# NOVO REGULAMENTO GERAL SOBRE PROTEÇÃO DE DADOS

## Sabe qual o impacto na sua organização?

## O que é o Regulamento Geral sobre a Proteção de Dados (RGPD)?

O RGPD regula a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, revogando a Diretiva 95/46/CE. O RGPD atualmente em vigor e de direta aplicação a partir de 25 de maio de 2018, introduz não só novas regras, como também elevadas coimas em caso de incumprimento, o que exige uma atenção cuidada das Organizações que lidam com dados pessoais.

O novo Regulamento reveste-se de alguma complexidade, com novos princípios e conceitos, novos direitos para os titulares de dados que significam novos deveres para as empresas que com eles lidam. A avaliação de impacto, a privacidade na conceção de novos produtos ou serviços com dados e a privacidade por defeito, notificações das violações de segurança e a figura do Encarregado de Proteção de Dados (DPO), são alguns exemplos.

### Porque o RGPD está a alarmar quem tem dados pessoais?

- Porque tem coimas avultadas e a CNPD será atuante
- Porque não se cinge a questões legais e IT. É transversal na organização e implica implementar um sistema de gestão de risco, um sistema de gestão de segurança da informação e a adoção de comportamentos novos
- Porque há muito trabalho a fazer para cumprir com o RGPD, num período de tempo que se vai reduzindo
- Porque cabe às Organizações provarem que cumprem com o regulamento.

*Coimas podem atingir 4% da faturação global anual ou 20 M€*

## Que dados?

Informação relativa a uma pessoa singular identificada ou identificável. Inclui dados genéticos e dados biométricos. Conceito de identificável inclui o nome, número de identificação, dados de localização, identificadores por via eletrónica, bem como um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular. Tratamento, inclui não só a recolha, mas também todo o "manuseamento".

## PRINCIPAIS DESAFIOS

| | |
|---|---|
| ***Consentimento*** | Qualquer tratamento de dados pessoais, mesmo que recolhidos antes do regulamento, terá de cumprir com o regulamento. Um dos alicerces é a necessidade de consentimento do titular de dados, para uma finalidade claramente definida. O consentimento tem que ser livre, específico, informado, explícito e por ato inequívoco. Retirar consentimento deverá ser tão simples quanto conceder.<br>É natural que muitos consentimentos já existentes não cumpram com todos os requisitos do RGPD, o que obriga obter novo consentimento. |
| ***Prova e Evidência de Cumprimento (Accountability)*** | As organizações têm de conseguir provar que cumprem com o regulamento, nomeadamente:<br>• Que os dados pessoais que possuem são legítimos e estão limitados ao que é necessário<br>• Que os dados estão atualizados, seguros e confidenciais<br>• Que têm políticas, procedimentos, códigos de conduta e instruções internas, formalizadas e capazes de serem disponibilizadas às entidades de supervisão<br>• Que possuem sistemas para monitorizar se as políticas e procedimentos estão a ser seguidas.<br>É assim necessário ter regras mas também acautelar registos probatórios do cumprimento do RGPD. |
| ***Novos Direitos, Necessidades de Adaptação*** | O RGPD enumera um conjunto de direitos dos titulares de dados, alguns dos quais requerem alterações significativas da forma como se tem operado, a salientar:<br>• Direito de ser esquecido: o titular de dados tem direito a solicitar que os dados sejam apagados<br>• Direito de portabilidade: o titular de dados pode solicitar que os dados que disponibilizou a um prestador de serviços sejam transferidos para outro prestador, desde que tecnicamente possível<br>• Direito de não sujeição a nenhuma decisão tomada apenas com base no tratamento automatizado. |
| ***Notificação da Violação de Dados*** | A CNPD terá de ser notificada (em 72 horas) de todas as violações de dados com risco para o titular.<br>Para tal, as Organizações têm de ser capazes detetar qualquer violação de dados, logo que ocorra. |
| ***A Segurança de Dados terá de ser Reforçada*** | A Segurança passa pela capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento, o que na prática significa a obrigatoriedade (por lei) de implementação de um sistema de gestão de segurança da informação.<br>É determinante localizar dados pessoais e eliminar os não conformes, quer nos diversos sistemas quer em papel, quer nas Organizações quer nos subcontratados para tratamento. Poderão existir custos significativos de adaptação dos sistemas às novas regras e a técnicas de proteção recomendadas.<br>É introduzido o conceito Privacy by Design, a proteção de dados desde a conceção e por defeito, o que requer a inclusão desta temática nos processos de desenvolvimento do tratamento de dados. |
| ***Data Protection Officer (DPO)*** | Autoridade 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, um Encarregado da Proteção de Dados.<br>Mesmo nas entidade em que não seja mandatório o DPO, a entidade deverá designar um responsável pelo tratamento e proteção dos dados pessoais. |
| ***Exigências para quem é subcontratado para processar dados pessoais*** | É muito comum que os dados pessoais sejam, total ou parcialmente, tratados por terceiros subcontratados. Os subcontratados passam a ter responsabilidades, o que implica, entre outros, que hajam contratos que definam regras entre as partes. Os contratos existentes têm de ser revistos.<br>Ao subcontratado cabe provar que cumpre com todas as regras do contrato e do próprio RGPD, nomeadamente em matérias de confidencialidade e segurança. |

## As várias fases do suporte BDO

**1 GAP para RGPD**

- Avaliação detalhada da situação face ao RGPD e recomendações
  - Inventariação dos dados pessoais existentes (quais, onde estão, para onde são transmitidos, quem tem acessos, qual o propósito principal para o seu processamento, por quanto tempo serão retidos)
  - Consentimentos, finalidades e requisitos gerais de licitude do tratamento de dados
  - Sistema de gestão de riscos e sua adequação aos riscos de privacidade e de dados pessoais
  - Direitos dos titulares de dados assegurados ou não
  - Efetividade do Sistema de gestão da segurança da informação
  - Políticas e procedimentos definidos, fluxos de informação sobre dados pessoais
  - Evidência de procedimentos existentes
  - Entidades subcontratadas, responsabilidades e contratos
  - Intervenientes no processo de gestão de dados pessoais e responsabilidades

**2 Adequação ao RGPD**

- Mapeamento dos riscos existentes: nível de risco e nível de esforço para redução de risco e/ou cumprimento do RGPD
- Opções existentes
- Sugestões
- Cronograma de ação
- Plano de investimentos

**3 Cumprimento do RGPD**

Implementação das ações tendentes ao cumprimento do RGPD, como sejam:

- Definição e redação de políticas internas de privacidade
- Formalização de questões de Governance (manuais de políticas e procedimentos, códigos de ação, estatutos, etc.)
- Definição de mecanismos de consentimento
- Revisão de contratos com subcontratados
- Sistemas de monitorização e controlos
- Definição de responsabilidades e funções DPO

**4 Manutenção do RGPD**

- Encarregado de Proteção de Dados: Exercício da função de DPO externo
- Training: Formação geral. Formação de temas específicos
- Auditorias regulares de Compliance & Awareness: Auditorias regulares sobre o cumprimento das disposições do RGPD (auditoria de conformidade)
- Privacy Impact Assessment: Avaliar impacto quando um novo tipo de tratamento é introduzido
- Vulnerability mapping & Intrusion Testing: Testar com regularidade e identificar as vulnerabilidades de intrusão e acesso aos dados, que permitam aferir os mecanismos de prevenção

**Onde estão os dados pessoais? Sistemas? Papel? Estão atualizados? Possuímos um registo organizado?**

**Temos consentimento dos titulares de dados com todos os requisitos do RGPD?**

**Estamos preparados para dar resposta a todos os direitos dos titulares de dados?**

**Os sistemas garantem a confidencialidade, integridade e disponibilidade dos dados?**

**Conseguimos detetar qualquer violação de dados logo que ocorra e comunicá-la em 72 horas?**

**Temos políticas e procedimentos que permitam avaliar e gerir os riscos?**

**Conseguimos recolher evidências e demonstrar que cumprimos com o RGPD?**

**E enquanto processador de dados por conta de terceiros, cumprimos o RGPD?**

**Já nomeámos um Encarregado da Proteção dos Dados (DPO)?**

*Muitas necessidades de adaptação para o pouco tempo remanescente*

Carlos Fontão de Carvalho
Head Advisory Services
Direto: +351 217 990 425
Telem: +351 937 607 040
fontao.carvalho@bdo.pt

Cristina Sousa Dias
Advisory Partner
Direto: +351 217 997 009
Telem: +351 937 997 009
cristina.dias@bdo.pt

Vasco Jara Schiappa
Manager / IT
Direto: +351 217 997 003
Telem: +351 937 990 180
vasco.schiappa@bdo.pt

Sílvia Margarida Atalaia
Advisory Supervisor
Telem: +351 937 990 306
silvia.atalaia@bdo.pt

**Lisboa**
Av. da República, 50 - 10º
1069-211 Lisboa
Tel: +351 217 990 420
Fax: +351 217 990 439

**Porto**
Rua S. João de Brito, 605 E, 3.2
4100-455 Porto
Tel: +351 226 166 140
Fax: +351 226 166 149

**Faro**
Av. 5 de Outubro, 14 - 2º
8000-076 Faro
Tel: +351 289 880 820
Fax: +351 289 880 829

**Funchal**
Rua dos Aranhas, 5 - r/c
9000-044 Funchal
Tel: +351 291 213 370
Fax: +351 291 213 399

**Luanda**
Rua Fernão Mendes Pinto, 51 a 53
Luanda - Angola
Tel: +244 929 589 050

**Praia**
Avenida Andrade Corvo, 30, r/c
CP 63 Praia - Cabo Verde
Tel: +238 261 32 08
Fax: +238 261 32 09

Siga-nos

## COMPROMISSO, RIGOR, CONFIDÊNCIALIDADE E INDEPENDÊNCIA

A BDO é a 5ª maior rede internacional de Auditoria e Consultoria, com mais de 1400 escritórios em 158 países.

Garantimos um elevado envolvimento dos partners em cada projeto, oferecendo uma assessoria técnica de alto nível e procurando relações profissionais de longo prazo, para uma melhor compreensão dos negócios de cada indústria e com o objetivo último de dar valor acrescentado aos nossos clientes.

Prestamos serviços de carácter multidisciplinar a empresas internacionais e a grupos locais, a grandes e médias empresas, a empresas familiares e a negócios com potencialidades de crescimento, em qualquer sector de atividade.

BDO & Associados, SROC, Lda., Sociedade por quotas, Sede Av. da República, 50 - 10º, 1069-211 Lisboa, Registada na Conservatória do Registo Comercial de Lisboa, NIPC 501 340 467, Capital 100 000 euros. Sociedade de Revisores Oficiais de Contas inscrita na OROC sob o número 29 e na CMVM sob o número 20161384. BDO Consulting, Lda., Sociedade por quotas, Sede Rua S. João de Brito, 605 E, 3.2, 4100-455 Porto, Registada na Conservatória do Registo Comercial do Porto, NIPC 505 275 970, Capital 50 000 euros.

BDO & Associados, SROC, Lda. e a BDO Consulting, Lda., sociedades registadas em Portugal, são membro da BDO International Limited, sociedade inglesa limitada por garantia, e fazem parte da rede internacional BDO de firmas independentes.