



FORMAÇÃO
PROFISSIONAL DE
PRIVACIDADE
DE DADOS (LGPD)

Realização



Apoiadores



Apresentação do Instrutor



<https://profmatheus.com>

@profmatheuspassos

Prof. Matheus Passos Silva

IAPP® CIPP/E, CIPM | EXIN® Certified DPO

EXIN® Certified Blockchain Foundation | Inteligência Artificial

- **Data Protection Officer** na L'Oréal Portugal.
- **Professor Convidado** na Faculdade de Direito da Universidade NOVA de Lisboa
- Doutorando em **Direito e Tecnologia** pela Universidade Nova de Lisboa
- Doutorando em Direito pela Universidade de Lisboa
- **Pós-Graduação Avançada em Direito da Proteção de Dados**
- Graduado e Mestre em Ciência Política
- Graduado em Ciência da Computação

Agentes de tratamento de dados pessoais

Em qual parte da lei estamos?



CAPÍTULO VI - OS AGENTES DE TRATAMENTO DE DADOS PESSOAIS

Artigos 37 ao 45 Seção I - Do Controlador e do Operador – artigos 37 ao 40 Seção II - Do Encarregado pelo Tratamento de Dados Pessoais – artigo 41 Seção III - Da Responsabilidade e do Ressarcimento de Danos – artigos 42 ao 45

Lembrando

Art. 5º Para os fins desta Lei, considera-se:

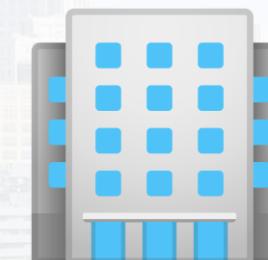
- **IX - agentes de tratamento:** o controlador e o operador.



Controlador



Dados
pessoais



Operador



Encarregado (ou DPO) não é um
agente de tratamento

Seção I

Do Controlador e do Operador

Registro de tratamento de dados

Art. 37. O controlador e o operador devem manter **registro das operações de tratamento de dados pessoais** que realizarem, especialmente quando baseado no legítimo interesse.

# tratamento	Qual a finalidade	Categorias de Dados tratados																	
		dados de identificação		dados de contacto		dados de faturação		vida familiar		vida profissional		informações de ordem financeira e patrimonial		dados de tráfego e de localização		dados de navegação na internet		outras categorias se	
		Dados	prazo de conservação	Dados	prazo de conservação	Dados	prazo de conservação	Dados	prazo de conservação	Dados	prazo de conservação	Dados	prazo de conservação	Dados	prazo de conservação	Dados	prazo de conservação	Dados	
T000	<i>ex: gestão de processamento de salários/gestão de sanções disciplinares/ controlo de assiduidade/ gestão de clientes/ marketing/gravação de chamadas na relação contratual/gestão de processos clínicos/ gestão de crédito e solvabilidade</i>	<i>ex: nome, fotografia, número de identificação civil</i>	<i>ex: 10 dias/2 meses/ 3 anos a partir da data da recolha dos dados/2 anos a partir do fim da relação contratual</i>	<i>ex: morada, e-mail, telefone</i>	<i>ex: 10 dias/2 meses/ 3 anos a partir da data da recolha dos dados/2 anos a partir do fim da relação contratual</i>	<i>ex: NIF, montante cobrado, data, IBAN</i>	<i>ex: 10 dias/2 meses/ 3 anos a partir da data da recolha dos dados/2 anos a partir do fim da relação contratual</i>	<i>ex: situação familiar, dados do agregado familiar, estado civil</i>	<i>ex: 10 dias/2 meses/ 3 anos a partir da data da recolha dos dados/2 anos a partir do fim da relação contratual</i>	<i>ex: CV, situação profissional, escolaridade, formação, distinções, diplomas</i>	<i>ex: 10 dias/2 meses/ 3 anos a partir da data da recolha dos dados/2 anos a partir do fim da relação contratual</i>	<i>ex: vencimento, situação financeira, dados bancário, rendimentos, património</i>	<i>ex: 10 dias/2 meses/ 3 anos a partir da data da recolha dos dados/2 anos a partir do fim da relação contratual</i>	<i>ex: endereços IP, logs, identificadores dos terminais, identificadores de ligação, dados de data e hora, dados de GPS, GSM, pontos wi-fi</i>	<i>ex: IP cookies de sessão, cookies de utilizador, cookies de terceiros, dados de navegação, device fingerprinting, medição de acesso a sites e interação através de ferramentas analíticas e de monitorização</i>	<i>ex: 10 dias/2 meses/ 3 anos a partir da data da recolha dos dados/2 anos a partir do fim da relação contratual</i>	<i>ex: 10 dias/2 meses/ 3 anos a partir da data da recolha dos dados/2 anos a partir do fim da relação contratual</i>	<i>ex: cor dos sapatos na festa de Natal</i>	
T001																			
T002																			
T003																			
T004																			
T005																			
T006																			
T007																			
T008																			
T009																			
T010																			
T011																			
T012																			
T013																			
T014																			
T015																			
T016																			

Registro de tratamento de dados

Art. 37. O controlador e o operador devem manter **registro das operações de tratamento de dados pessoais** que realizarem, especialmente quando baseado no legítimo interesse.

#	dados dos destinatários			categorias de dados	categoria do destinatário	Se transferência internacional nos termos do artigo 49.º, n.º 1, segundo parágrafo, link para o documento que comprove a existência de garantias adequadas	Tratamentos a que se aplica por referência à finalidade
	nome da entidade	NIF	país				
C000a	ex: Empresa destinatária 1	ex: NIF empresa 1	ex: Suíça	ex: nome, situação familiar, vencimento	ex: Subcontratante fora da UE		ex: T001
C000b	ex: Empresa destinatária 2	ex: NIF empresa 2		nome, vencimento, dados relativos às condenações	ex: Subcontratante dentro da EU/EEE		ex: T001
C001							
C002							
C003							
C004							
C005							
C006							
C007							
C008							
C009							
C010							
C011							
C012							
C013							
C014							
C015							
C016							
C017							
C018							
C019							
C020							
C021							
C022							
C023							
C024							
C025							
C026							
C027							
C028							
C029							

Registro de tratamento de dados

Art. 37. O controlador e o operador devem manter **registro das operações de tratamento de dados pessoais** que realizarem, especialmente quando baseado no legítimo interesse.

# medida	tipo de medida	Medidas concretas	Tempo de conservação (se aplicável)	Tratamentos a que se aplica
M000a	ex: Medidas de proteção lógica	ex: antivirus, palavras passe com utilização de no mínimo 8 caracteres alfanuméricos, implementação regular de atualizações de segurança, testes		ex: T000, T005, T011
M000b	ex: Controlo de acessos às instalações	ex: apenas utilizadores com cartão nominal da entidade podem aceder		ex: todos os tratamentos
M000c	ex: Registo de log	ex: logs de acesso e alteração ou eliminação de dados com identificador, data e hora da ligação, IP	ex: 2 anos	ex: T002 a T010
M000d	ex: Encriptação dos dados	ex: site acessível através de https, utilização de TLS, pseudonimização do campo data de nascimento		ex: T004
M000e	ex: Salvaguarda dos dados	ex: backups diários, redundância, plano de disaster recovery com centro alternativo	ex: os backups são conservados por 3 anos	ex: T012
M001				
M002				
M003				
M004				
M005				
M006				
M007				
M008				
M009				
M010				
M011				
M012				
M013				
M014				
M015				
M016				
M017				
M018				
M019				
M020				
M021				
M022				
M023				
M024				
M025				

Relatório de impacto à proteção de dados pessoais (RIPD)

Art. 38. A autoridade nacional poderá determinar ao controlador que elabore **relatório de impacto à proteção de dados pessoais**, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, **observados os segredos comercial e industrial**.

- Parágrafo único. Observado o disposto no *caput* deste artigo, o relatório deverá conter, no mínimo:
 - A descrição dos tipos de dados coletados
 - A metodologia utilizada para a coleta e para a garantia da segurança das informações
 - A análise do controlador com relação a medidas
 - Salvaguardas e mecanismos de mitigação de risco adotados.

Relatório de impacto à proteção de dados pessoais (RIPD)

- Software *open source* da CNIL:
<https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment>
- Versões para Mac, Windows, Linux, front end, back end



Relatório de impacto à proteção de dados pessoais (RIPD)

The screenshot shows the PIA - Privacy Impact Assessment software interface. At the top, there's a header with the logo 'Pia' and the text 'PIA - Privacy Impact Assessment' and 'Avaliação de Impacto da Proteção de Dados Privacy Impact Assessment'. Below the header, there's a navigation bar with 'PAINEL', 'MODELOS DE PIA', and 'Ferramentas'. On the left, a sidebar titled 'Teste' contains sections for 'CONTEXTO' (with 'Visão geral' selected), 'PRINCÍPIOS FUNDAMENTAIS', 'RISCOS', 'VALIDAÇÃO', and 'ANEXOS' (with 'Adicionar' button). A central panel titled 'Contexto' asks 'Qual é a finalidade de tratamento considerada no âmbito da análise?' and 'Quais são as responsabilidades inerentes ao tratamento de dados pessoais?'. To the right, a sidebar titled 'Base de conhecimento' lists 'Princípio', 'Descrição do tratamento', 'Definição', 'Responsável pelo tratamento', and 'Subcontratante'. At the bottom, there's a link 'Dados, processos e ativos de suporte »'.

Relatório de impacto à proteção de dados pessoais (RIPD)

Informação PIA

PIA

Análise de Pele com IA

Nome do autor

Dono do Projeto

Nome do assessor

Assessor do Dono do Projeto

Nome do validador

Matheus Silva (DPO)

Data de criação

04/09/2019

Nome do DPO

Matheus Silva

Modificação indesejada dos dados

Quais poderiam ser os impactos nos dados dos titulares se o risco ocorrer?

Discriminação social em decorrência do tipo de pele, Uso de email para propaganda indesejada

Quais são as principais ameaças que poderiam levar ao risco?

Colaboradores desonestos, Colaboradores mal treinados, Falhas em sistemas e equipamentos, Falhas em estruturas físicas, Falsas informações

Quais são as fontes de risco?

Humanas intencionais, Humanas não intencionais, Sistêmicas

Quais são os controlos identificados que mitigam o risco?

Cifragem, Anonimização, Controlo de acesso, Gerenciamento de violações de dados pessoais

Como estimas a gravidade do risco, esses controlos são suficientes para mitigá-lo?

Insignificante,

Insignificante: os titulares dos dados não serão prejudicados.

Visão geral dos riscos

Impactos potenciais

- Divulgação de nomes
- Divulgação de emails
- Uso de email para propaganda indesejada
- Discriminação social em decorrência do tipo de pele
- Envio de material não condizente com a realidade
- Não recebimento de informações
- Não recebimento de publicidade

Acesso ilegítimo dos dados

Gravidade : Significativo

Probabilidade : Limitado

Ameaças

- Colaboradores mal treinados
- Colaboradores negligentes
- Cracker
- Colaboradores desonestos
- Falhas em estruturas físicas
- Falha ou defeito de equipamento
- Falta de comunicações
- Problemas de/com software
- Existe a possibilidade de violar a privacidade

Modificação indesejada dos dados

Gravidade : Insignificante

Probabilidade : Insignificante

Operador x Controlador

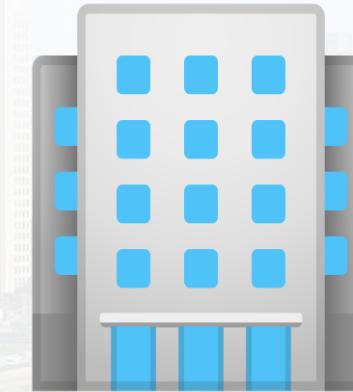
Art. 39. O operador deverá realizar o tratamento **segundo as instruções fornecidas pelo controlador**, que verificará a observância das próprias instruções e das normas sobre a matéria.



Controlador



Dados
pessoais



Operador

Outras obrigações dos agentes de tratamento

- Informação e transparência
- *Privacy by Design*
- Contratos entre Controlador e Operador
- Medidas de Segurança
- Notificações em caso de violação de dados pessoais

Padrões de interoperabilidade

Art. 40. A autoridade nacional poderá dispor sobre **padrões de interoperabilidade** para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência.



Seção II

Do Encarregado pelo Tratamento de Dados Pessoais

Será abordado no próximo módulo

Seção III

Da Responsabilidade e do Ressarcimento de Danos

Reparação de danos

Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

- § 1º A fim de assegurar a efetiva indenização ao titular dos dados:

I - o operador responde solidariamente pelos danos causados pelo tratamento quando **descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador**, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;

II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

Reparação de danos

Art. 42.

- § 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.
- § 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do *caput* deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.
- § 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

Quando agentes não serão responsabilizados?

Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:

- I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;
- II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
- III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Quando o tratamento é considerado irregular?

Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:

- I - o modo pelo qual é realizado;
- II - o resultado e os riscos que razoavelmente dele se esperam;
- III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.
- Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

Violação do direito do titular

Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente.