



REGULAMENTO GERAL DE PROTEÇÃO DE DADOS (RGPD)

(Aprovação pelo Parlamento Europeu e Conselho Europeu
em 27 de abril de 2016)

REGULAMENTO GERAL DE PROTEÇÃO DE DADOS (RGPD)



(Em vigor a partir de 25 de maio de 2018)

REGULAMENTO GERAL DE PROTEÇÃO DE DADOS (RGPD)

1. Enquadramento geral | Novo quadro jurídico

1.Enquadramento geral | Novo quadro jurídico

Há muito que o dados pessoais deixaram de ser apenas isso, “dados pessoais”.

O titular dos dados “deposita” a sua informação numa organização, confiando em três pressupostos:

- os dados estão seguros;
- os dados são trabalhados para que a organização lhes proporcione um melhor serviço;
- a informação contida nos seus dados irá trazer-lhe vantagens diretas e imediatas.

O RGPD é uma questão legal, processual e tecnológica.

1.Enquadramento geral | Novo quadro jurídico

Há muito que o dados pessoais deixaram de ser apenas isso, “dados pessoais”.

O titular dos dados “deposita” a sua informação numa organização, confiando em três pressupostos:

- os dados estão seguros;
- os dados são trabalhados para que a organização lhes proporcione um melhor serviço;
- a informação contida nos seus dados irá trazer-lhe vantagens diretas e imediatas.

O RGPD é uma questão legal, processual e tecnológica.

1.Enquadramento geral | História europeia da proteção de dados

- Convenção Europeia dos Direitos do Homem (CEDH), 1953: proteção de dados pessoais , artº 8º
- Criação do Tribunal Europeia dos Direitos do Homem, 1959 – garantia do cumprimento das obrigações, apreciação de queixas
- Convenção 108, em 1981 – aplica-se a todos os tratamentos de dados pessoais, proteção dos cidadãos contra os abusos, garantias relativas aos dados pessoais sensíveis (raça, saúde, opinião política, convicções religiosas, vida sexual ou registo criminal.
- Diretiva nº95/46/CE do Parlamento Europeu e do CE, 24.10.1995 – primeiro instrumento jurídico sobre a proteção de dados.
- Aprovação do RGPD pelo Parlamento Europeu e Conselho Europeu, em 27 de abril de 2016

1.Enquadramento geral | História portuguesa da proteção de dados

- Constituição Portuguesa de 1976, atº 35º - Utilização da informática:
 1. (...) direito de tomar conhecimento do que constar nos registos mecanográficos que lhe digam respeito (...)
 2. A informática não pode ser usada para tratamento de dados referentes a convicções políticas, religiosas ou da vida privada(...)
 3. É proibida a atribuição de um número nacional único.

Atualmente, este artigo vai um pouco mais longe.

-Lei nº10/91: Lei da Proteção de Dados Pessoais face à informática. Início da criação da Comissão Nacional de Proteção de Dados (a qual, genericamente pretendia controlar o processamento automatizado de dados pessoais).

-Lei nº28/94 – introdução de medidas de reforço da proteção de dados.

1.Enquadramento geral | Novo quadro jurídico

Qual a importância do RGPD?

■ Serve de motivação para compreender como é que as organizações protegem e obtêm valor de informações sensíveis dos clientes.

Mitiga o risco de:

- perda de confiança dos clientes e vendas – dano reputacional
- violações de segurança
- coimas e sanções
- ações judiciais

Mas também fornece um maior controlo e percepção das necessidades do cliente.

1.Enquadramento geral | Novo quadro jurídico

■Regulamento 2016: o “tratamento dos dados pessoais deverá respeitar (...) os direitos e liberdades fundamentais, nomeadamente o direito à protecção dos dados pessoais”.

O RGPD consubstancia-se num conjunto de normas legais que regula a forma de tratar informação sobre as pessoas, com respeito pelos direitos fundamentais. Importante:

-Não tem como objectivo proibir a utilização de informação pessoal

mas...

...procura harmonizar a “livre circulação dos dados pessoais” na UE e a tutela dos direitos e liberdade fundamentais

1.Enquadramento geral | Novo quadro jurídico

Principais novidades face à realidade atual:

- Alterado o modelo clássico de “notificações/autorizações prévias de tratamento” à CNPD (controlo externo).
- Relevância de medidas internas (exº: avaliação do impacto das operações de tratamento de dados, realização de auditorias, manutenção de registos de actividades de tratamentos de dados).
- Os titulares dos dados passam a ter novos direitos. As organizações devem adoptar procedimentos eficazes e expeditos de modo a assegurar o exercício efetivo destes direitos.
- As circunstâncias aplicáveis ao consentimento do titular dos dados e à legalidade do tratamento são mais exigentes.
- Surge a obrigação de comunicação de quebras de segurança às autoridades competentes e, em certos casos, aos próprios titulares dos dados. Eventual nomeação de um DPO (*Data Privacy Officer*).
- O custo do incumprimento é relevante, com sanções muito elevadas – para além de outros danos, por exemplo de natureza reputacional.

1.Enquadramento geral | Novo quadro jurídico

■ NOVAS OBRIGAÇÕES EM GERAL:

- Obrigação de registo das atividades de tratamento (arts. 30.º e seguintes do RGPD)
- Notificação de uma violação de dados pessoais à autoridade de controlo no prazo de 72 horas (art.33.º - RGPD)
- Obrigação de avaliação de impacto sobre a protecção de dados e consulta prévia (art. 35.º e art.36.º - RGPD)
- Nomeação de um encarregado da protecção de dados ("DPO") (arts. 37.º e seguintes do RGPD) e de Interlocutor/Subcontratante.

REGULAMENTO GERAL DE PROTEÇÃO DE DADOS (RGPD)

PRINCÍPIOS:

- Licitude, lealdade e transparência
- Exatidão
- Minimização dos dados
- Limitação das finalidades
- Limitação da conservação
- Integridade e confidencialidade
- Responsabilidade



REGULAMENTO GERAL DE PROTEÇÃO DE DADOS (RGPD)

OBJETIVOS DA IMPLEMENTAÇÃO DO RGPD:

- Aumentar a proteção dos dados pessoais das pessoas singulares;
- Facilitar o acesso, retificação, limitação, transferência e eliminação de dados pessoais fornecidos;
- Potenciar a monitorização do sistema de proteção de dados das pessoas singulares;
- Diminuir ou eliminar por completo os riscos de acesso ou tratamento indevido;
- Fortalecer a confiança dos utentes nas instituições;
- Proporcionar uma melhoria do serviço público prestado.

Alguns conceitos

Titular

Pessoa singular identificada ou identificável que dá o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas.

Dados pessoais

Informação relativa a uma pessoa singular identificada ou identificável (“titular dos dados”), independentemente do suporte em que seja recolhida (papel, digital ou outro). Nos agrupamentos de escolas incluem todos os dados relativos aos alunos, aos encarregados de educação, ao pessoal docente e ao pessoal não docente.

Alguns conceitos

Dados sensíveis

Os dados que, pela sua natureza, coloquem em causa direitos e liberdades fundamentais, prevenindo efeitos discriminatórios, tais como origem racial ou étnica; opinião política; religião ou convicções; filiação sindical; estado genético ou de saúde; dados biométricos; orientação sexual. E ainda os que se relacionem com condenações penais, infrações ou medidas de segurança (artº 10º).

Regra geral: proibição de tratamento (n.º 1 do artº 9º).
Excepções (n.º 2 do art. 9.º)

Alguns conceitos

Tratamento

“Uma 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.”

Novidade: “Limitação do tratamento”: “inserção de uma marca nos dados pessoais conservados com o objectivo de limitar o seu tratamento no futuro”

Relevo: art. 18.º (direito a limitação do tratamento)

Alguns conceitos

Responsável pelo tratamento de dados

Pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto, determina as finalidades e os meios de tratamento de dados pessoais e a quem competirá, entre outras funções, aplicar as medidas técnicas e organizativas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o RGPD (artº 4º, 7º e 24º e ss.)

Encarregado de proteção de dados

Técnico com conhecimentos especializados do domínio da legislação e práticas de proteção de dados, que assiste o responsável pelo tratamento da dados no controlo do cumprimento do RGPD (artº 39º)

- Dionísio Jesus Vieira – DGEstE – DSRC

Subcontratante/Interlocutor

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

Direitos dos titulares dos dados

(artº 12º e seguintes)

- Direito à proteção dos dados pessoais (artº 1º)
- Direito à informação (artº 13º)
- Direito de acesso (artº 15º)
- Direito de retificação (artº 16º)
- Direito ao apagamento de dados (artº 17º)
- Direito à limitação do tratamento (artº 18º)
- Direito à notificação (artº 19º)
- Direito de portabilidade dos dados (artº 20º)
- Direito de oposição (artº 21º)
- Direito a não ficar sujeito a decisões automatizadas (artº 22º)

Direitos dos titulares dos dados

(artº 12º e seguintes)

- Direito a ser avisado em caso de violação dos dados pessoais (artº 34º)
- Direitos relacionados com os princípios do tratamento de dados pessoais (artº 5º)

Limitações aos direitos dos titulares dos dados

(artº 23º do RGPD)

- Segurança do Estado
- A defesa
- A segurança pública
- Infrações penais
- Independência judiciária
- Outros objetivos importantes do interesse público geral
- Missão de controlo ou inspeção
- Defesa da liberdade ou direitos de outrem

Encarregado de Proteção de Dados

(DPA - *Data Privacy Officer*)

Obrigações de designação para responsáveis de tratamentos e subcontratantes:

- Autoridades e organismos públicos (excepto tribunais);
- Entidades cujas atividades principais consistam em operações de tratamento que, devido à natureza/âmbito/finalidade impliquem uma monitorização regular e sistemática dos titulares dos dados em grande escala;
- Entidades cujas atividades principais consistam em operações de tratamento em grande escala de categorias especiais de dados ("dados sensíveis") e dados pessoais relacionados com contra-ordenações penais/infracções;

Encarregado de Proteção de Dados (DPO)

■ Posição do encarregado da proteção de dados:

- deve ser envolvido em todas as questões relacionadas com a proteção de dados pessoais;
- independente: não pode ser destituído nem penalizado pelo exercício das suas funções;
- ponto de contacto com os titulares dos dados.

Perfil:

- Perito em legislação sobre dados pessoais e tratamento de dados pessoais (jurista ou técnico IT ou DRH ou CRM)
- Trabalhador ou prestador de serviços
- Único ou “partilhado”

Encarregado de Proteção de Dados (DPO)

■ Funções:

- Informar/aconselhar o responsável pelo tratamento/subcontratante/ trabalhadores a respeito das suas obrigações legais
- Monitorizar o cumprimento da lei
- Dar formação
- Realizar auditorias
- Prestar aconselhamento no que respeita à avaliação de impacto sobre a proteção de dados
- Cooperar e servir de ponto de contacto com a autoridade de controlo – Comissão Nacional de Proteção de Dados (CNPD)

Responsável pelo Tratamento (*Controller*)

■ Algumas obrigações:

- Adotar medidas técnicas e organizativas para assegurar que o tratamento de dados é efetuado conforme o RGPD (artº 24º, nº1)
- Comprovar que está a adotar essas medidas (artº 24º, nº1)
- Definir políticas adequadas (artº 24º, nº2)
- Proceder ao registo das atividades de tratamento (artº 30º)
- Cooperar com as autoridades de controlo (artº 31º)
- Adotar medidas técnicas e organizativas para assegurar um nível de segurança adequado (artº 32º)
- Notificar a autoridade de controlo em caso justificável (artº 33º)
- Proceder à avaliação de impacto (artº 35º)
- Se possível, adotar códigos de conduta (artº 40º)

Subcontratante/Interlocutor (*Processor*)

– *artº 28º e seguintes*

■ Algumas obrigações:

- Tratar os dados pessoais mediante instruções do responsável pelo tratamento e segundo o direito da UE;
- Assegurar que as pessoas autorizadas a tratar os dados pessoais assumiram um compromisso de confidencialidade;
- Adotar todas as medidas exigidas nos termos do artº 32º do RGPD;
- A tomar em conta a natureza do tratamento e prestar assistência ao responsável pelo tratamento;
- A disponibilizar ao responsável pelo tratamento todas as informações necessárias para demonstrar o cumprimento das obrigações previstas, facilitando e contribuindo para as auditorias.

2.Reforço e criação de obrigações (empresas...)

■ Substituição da obrigação geral de notificação pelo reforço de vários deveres e pela criação de obrigações novas:

- i. Avaliação de impacto das operações de tratamento de dados;
- ii. Registo de atividades de tratamento de dados;
- iii. Implementação de medidas técnicas e organizativas que garantam a conformidade com a lei e a integridade e segurança dos dados (ex.: pseudonimização, tratamento por defeito);
- iv. Consulta prévia em casos específicos.

2.Reforço e criação de obrigações (empresas...)

■ OBRIGAÇÕES PARA AS EMPRESAS – AVALIAÇÃO DE IMPACTO

Notas sobre a avaliação de impacto das operações de tratamento de dados:

-Tratamento (ou conjunto de tratamentos com riscos semelhantes) que, pela sua natureza, âmbito, contexto e finalidades (particularmente no caso de utilização de novas tecnologias), for susceptível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento sobre a proteção de dados pessoais.

2.Reforço e criação de obrigações (empresas...)

■ OBRIGAÇÕES PARAS AS EMPRESAS –AVALIAÇÃO DE IMPACTO

Avaliação é obrigatória em caso de:

- a.Avaliação sistemática e completa dos aspectos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adoptadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar;
- b.Operações de tratamento em grande escala de categorias especiais de dados ou de dados pessoais relacionados com condenações penais e infrações;
- c.Controlo sistemático de zonas acessíveis ao público em grande escala.

2.Reforço e criação de obrigações (empresas...)

OBRIGAÇÕES PARA AS EMPRESAS –REGISTO DE ATIVIDADES

- Notas sobre o registo de actividades de tratamento:
 - O responsável pelo tratamento de dados deve conservar um registo de todas as actividades de tratamento de dados sob sua responsabilidade.
 - Os registos são efectuados por escrito, incluindo em formato electrónico;
 - O responsável pelo tratamento e, sendo caso disso, o subcontratante, o representante do responsável pelo tratamento ou do subcontratante, disponibilizam, a pedido, o registo à autoridade de controlo (CNPD);
 - Há casos em que é obrigatório.

2.Reforço e criação de obrigações (empresas...)

- Os registos são efectuados por escrito, incluindo em formato electrónico;
- O responsável pelo tratamento e, sendo caso disso, o subcontratante, o representante do responsável pelo tratamento ou do subcontratante, disponibilizam, a pedido, o registo à autoridade de controlo (CNPD);
- As obrigações de registo aplicam-se:
 - a. às empresas ou organizações com, pelo menos, 250 trabalhadores;
 - b. em qualquer caso, quando o tratamento efetuado seja susceptível de implicar um risco para os direitos e liberdades do titular dos dados, não seja ocasional ou abranja “dados sensíveis” ou dados relativos a condenações penais e infrações.

3.RGPD – Aplicação / não aplicação

O RGPD aplica-se:

- A todas as pessoas singulares, independentemente da sua nacionalidade, relativamente ao tratamento dos seus dados pessoais;
- A todas as pessoas vivas
- Ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da EU, independentemente de o tratamento ocorrer dentro ou fora da EU;
- Às atividades dos tribunais no que respeita ao tratamento de dados pessoais (desde que não estejam no exercício da atividade jurisdicional);
- Ao tratamento de dados pessoais pelas instituições, órgãos ou agências da EU;
- A qualquer tratamento de dados pessoais de titulares da EU, mesmo que o responsável ou subcontratante não esteja estabelecido na EU.

3.RGPD – Aplicação / não aplicação

O RGPD não se aplica:

- A questões de defesa dos direitos e liberdades fundamentais;
- À livre circulação de dados pessoais relacionados com atividades fora do âmbito de aplicação do direito da EU, nomeadamente segurança nacional;
- A atividades relacionadas com a política externa e de segurança comum (EU);
- Ao tratamento de dados pessoais efetuado por pessoas singulares no exercício de atividades pessoais ou domésticas;
- Ao tratamento de dados pessoais relativos a pessoas coletivas, nomeadamente denominação, forma jurídica e contactos;
- A atividades de tratamento para efeitos de proteção das pessoas singulares no que respeita à prevenção, investigação, deteção e repressão de infrações penais ou execução de sanções penais.

4. Impactos na gestão de recursos humanos

- O Regulamento prevê a possibilidade de os Estados-Membros adoptarem normas internas específicas, designadamente ao nível do tratamento de dados pessoais no contexto laboral.
- O tratamento de dados sensíveis no contexto laboral, monitorização e controlo de dados tem suscitado enorme discussão na doutrina e jurisprudência.
- Consentimento dos trabalhadores como fundamento válido para o tratamento de dados pessoais por parte das entidades empregadoras, consentimento, entendido como uma manifestação de vontade livre, específica e informada. Mas raramente os trabalhadores estão em condições de dar, recusar ou revogar consentimento livremente, tendo em vista a dependência que resulta da relação empregador / empregado.
- Porém, o consentimento não deverá constituir, por si só, fundamento jurídico válido para o tratamento de dados pessoais dos trabalhadores.

5. Responsabilidades e sanções

■Direito de reclamação perante autoridade de controlo:

-direito que assiste aos titulares de dados de apresentar uma reclamação perante uma Autoridade de Controlo – v.g. da residência, do local de trabalho ou da prática da infracção - quando considerem que o tratamento de dados pessoais que lhes diga respeito viola o RGPD

-este direito não prejudica o recurso por parte do titular de dados a outras vias de recurso gracioso ou judicial

-a Autoridade de Controlo informa o autor da reclamação sobre o andamento e o resultado da reclamação.

5. Responsabilidades e sanções

■Direito à ação judicial contra a autoridade do controlo:

-direito que assiste a todas as pessoas singulares ou colectivas de intentar acção judicial contra a autoridade de controlo que:

a) tenha proferido uma decisão juridicamente vinculativa e que lhes diga respeito;

b) não tenha tratado da reclamação ou não tenha informado o titular dos dados, no prazo de três meses, sobre o andamento ou o resultado da reclamação que tenha apresentado.

Este direito não prejudica o recurso a outras vias extrajudiciais por parte dos titulares do direito de ação.

5. Responsabilidades e sanções

- Direito à ação judicial contra o responsável pelo tratamento:

- direito que assiste aos titulares de dados de intentarem acção judicial contra o responsável pelo tratamento de dados pessoais ou o subcontratante, quando considerem ter havido violação dos seus direitos nos termos do Regulamento

- este direito não prejudica o recurso a outras vias extrajudiciais por parte dos titulares de dados.

5. Responsabilidades e sanções

■ Condições gerais para aplicação de coimas:

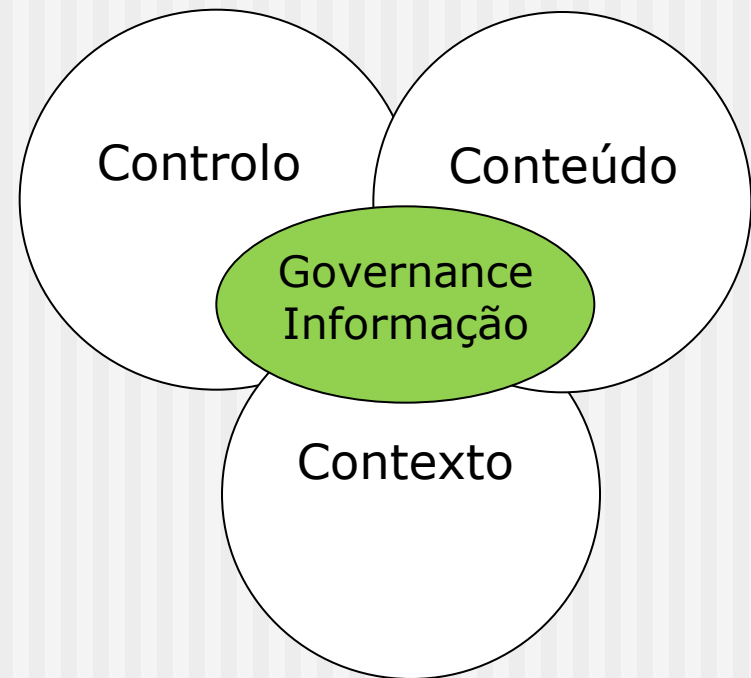
- se, no âmbito do mesmo tratamento de dados, forem violadas várias disposições do Regulamento, o montante total da coima não pode exceder o montante especificado para a violação mais grave;
- o Regulamento apenas prevê coimas para a violação de algumas das suas regras;
- a coima tem como limite (i) 10 000 000€ ou 20 000 000€, ou no caso de uma empresa, (ii) 2% ou 4% do volume de negócios anual a nível mundial correspondente ao exercício anterior, conforme o montante que for mais elevado;
- os Estados-Membros fixam as sanções aplicáveis às violações do Regulamento não sejam sujeitas a coima nos termos do Regulamento (v.g. crime –ver actualmente arts. 43º a 48º da Lei 67/98 de 26.10)

6. Plano de ação técnico e operacional



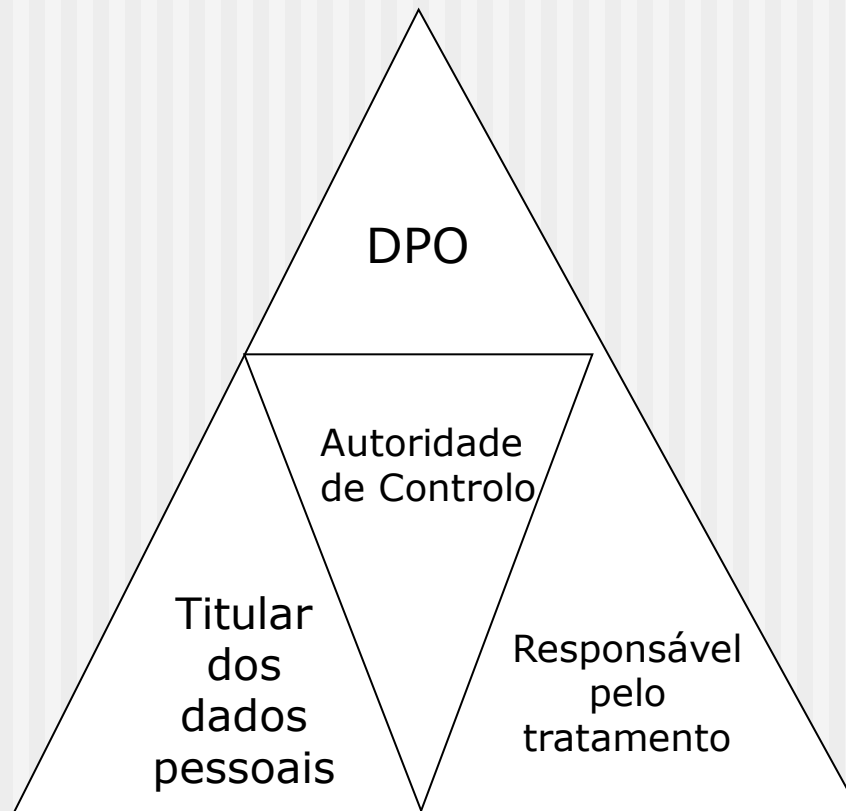
6. Plano de ação técnico e operacional

- Proteção de Dados
- Metadados
- Classificação
- Registos
- Preservação
- Auditoria
- Risco
- Segurança
- Ameaças
- Privacidade
- Conformidade
- Storage
- Cloud
- Mobile
- Imagens
- Redes Sociais



6. Plano de ação técnico e operacional

■ **COMO SE PREPARAR PARA ESTAR *COMPLIANCE***



6. Plano de ação técnico e operacional

■ **COMO SE PREPARAR PARA ESTAR *COMPLIANCE***

1. Informação e formação
2. Saber que dados pessoais existem na organização, origem, organização, finalidades
3. Fazer o *assessment* da tecnologia para a verificação de resposta às exigências do RGPD
4. Revisitar/melhorar políticas de privacidade e de segurança já existentes
5. Criação/melhoria de procedimentos internos face aos direitos dos titulares dos dados pessoais
6. Consentimentos dos titulares dos dados.
7. Rever/atualizar formulários usados até agora ou criar novos.

6. Plano de ação técnico e operacional (PATO)

■ **COMO SE PREPARAR PARA ESTAR *COMPLIANCE***

8. Verificar se a organização recolhe e trata dados sensíveis e dados de crianças
9. Verificar se a organização necessita de proceder ao registo de atividades de tratamento e atuar em conformidade
10. Ter atenção ao(s) contrato(s) com subcontratantes
11. Necessidade ou não de designar um DPO
12. Verificar se a organização adotou medidas técnicas e organizativas para garantir a segurança dos dados que possui, nomeadamente encriptação e mascaramento de dados
13. Necessidade ou não de avaliação de impacto
14. Adotar procedimentos para detetar, denunciar, reportar e investigar violações de dados.

6. Plano de ação técnico e operacional

Em síntese:

- Avaliação sumária/análise/ponto da situação: resumo das evidências analisadas e pontos de melhoria;
- Lista de não conformidades detetadas: lista de pontos que não estão em conformidade com o novo Regulamento identificados durante o processo de análise.
- Proposta de melhoria: análise com proposta de resolução tecnológica ou processual em linha com os requisitos do novo RGPD.

6. Plano de ação técnico e operacional

■ Implementação de regras organizacionais internas adequadas:

- formação aos funcionários sobre as regras relativas a segurança dos dados e as respetivas obrigações, especialmente em matéria de confidencialidade;
- proteção contra o acesso a instalações e a hardware e software do responsável pelo tratamento ou do subcontratante, incluindo controlos sobre a autorização de acesso;
- certificação de que as autorizações de acesso a dados pessoais foram concedidas pela pessoa competente e exigem documentação adequada;
- documentação exaustiva para outras formas de divulgação diferentes do acesso automatizado a dados, a fim de demonstrar que não ocorreram quaisquer missões ilegais de dados;
- realização de auditorias internas e externas.

RGPD:

entre a clareza/responsabilidade e a “monstruosidade”!



Vamos, todos,
colaborar para
esta missão!
Obrigado!
Vítor Martins