

Proteção e Privacidade de Dados

Compreender os riscos e aplicar boas práticas na proteção de dados pessoais e sensíveis

Bruno Marques
Outubro de 2026



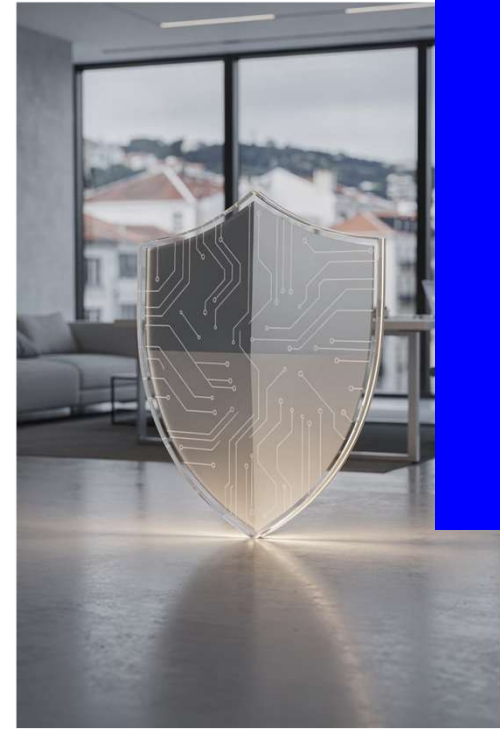
Agenda

1. Introdução
2. Fundamentos: dados pessoais e sensíveis
3. Visão do risco: Avaliação de Impacto (AIP) e sinergias
4. Casos especiais: dados de saúde e financeiros
5. *Framework* de trabalho e ética
6. Riscos emergentes: IA e privacidade
7. Análise de um caso
8. Conclusão e próximos passos

Quiz

Exercício

Análise de caso

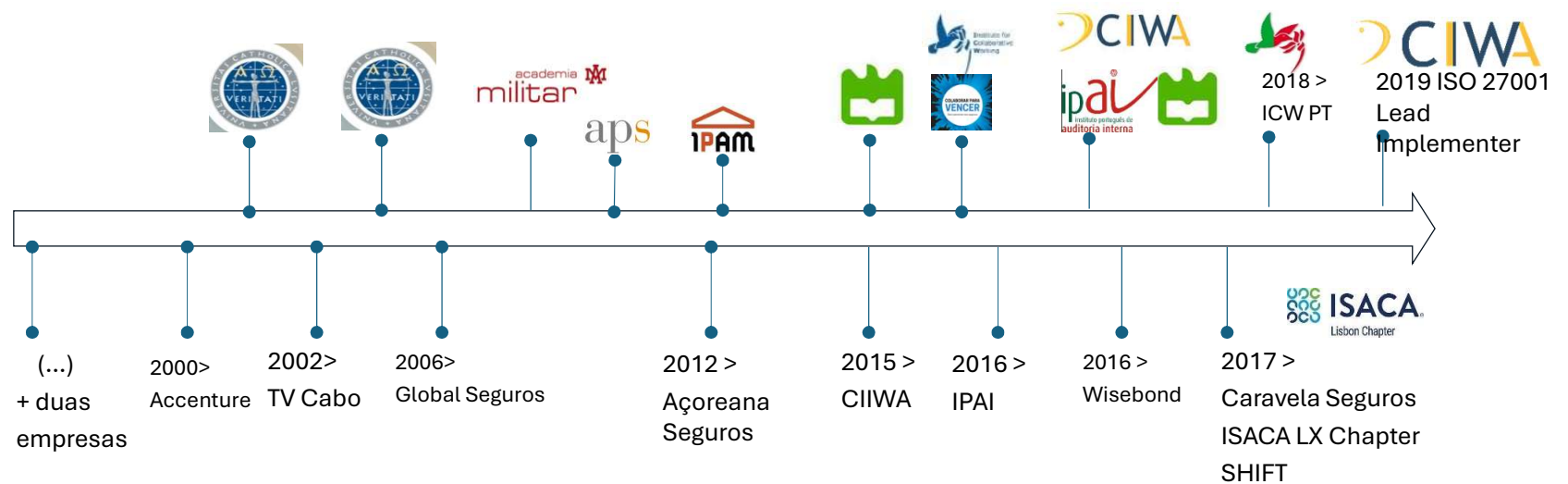


Apresentação



Bruno Marques

Business Consultant
IT Governance
IT Service management
IT Audit & Security



Apresentação | Expetativas



Powered by  **Poll Everywhere**

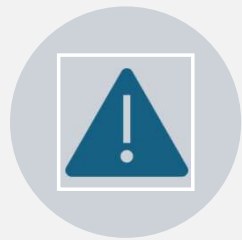
https://www.poll everywhere.com/free_text_polls/t8N0lhBt1Yat0wPPnouHA?preview=true&controls=none

Aceda a
pollev.com/ciiwa

Não é preciso registo – entrar
como **Guest** ou fazer **Skip**

Respostas anónimas

Objetivos gerais da sessão



Distinguir **dados pessoais, sensíveis e de risco elevado**



Aplicar a lógica da **AIPD** e sinergias com *Cyber*



Reconhecer riscos em **dados financeiros e de saúde**



Adotar **boas práticas e um sistema de gestão**

Um login, 100 mil registos: o que falhou?

>100 mil

utentes afetados em todo o país

1

credencial de um médico usada por terceiros

~48 h

entre o início do acesso e o primeiro alerta

4

reclamações de utentes deram o alerta

O QUE ACONTECEU

- Em maio de 2026, as credenciais de um médico de uma ULS foram usadas por terceiros para consultar dados de utentes do SNS, de forma automatizada.
- Quem deu o alerta foram os próprios utentes, notificados pelo SNS 24 de consultas que não reconheciam.
- Segundo a ULS e os SPMS, os dados acedidos eram administrativos, não clínicos.
- A PJ admite o uso de IA. A CNPD abriu uma averiguação. A investigação está em curso.

PARA DEBATE · 5 MINUTOS

- 1 Que danos pode sofrer um utente cujos dados foram consultados por um desconhecido?
- 2 Que obrigação do RGPD foi mais útil aqui: notificar a CNPD, informar os titulares ou demonstrar conformidade?
- 3 Segurança e privacidade: como se reforçam mutuamente neste caso?



1

Introdução

Confiança: o alicerce da economia digital

Clientes, parceiros e reguladores só partilham dados com quem demonstra que os protege. A confiança tornou-se um ativo estratégico — e passou a ser medida.

Privacidade

68%

dos europeus preocupam-se com a proteção dos seus dados pessoais online

Eurobarómetro PE · outono 2025

Segurança

80-90%

das intrusões iniciais analisadas na UE começam por phishing

ENISA | EC-Council | MSFT

IA responsável

>80%

da engenharia social observada no mundo já recorre a IA

ENISA · Threat Landscape 2025

Sem confiança não existe transformação digital



O que está em causa quando falamos do RGPD*?

The infographic is divided into two main sections. The left section features a cover of *The Economist* magazine from May 4th-12th 2017. The cover has a red header with the magazine's name, a list of articles including 'Theresa May v Brussels', 'Ten years on: banking after the crisis', 'South Korea's unfinished revolution', and 'Biology, but without the cells'. The main headline reads 'The world's most valuable resource' above an illustration of offshore oil rigs. Below the illustration, it says 'Data and the new rules of competition'. The right section is a blue iceberg floating in a light blue sky with clouds. The tip of the iceberg is labeled 'Confiança' (Trust) and contains the words 'Missão' (Mission) and 'Transparência' (Transparency). The submerged part of the iceberg is composed of several blue circles containing the following text: 'Dados pessoais' (Personal data), 'Histórico dos colaboradores' (Employee history), 'Contratos' (Contracts), 'Dossiê pessoais' (Personal file), 'Dossiê clínico' (Clinical file), 'Dados de menores' (Data of minors), and 'Arquivo' (Archive).

The Economist
May 4th-12th 2017

Theresa May v Brussels
Ten years on: banking after the crisis
South Korea's unfinished revolution
Biology, but without the cells

The world's most valuable resource

Data and the new rules of competition

Confiança
Missão Transparência

Dados pessoais
Histórico dos colaboradores
Contratos
Dossiê pessoais
Dossiê clínico
Dados de menores
Arquivo

 **RGPD – Um novo risco corporativo ou uma oportunidade?**

* Regulamento geral de proteção de dados

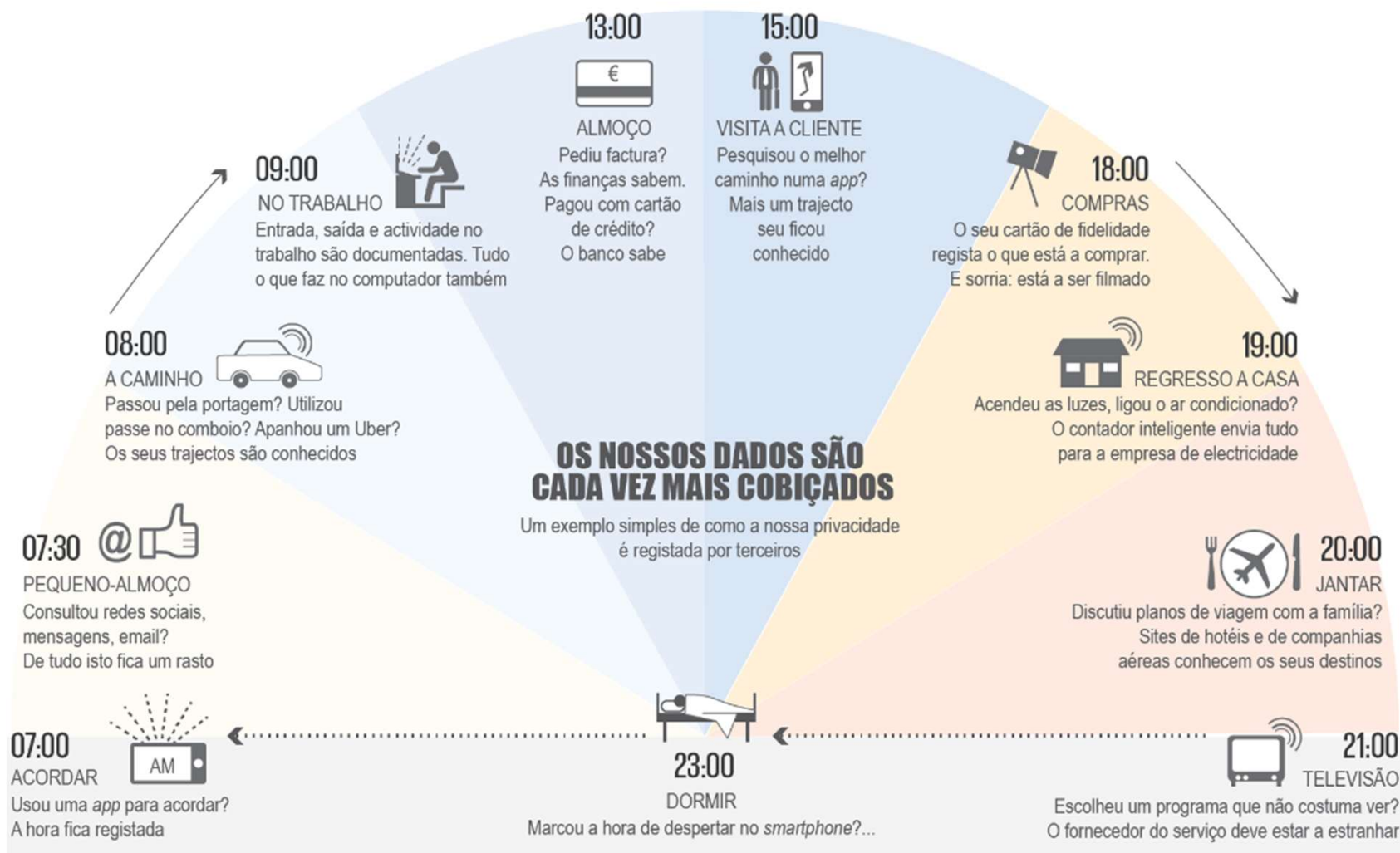
Motivação para o RGPD: o futuro é digital

A densidade digital continua a acelerar



Este slide (ainda) foi efetuado por um humano

Dados pessoais e a nossa pegada digital



Por que importa: a CNPD intensificou a supervisão em 2025

3.201

processos abertos

+12% face a 2024

472

violações de dados notificadas

+42% face a 2024

357

Notificações a entidades privacidades

76% do total

244

inspeções realizadas

o dobro de 2024 (122)



Causas mais frequentes declaradas à CNPD em 2025:

1. **Falha humana** — 128 casos (+28% face a 2024)
2. **Phishing e outra engenharia social** — 72 casos (+41%)
3. **Malware (49), ransomware (47) e ações fraudulentas (33)**

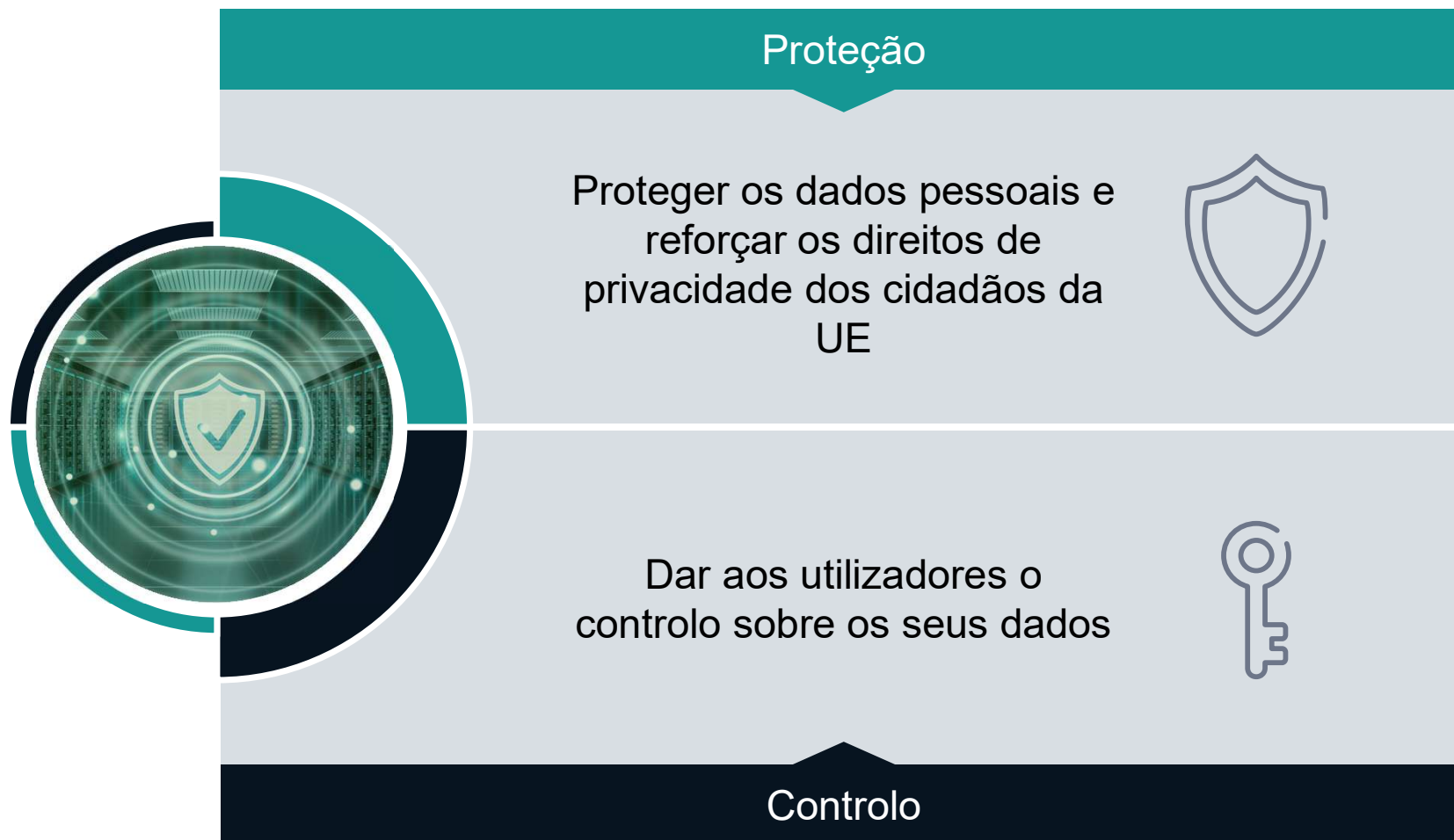


2

2.1 Fundamentos

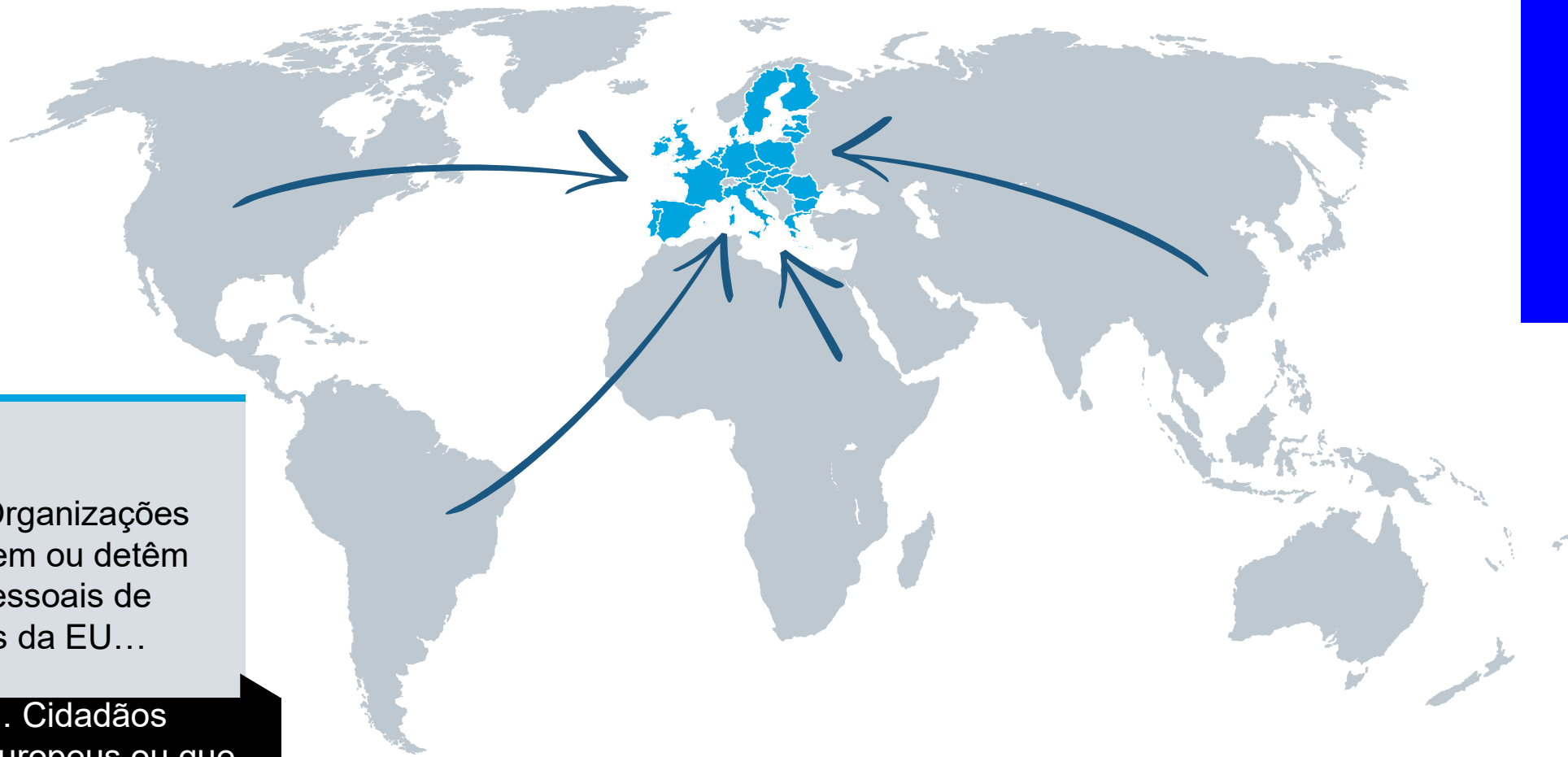
Conceitos fundamentais

Objetivos do regulamento



Conceitos fundamentais

Quem é afetado?



Todas as Organizações
que recolhem ou detêm
dados pessoais de
cidadãos da EU...

... Cidadãos
europeus ou que
residam no EEE

Conceitos fundamentais

Com o RGPD, a lógica é alterada para a auto-responsabilização 😊

Licitude e Limitação de finalidade

Os dados pessoais só podem ser tratados para fins determinados e legítimos.



Transparência e Lealdade

Dever de informar será um fator crítico de sucesso para uma relação de confiança



Integridade e confidencialidade

Os dados devem ser adequadamente protegidos contra o acesso de terceiros.



Minimização de dados

Apenas poderão ser recolhidos dados necessários e não dados supérfluos.



Limitação de armazenamento

Os dados só poderão ser armazenados durante o período em que forem necessários.



Orientação ao risco

Os registos de atividades devem ser sistematizados e avaliados em termos do risco

Requisitos centrais

Dados pessoais e categorias especiais de dados & risco especial exigem regime reforçado de proteção: menores; financeiros, localização etc.



Requisitos centrais

Direitos dos titulares de dados - exemplos



Direito de acesso

Visualizar e solicitar cópias dos seus dados pessoais para obter informações sobre a forma como os dados estão a ser utilizados.



Direito à portabilidade

Solicitar a transferência dos seus dados pessoais de uma entidade responsável para outra responsável pelo tratamento.



Direito ao apagamento

Os titulares dos dados têm o direito de solicitar a eliminação dos seus dados pessoais.

RGPD MULTAS

Se os seus dados
forem violados:

Deve denunciar
dentro de

72

horas

OU

Enfrentar uma multa até

20M € ou

4%

do volume global de negócio



*Privacy by
design*

Função
EPD*

Avaliação
do Risco

Oportunidade
e relação

*Encarregado de Proteção de Dados

Exemplos reais de fugas de dados em Portugal



Setor da Saúde

Acesso indevido a processos clínicos por colaboradores sem necessidade legítima. Dados de diagnóstico e medicação expostos internamente.



Phishing

Colaborador clicou em link malicioso. Base de dados de clientes com nomes, moradas e NIFs exportada para servidor externo.



Lapso de utilização email

Envio de email por lapso enviou lista de candidatos a cargo dirigente e respetivos documentos de análise — incluindo dados de RH — para todos os candidatos, expondo publicamente todos os seus dados pessoais

Quiz · Dados pessoais e sensíveis

P1

Um ficheiro com n.º de colaborador, departamento e avaliação, com nome “mascarado”, mas recuperável é:

a) Dado anónimo, fora do RGPD

b) Dado pessoal pseudonimizado, sujeito ao RGPD

c) Categoria especial (art. 9.º)

P2

Qual destas é uma categoria especial de dados?

a) Baixa médica com diagnóstico

b) IBAN do colaborador

c) Morada e telefone pessoal

P3

Para tratar dados de saúde, a organização precisa de:

a) Apenas consentimento do titular

b) Apenas medidas de segurança reforçadas

c) Consentimento e medidas de segurança reforçadas

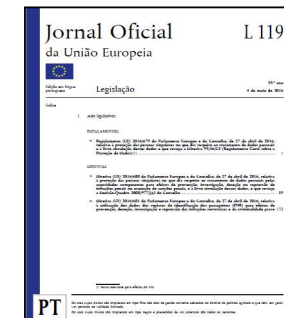


2

2.2 Medidas técnicas e organizativas

Os 7 Princípios do RGPD (Art. 5.º)

Ancorados nos FIPP da OCDE



1 Art. 5.º/1/a)	2 Art. 5.º/1/b)	3 Art. 5.º/1/c)	4 Art. 5.º/1/d)
Licitude, Lealdade e Transparência Dever de informar	Limitação das Finalidades	Minimização dos Dados	Exatidão
5 Art. 5.º/1/e)	6 Art. 5.º/1/f)	7 Art. 5.º/2	
Limitação da Conservação	Integridade e Confidencialidade	Responsabilidade (Accountability)	

Bases Legais para Tratamento (Art. 6.º RGPD)

a)

Consentimento do titular

Livre, específico, informado e inequívoco
(inc. nos casos de menores)

b)

Execução de contrato

Partes no contrato ou pré-contrato

c)

Obrigação legal

Base jurídica do Estado ou UE — mais comum
no setor público

d)

Interesses vitais

Proteção da vida do titular ou de terceiro

e)

Interesse público ou autoridade pública

Atribuições e missão de organismos públicos

f)

Interesse legítimo

Nunca ultrapassando os direitos e liberdades
dos titulares de dados

Primeiro o risco para as pessoas, depois o da organização

Riscos para os titulares

- Discriminação e exclusão
- Usurpação de identidade e fraude
- Perdas financeiras
- Danos reputacionais e psicológicos
- Perda de confidencialidade de dados sob sigilo
- Perda de controlo sobre os próprios dados

Riscos para a organização

Legal: coimas (art. 83.º) e indemnizações (art. 82.º)

Operacional: limitação ou suspensão do tratamento (art. 58.º)

Financeiro: custos de resposta, notificação e remediação

Reputacional: perda de confiança de clientes, cidadãos e colaboradores

Atenção: proteção de dados não se reduz a cibersegurança — um tratamento seguro pode ser ilícito

Quiz · Princípios FIPP (*fair principles*) e o RGPD

P1

Há uma política de privacidade aprovada, mas ninguém consegue provar que é aplicada. Falha o princípio da:

- a) Transparência
- b) Responsabilidade (accountability)
- c) Minimização de dados

P2

O processamento mensal do salário de um colaborador tem como fundamento principal:

- a) Consentimento do colaborador
- b) Interesse legítimo
- c) Execução de um contrato

P3

Qual destes temas é um risco para o titular, e não para a organização?

- a) Discriminação na negação de acesso a um serviço
- b) Coima aplicada pela CNPD
- c) Perda de Clientes



3

Visão do risco da privacidade (AIP)

A AIP* decide se o risco é aceitável

Quando é obrigatória: três fontes a verificar

1 · RGPD, art. 35.º, n.º 3

- Avaliação sistemática e automatizada, incluindo perfis, com efeitos jurídicos ou similares
- Grande escala de categorias especiais ou de condenações
- Controlo sistemático de zonas públicas em grande escala

2 · WP248 rev.01 — 9 critérios

- 1 Avaliação ou pontuação
- 2 Decisão automatizada
- 3 Controlo sistemático
- 4 Dados sensíveis ou muito pessoais
- 5 Grande escala
- 6 Combinação de dados
- 7 Titulares vulneráveis
- 8 Tecnologia inovadora
- 9 Impede exercício de direito

≥ 2 critérios → em regra, AIP

3 · Lista da CNPD

Regulamento n.º 1/2018 (lista nacional, art. 35.º, n.º 4).

Exemplos:

- Biométricos para identificação inequívoca
- Genéticos de pessoas vulneráveis
- Dados de dispositivos que transmitem por redes

Consultar a lista completa

Visão do risco de privacidade

Seis passos, do desenho à decisão documentada



Avaliar o risco exige escala e critérios explícitos

Impacto ↓					
		Máximo	Significativo	Limitado	Negligenciável
	Máximo	Médio	Elevado	Elevado	Elevado
	Significativo	Médio	Elevado	Elevado	Elevado
	Limitado	Baixo	Médio	Elevado	Elevado
	Negligenciável	Baixo	Baixo	Médio	Médio
		Negligenc.	Limitada	Signific.	Máxima
		Probabilidade →			

Gravidade ou Impacto no titular

Negligenciável: incómodo ultrapassável

Significativa: consequências sérias, ultrapassáveis com dificuldade

Máxima: consequências irreversíveis

Risco inerente vs. risco residual

Inerente: antes das medidas.

Residual: depois das medidas, com evidência de que estão implementadas.

Aceitar risco não dispensa uma obrigação legal.

Mitigar: medidas jurídicas, técnicas, humanas e de governo

Jurídicas e organizativas	Técnicas	Humanas	Governo
• Base legal e finalidade documentadas • Avisos de privacidade (arts. 13.º–14.º) • Contratos com subcontratados (28.º) • Prazos de conservação e eliminação	• Minimização e privacidade por defeito • Pseudonimização e cifragem • Controlo de acessos e MFA • Registos (logs) e alertas	• Formação específica por função • Instruções a quem trata dados (art. 29.º) • Compromissos de sigilo • Canal de reporte de incidentes	• Parecer do EPD • Análise dos RAT: Registos de atividade de tratamento • Revisão periódica da AIP • Indicadores de eficácia • Responsável e prazo por medida Sistema de gestão de privacidade de dados

Regra de ouro: uma medida de segurança não substitui um fundamento de licitude.

Exercício: AIP — sim ou não? Quais os critérios?

A

Hospital

Trata dados genéticos e de saúde de todos os doentes num novo sistema clínico.

B

Revista online

Envia a newsletter diária aos subscritores a partir de uma lista de emails.

C

Município

Instala leitura automática de matrículas para restringir carros antigos no centro.

D

Banco

Usa um modelo de IA para decidir automaticamente pedidos de crédito.

Quiz - Avaliação de Impacto

P1

Tipicamente, uma AIP deve ser realizada:

- a) Após a entrada em produção
- b) Apenas se a CNPD a pedir
- c) Antes do início do tratamento

P2

Após a AIP, quem decide sobre o tratamento?

- a) O responsável pelo tratamento, ouvido o EPD
- b) O EPD, que aprova a AIP
- c) O fornecedor da solução

P3

O que podem ser controlos para mitigar o risco potencial?

- a) Autenticação forte 2FA e controlo de acessos *need to know*
- b) Aviso de privacidade eficaz no momento da recolha dos dados
- c) Opção a) e b) estão corretas



4

Casos especiais: dados de saúde e financeiros

Dados financeiros: fora do art. 9.º, mas alvo de fraude

1 Dados do cartão

PAN (número), titular, validade

2 Dados sensíveis de autenticação

CVV2, PIN, banda/chip — não armazenar após autorização

3 Dados bancários

IBAN, comprovativos, mandatos de débito

4 Fiscais e rendimentos

NIF, recibos de vencimento, declarações de IRS

5 Crédito e scoring

Histórico de crédito, incidentes, avaliações de risco

6 Transações

Padrões de consumo que podem revelar saúde, religião ou rotinas

Enquadramento: «dados de natureza altamente pessoal» (WP248) — elevam o risco e a exigência de controlos.

Riscos e fraudes: o elo mais fraco é muitas vezes humano

Phishing, smishing, vishing, quishing	Mensagens e chamadas que imitam banco, fornecedor ou chefia
Fraude de alteração de IBAN	Email de «fornecedor» com novos dados bancários
Fraude do CEO / BEC	Pedido urgente de transferência, fora do processo
Roubo de conta e SIM swap	Credenciais ou número de telefone capturados
E-skimming	Código malicioso na página de pagamento online
Acesso indevido interno	Consulta ou exportação sem necessidade funcional

72

violações notificadas à CNPD em 2025 com origem em phishing ou engenharia social (+41%)

Exemplo · El Corte Inglés, Mar.2025

A empresa informou os clientes de um acesso não autorizado a dados pessoais num fornecedor externo. Dados de identificação e contacto e números do cartão de compras El Corte Inglés. Risco: **phishing credível**

Menos dados guardados, mais verificação nos pagamentos

Obrigações e referenciais

RGPD — minimização, integridade e confidencialidade (art. 5.º); segurança adequada ao risco (art. 32.º)

PCI DSS v4.0.1 — exigência contratual a quem trata dados de cartão: não guardar CVV/PIN, mascarar o PAN

DORA — resiliência digital das entidades financeiras (desde 17.01.2025)

Boas práticas recomendadas

- Nunca pedir ou enviar dados de cartão por email ou telefone
- Confirmar alterações de IBAN por canal independente
- Dupla validação e segregação de funções em pagamentos
- Simulações de phishing *baseline* + estratificadas e em linha com áreas de maior risco
 - Eg: AT, Alteação de IBAN para salários, etc.
- Usar prestador de pagamentos certificado e tokenização

Dados de saúde: sigilo e necessidade de conhecer

O que são	Com que fundamento	Em Portugal
Dados sobre saúde física ou mental, incluindo prestação de cuidados, que revelem o estado de saúde (art. 4.º, n.º 15). <i>Ex.: diagnósticos, baixas médicas, aptidão, consultas, medicação, dados de wearables.</i>	• Proibição geral (art. 9.º, n.º 1) • Exceções típicas: medicina e gestão de cuidados (al. h); saúde pública (al. i); obrigações laborais (al. b) • Tratamento por profissional sujeito a sigilo (art. 9.º, n.º 3)	• Lei 58/2019, art. 29.º: sigilo, necessidade de conhecer e segurança adequada • Código do Trabalho, art. 17.º: o médico só comunica ao empregador se o trabalhador está apto • Espaço Europeu de Dados de Saúde — Reg. (UE) 2025/327, aplicação faseada

Na organização: RH e chefias não precisam de diagnósticos — baixas e medicina do trabalho circulam por canais restritos.

Seis controlos para a confidencialidade dos dados de saúde

1 Acesso por função

Perfis por papel clínico ou administrativo; nada por defeito

2 Ciclo de vida das contas / utilizadores

Entradas, mudanças e saídas ligadas aos RH; revisão periódica

3 Rastreabilidade

Registo de quem acedeu, a quê e quando; alertas de anomalias

4 DLP – *Data loss prevention*

Classificação de informação e atuação proativa – humana e tecnológica para prevenir *fugas ou lapsos*

5 Cifragem e segregação

Em repouso e em trânsito; sem dados reais em testes

6 AIP e envolvimento do EPD

Obrigatória em grande escala (art. 35.º, n.º 3, al. b) – e casos já citados (lista negra)

Riscos comuns: a maioria nasce dentro da organização

22

violações notificadas à CNPD em 2025 por entidades públicas do setor da saúde

Fonte: CNPD, Relatório de Atividades 2025, p. 34

Acesso por curiosidade

Consulta de processos de familiares, colegas ou figuras públicas (VIP)

Envio para o destinatário errado

Resultados, relatórios ou listas de doentes por email (vs. *Data Loss Prevention*)

Contas em não conformidade

Ex-colaboradores e prestadores com acessos ativos

Ransomware

Indisponibilidade de sistemas clínicos e exfiltração

Dados de saúde dos colaboradores

Baixas e aptidão acessíveis a RH ou chefias

Apps e dispositivos

Partilha de dados de saúde com terceiros sem controlo

Hospital do Barreiro: centenas de perfis «médico» a mais

Contexto	Inspeção da CNPD em julho de 2018, após participação da Ordem dos Médicos.
Factos	Cerca de 985 utilizadores com perfil «médico» para 296 médicos em funções; outros profissionais com acesso a processos clínicos.
Decisão	Três coimas da CNPD (150 + 150 + 100 mil €), por falhas de minimização, confidencialidade e segurança.
Depois	Coima única de 380 mil €; em 2020 a CNPD aceitou a dispensa (entidade pública), mantendo a valoração da conduta.

Intervenientes

- Centro hospitalar (responsável)
- SPMS — fornecedor do sistema
- Profissionais e doentes
- CNPD e Ordem dos Médicos

Dilema: o hospital alegou que os perfis eram definidos por terceiros. Quem responde?

Mini-caso 1 · Barreiro: Top 3 falhas

Identifiquem as três falhas mais graves e o requisito ou critério que cada uma viola.

1 Falha Requisito / critério: 	2 Falha Requisito / critério: 	3 Falha Requisito / critério:
---	---	---

Pistas: necessidade de conhecer · ciclo de vida das contas · minimização · demonstração de conformidade · fornecedor

Quiz | Dados de saúde

P1

Dados de saúde incluem:

a) Apenas diagnósticos médicos

b) Apenas dados tratados por hospitais

c) Qualquer informação que revele o estado de saúde

P2

Após o exame de medicina do trabalho, a chefia deve receber:

a) O relatório clínico completo

b) Apenas a indicação de apto ou inapto

c) O diagnóstico, se o colaborador consentir

P3

Contra o acesso por «curiosidade», a medida mais eficaz é:

a) Acesso por necessidade de conhecer + revisão dos registos

b) Um aviso no ecrã de login

c) Cifrar a base de dados

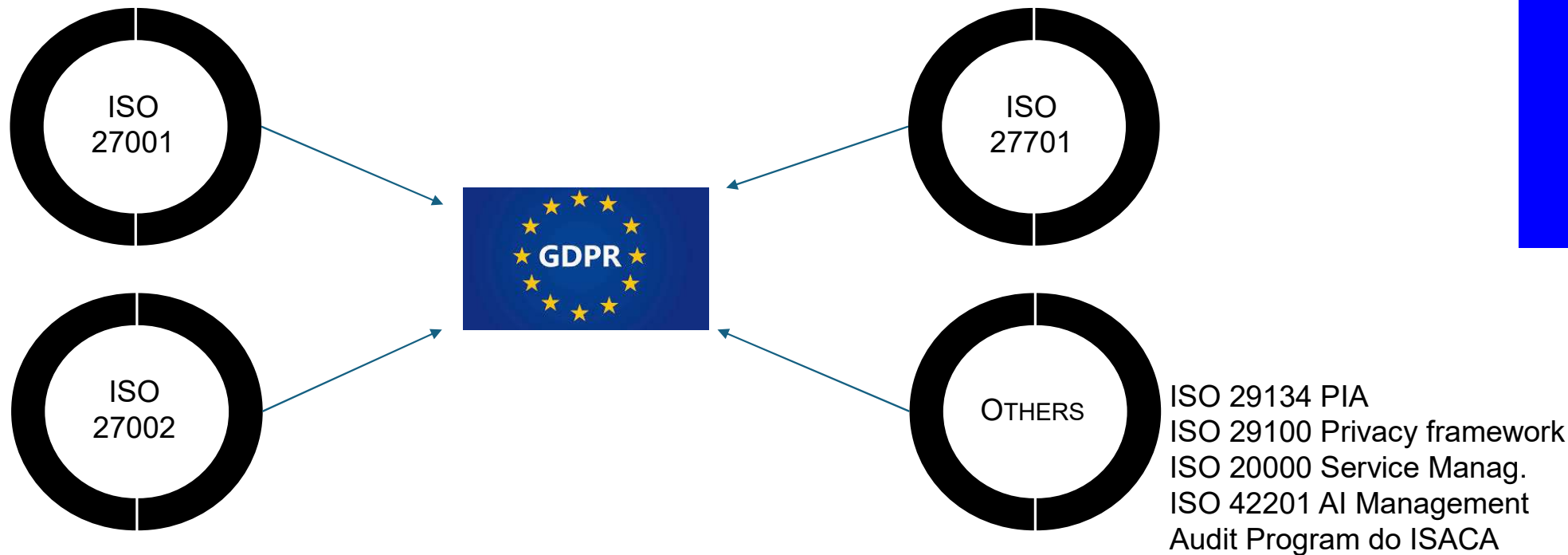


5

***Framework* de trabalho:
boas práticas e ética**

Operar um *framework* de trabalho multidisciplinar

Quadro de boas práticas aplicáveis



O sistema de gestão de privacidade e proteção de dados

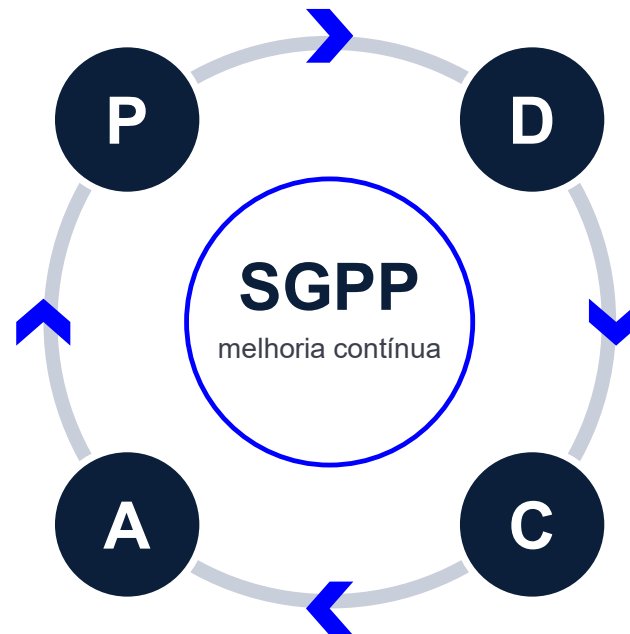
A privacidade gere-se com vários instrumentos, numa lógica de melhoria contínua

Planear O que tratamos e com que risco?

- Contexto e partes interessadas
- Inventário de dados e RAT
- Gap analysis e maturidade
- Avaliação do risco e AIP

Agir O que corrigimos e melhoramos?

- Ações corretivas
- Lições de incidentes
- Atualizar RAT e AIPD
- Melhoria contínua



Executar Como transformamos em rotina?

- Políticas e avisos de privacidade
- Direitos dos titulares
- Segurança para a privacidade
- Subcontratantes e formação

Verificar Funciona? Como sabemos?

- Indicadores (KPI/KRI)
- Auditoria interna
- Monitorização pelo EPD
- Revisão pela gestão

Planejar: governo, inventário e risco antes de tudo

	Item de verificação	Evidência esperada	Fundamento
PLANEAR			
☐	Modelo de governo e papéis definidos (RACI)	Deliberação, nomeação do EPD e notificação à CNPD	Arts. 24.º, 37.º–39.º
☐	Inventário de dados e RAT completos	RAT com responsável e data de revisão	Art. 30.º
☐	Finalidades e bases de licitude validadas	RAT; avaliação de interesse legítimo, se aplicável	Arts. 5.º, 6.º e 9.º
☐	Risco avaliado e AIP nos casos exigidos	AIP com parecer do EPD e decisão do RT	Arts. 35.º–36.º
☐	Gap analysis e plano de ação priorizado	Relatório de maturidade; plano com donos e prazos	Art. 24.º; boa prática

Executar: transformar requisitos em rotina com evidência

	Item de verificação	Evidência esperada	Fundamento
EXECUTAR			
☐	Avisos de privacidade coerentes com o RAT	Inventário de avisos; versões publicadas	Arts. 12.º–14.º
☐	Procedimento de direitos dos titulares	Registo de pedidos; respostas no prazo de 1 mês	Arts. 12.º, 15.º–22.º
☐	Segurança para a privacidade	Matriz de controlos; revisões de acessos	Arts. 25.º e 32.º
☐	Subcontratantes avaliados e contratados	Due diligence; contratos do art. 28.º	Arts. 28.º e 44.º ss.
☐	Gestão de violações testada	Registo de violações; simulação anual	Arts. 33.º–34.º
☐	Formação e sensibilização	Taxa de conclusão; simulações de phishing	Art. 39.º, n.º 1, al. b)

Verificar e agir: medir, auditar e melhorar

	Item de verificação	Evidência esperada	Fundamento
VERIFICAR			
☐	Indicadores definidos e reportados	Dashboard trimestral à gestão	Art. 32.º, n.º 1, al. d)
☐	Auditoria interna e monitorização do EPD	Plano e relatórios de auditoria	Art. 39.º, n.º 1, al. b)
☐	Revisão pela gestão	Ata com decisões e recursos	ISO/IEC 27701:2025
AGIR			
☐	Ações corretivas seguidas até ao fecho	Registo de não conformidades e evidência de fecho	Art. 24.º, n.º 1
☐	Lições de incidentes e AIP incorporadas	RAT, AIP e políticas atualizados	Art. 35.º, n.º 11
Indicadores sugeridos: % RAT revisto em 12 meses · % pedidos no prazo · tempo deteção→notificação · % colaboradores formados · % subcontratados críticos avaliados			

Quiz · Ética, boas práticas e sistema de gestão

P1

O EPD deve:

- a) Aprovar tratamentos e aceitar o risco
- b) Aconselhar e monitorizar, com independência
- c) Gerir a segurança informática

P2

Enviou por engano um ficheiro com dados de clientes. Deve:

- a) Pedir ao destinatário que apague e não dizer nada
- b) Esperar para ver se há impacto
- c) Reportar de imediato pelo canal interno

P3

No ciclo PDCA, a fase «Verificar» inclui:

- a) Auditoria, indicadores e revisão pela gestão
- b) Elaborar o RAT
- c) Assinar contratos com subcontratados

Ética: o que é legal nem sempre é aceitável

1

Dignidade

Pessoas, não registos

2

Justiça

Sem discriminação nem exclusão

3

Transparência

Explicar o que se faz e porquê

4

Proporcionalidade

Possível ≠ necessário

5

Responsabilidade

Assumir e demonstrar

Exemplo - Reidentificação (EUA, anos 1990)

O Group Insurance Commission (GIC), entidade que gere os seguros de saúde dos funcionários públicos do estado de Massachusetts, disponibilizou a investigadores dados hospitalares de cerca de 135 mil funcionários e familiares. Manteve diagnósticos, medicação e procedimentos, e também três campos aparentemente inofensivos: código postal, data de nascimento e sexo. O governador William Weld garantiu publicamente que os doentes estavam protegidos.

Conclusão: Com **código postal, data de nascimento e sexo, cruzados com os cadernos eleitorais**, uma investigadora do MIT identificou o registo clínico «anónimo» do governador do Massachusetts.

Juntos, estes três dados identificam cerca de 87% dos norte-americanos.

Comportamentos de risco e o que fazer em vez disso

Comportamento de risco

Prática esperada

Enviar listas com todos os destinatários em «Cc»

→

Usar «Bcc» ou plataforma; verificar antes de enviar

Exportar dados para Excel, USB ou cloud pessoal

→

Usar repositórios aprovados; *levar* só o necessário

Consultar dados «por curiosidade»

→

Aceder apenas com necessidade funcional

Partilhar credenciais ou deixar o ecrã desbloqueado

→

Credenciais pessoais, MFA, bloquear sempre (lembrar NIS2 e DORA)

Colar dados pessoais em ferramentas de IA públicas

→

Usar só ferramentas aprovadas; anonimizar

Clicar em links ou anexos inesperados

→

Reportar a mensagem como suspeita

Esconder um erro ou incidente

→

Reportar de imediato ao canal interno



6

Riscos emergentes: IA e a privacidade

Inteligência Artificial e Privacidade

O EU AI Act entrou em vigor.

Usar ferramentas de IA no trabalho sem critério pode constituir uma violação do RGPD.



DATA DROP #1: O Paradoxo da Experimentação

"Para cada **10** profissionais que experimentaram IA, apenas **2** trabalham em organizações preparadas para a gerir"

97,1% experimentaram ferramentas de IA

Apenas **22,9%** têm políticas organizacionais formalizadas

Lacuna crítica: 74,2 pontos percentuais



Esta disparidade não é apenas uma estatística - é um retrato de um mercado... em transição

Reality check: como vai ser o futuro?

O reverso da medalha da AI: quais os riscos que as empresas já ponderam?

The business case for investing in AI

75% of knowledge workers already using AI at work (doubled in the past 6 months)¹

30 min saved a day, equating to 10 hours per month by Copilot users²

65% of organizations using and deriving business value from gen-AI in 2024³

\$3.5 return on investment for every \$1 invested into AI⁴

1. [Work Trends Index](#)
2. [Work Trends Index](#)
3. [McKinsey](#)
4. [IDC](#)

Data security **41%**

Data governance **41%**

Privacy **39%**

Compliance with regulations **39%**

Threat actors using AI or breaching/hacking into AI **31%**



Níveis de Segurança e Privacidade na Utilização de IA

Compreender os diferentes níveis de segurança disponíveis permite às organizações tomar decisões informadas que equilibram funcionalidade, custo e proteção de informação sensível.

Quanto mais sensíveis os dados, mais controlo é preciso — e mais responsabilidade se assume.

NÍVEL 1

Versões gratuitas

Sem garantias contratuais; os dados podem ser usados para treino, consoante os termos.

DADOS ADMITIDOS

Nenhum dado pessoal ou confidencial

NÍVEL 2

Versões Pro / Business

Termos profissionais, opção de não treino, políticas de retenção e separação de ambientes.

DADOS ADMITIDOS

Dados internos não sensíveis, se a ferramenta for aprovada

NÍVEL 3

Empresariais avançadas

Cifragem, registos de auditoria, gestão de identidades, certificações e contrato do art. 28.º.

DADOS ADMITIDOS

Dados pessoais, com AIP e avaliação de transferências

NÍVEL 4

Versões on-premise

Instalação local ou nuvem privada. Controlo total de dados e modelos — e responsabilidade total pela segurança.

DADOS ADMITIDOS

Dados sensíveis, com AIP e equipa capaz de operar

Visão do risco de Privacidade na IA

Contexto de utilização de ferramentas *free*

✓ Risco reduzido

- Redigir textos genéricos sem dados pessoais
- Resumir documentos internos não sensíveis
- Apoio à criatividade e brainstorming



⚠ Com Cautela

- Traduzir ou rever contratos com dados da Organização **(ex: fuga de dados)**
- Analisar ficheiros com informação colaboradores
- Colocar Docs. Corporativos em ferramentas de IA **(ex. sanitizados)**



⊘ Risco Extremo

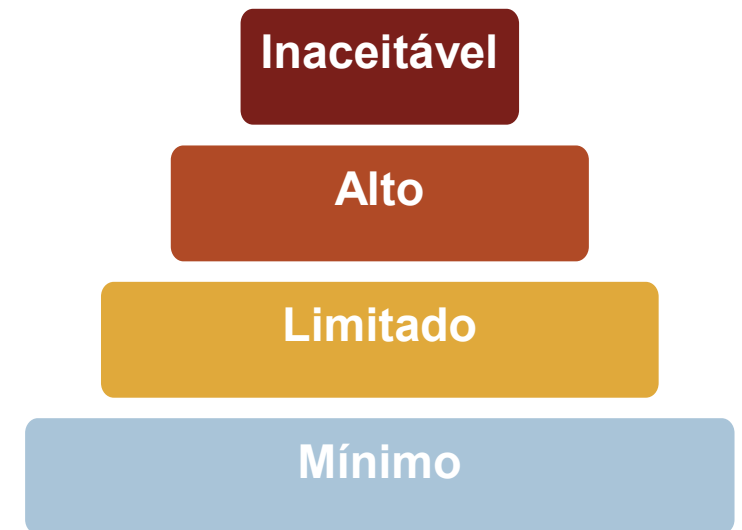
- Inserir dados pessoais ou sensíveis de titulares
- Partilhar informação confidencial ou classificada
- Usar IA para decisões automatizadas sem revisão humana

IA GRC

EU AI ACT

Controlos por nível de risco

O que auditar, que evidência pedir e onde estão os casos de uso típicos



IA GRC

ABORDAGEM BASEADO NO RISCO

Quatro níveis de risco, controlos proporcionais

NÍVEL	O QUE A LEI EXIGE	EXEMPLOS
Inaceitável	Proibido art. 5.º · em vigor	Classificação social de clientes; reconhecimento de emoções de colaboradores; manipulação de clientes vulneráveis
Alto risco	Requisitos completos + conformidade arts. 6.º a 27.º · a partir de 02 dez 2027	Scoring de crédito a particulares; pricing de seguros de vida e saúde; triagem de candidatos
Limitado	Transparência art. 50.º · em vigor	Assistente virtual de apoio ao cliente; conteúdos de comunicação gerados por IA
Mínimo	Sem requisitos específicos arts. 4.º e 95.º · literacia, códigos voluntários	Deteção de fraude; previsão de liquidez; classificação de documentos e e-mails

Transversal — modelos de IA de finalidade geral (GPAI): obrigações do fornecedor do modelo desde 02 ago 2025. O nível de risco pertence ao **caso de uso**, não à tecnologia.



7

Análise de caso

CASO FICTÍCIO

Vértice Seguros: como estão a ser geridos dados pessoais?



Contexto

Seguradora com 450 mil clientes. O call center, subcontratado, tem 60 operadores em dois turnos e pode alterar dados de clientes no sistema de apólices.

Factos

A 3 de março, a morada de um cliente foi alterada para uma zona de elevado risco sísmico. Na renovação automática de abril, o prémio passou de 380 € para 1 140 € e a cobertura sísmica ficou com franquias agravadas.

Reclamação

O cliente nega ter pedido a alteração. Pede ao EPD que identifique quem a fez, quando e porquê, e anuncia que vai apresentar queixa à CNPD.

Investigação

O registo mostra apenas «callcenter01»: uma conta genérica, com a palavra-passe «password123», partilhada por todos os operadores. Não há gravação da chamada associada. Os operadores também acedem a alguns dados clínicos – associados ao Seguro de Saúde

EM NÚMEROS

60 operadores
1 conta e 1 palavra-passe
0 forma de saber quem foi
46 dias até o cliente reclamar

Agravante: todos os colaboradores usam a mesma palavra-passe genérica para aceder aos diretórios partilhados, com apólices, peritagens e relatórios clínicos de sinistros.

CASO FICTÍCIO

Vértice: quatro decisões para as próximas 72 horas

1 Violação e notificação

Isto é uma violação de dados pessoais? Notifica-se a CNPD? Em que prazo e a contar de quando?

2 Direitos do cliente

O que tem de ser corrigido já? O que pode e deve ser respondido ao pedido de identificação do colaborador?

3 Top 5 falhas

Quais as três falhas mais graves e que requisito do RGPD viola cada uma? **(ver próximo slide)**

4 Recomendações

Que medidas, com dono e prazo, impedem que volte a acontecer? Qual o papel do EPD?

CASO FICTÍCIO

Caso Vértice: Top 5 falhas



1	Falha n.º	Requisito
2	Falha n.º	Requisito
3	Falha n.º	Requisito
4	Falha n.º	Requisito
5	Falha n.º	Requisito

LISTA DE FALHAS POSSÍVEIS

- 1 Ausência de testes de segurança (pen testing)
- 2 Sem gestão de utilizadores com contas nominativas
- 3 Palavra-passe partilhada, sem regras de utilização aceitável
- 4 Acessos sem o princípio da necessidade de conhecer
- 5 Alteração de dados pessoais sem dupla validação
- 6 Rede e recursos sem segmentação
- 7 Sem registos (logs) que atribuam cada alteração a alguém
- 8 Sem DLP para controlar fugas de dados
- 9 Sem procedimento de resposta a incidentes

CASO FICTÍCIO

Caso Vértice: solução final



Princípios do RGPD

Que princípios foram violados?

1

2

Medidas técnicas

O que teria evitado ou provado a alteração?

1

2

Outras recomendações

Organizativas, humanas e de governo

1

2



8

Conclusão

5 ideias-chave

1 Licitude primeiro

Base legal, finalidade e minimização. Os dados sensíveis exigem mais.

2 AIP é decisão chave

Visão do risco e dos controlos adequados. Com *governance*: dono, prazo e evidência.

3 Saúde e finanças são alvo

Alto valor para os atacantes, alto impacto para as pessoas.

4 Credenciais e erro humano abrem a porta

Detetar e reportar cedo conta: a contagem das 72 h já começou & sinergias com *cyber*

5 A privacidade gere-se como sistema

Planear, executar, verificar, agir. Accountability é conseguir demonstrar, não apenas declarar.

Obrigado!