentimento, aos tratamentos em que for aplicável,
- \* 7- O prazo de retenção dos dados,
- \* 8- Onde ou por que meios comunicaram e/ou publicaram informação sobre proteção da privacidade dirigida a mim e outros cidadãos equivalentes,

## 4. Direitos dos Titulares de Dados

- \* 9- O meio de acesso para retificação da minha informação, se vier a ser necessário,
- \* 10- O meio de revogação de consentimento, nos tratamentos em que for aplicável e
- \* 11- Uma declaração em como a vossa entidade cumpre os requisitos de proteção da privacidade e dos meus dados pessoais definidos no Regulamento EU 2016/679.

Como define o Regulamento supra indicado no seu nº3 do artº 12º espero resposta no prazo mais curto possível mas não superior a um mês, que pode ser enviada para

....@....

# 4. Direitos dos Titulares de Dados

## 4.2 Direito de retificação – art 16

É assegurado aos titulares dos dados o direito a obterem a retificação dos seus dados pessoais que estejam desatualizados, incorretos ou incompletos.

# 4. Direitos dos Titulares de Dados

## 4.3 Direito ao apagamento – art 17

Novidade introduzida pelo RGPD que possibilita aos titulares dos dados o direito de solicitar ao responsável pelo tratamento dos dados o apagamento dos seus dados.

Garante-se aos titulares dos dados, dentro das limitações estabelecidas por lei, o direito de obter a eliminação dos seus dados pessoais desde que:

# 4. Direitos dos Titulares de Dados

## \* 4.3 Direito ao apagamento – art 17 (continuação)

- \* - Os dados se revelem desnecessários para as finalidades para os quais foram recolhidos ou tratados;
- \* - O titular retire o consentimento, quando o tratamento for necessariamente fundamentado neste e não exista outro fundamento legal para o tratamento dos dados;
- \* - O titular se oponha ao tratamento de dados pessoais utilizados para fins automatizados e/ou de profiling;
- \* - Quando os dados pessoais tenham sido tratados de forma ilícita.

# 4. Direitos dos Titulares de Dados

## 4.3 Direito ao apagamento – art 17 (cont.)

Se o responsável pelo tratamento os tornou públicos:

- deverá informar os restantes responsáveis pelo tratamento dos dados que o titular solicitou o “apagamento das ligações para esses dados” bem como das “cópias e reproduções” dos mesmos,
- tomando “as medidas que forem razoáveis, incluindo de carácter técnico, tendo em consideração a tecnologia disponível e os custos da sua aplicação.”

# 4. Direitos dos Titulares de Dados

## 4.4 Direito à limitação do tratamento – art 18

Em paralelo ao direito ao apagamento:

-o direito à limitação do tratamento ao prever que o titular dos dados tem o direito de exigir a limitação do tratamento nas seguintes situações:

- \* se contestar a exatidão dos dados pessoais, durante um período que permita ao responsável pelo tratamento verificar a sua exatidão;
- \* se o tratamento for ilícito e o titular dos dados se opuser ao apagamento dos dados pessoais e solicitar, em contrapartida, a limitação da sua utilização;

# 4. Direitos dos Titulares de Dados

## 4.4 Direito à limitação do tratamento – art 18 (cont.)

- \* se o responsável pelo tratamento deixar de precisar dos dados pessoais para fins de tratamento, mas esses dados sejam requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial;
- \* se se tiver oposto ao tratamento até se verificar que os motivos legítimos do responsável pelo tratamento prevalecem sobre os do titular dos dados.

# 4. Direitos dos Titulares de Dados

## 4.5 Direito de portabilidade dos dados – art 20

- confere-se aos titulares o direito a solicitarem ao responsável pelo tratamento dos dados, os seus dados pessoais,
- num formato de uso comum e
- mesmo a sua transferência para outro responsável pelo tratamento.

# 4. Direitos dos Titulares de Dados

## 4.5 Direito de portabilidade dos dados – art 20 (cont.)

- apenas poderá exigir que os seus dados sejam entregues a outro responsável pelo tratamento se tal for “tecnicamente possível”.

- os responsáveis pelo tratamento não tem a obrigatoriedade de adotar ou manter sistemas de tratamento que sejam tecnicamente compatíveis, mas são encorajados a desenvolver formatos interoperáveis.

# 4. Direitos dos Titulares de Dados

## 4.6 Direito de oposição – art 21

Opor-se a qualquer momento ao tratamento dos dados pessoais que lhe digam respeito tendo em vista a sua situação particular, a definição de perfis ou *marketing* direto.

Caso se verifique a oposição, o responsável pelo tratamento deve cessar o tratamento dos dados pessoais, a não ser que:

- apresente razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados,
- ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

# 4. Direitos dos Titulares de Dados

## 4.7 Direito a não ficar sujeito a decisões individuais automatizadas – art. 22

São tratamentos exclusivamente automatizados incluindo definição de perfis – com exclusão de mão humana.

A não ser que:

- decisão necessária para cumprimento de contrato;
- decisão autorizada pela legislação (casos de fraude ou evasão fiscal por ex:);
- decisão baseada em consentimento explícito.

## 5. Obrigações do Responsável pelo Tratamento de Dados

As organizações terão que conseguir provar que cumprem o regulamento e como tal, que o tratamento dos dados foi efetuado em conformidade com o RGPD, especificadamente:

- \* Que os dados pessoais que têm em sua posse são legítimos e estão limitados ao estritamente necessário;
- \* Que os dados estão atualizados, seguros e confidenciais;
- \* Que adotou políticas, procedimentos, códigos de conduta e instruções internas formalizadas aptas para serem disponibilizadas às entidades de supervisão;
- \* Que possuiu sistemas para monitorizar se as políticas e procedimentos estão a ser seguidos;

## 5. Obrigações do Responsável pelo Tratamento de Dados

### Têm ainda que:

- \* Implementar mecanismos permanentes e dinâmicos de verificação da conformidade com o RGPD;
- \* Provar por evidência que respeita o RGPD;
- \* Promover auditorias no âmbito de um controlo contínuo para verificar a eficácia das medidas implementadas e, se necessário, modificá-las;
- \* Proteger os dados desde a conceção e por defeito.

# 6. Avaliação de Impacto

## **Art. 35**

Quando:

- o tratamento de dados pessoais for suscetível de resultar em um alto risco para os direitos e liberdades das pessoas em causa,
- o Responsável pelo Tratamento, antes de iniciar o tratamento, deverá efetuar uma Avaliação de Impacto das operações de tratamento sobre a proteção de dados, (que contará com o parecer do Encarregado da Proteção de Dados de este tiver sido designado).

## 6. Avaliação de Impacto

Está previsto que a autoridade de controlo elabore e torne pública uma lista com os tipos de operações consideradas de elevado risco.

## 7. Encarregado de Protecção de Dados (DPO)

### Art. 37

O Data Protection Officer (DPO)

-Uma das principais novidades introduzidas pelo RGPD é a figura do Encarregado de Protecção de Dados, o Data Protection Officer (DPO).

-As autoridades ou organismos públicos, entidades que controlem regularmente dados pessoais em grande escala e/ou que tratem dados sensíveis em grande escala devem nomear um DPO.

## 7. Encarregado de Protecção de Dados (DPO)

-O DPO reporta diretamente ao mais alto nível da organização, porquanto as funções que lhe são atribuídas pelo RGPD requerem a satisfação de determinadas condições.

-O DPO tem a responsabilidade de assegurar que a empresa/entidade que o contrata está devidamente *compliant* (conforme) com as regras da proteção de dados.

## 7. Encarregado de Protecção de Dados (DPO)

O DPO deve:

- informar, aconselhar e orientar a direcção da organização, bem como os seus trabalhadores, a respeito das obrigações constantes do RGPD,
- servir ainda como ponto de contacto com a autoridade de controlo nacional, a Comissão Nacional de Protecção de Dados.

## 7. Encarregado de Protecção de Dados (DPO)

O DPO deve notificar a Autoridade de Controlo para os casos de quebra de segurança e/ou violação de dados, melhorando os processos de gestão por forma a evitar:

- \* Ataques de códigos maliciosos não autorizados;
- \* Violação de sistemas de segurança;
- \* Acessos não autorizados;
- \* Incidentes com sistemas e equipamentos de apoio.

## 7. Encarregado de Protecção de Dados (DPO)

A função do DPO deverá ser integrada numa equipa multidisciplinar, com as seguintes competências e critérios:

- \* Nível de especialização: ter em conta a sensibilidade e complexidade dos dados; comunicação com os restantes departamentos;
- \* Qualidades profissionais: conhecimento da lei, regras e sistemas de informação; formação contínua;
- \* Capacidade para desempenhar as funções: integridade e ética; promoção de uma cultura de protecção de dados .

# 7. Encarregado de Protecção de Dados (DPO)

## **O DPO :**

- \* Deve ser independente, não recebendo instruções quanto à forma de tratar uma questão;
- \* Não deve receber instruções no sentido de adotar determinada perspetiva ou resultado de qualquer questão;
- \* Deve elaborar um relatório anual de atividades a apresentar ao Conselho de Administração/Direção;
- \* Não pode ser penalizado ou destituído pelo exercício regular das suas funções;
- \* Não tem responsabilidade pessoal.

# 7. Encarregado de Protecção de Dados (DPO)

## O DPO deve:

- \* Ter em consideração os riscos associados às operações de tratamento – natureza, âmbito, contexto, finalidade;
- \* Centrar esforços em questões de maior risco, identificando áreas que devam ser objeto de auditorias;
- \* Colaborar com a Autoridade de Controlo, nomeadamente com consultas prévias;
- \* Ser ponto de contacto com os titulares dos dados – contacto direto é crucial para que nenhuma consequência nefasta advenha da violação registada;

# 7. Encarregado de Protecção de Dados (DPO)

## O DPO deve ainda:

- \* Conhecer bem a organização e o negócio;
- \* Proceder a ações de consciencialização;
- \* Estar preparado para incorporar na organização conceitos de privacy by design e privacy by default (privacidade na conceção e privacidade por defeito);
- \* Adotar procedimentos de deteção de incidentes; adotar procedimentos de reação ao incidente; adotar procedimentos para cumprir prazos de resposta ao titular dos dados (30 dias) e de comunicação de qualquer violação (72 horas)

## 8. Notificação de Incidentes de Violação

### Art. 33

Em caso de violação de dados os responsáveis pelo tratamento devem notificar a Autoridade de Controlo, exceto se não apresentar risco para os direitos e liberdades dos titulares dos dados, logo que possível, no prazo máximo de 72 horas após conhecimento.

# 8. Notificação de Incidentes de Violação

Art. 33 n° 2

A notificação deve conter os seguintes elementos:

- \* natureza da violação,
- \* categorias de dados;
- \* número de titulares afetados;
- \* número de registos em causa;
- \* contactos;
- \* consequências do incidente ocorridas;
- \* medidas adotadas para reparar ou mitigar potenciais efeitos adversos.

## 8. Notificação de Incidentes de Violação

No caso da violação de dados pessoais ser suscetível de implicar um risco elevado para os titulares dos dados, os mesmos deverão ser imediatamente notificados.

Deve manter-se um registo dos incidentes de segurança verificados.

## 9. Quadro Sancionatório

### Art. 83

O incumprimento das obrigações do Regulamento pode conduzir à aplicação de coimas elevadas às organizações.

Consoante a natureza da infração o Regulamento prevê coimas que podem ascender aos 20 Milhões € ou até 4 % dos resultados globais da empresa (consoante o que for superior);

## 9. Quadro Sancionatório

- A coima a aplicar dependerá de fatores como:  
a natureza, gravidade, carácter intencional ou negligente da infração, medidas, segurança/controlo implementadas, grau de cooperação com a CNPD, existência de um Encarregado de Proteção de Dados, etc...
- O Regulamento prevê também indemnização por danos materiais e não materiais – art. 82.
- Poderá também existir responsabilidade criminal – a definir pela lei nacional.

## 10. Como fazer a preparação para conformidade com o Regulamento

- \* **1. Criar equipa de implementação**
- \* **2. Levantamento e mapeamento de todos os tratamentos de dados pessoais**
- \* **3. Diagnóstico**
- \* **4. Definição de medidas**
- \* **5. Implementação**

# 10. Como fazer a preparação para conformidade com o Regulamento

## **Diagnóstico:**

Cada organização deverá fazer o seu diagnóstico para que possa adotar medidas que a coloquem em *compliance* (conformidade), respondendo às seguintes questões:

- \* O tratamento recai no âmbito de aplicação do RGDP? (âmbito territorial e âmbito material)
- \* Categoria dos dados tratados? (Crianças? Dados sensíveis? Dados referentes a condenações penais?)
- \* O tratamento é lícito? (Consentimento do titular? Cumprimento de uma obrigação jurídica?...)
- \* Foi garantido o direito à informação? (Finalidade da recolha? Prazo de manutenção? O direito de reclamar?...)

# 10. Como fazer a preparação para conformidade com o Regulamento

## **Algumas medidas a adotar:**

- \* Informação e formação;
- \* Elencar os dados pessoais existentes na organização;
- \* Avaliar a tecnologia existente na organização e verificar se a mesma é adequada às exigências do RGPD;
- \* Criar ou rever a política de privacidade;

# 10. Como fazer a preparação para conformidade com o Regulamento

## **Algumas medidas a adotar: (cont.)**

- \* Criação de procedimentos internos para resposta ao exercício dos direitos dos titulares;
- \* Revisão dos termos de consentimentos já existentes;
- \* Revisão e atualização de formulários;
- \* Análise dos contratos de trabalho;

# Como fazer a preparação para cumprimento do regulamento

- \* **Algumas medidas a adoptar: (cont.)**
- \* Análise dos contratos dos subcontratados (prestações de serviços;)
- \* Identificar a eventual obrigatoriedade/necessidade de designação de DPO;
- \* Adotar medidas técnicas e organizativas que garantam a segurança dos dados;
- \* Elaborar uma avaliação de impacto quando necessário.

OBRIGADO