EXIN
Privacy & Data Protection
Foundation

PORTAL DO TREINAMENTO!
EDUCAÇÃO EM TI

Sejam muito bem-vindos!

Muito obrigado por escolher e participar do treinamento oficial

EXIN PRIVACY AND DATA PROTECTION FOUNDATION - PDPF

com a
Portal do Treinamento !

Temos o prazer de tê-los como alunos e transmitir toda a nossa experiência e conhecimento de maneira única e inovadora a vocês.

Treinamentos

PORTAL DO TREINAMENTO!

EDUCAÇÃO EM TI

- **+ de 15 anos** de história de ensino em TI relacionados ao Gerenciamento de Serviços, Governança, Privacidade de Dados, Segurança da Informação, Agile e Inovação &Tecnologia.

- **Portal do Treinamento** é um centro oficial de treinamentos e exames EXIN, AXELOS/PEOPLECERT e outras certificadoras reconhecidas internacionalmente.

follow us on facebook

Follow us on Instagram

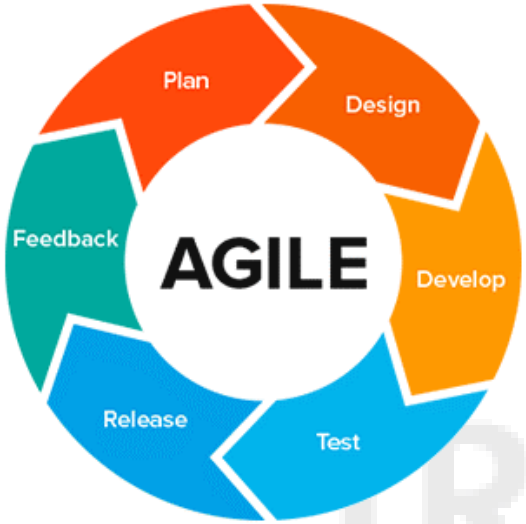
Follow us on LinkedIn

Treinamentos

PORTAL DO TREINAMENTO!
EDUCAÇÃO EM TI

- **Treinamentos *online*, ao vivo**, com turmas pequenas e grande interação professor-alunos.
- Turmas abertas e *in company*.
- Os instrutores são **profissionais de mercado** com larga experiência no assunto ministrado e vivência acadêmica.

Agile

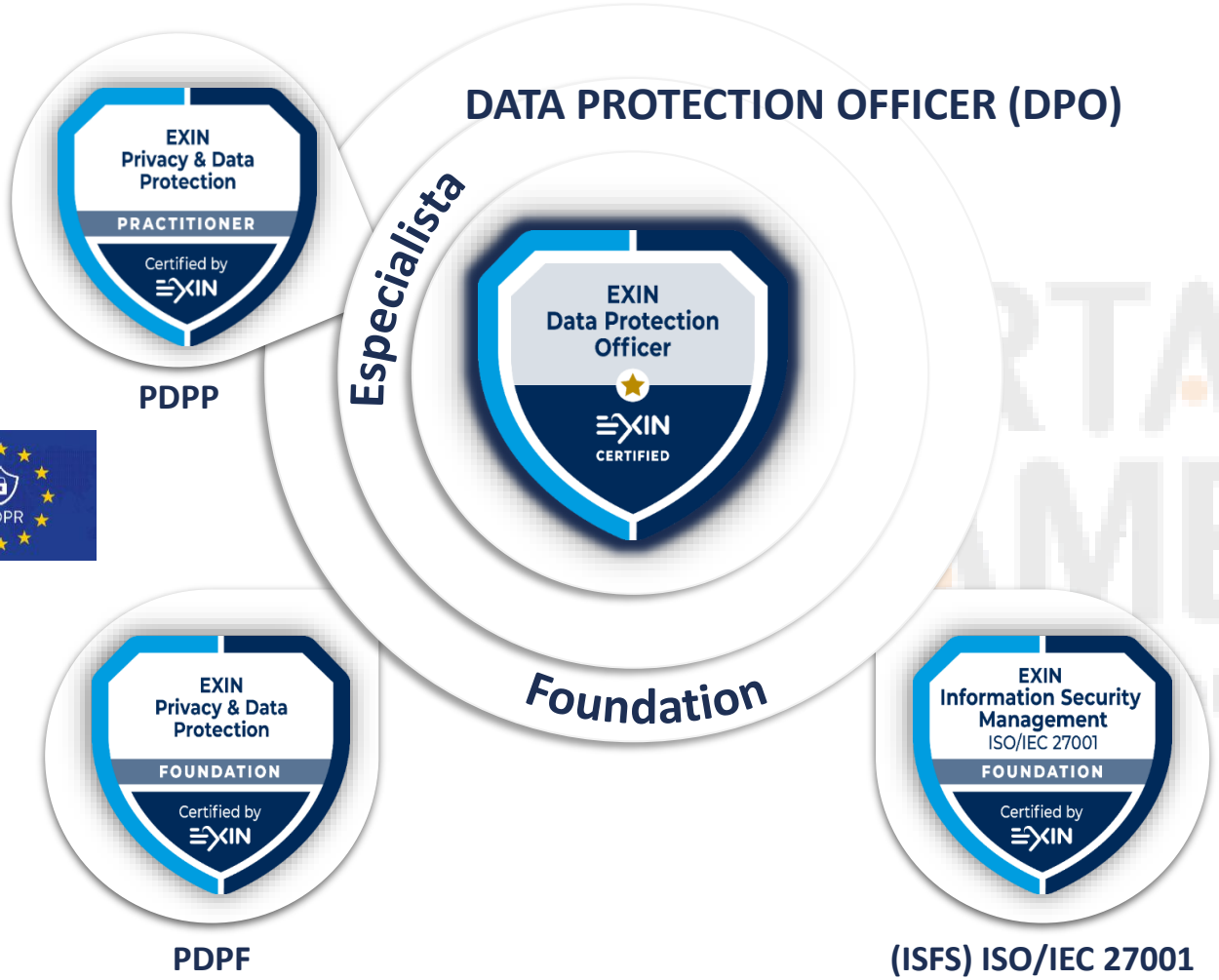


- Scrum Master
- Product Owner
- DevOps Master
- Lean IT
- Cloud Computing
- Projetos Ágeis de LGPD

Governança, Arquitetura, Gestão

- COBIT® 5
- COBIT® 2019 FB
- ITIL® 4
- ISO 20000 FB
- TOGAF®
- Management 3.0
- Ger. Projetos LGPD
  (Abordagem Cascata)
- CISM®

Privacidade de Dados



PDPE

LGPD

Lei Geral de Proteção de Dados

DPO = ISFS + PDPF + PDPP

PÚBLICO ALVO

Profissionais de TI, SI, negócio, gerentes de projetos, advogados e demais interessados na **LGPD** e privacidade de dados.

Privacidade

DATA PROTECTION OFFICER (DPO)

DPO = ISFS + PDPF + PDPP

Próximas turmas:

Privacy & Data Protection Foundation – PDPF

ISO 27001 Foundation (Segurança da Informação)

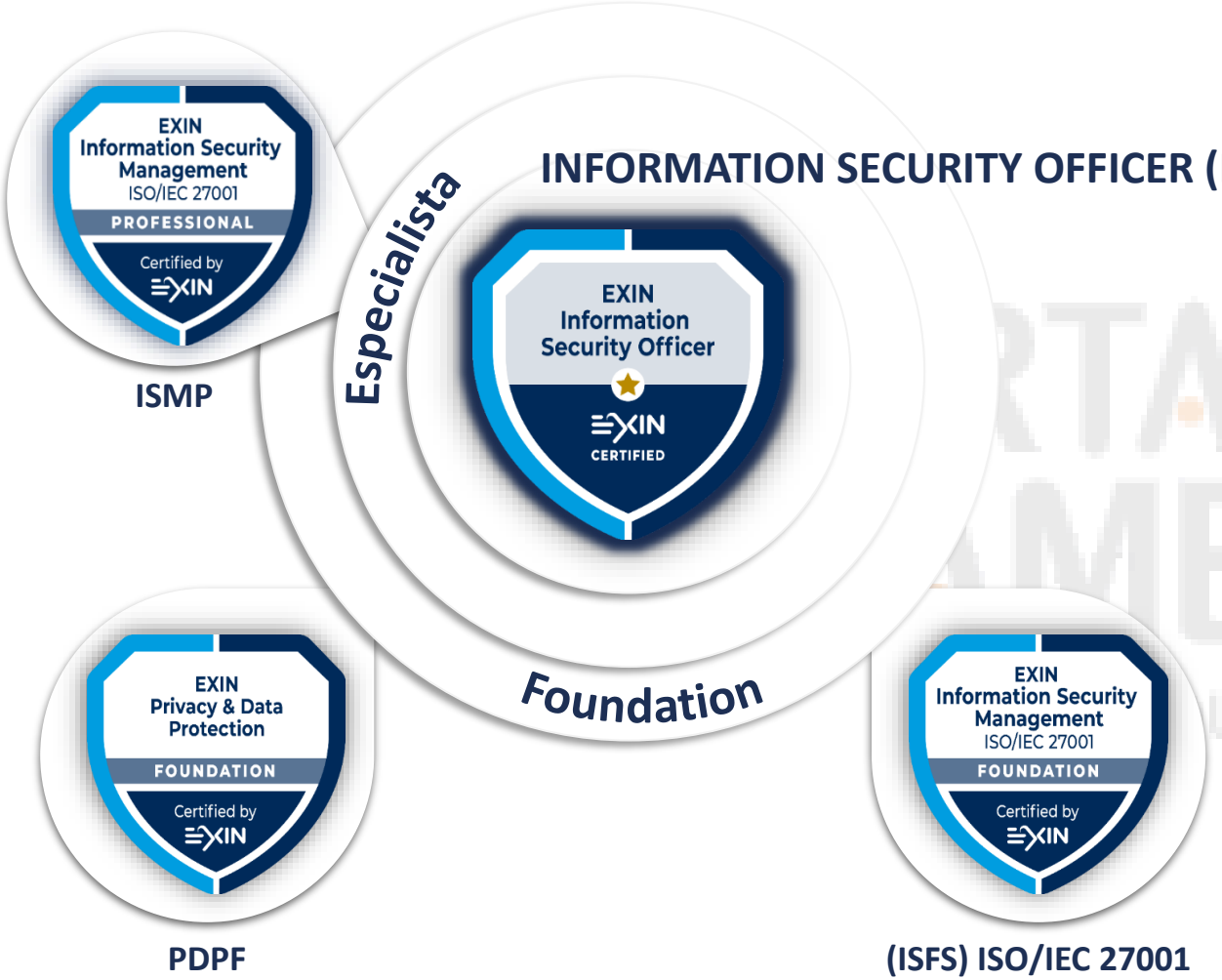
Privacy & Data Protection Practitioner - PDPP

Validação site EXIN. Ex. Prof. Adrianne Lima:
https://app.exeed.pro/holder/profile/28074

Mais informações:

https://www.portaldotreinamento.com.br/dpo-data-protection-officer/

Segurança da Informação

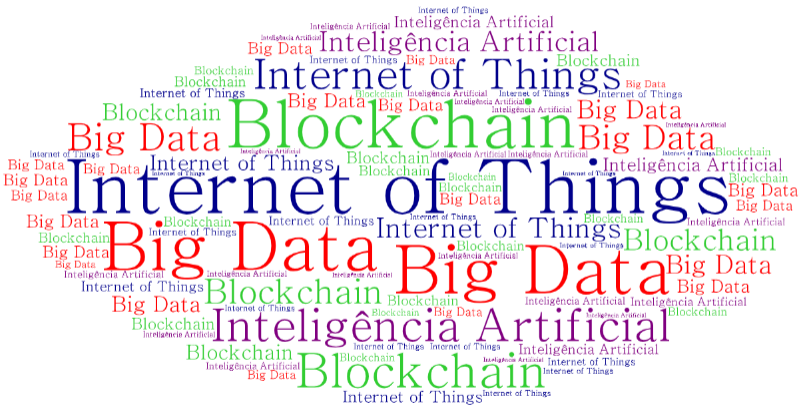


ISO = ISFS + PDPF + ISMP

PÚBLICO ALVO

Gerentes e demais profissionais ligados e/ou interessados em **Segurança da Informação**.

Novas Tecnologias

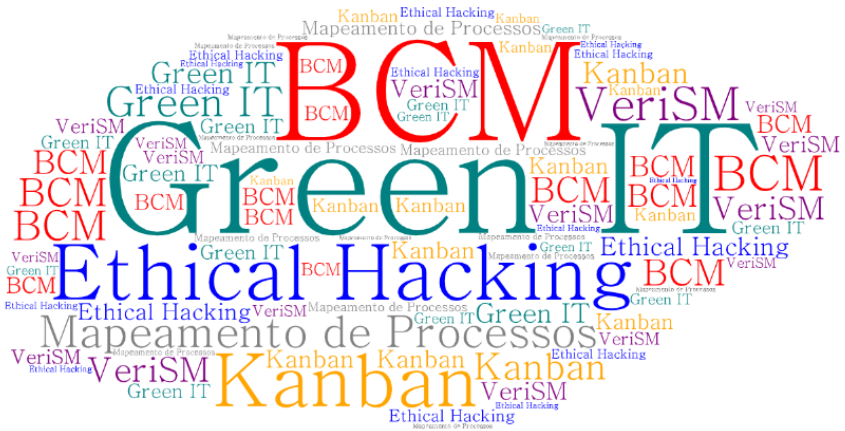


- IoT **novo**
- Big Data **novo**
- Blockchain **novo**
- I.A. **novo**

Treinamentos preparatórios para certificação

- Ethical Hacking
- BCM
  (Business Continuity Management)
- Green IT
- VeriSM

Cursos de aperfeiçoamento



- Mapeamento de Processos
- Kanban
- Implementação do SGPD
- Gerenciamento de Projetos – LGPD (abordagens ágil e cascata)

Formação Mainframe

- z/OS
- TSO
- Lógica Estruturada
- COBOL
- VSAM, SQL/DB2

PORTAL DO TREINAMENTO!
EDUCAÇÃO EM TI

PORTAL DO TREINAMENTO!
EDUCAÇÃO EM TI

@Portaldotreinamento

Telegram

portaldotreinamento

Portal do Treinamento

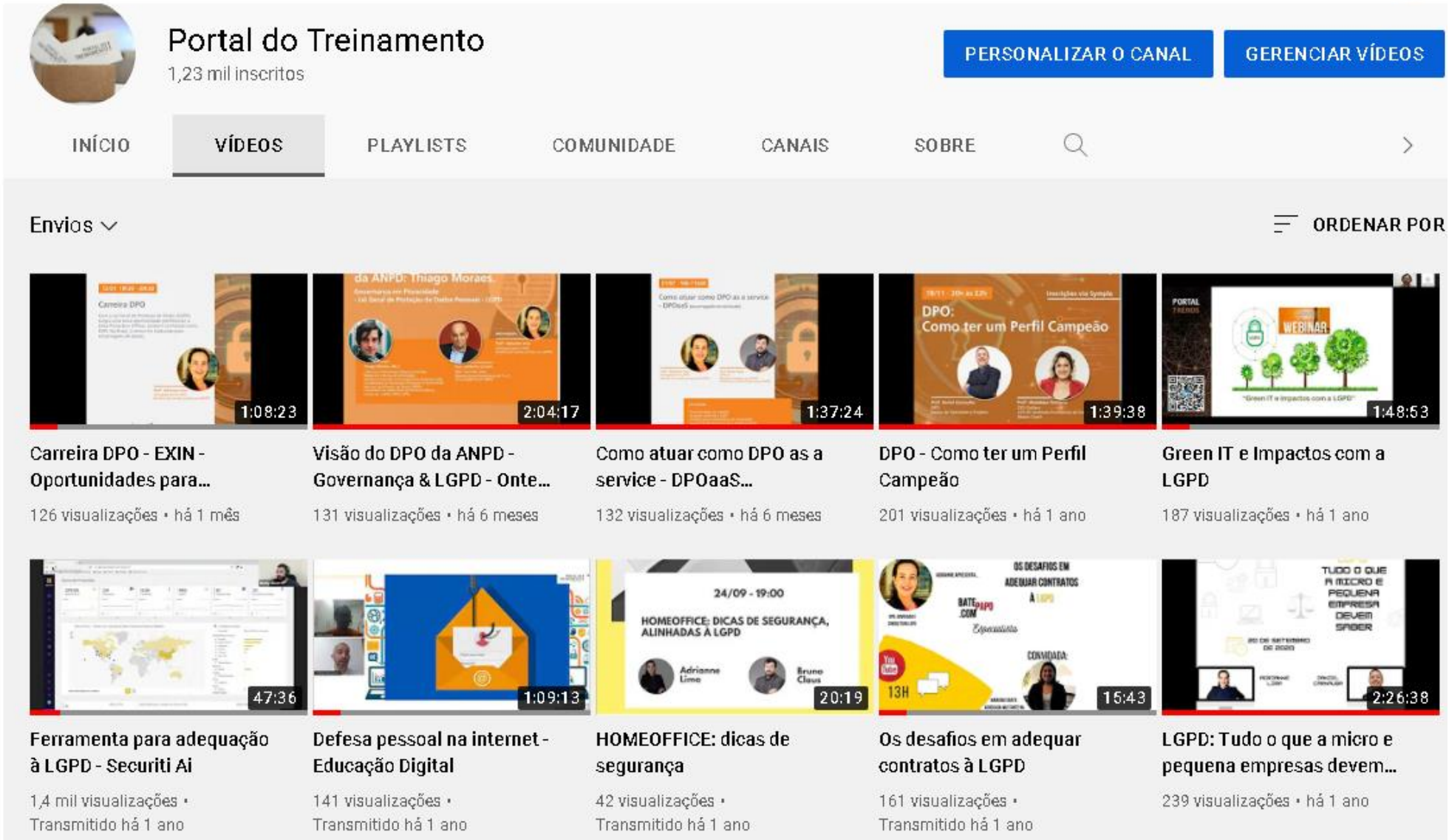
+55 11 92004-3018

PORTAL DO TREINAMENTO!
EDUCAÇÃO EM TI

Telegram

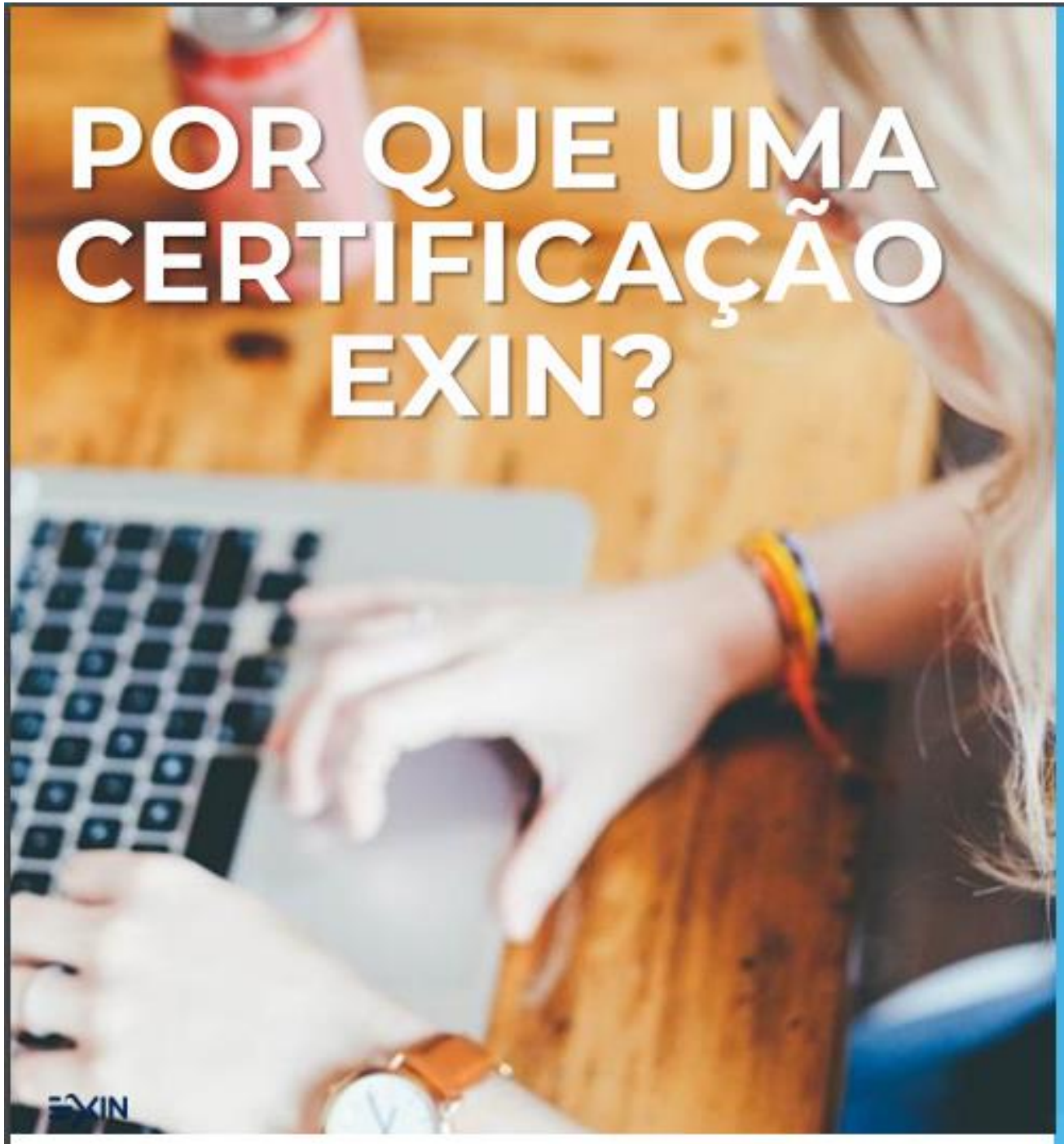
Adicione o canal do Portal do Treinamento no Telegram:
https://t.me/joinchat/QZrcFxv6i3YR5ROu8o7ZsQ

Atualizações de vagas de trabalho, notícias, cursos e *lives* sobre proteção de dados e privacidade



https://www.youtube.com/c/PortaldotreinamentoBrEducacaoemTI/videos

PORTAL DO TREINAMENTO!
EDUCAÇÃO EM TI



POR QUE UMA CERTIFICAÇÃO EXIN?

- 35 anos de mercado
- Instituto Independente
- Mais de 2 Milhões de profissionais certificados pelo EXIN
- Amplo Portfolio no universo TI/Negócios
- Certificações Alinhadas com as demandas de mercado
- Disponível em múltiplos idiomas
- Fácil acesso (cursos, exames, certificados)

PORTAL DO TREINAMENTO!

APRESENTAÇÃO

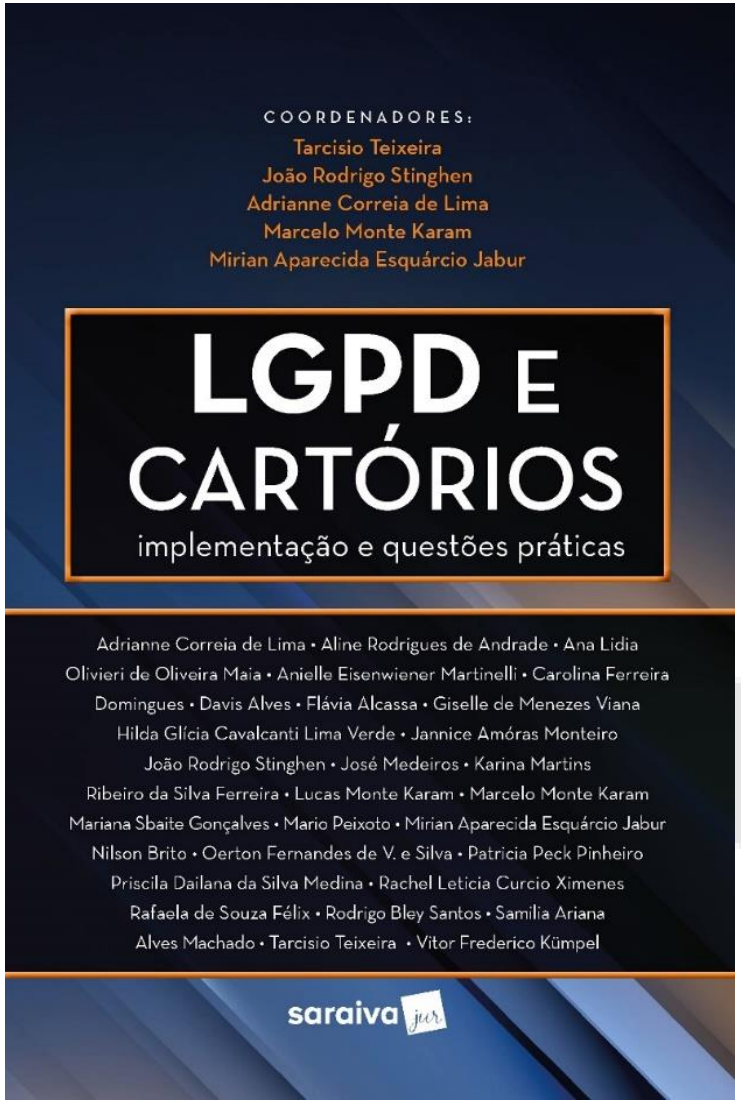
- Quem sou ...
- O que faço ...
- Por que estou aqui ...

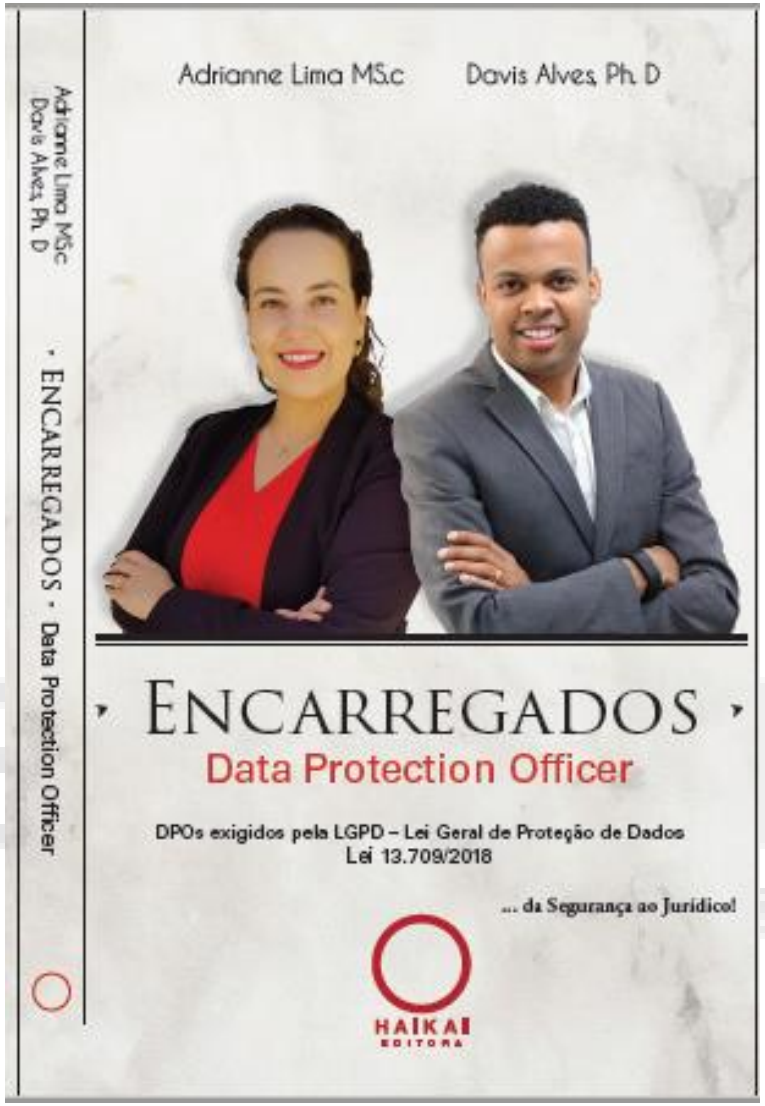
Pode me seguir:

Adrianne Lima

@profadrianne

- Advogada
- **Professora, consultora , Lead Implementer ISO 27701 e *Data Protection Officer* - DPO**
- Diretora do Comitê Jurídico da ANPPD
- **Membro da comissão de estudos da ABNT "Segurança da Informação, Segurança Cibernética e Proteção da Privacidade"**
- Professora no Portal do Treinamento e cursos de pós-graduação em Proteção de Dados e Compliance Digital da Universidade Mackenzie e PUC Campinas
- **Mestre em Administração e Desenvolvimento de Negócios - Universidade Mackenzie**



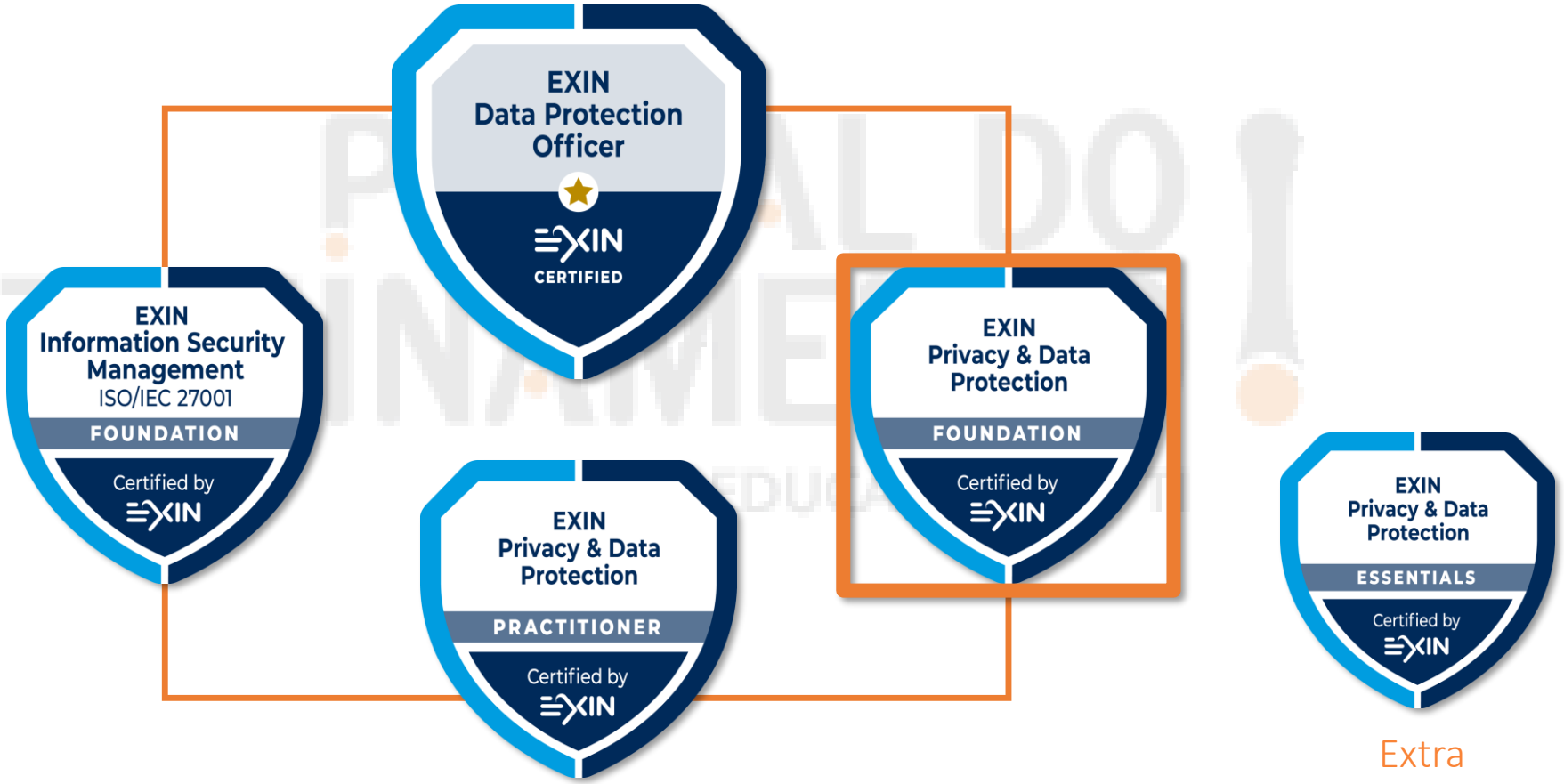


Clique nos ícones!

Disponíveis na Amazon.com.br

PORTAL DO TREINAMENTO!

CARREIRA DPO



Extra

PORTAL DO TREINAMENTO!

OBJETIVOS DO TREINAMENTO

Dar aos participantes a compreensão sobre a proteção de dados e os requisitos legais europeus, conforme definido no GDPR.

Este treinamento se destina a :

- ✓ Data Protection Officers (DPO),
- ✓ Profissionais das áreas Jurídica, SI, Marketing, TI,
- ✓ Compliance Officers,
- ✓ Security Officers,
- ✓ Funcionários de RH,
- ✓ Gerentes de Processos e de Projetos e outros

Orientações

Mantenha o microfone mutado, e abra apenas quando for falar.

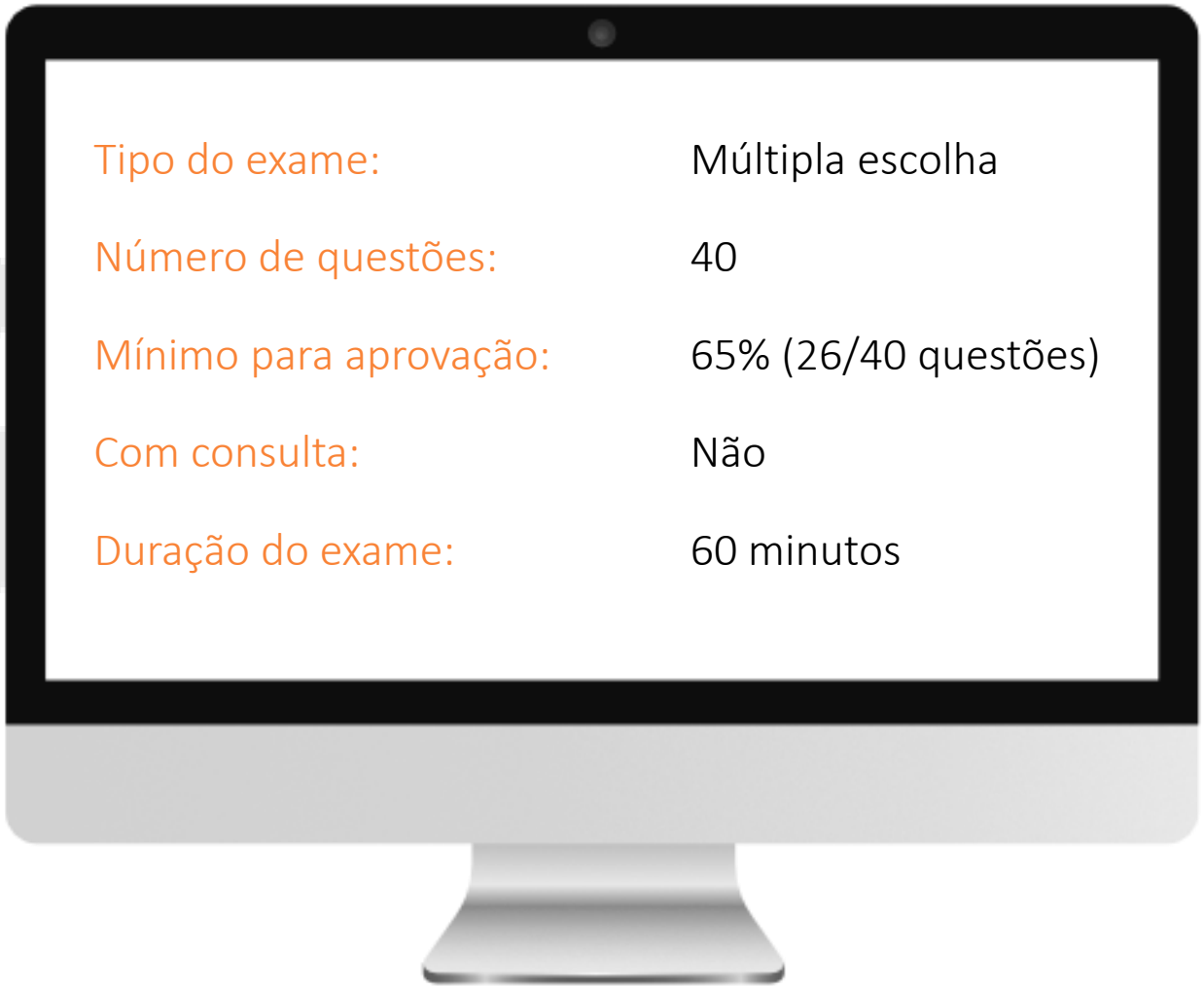
Podem enviar as dúvidas via chat e vamos respondendo quando possível.

Este assunto é de aprendizagem contínua, então ao sair da aula, continue estudando e se aperfeiçoando.

O EXAME

EXIN Privacy & Data Protection Foundation (PDPF)

Certificação que valida o conhecimento e compreensão de um profissional sobre a proteção de dados pessoais, as regras e regulamentos da União Europeia (UE) em matéria de proteção de dados.



Requisitos do exame

Os requisitos do exame são definidos nas especificações do exame. A tabela a seguir lista os tópicos (requisitos do exame) e subtópicos (especificações do exame) do módulo.

Requisitos do exame	Especificações do exame	Peso
1. Fundamentos e regulamentação de privacidade e proteção de dados		**47,5%**
	1.1 Definições	7,5%
	1.2 Dados pessoais	17,5%
	1.3 Fundamentos legítimos e limitação de finalidade	5%
	1.4 Requisitos adicionais para processamento legítimo de dados pessoais	5%
	1.5 Direitos dos titulares dos dados	2,5%
	1.6 Violação de dados pessoais e procedimentos relacionados	10%
2. Organizando a proteção de dados		**35%**
	2.1 Importância da proteção de dados para a organização	12,5%
	2.2 Autoridade supervisora[1]	7,5%
	2.3 Transferência de dados pessoais para países terceiros	7,5%
	2.4 Regras corporativas vinculantes (BCR) e proteção de dados em contratos	7,5%
3. Práticas de proteção de dados		**17,5%**
	3.1 Proteção de dados desde a concepção (by design) e por padrão (by default)	5%
	3.2 Avaliação de Impacto sobre a Proteção de Dados (DPIA)	5%
	3.3 Dados pessoais em uso	7,5%
	Total	**100%**

O exame poderá avaliar se…

1 Fundamentos e regulamentação de privacidade e proteção de dados

1.1 Definições

O candidato é capaz de …

1.1.1 definir privacidade.

1.1.2 relacionar privacidade a dados pessoais e proteção dos dados.

1.1.3 descrever o contexto da legislação da União e do Estado-Membro.

1.2 Dados pessoais

O candidato é capaz de …

1.2.1 definir dados pessoais de acordo com o GDPR.

1.2.2 distinguir dados pessoais e categorias especiais de dados, como dados pessoais sensíveis.

1.2.3 descrever os direitos do titular dos dados com relação aos dados pessoais.

1.2.4 definir processamento de dados pessoais que se enquadre no escopo do GDPR.

1.2.5 listar os papéis, responsabilidades e partes interessadas conforme o GDPR.

1.3 Fundamentos legítimos e limitação de finalidade

O candidato é capaz de …

1.3.1 listar os seis fundamentos legítimos para processamento.

1.3.2 descrever o conceito e a limitação de finalidade.

1.3.3 descrever proporcionalidade e subsidiariedade.

1.4 Requisitos adicionais para processamento legítimo de dados pessoais

O candidato é capaz de …

1.4.1 descrever os requisitos para processamento legítimo de dados.

1.4.2 descrever a finalidade do processamento de dados.

1.4.3 explicar os princípios relacionados ao processamento de dados pessoais.

O exame poderá avaliar se…

1.5 Direitos dos titulares dos dados

O candidato é capaz de…

- 1.5.1 descrever os direitos relacionados à portabilidade de dados e direito de inspeção.
- 1.5.2 descrever o direito ao esquecimento.

1.6 Violação de dados pessoais e procedimentos relacionados

O candidato é capaz de …

- 1.6.1 descrever o conceito de violação de dados pessoais.
- 1.6.2 explicar os procedimentos sobre como agir quando ocorre uma violação de dados pessoais.
- 1.6.3 dar exemplos de categorias de violação de dados pessoais.
- 1.6.4 descrever a diferença entre uma violação de segurança (incidente) e violação de dados pessoais.
- 1.6.5 listar as partes interessadas relevantes que devem ser informadas no caso de uma violação de dados pessoais.

O exame poderá avaliar se…

2 Organizando a proteção de dados

2.1 Importância da proteção de dados para a organização

O candidato é capaz de …

- 2.1.1 listar os diferentes tipos de administração (artigos 28 e 30 do GDPR).
- 2.1.2 indicar quais atividades são necessárias para estar em conformidade com o GDPR.
- 2.1.3 definir a proteção de dados desde a concepção (by design) e por padrão (by default).
- 2.1.4 dar exemplos de violação de dados pessoais.
- 2.1.5 descrever a obrigação de notificação de violação de dados pessoais conforme estabelecido no GDPR.
- 2.1.6 descrever a execução das regras mediante a emissão de sanções, incluindo multas administrativas.

2.2 Autoridade supervisora

O candidato é capaz de …

- 2.2.1 descrever as responsabilidades gerais de uma autoridade supervisora.
- 2.2.2 descrever o papel e as responsabilidades de uma autoridade supervisora em relação a violações de dados pessoais.
- 2.2.3 descrever como uma autoridade supervisora contribui para a aplicação do GDPR.

2.3 Transferência de dados pessoais para países terceiros

O candidato é capaz de …

- 2.3.1 descrever a regulamentação que é aplicada na transferência de dados dentro da Área Econômica Europeia (AEE).

O exame poderá avaliar se…

2.4 Regras corporativas vinculantes (BCR) e proteção de dados em contratos

O candidato é capaz de …

2.4.1 descrever o conceito de BCR.

2.4.2 descrever como a proteção de dados é formalizada em contratos entre o controlador e o processador.

2.4.3 descrever as cláusulas desse tipo de contrato.

3 Práticas de proteção de dados

3.1 Proteção de dados desde a concepção (by design) e por padrão (by default)

O candidato é capaz de …

3.1.1 descrever os benefícios da proteção de dados desde a concepção e por padrão.

3.1.2 descrever os sete princípios da proteção de dados desde a concepção.

3.2 Avaliação de Impacto sobre a Proteção de Dados (DPIA)

O candidato é capaz de …

3.2.1 descrever o que um DPIA aborda e quando um DPIA deve ser realizado.

3.2.2 mencionar os oito objetivos de um DPIA.

3.2.3 listar os tópicos de um relatório de DPIA.

O exame poderá avaliar se…

3.3 Dados pessoais em uso

O candidato é capaz de …

3.3.1 descrever os objetivos da Gestão do Ciclo de Vida do Dado (GCVD).

3.3.2 explicar a retenção e minimização de dados.

3.3.3 descrever o que é um cookie e qual a sua finalidade.

3.3.4 descrever o direito de oposição ao processamento de dados pessoais com finalidade de marketing direto, inclusive definição de perfis.

PORTAL DO TREINAMENTO!

BIBLIOGRAFIA INDICADA

- **White Paper – Privacidade, Dados Pessoais e GDPR** - L. Besemer

  PDF gratuito em: http://bit.ly/PDPF_PR_literature

- **General Data Protection Regulation (GDPR) Regulation (EU) 2016/679)**

  https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN

PORTAL DO TREINAMENTO!

AGENDA

- Fundamentos
- Organizando a Proteção de Dados
- Práticas de Proteção de Dados

PORTAL DO TREINAMENTO!

CURIOSIDADES.. Estados Unidos

Proteção de Dados no Direito Comparado - EUA

O congresso americano é reticente em criar uma legislação federal única sobre proteção de dados (KOURFF, 2010)

Como consequência dessa passividade, a Federal Trade Commission (FTC), entidade governamental que supervisiona o comércio nos Estados Unidos, acabou por incentivar a auto-regulação e o uso de tecnologias em benefício da proteção de dados

Protecting Consumer Privacy and Security | Federal Trade Commission (ftc.gov)

CURIOSIDADES.. Estados Unidos

Regra: há a quebra de privacidade de dados pessoais para atendimento a atividades governamentais.

Leis estaduais e federais de privacidade, específicas para cada segmento. Dentre elas:

- Lei de Proteção de Privacidade do Motorista (1994) - *Drivers Privacy Protection Act* (DPPA) – Código dos EUA 18, 2721.

  O DPPA foi aprovado, em reação a uma série de acontecimentos decorrentes do acesso a dados pessoais dos motoristas, que eram mantidos pelo governo

  Ex: Uma atriz (Rebecca Schaeffer) foi assassinada na California, em 1989, após um fã conseguir obter o seu endereço, por meio dos dados de registro de seu veículo.

CURIOSIDADES.. Estados Unidos

- É permitido o uso de informações pessoais para atividades do governo, segurança de veículos (roubo) e necessidades diversas, como para a venda do veículo.

- DPPA exige que os estados protejam a privacidade dos dados pessoais contidos nos registros de veículos e obtenham o consentimento expresso do motorista, antes de permitir o acesso de qualquer informação pessoal a terceiros.

PORTAL DO TREINAMENTO!

CURIOSIDADES.. Estados Unidos

- Privacy Act (1974 – dados pessoais em agências federais) - informações pessoais tratadas pelo poder executivo federal / Não se aplica a estados/cidades e empresas privadas;
- Stored Communications Act – SCA (1986 – limita fornecimento de dados a entidades não governamentais);
- Clarifying Lawful Overseas Use of Data Act - CLOUD Act (2018 – trata do compartilhamento de dados com governos estrangeiros);
- Privacy Shield (2017 – acordo com a UE para o compartilhamento internacional de dados) - https://www.privacyshield.gov/welcome ;

CURIOSIDADES.. Estados Unidos

Acordo EUA e EU

Em 2016, a Comissão Europeia e os Estados Unidos fecharam um marco jurídico sobre a transferência dos dados pessoais com fins comerciais.

O acordo, chamado de "Privacy Shield" (Escudo de Privacidade) protege os direitos fundamentais de qualquer pessoa na UE cujos dados pessoais sejam transferidos para os Estados Unidos para fins comerciais. Ele permite a transferência gratuita de dados para empresas certificadas nos EUA pelo Privacy Shield. Inclui:

- fortes obrigações de proteção de dados para empresas que recebem dados pessoais da UE
- salvaguardas sobre o acesso do governo dos EUA aos dados
- proteção e reparação eficazes para os indivíduos
- uma revisão anual conjunta da UE e dos EUA para monitorizar a correta aplicação do acordo

CURIOSIDADES.. Estados Unidos

Acordo EUA e EU

Nota: Atualização na estrutura do Privacy Shield:

“Em 16 de julho de 2020, o Tribunal de Justiça Europeu emitiu uma sentença declarando inválida a Decisão 2016/1250 / EC da Comissão Europeia de 12 de julho de 2016 sobre a adequação da Estrutura de Escudo de Privacidade UE-EUA. Continuamos esperando que as empresas cumpram suas obrigações contínuas com relação às transferências feitas sob a Estrutura do Privacy Shield. Também encorajamos as empresas a continuarem a seguir princípios de privacidade robustos, como os subjacentes à Estrutura do Privacy Shield, e a revisar suas políticas de privacidade para garantir que descrevam suas práticas de privacidade com precisão, inclusive com relação a transferências internacionais de dados. Atualizado em 21 de julho de 2020”.

CURIOSIDADES.. Estados Unidos

- *Data Protection Act of 2020* - Fevereiro/2020: apresentação do projeto de Lei de Proteção de Dados de 2020 - no Senado dos EUA.

- *California Consumer Privacy Act* – CCPA– a Lei de Privacidade do Consumidor da Califórnia –

  A CCPA foi sancionada em 28 de junho de 2018 e entrou em vigor em 1º de janeiro de 2020. A CCPA concede aos consumidores da Califórnia direitos robustos de privacidade de dados e controle sobre suas informações pessoais, incluindo o direito de saber, o direito de excluir e o direito recusar a venda de informações pessoais que as empresas coletam, bem como proteções adicionais para menores.

Fonte: https://oag.ca.gov/privacy/ccpa e
http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5.&part=4.&chapter=&article=

1. FUNDAMENTOS E REGULAMENTAÇÃO DE PRIVACIDADE E PROTEÇÃO DE DADOS

1. FUNDAMENTOS E REGULAMENTAÇÃO DE PRIVACIDADE E PROTEÇÃO DE DADOs

Tópicos

- Contexto Histórico e Escopo
- Definições
- Dados pessoais
- Bases legais e limitação de finalidade
- Direitos dos titulares dos dados
- Violação de dados pessoais

1.1 CONTEXTO HISTÓRICO E ESCOPO

PORTAL DO TREINAMENTO!

CONTEXTO HISTÓRICO

Até o século XIX, o comportamento social pressupunha o compartilhamento de diversos atos pessoais cotidianos com a coletividade, como parir, velar os mortos, tomar banho ou mesmo dormir.

As razões poderiam ser muitas, como: as limitações de produção e oferta de serviços e bens para essas finalidades, como camas, casas segmentadas em cômodos e banheiros isolados, por exemplo.

Em Roma, por exemplo, o banho, assim como as latrinas, era público.

Fonte: TripAdvisor

PORTAL DO TREINAMENTO!

CONTEXTO HISTÓRICO

"As recentes invenções e métodos de negócios chamam a atenção para o próximo passo que deve ser tomado para a proteção da pessoa e para assegurar ao indivíduo ... o direito de "estar sozinho" ... Vários dispositivos mecânicos ameaçam cumprir a previsão de que "o que é sussurrado no armário será proclamado do topo das casas" (Brandeis, 1890)

Artigo dos juristas norte-americanos Samuel

Warren e Louis Brandeis, publicado em 1890 pela revista Harvard Law Review.

https://www.brandeis.edu/now/2013/july/privacy.html

PORTAL DO TREINAMENTO!

CONTEXTO HISTÓRICO

Artigo XII

Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.

PORTAL DO TREINAMENTO!

CONTEXTO HISTÓRICO

Síntese

Diretrizes da OCDE para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais

Overview

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

As Diretrizes para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais (1980)

As Diretrizes para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais (as "Diretrizes sobre a Privacidade") foram adotadas enquanto Recomendação do Conselho da OCDE em apoio aos três princípios comuns aos países membros da OECD : democracia pluralista, respeito aos direitos humanas e economias de mercado aberto. Entraram em vigor em 23 de setembro de 1980.

As Diretrizes sobre a Privacidade representam um consenso internacional sobre a orientação geral a respeito da coleta e do gerenciamento da informação pessoal. Os princípios determinados nas Diretrizes sobre a Privacidade são caracterizados pela clareza e flexibilidade de aplicação e pela formulação, suficientemente ampla para possibilitar a adaptação às mudanças tecnológicas. Esses princípios abrangem todos os meios utilizados para o processamento automatizado de dados referentes a indivíduos (do computador local à rede de complexas ramificações nacionais e internacionais), todos os tipos de processamento de dados pessoais (da administração do pessoal ao levantamento de perfis de consumidores) e todas as categorias de dados (da circulação de dados ao seu conteúdo, dos mais comuns ao mais sensíveis). Os princípios aplicam-se a ambos os níveis nacional e internacional. Ao longo dos anos, foram postos em aplicação em grande número de instrumentos de regulamentação nacionais ou de auto-regulamentação, e ainda são amplamente utilizados em ambos os setores público e privado.

PORTAL DO TREINAMENTO!

CONTEXTO HISTÓRICO

Síntese

Diretrizes da OCDE para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais

Overview

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

Parte I : Generalidades

Definições

1. Para as finalidades destas Diretrizes :

   1. "controlador de dados" significa a parte que, de acordo com a lei doméstica, tem competência para decidir do conteúdo e da utilização de dados pessoais independentemente de tais dados serem ou não coletados, armazenados, processados ou divulgados por esta parte ou por um agente em nome dela.

   2. "dado pessoal" significa qualquer informação relacionada com um indivíduo identificado ou identificável (sujeito dos dados);

   3. "fluxos transfronteiriços de dados pessoais" significam o movimento de dados pessoais além das fronteiras nacionais.

Alcance das Diretrizes

2. Estas Diretrizes aplicam-se a dados pessoais que representam, seja no setor público ou privado, uma ameaça para a privacidade e a liberdade individual em razão de seu modo de processamento, de sua natureza ou do contexto de utilização.

3. Estas Diretrizes não devem ser interpretadas como impedindo :

   1. a aplicação de várias medidas de proteção a diversas categorias de dados pessoais, em função de sua natureza e do contexto em que são coletados, armazenados, processados ou divulgados;

   2. a exclusão, quando da aplicação das Diretrizes, dos dados pessoais que obviamente não representam risco nenhum para a privacidade e a liberdade individual ; ou

   3. a aplicação destas Diretrizes ao único processamento automatizado de dados.

PORTAL DO TREINAMENTO!

CONTEXTO HISTÓRICO

Cronologia de proteção de dados

Ano	Nome	Sigla
1948	**Declaração Universal dos Direitos Humanos**	**DUDH (UHDR)**
1950	Convenção Europeia sobre Direitos Humanos	CEDH (ECHR)
1981	Convenção para Proteção de Indivíduos relativamente ao Processamento Automático de Dados Pessoais - Convenção 108	ETS 108 = EU Tratado de Estrasburgo
1995	**Diretiva 95/46 / CE relativa à proteção das pessoas físicas no que diz respeito ao processamento de dados pessoais e à livre circulação desses dados**	**Diretiva de Privacidade** (válida até 25/5/2018)
2002	Carta dos Direitos Fundamentais da União Europeia	CEDH (EU Charter)
2016	**Regulamento Geral de Proteção de Dados (EU - 2016/679)**	**'GDPR'** (a partir de 25/5/2018,revoga a Diretiva 95/46/CE)
2016	Diretiva 2016/680 (cooperação judiciário e polícia para assuntos criminais)	
2016	Diretiva 2016/681 (sobre o uso de dados de registro de nome de passageiros – PNR)	

PORTAL DO TREINAMENTO!

DIRETIVA E REGULAMENTO

Directiva 95/46/CE

Diretiva que deve ser assimilada dentro da legislação nacional de cada Estado-Membro, a partir dela cada estado membro cria suas leis internas .

Regulamento é vinculante e diretamente aplicável a todos os Estados-Membros.

Aplica-se a todos os países do Espaço Econômico Europeu (EEE) ou da Área Econômica Europeia (AEE), composto : Estados-Membros da UE, Islândia, Liechtenstein e Noruega.

ESCOPO MATERIAL

Artigo 2.o

Âmbito de aplicação material

1. O presente regulamento aplica-se ao processamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao processamento por meios não automatizados de dados pessoais que fazem parte de um sistema de arquivo ou se destinam a fazer parte de um sistema de arquivo / ficheiro.

O GDPR trata somente da proteção dados pessoais, e não de todos os tipos de dados

ESCOPO MATERIAL

Âmbito de aplicação material - Exceções

- Efetuado pelos Estados-Membros e Políticas Externas
- Processamento por autoridades competentes para efeitos de prevenção, investigação, detecção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública
- Processamento de dados pessoais por uma pessoa natural "no curso de uma atividade puramente pessoal ou doméstica"

ESCOPO TERRITORIAL

Artigo 3.o

Âmbito de aplicação territorial

- Controlador ou Processador situado no território da União, independentemente de o processamento ocorrer dentro ou fora da União.
- Controlador ou Processador situado fora do território da União, tratando dados pessoais para oferta de bens, serviços ou controle de comportamento de titulares residentes no território da União

Considerando 23

Apresenta a proteção a qualquer pessoa natural que por ventura esteja em território da União Europeia

Considerando 25

Aplicabilidade do GDPR por força do direito internacional público (Consulado,Navio, Avião)

1.2 DEFINIÇÕES

PORTAL DO TREINAMENTO!

GDPR - OBJETIVO

"...O presente regulamento tem como objetivo **contribuir para a realização de um espaço de liberdade, segurança e justiça** e de uma união econômica, para o progresso econômico e social, a consolidação e a convergência das economias a nível do mercado interno e para o bem-estar das pessoas físicas." (**Considerando 1**)

PORTAL DO TREINAMENTO!

USO DE DADOS PESSOAIS ATUALMENTE..

PRIVACIDADE

- Direito a respeitar a vida privada e familiar de uma pessoa, sua casa e correspondência
- Direito de ser deixado em paz

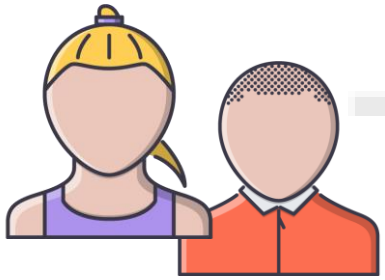
PROTEÇÃO DE DADOS

São dispositivos, leis, medidas técnicas e organizacionais que devem ser aplicadas de forma a proteger os dados das pessoas físicas .

Uma pessoa física não pode ter privacidade (fim) sem proteção de dados (meio).

PESSOA FÍSICA E PESSOA JURÍDICA

A personalidade jurídica tem como definição quase invariável a «suscetibilidade de ser sujeito de direitos e obrigações». A personalidade jurídica pode ser física ou jurídica.



É física/singular/natural quando referida a pessoa humana. Neste caso, adquire-se no momento do nascimento completo e com vida e cessa com a morte.

Pessoas Falecidas : Conforme o Considerando 27 , o GDPR não se aplica a pessoas falecidas .

É jurídica/coletiva quando referida a organizações de pessoas e/ou de bens (associações, fundações).

DADOS PESSOAIS

Artigo 4º, 1 - “informação relativa a uma pessoa física identificada ou identificável...”

Titular dos Dados

Pessoa física (natural) a quem se referem os dados pessoais que são objeto de processamento

DADOS PESSOAIS

- o nome e apelido
- o endereço de uma residência
- o número de um cartão de identificação
- dados de localização
- um endereço IP (protocolo de internet)
- registros de conexão (cookies)
- o identificador do seu telefone
- a placa de um veículo

https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_pt#exemplos-de-dados-no-considerados-pessoais

PORTAL DO TREINAMENTO!

TIPO DE DADOS PESSOAIS

Dados pessoais diretos

Dados que podem ser atribuídos diretamente a uma pessoa física específica sem o uso de informações adicionais

Dados pessoais indiretos

Dados que podem ou poderão vir a ser vinculados a uma pessoa física específica utilizando-se informações adicionais.

ANONIMIZAÇÃO & PSEUDONIMIZAÇÃO

Anonimização

"Utilização de meios técnicos razoáveis e disponíveis no momento do processamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo"

(Considerando 26 – não aplicação GDPR)

ID	Nome	Gênero	Nascimento	email	Partido
1	João Silva	Masculino	1959	joao@email	A
2	José Souza	Masculino	1965	jose@email	A
3	Maria Costa	Feminino	1973	maria@email	B
4	Mario Melo	Masculino	1964	mario@email	A
5	Lucia Maria	Feminino	1975	lucia@email	B

Fonte: Prof. Daniel Carnauba

Exemplo Dado Anonimizado

ID	Nome	Gênero	Nascimento	Partido
xxxxxx	xxxxxxx	Masculino	1959-1970	A

Quantidade Pessoas	Gênero	Nascimento	Partido
3	Masculino	1959 - 1970	A

Fonte: Prof. Daniel Carnauba

https://www.youtube.com/watch?v=DEdwRRMIE2g

Orientação do Information Commissioner’s Officer (ICO) - Reino Unido:

É sugerida a contratação de terceiros para testar a qualidade do processo de anonimização, por meio testes que busquem reidentificar os dados.

ANONIMIZAÇÃO & PSEUDONIMIZAÇÃO

Pseudonimização

Artigo 4º, 5 - "processamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular dos dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa física identificada ou identificável"

Dados pessoais pseudonimizados

Dados pessoais que passaram por processamento de pseudonimização, deixando de ser identificável diretamente

Exemplo PseudoAnonimizado

Nome	E-mail	Referência	Gênero	Idade
Daniel	Daniel@email	1234	Masculino	50

Nome	E-mail	Referência	Referência	Gênero	Idade
Daniel	Daniel@email	1234	1234	Masculino	50

Fonte: Prof. Daniel Carnauba

DADOS ESPECIAIS OU DADOS SENSÍVEIS

O GDPR define no Artigo 9º, 1 atenção especial a questão de processamento de certas categorias de dados pessoais. Sendo proibido o processamento destas categorias sem base legal.

O tema primordial sobre esta proteção é o possível uso em discriminação .

- Merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais

DADOS ESPECIAIS OU DADOS SENSÍVEIS

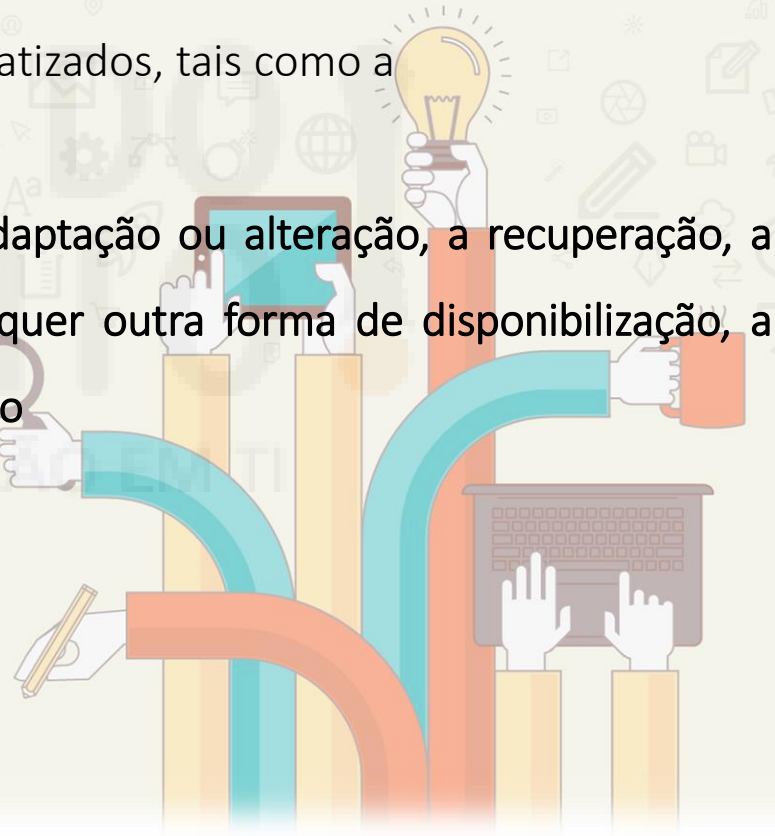
- origem racial ou étnica,
- opiniões políticas,
- convicções religiosas ou filosóficas,
- filiação sindical,
- dados genéticos,
- dados biométricos ,
- dados relativos à saúde
- dados relativos à vida sexual
- orientação sexual de uma pessoa.

PORTAL DO TREINAMENTO!

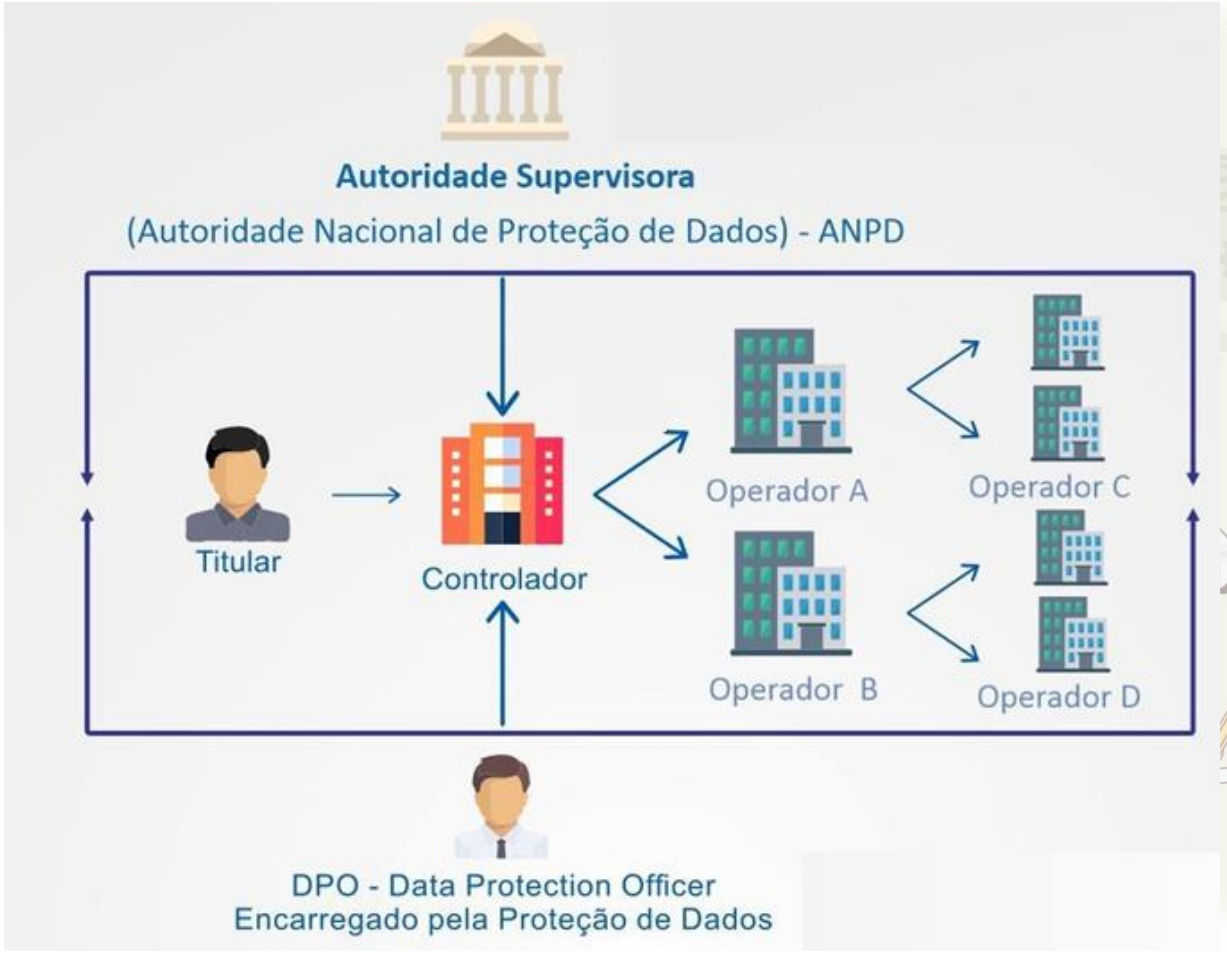
PROCESSAMENTO

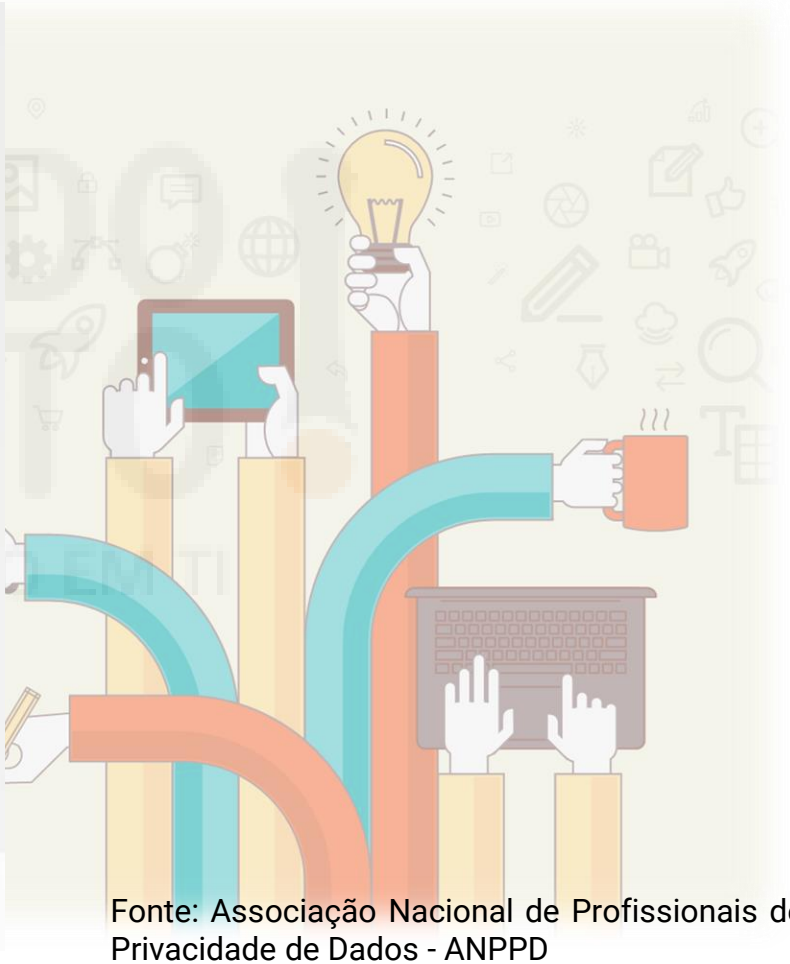
Artigo 4º, 2 - “uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a

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



PROCESSAMENTO





Fonte: Associação Nacional de Profissionais de Privacidade de Dados - ANPPD

PROCESSAMENTO

PORTAL DO TREINAMENTO!

CONTROLADOR/RESPONSÁVEL PELO TRATAMENTO

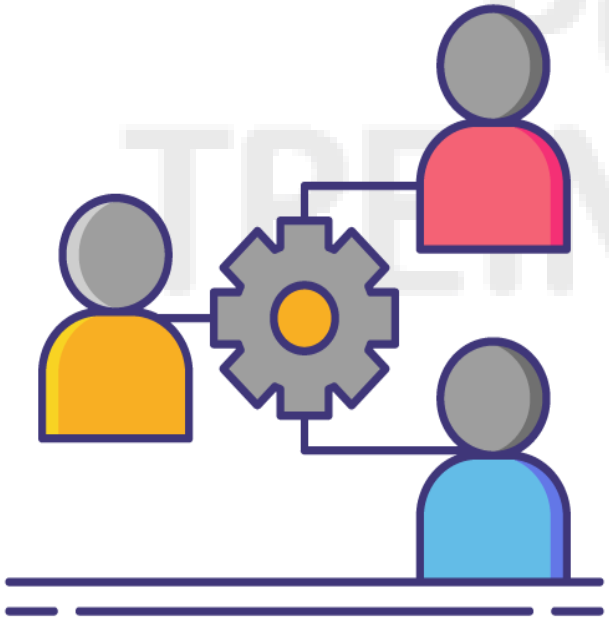
Uma pessoa física ou jurídica, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de processamento de dados pessoais.
(Responsável pelo tratamento)

Responsabilidades

- ✓ Determinar as finalidades e os meios de processamento de dados pessoais
- ✓ Implementar medidas técnicas e organizacionais apropriadas para cumprir o GDPR, incluindo políticas apropriadas de proteção de dados.
- ✓ Comprovar adequação

PROCESSADOR / SUBCONTRATANTE

Pessoa física ou jurídica, a autoridade pública, agência ou outro organismo que trate os dados pessoais em nome do controlador.
(Subcontratante)



Um processador sempre age “em nome do controlador”, devendo cumprir as instruções do controlador.

DATA PROTECTION OFFICER

Pessoa que tem a tarefa formal de garantir que a organização esteja ciente e cumpra suas responsabilidades e obrigações de proteção de dados de acordo com o GDPR e as leis do Estado-Membro.
(Encarregado da proteção de dados)

Conforme o Artigo 37º, 5 , O encarregado da proteção de dados é designado com base nas suas qualidades profissionais e, em especial, nos seus conhecimentos especializados no domínio do direito e das práticas de proteção de dados.

DATA PROTECTION OFFICER - DESIGNAÇÃO

Artigo 37º, 1 - Um DPO é designado sempre que:

- O processamento for efetuado por uma autoridade ou um organismo público, excetuando os tribunais no exercício da sua função jurisdicional;

- As atividades principais do controlador ou processador consistam em operações de processamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala; ou

- As atividades principais do responsável pelo processamento ou do subcontratante consistam em operações de processamento em grande escala de categorias especiais de dados nos termos do artigo 9.o e de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10.o.

DATA PROTECTION OFFICER - DESIGNAÇÃO

O encarregado da proteção de dados pode ser um elemento do pessoal da entidade responsável pelo tratamento ou do subcontratante, ou exercer as suas funções com base num contrato de prestação de serviços.

O responsável pelo tratamento ou o subcontratante publica os contatos do encarregado da proteção de dados e comunica-os à autoridade de controlo.

DATA PROTECTION OFFICER - POSIÇÃO

Artigo 38º, 1 a 3 - O controlador e o processador asseguram que :

DPO seja envolvido, de forma adequada e em tempo útil, a todas as questões relacionadas com a proteção de dados pessoais

Apoiam o DPO no exercício das funções, fornecendo-lhe os recursos necessários ao desempenho dessas funções e à manutenção dos seus conhecimentos, bem como dando-lhe acesso aos dados pessoais e às operações de processamento

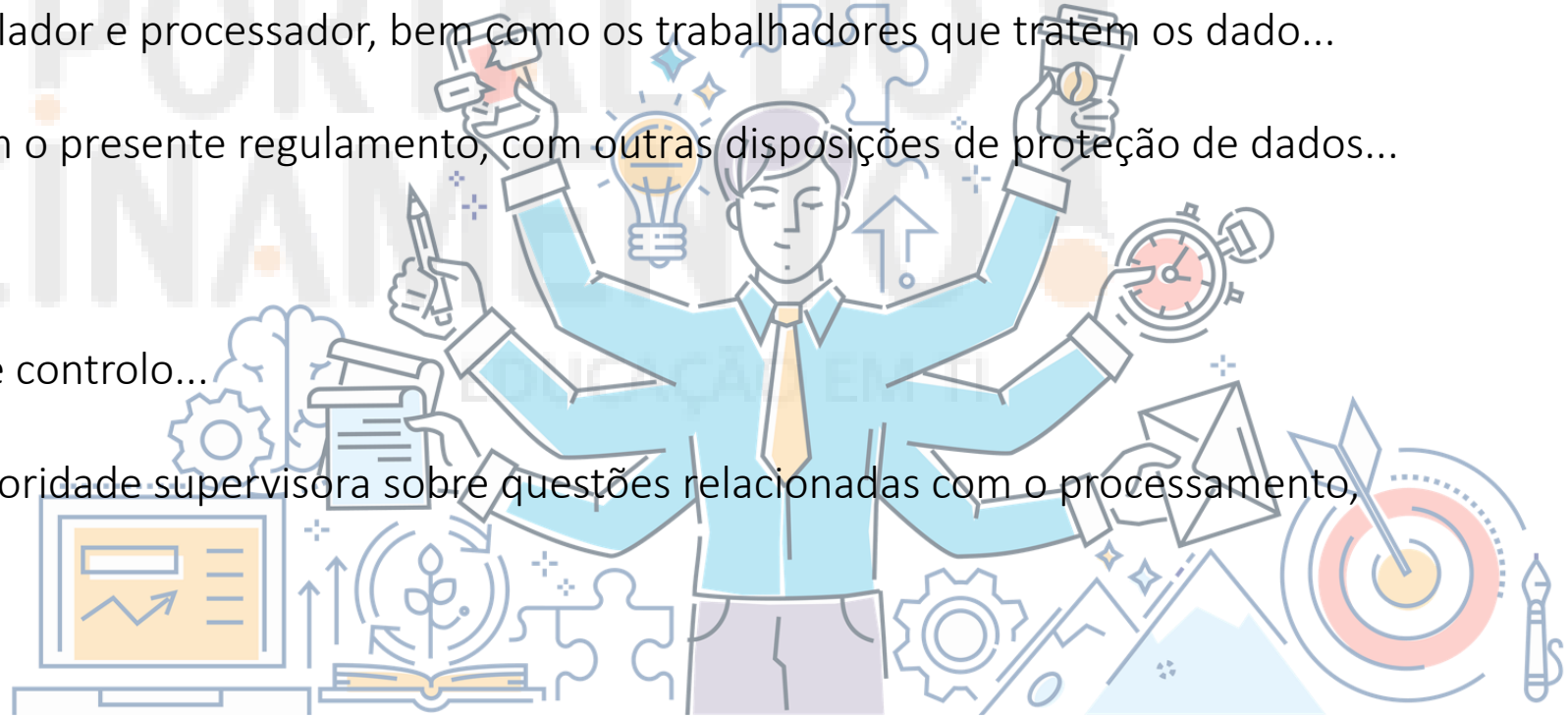
o DPO não receba instruções relativamente ao exercício das suas funções. O DPO não pode ser destituído nem penalizado pelo controlador ou processador pelo fato de exercer as suas funções. O DPO responde diretamente a direção ao mais alto nível do controlador ou processador

PORTAL DO TREINAMENTO!

DATA PROTECTION OFFICER – TAREFAS

Artigo 39º, 1 : O DPO tem, pelo menos, as seguintes funções:

- Informa e aconselha o controlador e processador, bem como os trabalhadores que tratem os dado...
- Controla a conformidade com o presente regulamento, com outras disposições de proteção de dados...
- Presta aconselhamento...
- Coopera com a autoridade de controlo...
- Ponto de contacto para a autoridade supervisora sobre questões relacionadas com o processamento, incluindo a consulta



Procuradoria do RJ cria o cargo de encarregado

31 DE JULHO DE 2020

Tratamento de Dados Pessoais

Foi publicada, no Diário Oficial desta sexta-feira (31), a Resolução PGE nº 4.586, que criou, no âmbito da Procuradoria-Geral do Estado, a função de Encarregado pelo Tratamento de Dados Pessoais (DPO) - vinculada diretamente ao Gabinete do Procurador-Geral.
O Encarregado pelo Tratamento de Dados Pessoais (DPO) terá a missão de atuar como canal de comunicação entre o controlador, titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD) e de orientar os Procuradores do Estado, servidores e demais colaboradores da PGE-RJ sobre as práticas relativas à proteção de dados. O Encarregado também integrará o Comitê de Tecnologia da Informação e Comunicação, criado pela resolução PGE nº 3.859, de15 de março de 2016.

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES

PORTARIA Nº 1197, DE 25 DE AGOSTO DE 2020

Atribui à Assessoria de Relações com os Usuários (ARU) o exercício das atividades de Encarregado pelo Tratamento de Dados Pessoais no âmbito da Agência Nacional de Telecomunicações e dá outras providências.

O PRESIDENTE DA AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES, no uso das atribuições que lhe foram conferidas pelo art. 135 do Regimento Interno da Anatel, aprovado pela Resolução nº 612, de 29 de abril de 2013, e

CONSIDERANDO as disposições constantes na Lei nº 13.709, de 14 de agosto de 2018;

CONSIDERANDO as razões e os fundamentos do Informe nº Nº 14/2020/SUE;

CONSIDERANDO o constante dos autos do processo nº 53500.001165/2020-86,

RESOLVE:

Art. 1º Atribuir à Assessoria de Relações com os Usuários (ARU) as competências institucionais relativas ao exercício das atividades de Encarregado pelo tratamento de dados pessoais no âmbito da Agência Nacional de Telecomunicações, nos termos da Lei nº 13.709, de 14 de agosto de 2018.

Art. 2º Designar o Chefe da Assessoria de Relações com os Usuários (ARU) como Encarregado pelo tratamento de dados pessoais da Anatel para o exercício das seguintes atribuições:

I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II - receber comunicações da Autoridade Nacional e adotar providências;

III- orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;

IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

ANS nomeia encarregado para tratamento de dados pessoais

por Time BL Consultoria / LGPD, Noticias sobre Direito Digital, Proteção de Dados / 12/08/2020

Compartilhe!

A Agência Nacional de Saúde Suplementar (ANS) nomeou na última segunda-feira (10/08) seu **encarregado para tratamento e proteção de dados pessoais** colhidos pelo órgão. O **DPO** (Data Protection Officer, na sigla em inglês) é uma das figuras mais importantes na estrutura de governança da proteção de dados. Na ANS, órgão que é responsável pela regulação, normatização, controle e fiscalização das atividades relativas à assistência privada à saúde, quem assumirá a função é o servidor Luiz Gustavo Meira Homrich.

https://blconsultoriadigital.com.br/ans-encarregado-dados-pessoais/#:~:text=A%20Ag%C3%AAncia%20Nacional%20de%20Sa%C3%BAde,governan%C3%A7a%20da%20prote%C3%A7%C3%A3o%20de%20dados.

Andrea Mattos integra a recém-criada área de compliance da **Vivo** desde agosto de 2019. Mas sua trajetória na empresa começou em 2002, na área jurídica da Telefônica Brasil. Agora, como Diretora de Compliance e DPO, Mattos atua em um projeto multidisciplinar preparatório na companhia, como parte do processo de adequação à LGPD.

Carreira DPO: https://www.youtube.com/watch?v=OjR7sfcWjdY&t=1185s

Exemplos:
https://portal.fgv.br/en/personal-data-protection
https://www.pwc.de/en/privacy-policy.html
https://www.oracle.com/legal/privacy/privacy-policy.html
https://www.basf.com/global/en/legal/data-protection.html

Outros exemplos

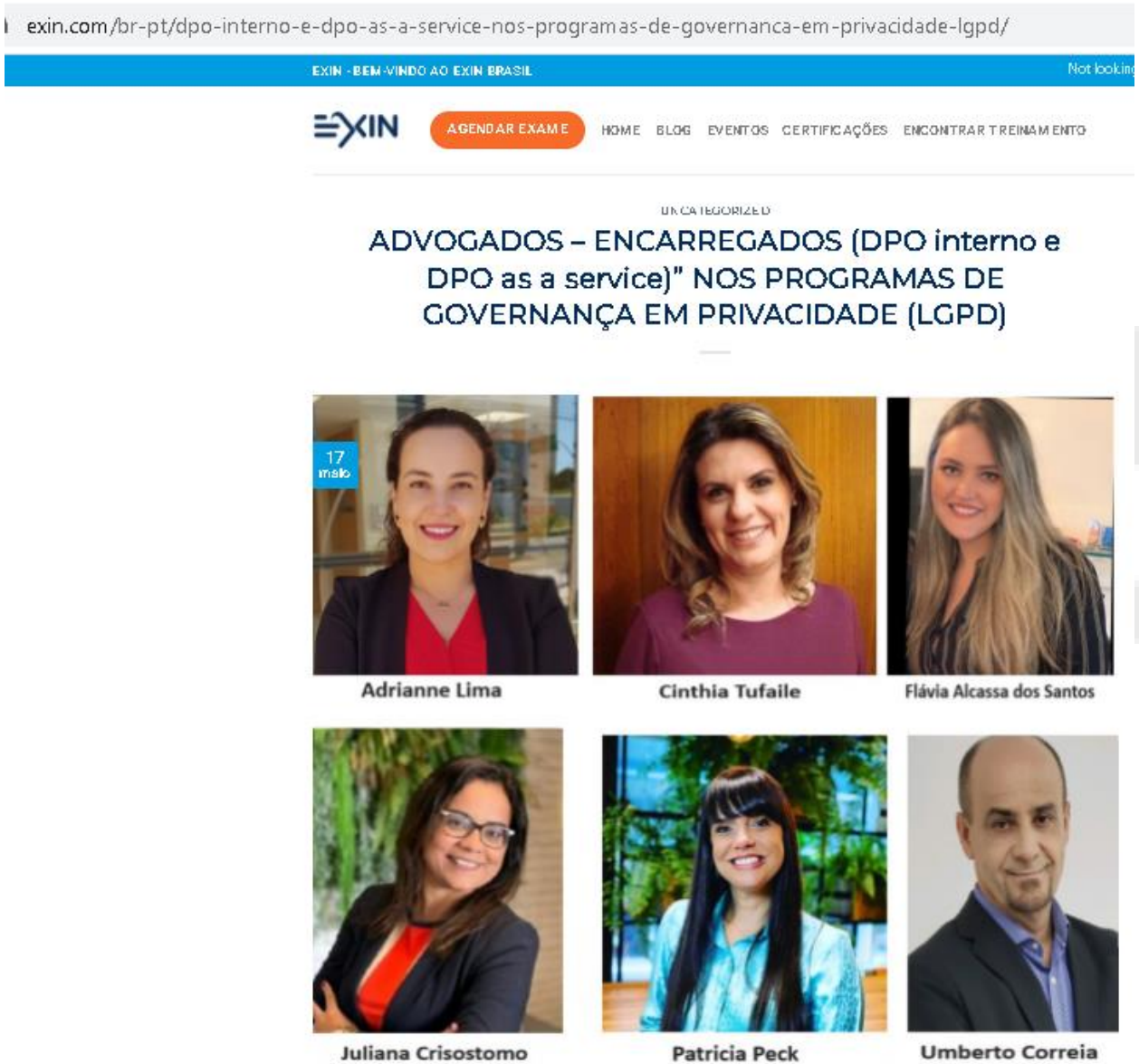
- ✓ **Encarregado interno**: auxiliará a empresa no projeto de adequação, constituição do grupo de trabalho e acompanhamento do programa de governança em privacidade.

  Também pode ser a pessoa responsável pelo tratamento de respostas às solicitações que virão da ANPD, de titulares e operadores.

- ✓ **Terceirização ou *DPO as a Service*:** é a terceirização do trabalho, sendo apontada uma pessoa externa para atuar como encarregada perante a ANPD e os titulares dos dados pessoais. A prestação desse serviço pode compreender atividades diversas dentro do programa de governança em privacidade (art. 50, I, LGPD).

- ✓ **Terceirização de parte do trabalho, para apoio ao Encarregado**: auxiliará o Encarregado, atuando em complemento, seja para responder os titulares, para emitir pareceres, apoiá-lo na implementação do programa de governança em privacidade.

DPO interno ou DPO as a service (terceirizado)



DPO INTERNO E DPO *AS A SERVICE*

Se a LGPD obriga as empresas a indicarem um DPO, alguns questionamentos podem ser levantados sobre esse novo cargo:

– O DPO deve ser um colaborador da empresa ou profissional externo?

– Pode ser pessoa jurídica ou somente pessoa física?

– Se for funcionário da empresa, pode acumular funções?

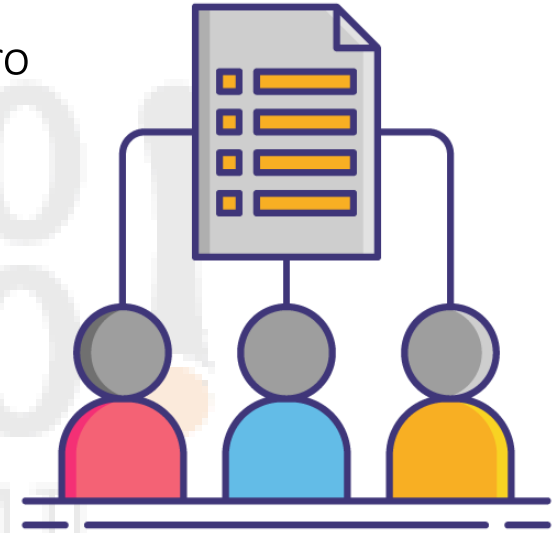
– A quem ele se reporta?

https://www.exin.com/br-pt/dpo-interno-e-dpo-as-a-service-nos-programas-de-governanca-em-privacidade-lgpd/

DESTINATÁRIO & TERCEIRO

Destinatário

uma pessoa física ou jurídica, autoridade pública, agência ou outro organismo para a qual os dados pessoais são divulgados.



Terceiro

Um terceiro é uma pessoa sem motivos legítimos específicos ou autorização para processar dados pessoais. Em outras palavras, um terceiro é uma pessoa que originalmente não deveria processar dados pessoais. No entanto, um terceiro que receber dados pessoais - legal ou ilegalmente - será, em princípio, um novo controlador (desde que esteja sob o GDPR).

AUTORIDADE SUPERVISORA

Uma autoridade pública independente criada por um Estado-Membro

Responsabilidades

- ✓ Fiscalização da aplicação do presente regulamento
- ✓ Defender os direitos e liberdades fundamentais das pessoas físicas relativamente ao processamento
- ✓ Facilitar a livre circulação dados pessoais na União

Exercício

Alguns processamentos de dados estão fora do escopo material do GDPR.

Que tipo de processamento não está sujeito ao GDPR?

a. Coleta de informações de nome e endereço para um clube de ginástica
b. Criação de um backup de dados biométricos para fins de segurança dos dados
c. Edição de fotografias pessoais antes de imprimi-las em casa

Exercício

Os dados pessoais, de acordo com a definição no GDPR, podem ser divididos em vários tipos. Um desses tipos é descrito do seguinte modo:

Dados que revelem direta ou indiretamente as origens raciais ou étnicas de uma pessoa, suas visões políticas, filosóficas ou religiosas, afiliação sindical e dados relacionados à saúde, vida sexual ou orientação sexual.

Que categoria de dados pessoais é esta?

a. Dados pessoais diretos
b. Dados pessoais indiretos
c. Dados pseudonimizados
d. Dados pessoais de categoria especial 

Exercício

Uma pessoa física ou jurídica, autoridade pública, agência ou outro organismo que, isoladamente ou em conjunto com outras partes, determina os objetivos e os meios de processamento de dados pessoais.

Que papel na proteção de dados é definido aqui?

A) Controlador 

B) Processador

C) Autoridade supervisora

D) Terceiro

PORTAL DO TREINAMENTO!

Exercício

De acordo com o General Data Protection Regulation, que categoria de dados pessoais é considerada como dados sensíveis?

A) Detalhes do cartão de crédito

B) Associação sindical 

C) Número do passaporte

D) Número do CPF

Exercício

De acordo com o General Data Protection Regulation (GDPR), qual é a definição de "processamento" de dados pessoais?

A) Qualquer operação que possa ser realizada com dados pessoais 

B) Qualquer operação que possa ser realizada com dados pessoais, exceto exclusão e destruição

C) Apenas operações nas quais os dados sejam compartilhados em mídias sociais ou transferidos por e-mail ou de outro modo pela internet

D) Apenas operações nas quais os dados pessoais sejam usados para as finalidades para as quais foram coletados

1.3 PROCESSAMENTO DE DADOS PESSOAIS

PORTAL DO TREINAMENTO!

PRINCÍPIOS - PROCESSAMENTO DE DADOS PESSOAIS

Legalidade, Justiça e Transparência	O titular dos dados pode perguntar como seus dados são processados, se não estiver claro para eles.
Limitação de Finalidades	Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser processados posteriormente de uma forma incompatível com essas finalidades. Exceção : processamento posterior é permitido para: • fins de arquivamento de interesse público, • pesquisa científica ou histórica ou • fins estatísticos,
Minimização de dados	Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são processados

PORTAL DO TREINAMENTO!

PRINCÍPIOS - PROCESSAMENTO DE DADOS PESSOAIS

Exatidão de Dados	Exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são processados, sejam apagados ou retificados sem demora
Limitação de Tempo de Armazenamento	Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são processados;
Integridade e confidencialidade	processados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu processamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas

Prestação de contas : Controlador e processador são responsáveis pelo cumprimento dos princípios e tem de poder comprová-lo

PORTAL DO TREINAMENTO!

Exercício

De acordo com o princípio de limitação de finalidade, os dados não devem ser processados além do objetivo legítimo definido. Contudo, o processamento adicional é permitido em alguns casos específicos, desde que sejam adotadas salvaguardas apropriadas aos direitos e liberdades dos titulares dos dados.

Para qual finalidade o processamento adicional **não** é permitido?

a. Para fins de arquivamento por interesse público
b. Para fins comerciais e de marketing direto 
c. Para fins estatísticos em geral
d. Para fins de pesquisa histórica ou científica

1.4 FUNDAMENTOS LEGÍTIMOS E LIMITAÇÃO DE PROPÓSITO

PORTAL DO TREINAMENTO!

BASES LEGAIS

Artigo 6º , 1

O processamento só é lícito se for verificada pelo menos uma das seguintes situações:

- ✓ Consentimento
- ✓ Cumprimento de um contrato
- ✓ Cumprimento de uma obrigação jurídica
- ✓ Defesa de interesses vitais do titular dos dados
- ✓ Exercício de funções de interesse público
- ✓ Legítimo Interesse

PORTAL DO TREINAMENTO!

BASES LEGAIS

Empresa processou dados pessoais sem base legal suficiente. O titular dos dados recebeu várias centenas de chamadas e mensagens SMS não solicitadas.

€ 9,5M

GERMANY	The Federal Commissioner for Data Protection and Freedom of Information (BfDI)	2019-12-09	9,550,000	Telecoms provider (1&1 Telecom GmbH)	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	The Controller is a company offering telecommunication services. A caller could obtain extensive information on personal customer

PORTAL DO TREINAMENTO!

BASES LEGAIS

O banco manteve os dados pessoais de um titular dos dados durante vários anos, mesmo depois de o titular dos dados deixar de ser um cliente. Os dados também estavam acessíveis aos funcionários do banco durante esse período. Isso constituiu uma **violação do princípio da limitação da finalidade**.

€ 50K

SPAIN	Spanish Data Protection Authority (aepd)	2020-08-28	50,000	Bankia S.A.	Art. 5 (1) b) GDPR	Non-compliance with general data processing principles	The bank kept personal data of a data subject for several years, even after the data subject was no longer a customer. The data was also accessible to

BASES LEGAIS

PORTAL DO TREINAMENTO!

BASES LEGAIS

Google – €50M – **Coleta de dados sem autorização**

Google emitiu um comunicado sobre as mudanças em suas políticas de privacidade e proteção de dados para se adequar ao GDPR e até criou uma página para esclarecer dúvidas sobre a relação com a legislação europeia. Porém, mesmo assim, a companhia acabou descumprindo regras da diretiva e foi severamente punida por isso.

De acordo com as autoridades, a gigante das buscas **foi denunciada por coletar dados dos celulares conectados em suas contas sem a autorização dos usuários franceses**. A prática acontecia porque o Google não indicava de forma clara que os dados estavam sendo recolhidos nem como desabilitar a captação.
Além disso, o Google já tinha sido denunciado por sete países da União Europeia por recolher dados sobre a localização dos seus usuários mesmo quando o GPS de seus smartphones estava desligado.

CONSENTIMENTO DE CRIANÇAS

Artigo 8º, 1 :

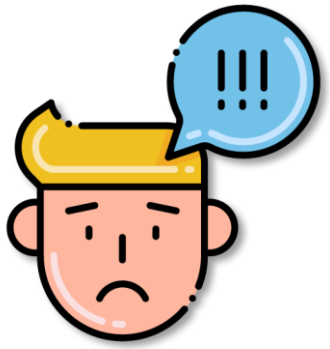
... Caso a criança tenha menos de 16 anos, o processamento só é lícito se e na medida em que o consentimento seja dado ou autorizado pelos titulares das responsabilidades parentais da criança...

LIMITAÇÃO DE FINALIDADE

Artigo 5º, 1, b

Dados pessoais são : Coletados para finalidades determinadas, explícitas e legítimas e não podendo ser processados posteriormente de uma forma incompatível com essas finalidades.

Determinação da finalidade



- O Controlador deve considerar cuidadosamente qual a finalidade ou finalidades para as quais os dados pessoais serão usados e não pode coletar dados pessoais que não sejam necessários, adequados ou relevantes para a finalidade ou finalidades que se pretende servir.
- O objetivo ou determinação da finalidade deve ser definida e comunicada antes da coleta dos dados pessoais
- A determinação de finalidade deve ser apresentada de forma clara , direta e detalhada.

LIMITAÇÃO DE FINALIDADE

Explícitos

- Os dados pessoais devem ser coletados para fins explícitos. Os objetivos devem ser claramente revelados, explicados ou expressados de alguma forma inteligível.
- Deve ser claro e não deve deixar dúvidas ou dificuldades de compreensão.

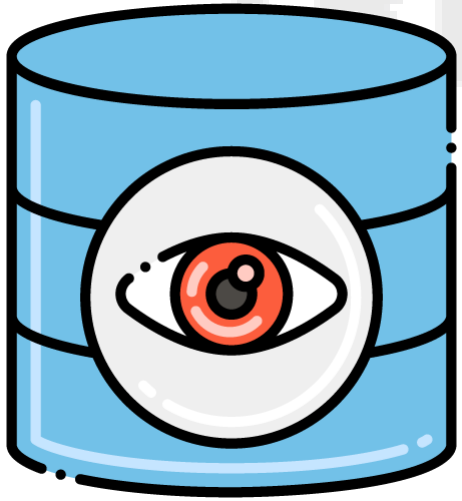
Legítimo

- As finalidades devem ser "conformes à lei" no sentido mais amplo. Incluindo todas as formas de lei escrita ,de legislação primária e secundária, decretos municipais, precedentes judiciais, princípios constitucionais, direitos fundamentais, e outros

PROPORCIONALIDADE E SUBSIDIARIEDADE

Proporcionalidade

Os dados pessoais coletados devem ser limitados ao necessário para atingir os objetivos, necessários no limite da sua relevância. Em nível prático, temos o princípio de minimização de dados: os dados pessoais devem ser adequados, relevantes e limitados ao necessário em relação às finalidades para os quais são processados.



Subsidiariedade

A coleta dos dados pessoais para processamento somente deverá ocorrer se não houver outros meios para alcançar o objetivo (menos invasivo).

PORTAL DO TREINAMENTO!

Exercício

O “consentimento livre e informado” é uma base legal para o processamento de dados pessoais de acordo com o GDPR. Deve-se documentar a finalidade do processamento para a qual o consentimento é fornecido.

A) Após a apresentação da especificação da finalidade e antes da coleta dos dados pessoais

B) Antes que a especificação do propósito seja concebida e apresentada
C) Antes do processamento dos dados pessoais
D) Antes da publicação ou disseminação dos dados pessoais

PORTAL DO TREINAMENTO!

Exercício

Quando os dados pessoais forem processados, a proporcionalidade e a subsidiariedade devem ser verificadas.

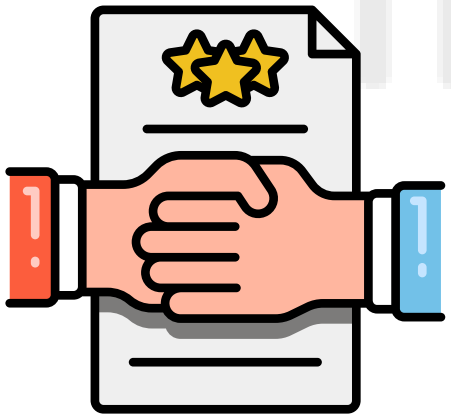
Qual é o requisito para o processamento dos dados pessoais?

A) Eles devem ser manipulados pelo menor número de funcionários possível, e estes devem trabalhar para o controlador ou uma afiliada.
B) Eles devem ser sempre limitados ao que for necessário para atingir os objetivos definidos e devem ser limitados aos dados menos “invasivos”.
C) Eles devem ser limitados a um tamanho de armazenamento predefinido e o sistema usado deve ser financiado pelo controlador.
D) Eles devem ser usados para o menor número de finalidades possível e isto não pode ser realizado fora das premissas do Processador.

1.5 DIREITOS DOS TITULARES DOS DADOS

INFORMAÇÃO TRANSPARENTE

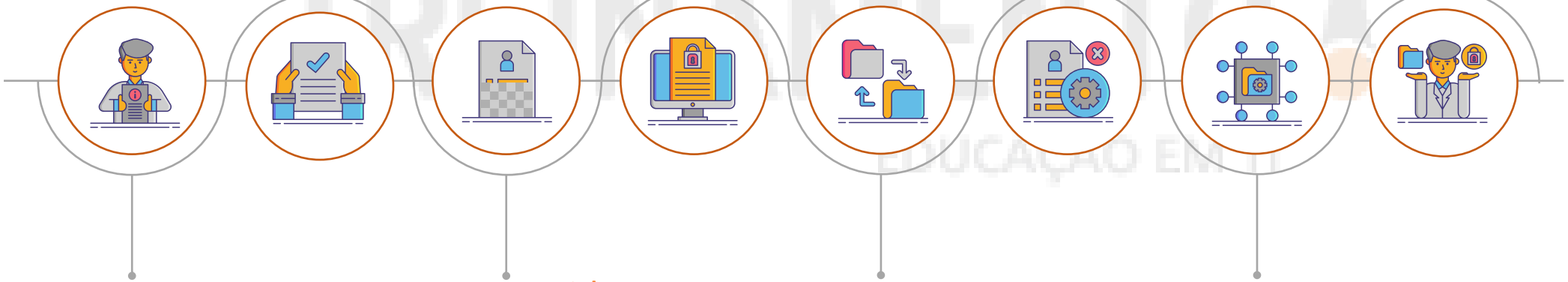
- O Controlador toma as medidas adequadas para fornecer ao titular as informações a respeito do processamento, de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples, em especial quando as informações são dirigidas especificamente a crianças



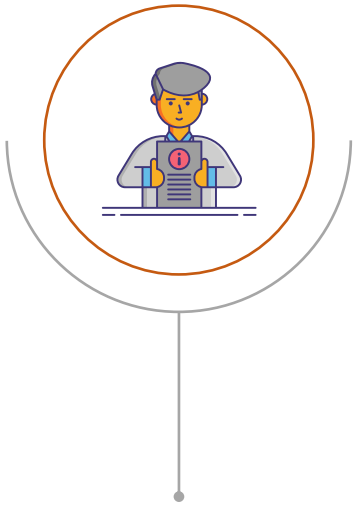
- As informações são prestadas por escrito ou por outros meios, incluindo, se for caso disso, por meios eletrônicos, ou oralmente
  - O controlador facilita o exercício dos direitos do titular dos dados e não pode recusar-se a dar seguimento ao pedido do titular

PORTAL DO TREINAMENTO!

DIREITOS DOS TITULARES DOS DADOS



DIREITOS DOS TITULARES DOS DADOS



Acesso

Artigo 15º, 1

O titular dos dados tem o direito de obter do responsável pelo processamento a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de processamento e, se for esse o caso, o direito de acessar os seus dados pessoais, bem como das seguintes informações

- A identidade e os contactos do Controlador
- Os contatos do DPO
- As finalidades do processamento
- Informa se o processamento se basear em “Legítimo Interesse”
- Os destinatários dos dados pessoais
- Se o controlador pretende transferir dados pessoais para um país terceiro
- Prazo de conservação dos dados pessoais
- Direitos do titular dos dados
- A existência de decisões automatizadas, incluindo a definição de perfis

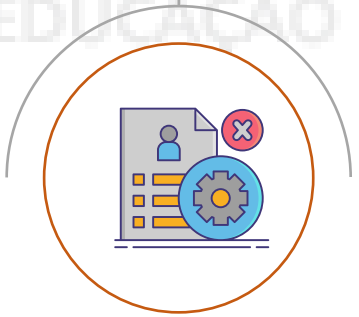
DIREITOS DOS TITULARES DOS DADOS

Retificação

Artigo 16º

O titular tem o direito de obter, sem demora injustificada, do controlador a retificação dos dados pessoais inexatos que lhe digam respeito. Tendo em conta as finalidades do processamento, o titular dos dados tem direito a que os seus dados pessoais incompletos sejam completados, incluindo por meio de uma declaração adicional.

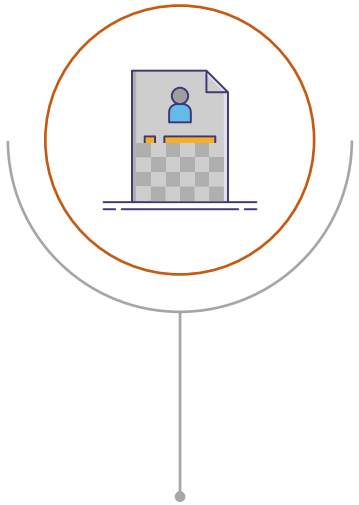
Oposição



Artigo 21º, 1

O titular dos dados tem o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao processamento dos dados pessoais que lhe digam respeito com base no interesse publico ou legítimo interesse, incluindo a definição de perfis com base nessas disposições.

DIREITOS DOS TITULARES DOS DADOS



Ser Esquecido

Artigo 17º, 1

O titular tem o direito de obter do controlador o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando se aplique um dos seguintes motivos:

- Os dados não são mais necessários para as finalidades de processamento
- Retirada do consentimento
- Os dados foram coletados para uma oferta de serviços de informação diretamente a uma criança menor de 16 anos.
- Objeções ao processamento
- processamento Ilegal
- Conformidade com a legislação da União ou do Estado-Membro aplicável ao controlador

O direito de apagar só tem efeito quando o motivo específico para o processamento for o consentimento

DIREITOS DOS TITULARES DOS DADOS

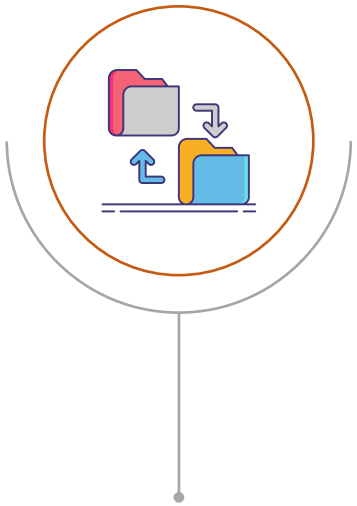
Limitação de processamento

Artigo 18º,1

O titular dos dados tem o direito de obter do controlador a limitação do processamento, se se aplicar uma das seguintes situações:

- A precisão dos dados é contestada pelo titular dos dados
- O processamento é ilegal e o titular dos dados se opõe ao processamento
- O controlador não precisa mais dos dados pessoais para fins de processamento, mas eles são exigidos pelo titular dos dados para o estabelecimento, exercício ou defesa de reivindicações legais
- O titular dos dados se opuser ao processamento nos termos do artigo 21 (1) (direito de objeção) enquanto se aguarda a verificação se os motivos legítimos do controlador substituem os do titular dos dados

DIREITOS DOS TITULARES DOS DADOS

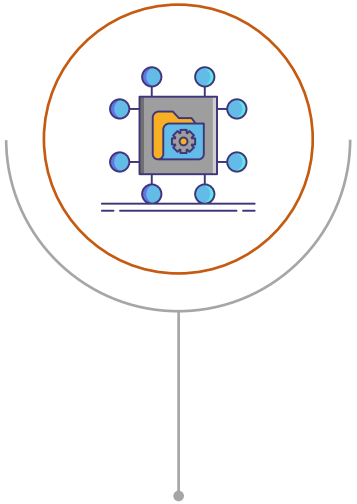


Portabilidade

Artigo 20º, 1

Se o processamento se basear no consentimento ou em um contrato, e o processamento é realizado por meios automatizados, o titular dos dados tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido a um controlador, em um formato estruturado, de uso corrente e de leitura automática, e o direito de transmitir esses dados a outro responsável pelo processamento sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir.

DIREITOS DOS TITULARES DOS DADOS

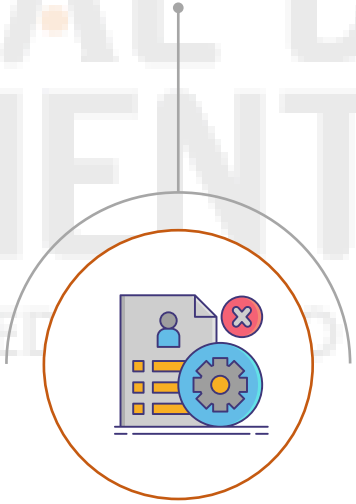


Não ficar sujeito a decisões automatizadas

Artigo 22º, 1

O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no processamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar.

Apresentar reclamação à Autoridade Supervisora



Artigo 77º, 1

Sem prejuízo de qualquer outra solução administrativa ou judicial, todos os titulares dos dados têm o direito de apresentar uma reclamação a uma autoridade supervisora e o titular dos dados considera que o processamento de dados pessoais que lhe digam respeito viola o presente regulamento.

PORTAL DO TREINAMENTO!

OBRIGAÇÃO DE NOTIFICAÇÃO

Artigo 19º : O responsável pelo processamento comunica a cada destinatário a quem os dados pessoais tenham sido transmitidos qualquer retificação ou apagamento dos dados pessoais ou limitação do processamento a que se tenha procedido em conformidade com o artigo 16.o, o artigo 17.o, n.o 1, e o artigo 18.o, salvo se tal comunicação se revelar impossível ou implicar um esforço desproporcionado. Se o titular dos dados o solicitar, o responsável pelo processamento fornece-lhe informações sobre os referidos destinatários.

A consequência disto é que , além de implementar sistemas e procedimentos para garantir os direitos do titular dos dados, os controladores precisam implementar sistemas e procedimentos para notificar terceiros afetados sobre o exercício desses direitos

PORTAL DO TREINAMENTO!

GRATUIDADE

Artigo 12º : Se os pedidos apresentados por um titular de dados forem manifestamente infundados ou excessivos, nomeadamente devido ao seu caráter repetitivo, o responsável pelo tratamento pode:

a) Exigir o pagamento de uma taxa razoável tendo em conta os custos administrativos do fornecimento das informações ou da comunicação, ou de tomada das medidas solicitadas; ou

b) Recusar-se a dar seguimento ao pedido.

Cabe ao responsável pelo tratamento demonstrar o caráter manifestamente infundado ou excessivo do pedido.

PORTAL DO TREINAMENTO!

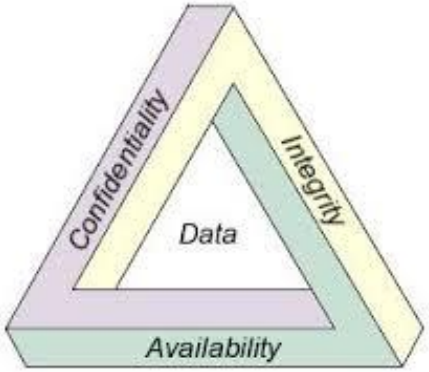
Exercício

Que direito do titular dos dados é definido pelo GDPR?

A) Uma cópia dos dados pessoais deve ser fornecida no formato solicitado pelo titular dos dados.
B) O acesso aos dados pessoais deve ser fornecido sem custo para o titular dos dados.
C) Os dados pessoais sempre devem ser alterados mediante solicitação do titular dos dados.
D) Os dados pessoais devem ser apagados sempre que isso for solicitado pelo titular dos dados.

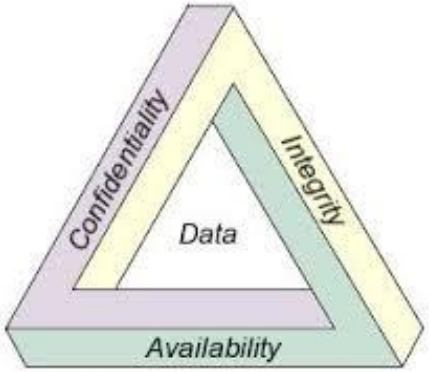
1.6 VIOLAÇÃO DE DADOS PESSOAIS

CRITÉRIOS DA SEGURANÇA DA INFORMAÇÃO



- Antes de implementar medidas de segurança/proteção de DPs, é necessária a análise do risco em específico
- Situações públicas atuais demonstram que é importante um programa voltado também para a continuidade do negócio (ou atividade pública)

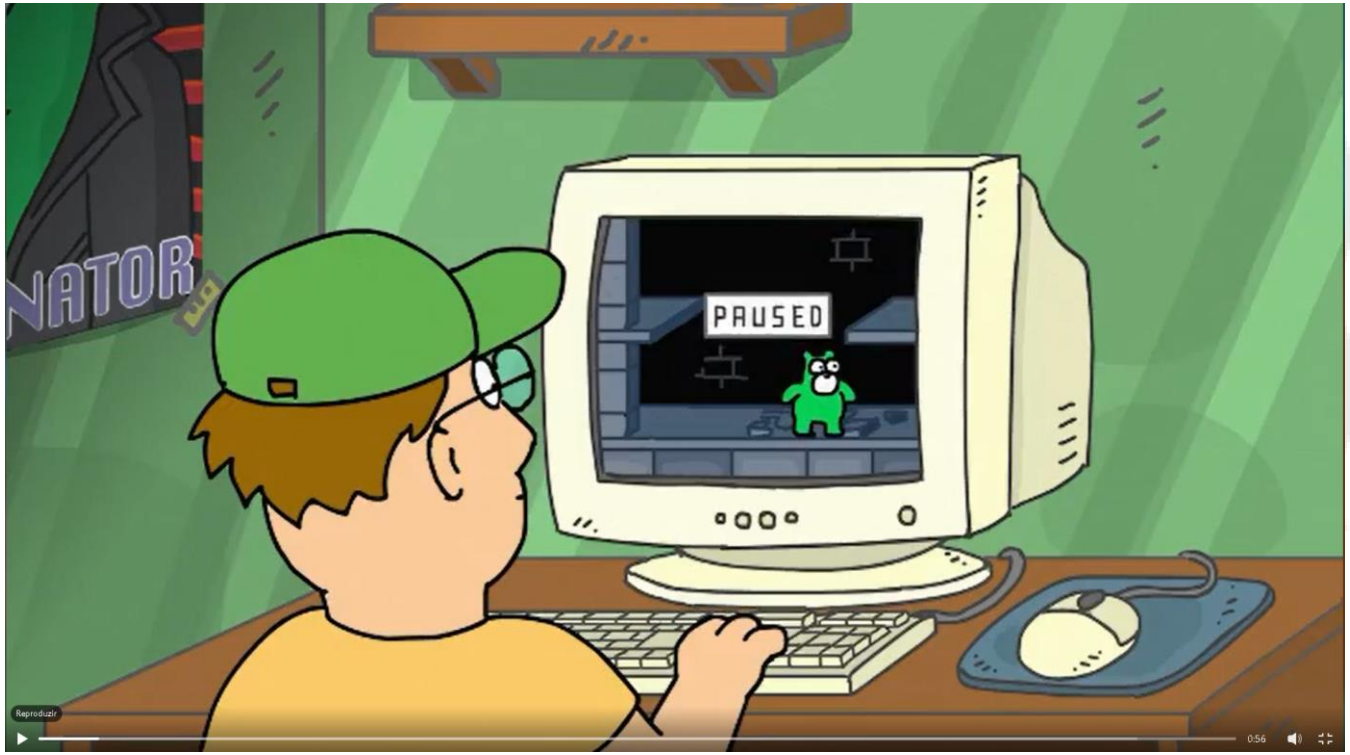
CRITÉRIOS DA SEGURANÇA DA INFORMAÇÃO



- Práticas adotadas pelas empresas: mitigar riscos à informação.
- A segurança da informação deve garantir a proteção da informação.
- A proteção da informação (Segurança da Informação) é dada por 3 critérios = CID: **confidencialidade** (ex: senha; armário com chave), **integridade** (ex: a informação deve ser exata; alteração de um arquivo quando houver permissão), **disponibilidade** (ex: acesso à informação quando necessária; a disponibilidade não é identificada quando o furto de um notebook impacta a impossibilidade de acesso à informação).

PORTAL DO TREINAMENTO!

EXEMPLOS DE SITUAÇÕES DE RISCO



https://www.linkedin.com/posts/adrianneclima_lgpd-consultoria-protecaodados-activity-6951529899056615424-yO5x?utm_source=share&utm_medium=member_desktop

Fazer avaliação e aplicar medidas PDRC da ISO 27001 etc:

- preventiva (ex. firewall)
- detectiva (físicas, técnicas e organizacionais. ex. softwares identificadores de invasão, IPS)
- repressiva (ex. fechar portas para não ir de um servidor para outro)
- corretiva (ex: o hacker já entrou, o que fazer para remediar / corrigir).

PORTAL DO TREINAMENTO!

Exemplo de análise de risco:

Risco: roubo da casa

Ativos (o que possui valor):

Vulnerabilidade (fraquezas):

Ameaça (quem pode explorar a vulnerabilidade):

Impactos:

Preventivas:

Detectivas:

Repressivas:

Corretivas:

Exemplo de análise de risco:

1) **Qual é o risco?** Ex. violação de proteção de determinados dados pessoais

2) **Ativos** (tudo que tem valor). Ex. dados pessoais em uma base armazenada

3) **Vulnerabilidades** (pontos fracos). Ex. Software desatualizado.

4) **Ameaças** (tudo que pode explorar uma vulnerabilidade). Ex. Hacker.

5) **Impactos** (consequências). Ex: Cópia, exclusão de banco de dados.

6) **PDRC. Preventivo**: implementar o firewall, softwares atualizados, políticas, treinamento, backup; **Detectivo:** IPS e outros softwares de alertas de acessos não autorizados; **Repressiva** : VLAN, software que interrompa as atividades, chamada de especialistas; **Corretiva** (como recupero): restauração do backup (*disaster recovery)*.

PORTAL DO TREINAMENTO!

POSSÍVEIS OPÇÕES PARA O TRATAMENTO DO RISCO:

- Aplicar os controles apropriados para reduzir os riscos
- Assumir o risco
- Evitar o risco ao decidir não iniciar ou continuar com a atividade que dá origem ao risco
- Compartilhar os riscos associados para outras partes

VIOLAÇÃO DE DADOS

Artigo 4º, 12

Violação de dados pessoais, uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de processamento.

Incidente de Segurança : pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação levando a perda de um ou mais princípios da Segurança da Informação como: Confidencialidade, Integridade, Disponibilidade e Autenticidade.

MEDIDAS PROTETIVAS

Artigo 32º, 1

Exige que controladores e processadores implementem medidas técnicas e organizacionais apropriadas para garantir um nível de segurança adequado ao risco.

PORTAL DO TREINAMENTO!

MEDIDAS PROTETIVAS

Este incidente envolveu em parte o tráfego de usuários para o site da British Airways sendo desviado para um site fraudulento. Por meio desse site falso, os detalhes do cliente foram coletados pelos invasores.

UNITED KINGDOM	Information Commissioner (ICO)	2019-07-08	204,600,000	British Airways	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	Please note: This fine is not final but will be decided on when the company and other involved supervisory authorities of other member states have made their

MEDIDAS PROTETIVAS

PORTAL DO TREINAMENTO!

MEDIDAS PROTETIVAS

Centro Hospitalar Barreiro - €400K

Hospital português recebeu notificações por utilizar os dados de forma inadequada. As multas totalizaram mais de 400 mil euros.

O que **foi reportado é que funcionários que não atuavam na área hospitalar usavam os dados de terceiros para conseguir acesso ao sistema**.

A suspeita surgiu porque **o hospital tinha 985 usuários registrados como médicos, mas apenas 296 médicos realmente trabalhando no local**.

- violação aos artigos 5º (1) f e 32 do GDPR, isto é, ao princípio da integridade e confidencialidade em virtude de não aplicação de medidas técnicas e organizativas tendentes a impedir o acesso indevido a dados pessoais.

MEDIDAS PROTETIVAS

THE NETHERLANDS	2019-06-18	460,000	Haga Hospital	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	link

	ETid-1050	ALEMANHA	2020	Valor da multa entre EUR 50 e EUR 100	Restaurante	Arte. 32 GDPR	Medidas técnicas e organizacionais insuficientes para garantir a segurança da informação	link

Autoridade Autoridade de Proteção de Dados de Hamburgo

Setor Hospedagem e Hospitalidade

Resumo Para combater a pandemia de Covid 19, um restaurante divulgou uma lista aberta na qual os visitantes tinham que inserir seus dados de contato. O fato de a lista ter sido exibida abertamente permitiria que terceiros não autorizados tivessem acesso aos dados.

MEDIDAS PROTETIVAS

Vueling- €30K

A Autoridade da Espanha aplicou multa à companhia aérea, que não disponibilizava em seu site um painel para configuração de cookies

Há, simplesmente, a mensagem: "ao visitar o site, concorda com os cookies".

Exercício

Uma violação da segurança que provoque a destruição, perda, alteração, divulgação não autorizada ou acesso acidental ou ilegal de dados pessoais transmitidos, armazenados ou processados de outro modo.

Qual é o termo exato associado a esta definição no GDPR?

a. Violação da confidencialidade
b. Violação de dados pessoais 
c. Violação de segurança
d. Incidente de segurança

NOTIFICAÇÃO DE VIOLAÇÃO DE DADOS PESSOAIS

Autoridade Supervisora

Artigo 33º, 1 : Em caso de violação de dados pessoais, o controlador notifica a autoridade supervisora competente, sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma.

Se a notificação à autoridade supervisora não for efetuada no prazo de 72 horas, deve ser acompanhada dos motivos do atraso.

Exceção :

A menos que a violação dos dados pessoais não seja suscetível de resultar em um risco para os direitos e liberdades das pessoas físicas.

NOTIFICAÇÃO DE VIOLAÇÃO DE DADOS PESSOAIS

ao Controlador

Artigo 33º, 2

O processador notifica o controlador sem demora injustificada após ter conhecimento de uma violação de dados pessoais.

Sendo esta a única obrigação de notificação ou relatório sob o GDPR devida ao processador. Cabe ao controlador todas as outras notificações e relatórios.

NOTIFICAÇÃO DE VIOLAÇÃO DE DADOS PESSOAIS

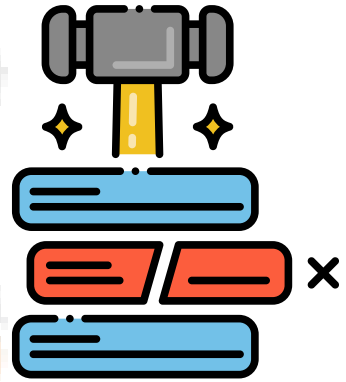
ao Titular dos Dados

Artigo 34º, 1 : Quando a violação dos dados pessoais for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas físicas, o controlador comunica a violação de dados pessoais ao titular dos dados sem demora injustificada.

NOTIFICAÇÃO DE VIOLAÇÃO DE DADOS PESSOAIS

Exceções :

Artigo 34º, 1 : A comunicação ao titular dos dados não é exigida se for preenchida uma das seguintes condições:

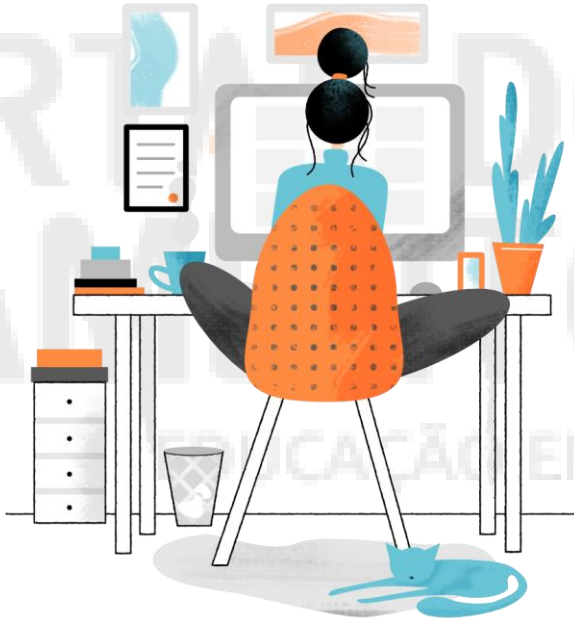


- O controlador tiver aplicado medidas de proteção adequadas, tanto técnicas como organizacionais, especialmente medidas que tornem os dados pessoais incompreensíveis para qualquer pessoa não autorizada a aceder a esses dados, por exemplo criptografia

- O controlador tiver tomado medidas subsequentes que assegurem que o elevado risco para os direitos e liberdades dos titulares dos dados já não é suscetível de se concretizar. Medidas de mitigação do risco

- Implicar um esforço desproporcional. Nesse caso, é feita uma comunicação pública ou tomada uma medida semelhante

EXERCÍCIOS



Exercício

Ocorreu uma violação de segurança em um sistema de informação que também contém dados pessoais. De acordo com o GDPR, qual é a primeira coisa que o controlador deve fazer?

a. Verificar se a violação pode ter provocado a perda ou o processamento ilegal de dados pessoais
b. Fazer uma Avaliação de Impacto sobre a Proteção de Dados (DPIA)
c. Determinar se dados pessoais de caráter sensível foram ou possam ter sido processados ilegalmente
d. Relatar a violação imediatamente a todos os titulares dos dados e à autoridade supervisora relevante

Exercício

Privacidade e a proteção de dados estão relacionadas . Como isto ocorre ?

a. A proteção de dados decorre da privacidade
b. Você não pode ter privacidade sem proteção de dados 
c. A privacidade sempre decorre da proteção de dados
d. São a mesma coisa

PORTAL DO TREINAMENTO!

Exercício

Determino as finalidades e os meios de processamento de dados pessoais.

A quem a afirmação acima se refere?

a. Autoridade Supervisora
b. Estado membro da UE
c. Controlador 
d. Encarregado

Exercício

Diretiva que foi substituída pelo GDPR.

a. 95/46 / CE 
b. DUDH
c. 47/95 / CE
d. CEDH/47

Exercício

Qual é a definição de dados pessoais conforme o GDPR ?

a. Qualquer informação que os residentes na Europa precisem proteger.
b. Dados que de alguma forma revelem origens raciais ou étnicas, convicções religiosas, dados relacionados à saúde e hábitos sexuais.
c. Preservação da confidencialidade, integridade e disponibilidade das informações.
d. Qualquer informação relativa a uma pessoa física identificada ou identificável.

Exercício

O objetivo primeiro do GDPR é ?

a. Fazer com que países não pertencentes a UE respeitem o direito à privacidade dos indivíduos em todo o mundo.
b. Fazer da privacidade um direito humano fundamental para todos.
c. Fortalecer e unificar a proteção de dados para indivíduos na UE.
d. Ser uma base comum sobre a qual os estados membros possam criar suas próprias leis.

Exercício

Leia a seguinte afirmação: “O presente regulamento aplica-se ao processamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo processamento (Controlador) ou de um subcontratante (Processador) situado no território da União, quando o processamento ocorrer somente dentro da União”. É verdadeira ou falsa?

a. Verdadeiro
b. Falso 

PORTAL DO TREINAMENTO!

Exercício

Quais dos abaixo não são dados pessoais conforme o GDPR?

a. Dados pseudonimizados
b. Nome
c. Dados especiais
d. Dados Anonimizados 

Exercício

A coleta, armazenamento, modificação, divulgação ou disseminação ilegal de dados pessoais constitui uma ofensa de acordo com a lei europeia.

Que tipo de ofensa é essa?

a. Uma ofensa relacionada ao conteúdo
b. Uma ofensa econômica
c. Uma ofensa à propriedade intelectual
d. Uma ofensa à privacidade 

2. ORGANIZANDO A PROTEÇÃO DE DADOS

2. ORGANIZANDO A PROTEÇÃO DE DADOS

Conteúdo

- Importância da proteção de dados para a organização
- Autoridade supervisora
- Transferência de dados pessoais transfronteiriços
- Regras corporativas vinculantes
- Proteção de dados em contratos

2.1 IMPORTÂNCIA DA PROTEÇÃO DE DADOS PARA A ORGANIZAÇÃO

IMPORTÂNCIA

Mais que uma questão de cumprimento de lei, ou de evitar multas , a proteção de dados ao tratar dados pessoais protege a imagem da organização .

O processamento de dados pessoais de maneira profissional garante qualidade, a gestão da segurança e governança.

REQUISITOS À CUMPRIR COM O GDPR

Princípios

- O objetivo deve ser claro, detalhado e especificado, e se enquadrar em pelo menos uma das seis bases legais
- Os direitos do titular dos dados devem ser garantidos e medidas adequadas de proteção de dados devem estar ativas .

PORTAL DO TREINAMENTO!

REQUISITOS À CUMPRIR COM O GDPR

Princípios

Não conformidade com os princípios gerais de processamento de dados.

€ 14,5M

GERMANY	Data Protection Authority of Berlin	2019-10-30	14,500,000	Deutsche Wohnen SE	Art. 5 GDPR, Art. 25 GDPR	Non-compliance with general data processing principles	The company used an archiving system for the storage of personal data of tenants that did not provide for the possibility of removing data that was no longer required. Personal

REQUISITOS À CUMPRIR COM O GDPR

Estrutura

- Definir papeis : controladores e processadores
- Controlador : determina as finalidades e os meios de processamento, implementa medidas técnicas e organizacionais apropriadas para assegurar que o processamento seja realizado de acordo com o GDPR. responsável por ter as "medidas apropriadas" implementadas pelo processador, e, um processador não pode terceirizar parte do processamento para um subprocessador sem autorização prévia por escrito do controlador.
- Entre o controlador e o processador um contrato legal deve ser realizado.

REQUISITOS À CUMPRIR COM O GDPR

Estrutura

- Processador somente trata os dados pessoais baseado em instruções documentadas do controlador. O contrato entre o processador e o controlador deve definir:

  - ✓ objeto do processamento
  - ✓ a duração do processamento
  - ✓ a natureza e o objetivo do processamento, como definido pelo controlador
  - ✓ o tipo de dados pessoais envolvidos
  - ✓ as categorias dos titulares dos dados
  - ✓ as obrigações e direitos do controlador

REQUISITOS À CUMPRIR COM O GDPR

Avaliação de Impacto

- Artigo 35º, 1 : Quando um certo tipo de processamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas físicas, o controlador procede, antes de iniciar o processamento, a uma avaliação de impacto das operações de processamento previstas sobre a proteção de dados pessoais.
- Se um conjunto de operações de processamento que apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação.
- Os termos DPIA. e PIA (avaliação do impacto na privacidade) são utilizados com o mesmo sentido.

REQUISITOS À CUMPRIR COM O GDPR

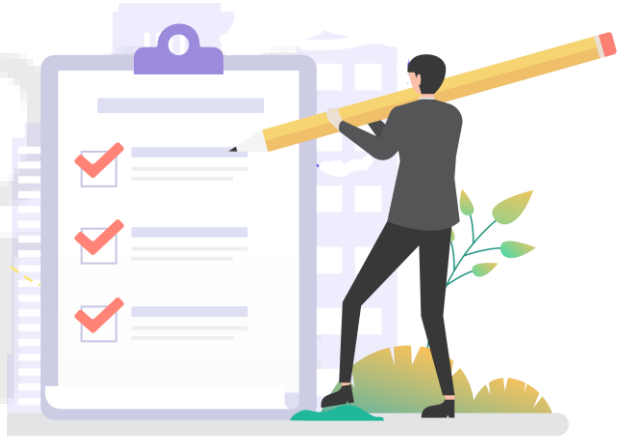
Consulta prévia

- Artigo 36º, 1 : O controlador consulta a autoridade supervisora antes de proceder ao processamento quando a avaliação de impacto sobre a proteção de dados indicar que o processamento resultaria num elevado risco na ausência das medidas tomadas pelo controlador para atenuar o risco.

ATIVIDADES REQUERIDAS DE ADMINISTRAÇÃO

Registro de atividades de processamentos

- Artigo 30º, 1 : Cada controlador e, sendo o caso, o seu representante conserva um registo de todas as atividades de processamento sob a sua responsabilidade.

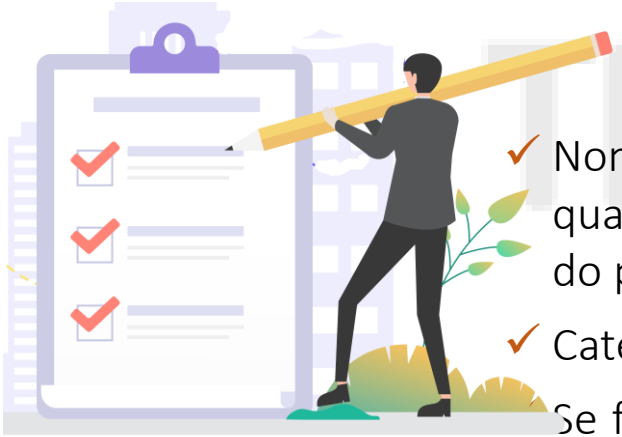


  - ✓ O nome e detalhes de contato do (s) controlador (es) ou seus representantes e DPO
  - ✓ Finalidades do processamento
  - ✓ Descrição das categorias de titulares de dados e categorias de dados pessoais
  - ✓ Categorias de destinatários a quem tenham sido ou venham a ser divulgados os dados pessoais,
  - ✓ Se aplicável, as transferências de dados pessoais para um país terceiro ou uma organização internacional
  - ✓ Sempre que possível, os prazos previstos para o apagamento das diferentes categorias de dados
  - ✓ Sempre que possível, uma descrição geral das medidas técnicas e organizacionais de segurança

ATIVIDADES REQUERIDAS DE ADMINISTRAÇÃO

Registro de atividades de processamento

- Artigo 30º, 2 : O processador também precisa manter registros caso realizar atividades de processamento por instrução do controlador. Este registro deve conter :



- ✓ Nome e detalhes de contato do (s) processador (es) e de cada controlador em nome do qual o processador está agindo e, quando aplicável, do representante do controlador ou do processador e do Data Protection Officer (DPO)
- ✓ Categorias de processamento realizadas em nome de cada controlador
- Se for caso, transferências de dados pessoais para um país terceiro ou uma organização internacional
- ✓ Sempre que possível, uma descrição geral das medidas técnicas e organizacionais de segurança

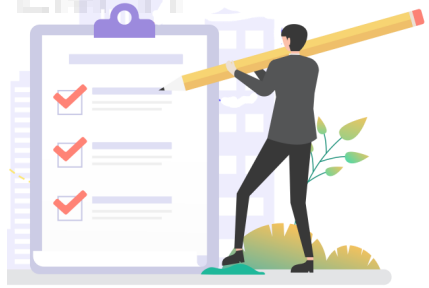
ATIVIDADES REQUERIDAS DE ADMINISTRAÇÃO

Registro de atividades de processamento

Exceção

Artigo 30º, 5 : A obrigação de registro das atividades não se aplica às empresas ou organizações com menos de 250 trabalhadores, a menos que o processamento efetuado seja suscetível de implicar um risco para os direitos e liberdades do titular dos dados, não seja ocasional ou abranja as categorias especiais de dados ou dados pessoais relativos a condenações penais e infrações .

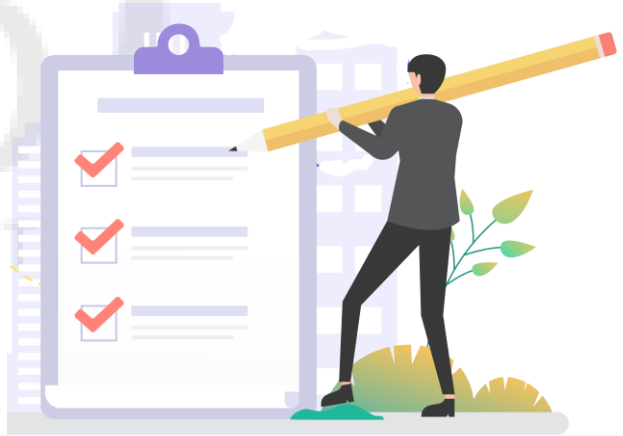
Nota: Esta exceção não isenta o controlador da obrigação de demonstrar conformidade.



ATIVIDADES REQUERIDAS DE ADMINISTRAÇÃO

Registro de violações de dados pessoais

- Artigo 33º, 5 : O controlador documenta quaisquer violações de dados pessoais, compreendendo os factos relacionados com as mesmas, os respetivos efeitos e a medida de reparação adotada.



- ✓ Nome e detalhes de contato do DPO ou outro contato do contato onde mais informações podem ser obtidas
- ✓ A natureza da violação de dados
- ✓ As categorias e o número aproximado de titulares de dados envolvidos
- ✓ As categorias e número aproximado de registros de dados pessoais afetados
- ✓ As prováveis consequências em termos de risco para os direitos e liberdades das pessoas físicas
- ✓ As medidas tomadas ou a tomar para resolver as consequências da violação de dados

2.2 AUTORIDADE SUPERVISORA

RESPONSABILIDADE DA AUTORIDADE SUPERVISORA

Artigo 51º, 1

A principal responsabilidade de uma Autoridade Supervisora (também chamada em alguns países de 'Autoridade de Proteção de Dados' - DPA) é monitorar e fazer cumprir a aplicação do GDPR com o objetivo de proteger os direitos e liberdades fundamentais das pessoas físicas em relação ao processamento e facilitar o livre fluxo de dados pessoais na União .

RESPONSABILIDADE DA AUTORIDADE SUPERVISORA

- Controla e executa a aplicação do presente regulamento
- Promove a conscientização do público
- Promove a conscientização dos controladores e processadores
- Elabora exigência de realizar uma DPIA / AIPD
- Incentiva a elaboração de códigos de conduta, dá parecer sobre eles e aprova
- Incentiva o estabelecimento de procedimentos de certificação
- Adota e/ou autoriza as cláusulas contratuais padrões
- Aprova as regras corporativas vinculantes
- Por solicitação presta informações a qualquer titular dos dados
- Trata a reclamação(ões) apresentada(s)
- Dá orientações sobre as operações de processamento
- Desempenha quaisquer outras tarefas sobre proteção de dados

COOPERAÇÃO COM OUTRAS AUTORIDADES

Artigo 63º : A fim de contribuir para a aplicação coerente do presente regulamento em toda a União, as autoridades de controlo cooperam entre si e, quando for relevante, com a Comissão, através do procedimento de controlo da coerência previsto na presente secção

https://edpb.europa.eu/about-edpb/about-edpb/members_en

Por meio do mecanismo de consistência, as Autoridades Supervisoras compartilham informações e fornecem assistência mútua a outras Autoridades Supervisoras, com Autoridade Europeia para a Proteção de Dados (EDPS) e com o "Comitê Europeu de Proteção de Dados", com o objetivo de garantir a consistência da aplicação e aplicação do GDPR'.

AUTORIDADE SUPERVISORA – VIOLAÇÃO DE DADOS

Ao receber uma notificação de uma violação de dados pessoais, verificará os critérios para avaliar a importância da violação de dados pessoais, bem como avaliar como a proteção de dados foi implementada pelo controlador e pelo processador ou processadores.

A Autoridade Supervisora pode receber amplos poderes para monitorar a investigação e ordenar que os controladores e processadores envolvidos tomem as medidas necessárias para adequar as operações de processamento com o GDPR e até para restringir ou bloquear o processamento.

Cabe ao controlador

- investigar a violação de dados pessoais
- as circunstâncias em que isso aconteceu
- a avaliação dos riscos envolvidos para os titulares de dados
- adotar medidas de mitigação para minimizar as consequências negativas para os direitos e liberdades dos titulares dos dados e outras pessoas envolvidas.

PORTAL DO TREINAMENTO!

AUTORIDADE SUPERVISORA E A APLICAÇÃO DO GDPR

Poderes de investigação da Autoridade Supervisora

Artigo 58º, 1 : A Autoridade Supervisora dispõe dos seguintes poderes de investigação:

- ordenar ao controlador e ao processador que forneçam qualquer informação necessária para o desempenho de suas tarefas.
- realizar investigações sob a forma de auditorias de proteção de dados
- proceder a uma revisão das certificações emitidas
- notificar o controlador ou o processador de uma alegada infração ao presente regulamento.
- obter, do controlador e do processador, acesso a todos os dados pessoais e a todas as informações necessárias para o desempenho de suas tarefas
- obter acesso a quaisquer instalações do controlador e do processador

PORTAL DO TREINAMENTO!

AUTORIDADE SUPERVISORA E A APLICAÇÃO DO GDPR

Poderes corretivos da Autoridade Supervisora

Artigo 58º, 2: Cada autoridade supervisora dispõe dos seguintes poderes de correção

- Fazer advertências ao controlador ou ao processador
- Fazer repreensões ao controlador ou processador
- Ordenar ao controlador ou processador que atenda os pedidos de exercício de direitos
- Ordenar ao controlador ou processador que tome medidas e prazo para que as operações de processamento cumpram as disposições do presente regulamento
- Ordenar ao controlador que comunique ao titular dos dados uma violação de dados pessoais
- Impor uma limitação temporária ou definitiva ao processamento de dados, ou mesmo a sua proibição
- Ordenar a retificação ou o apagamento de dados pessoais ou a limitação do processamento
- Retirar a certificação ou ordenar ao organismo de certificação que retire uma certificação
- Impor uma multa
- Ordenar a suspensão do envio de dados para países terceiros ou para organizações internacionais

MULTAS ADMINISTRATIVAS

As sanções e multas administrativas devem ser proporcionais e dissuasivas.

Proporcionais

A Autoridade Supervisora deve dar a devida atenção às circunstâncias

- a natureza, a gravidade e a duração da infração
- a finalidade do processamento
- o número de titulares de dados afetados
- o nível de danos causados a eles
- o grau de responsabilidade dos controladores e processadores
- as medidas técnicas e organizacionais implementadas
- A cooperação dos controladores e processadores com a Autoridade Supervisora

Multas Dissuasivas

Uma multa também deve ser dissuasiva, com o objetivo de deixar claro a organização que não vale o risco de não cumprir o GDPR, pois o custo das mesmas serão maiores que o custo da conformidade

Ainda assim, a intenção é incentivar as empresas a cumprir o GDPR, e não as destruir financeiramente

MULTAS ADMINISTRATIVAS

Valores das Multas – Artigo 83º

- multas de € 10.000.000 ou 2% do volume de negócios mundial da empresa no ano financeiro anterior, o que for maior.

  Aplicada em casos de

  - violações das obrigações do controlador e do processador,

- multas de € 20.000.000 ou 4% do faturamento mundial da empresa no exercício financeiro anterior, o que for maior.

  Aplicada em caso de

  - violação dos princípios básicos de processamento, incluindo as condições de consentimento
  - violação dos direitos dos titulares de dados
  - as transferências de dados pessoais para um destinatário num país terceiro ou uma organização internacional
  - descumprimento de uma encomenda ou limitação temporária ou definitiva do processamento ou suspensão da transmissão de dados pela Autoridade Supervisora

PORTAL DO TREINAMENTO!

Exercício

Um controlador holandês contratou um processador em um país sem decisão de adequação e sem ter salvaguardas para o processamento de dados pessoais sensíveis. Isso foi descoberto e ele foi penalizado pela autoridade supervisora. Seis meses depois, a autoridade descobre que o controlador é novamente culpado da mesma transgressão em outra operação de processamento.

Qual é a multa máxima que a autoridade supervisora pode impor nesse caso?

a. € 600.000

b. € 1.500.000

c. € 10.000.000 ou 2% do volume global de negócios da empresa, o que for maior

d. € 20.000.000 ou 4% do volume global de negócios da empresa, com um mínimo de € 20.000.000, o que for maior

2.3 TRANSFERÊNCIA DE DADOS PESSOAIS PARA PAÍSES TERCEIROS

TRANSFERÊNCIA DE DADOS DENTRO DA EEE

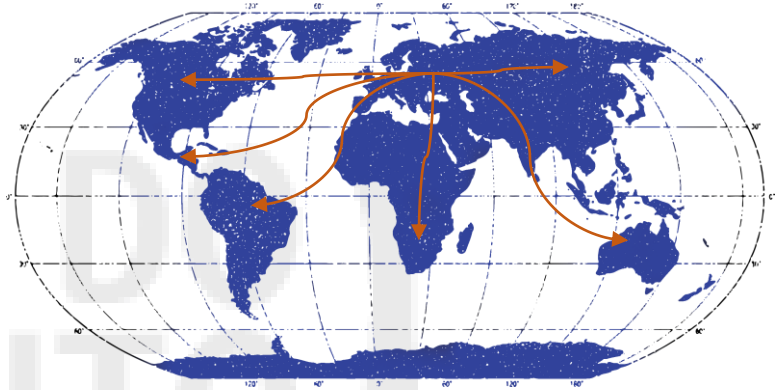
A regra é que a supervisão da atividade transfronteiriças de dados pessoais, ou processamento envolvendo cidadãos de mais de um país da UE, é liderada por apenas uma Autoridade Supervisora, denominada "Autoridade Supervisora principal". Este é princípio do Balcão Único – "One Stop Shop".

Considerando 36, nos casos que envolvem um controlador e um processador, a Autoridade Supervisora Competente será a autoridade do Estado-Membro onde o controlador tenha seu principal estabelecimento. A Autoridade Supervisora do processador é considerada uma «Autoridade Supervisora em causa» e deve participar no procedimento de cooperação.

Curiosidade: https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions_en

TRANSFERÊNCIA DE DADOS PARA FORA DO EEE

É permitido a transferência de dados pessoais para fora da EU, desde que cumpridas uma série de condições consideradas "adequadas" para a proteção de dados pessoais. Sendo :



1. Informar ao Titular dos dados

O controlador deve informar aos titulares dos dados quando da obtenção do consentimento expresso, que :

- pretende transferir os seus dados pessoais para um terceiro país fora da União Europeia;
- Que essa transferência se dará para um país que obteve uma decisão de adequação de um nível de proteção de dados pessoais, ou tem às proteções adequadas ou apropriadas para garantir seus direitos

TRANSFERÊNCIA DE DADOS PARA FORA DO EEE

2. Decisão de adequação

O país ao qual se pretende transferir os dados pessoais assegura um nível de proteção adequado e possui uma "Decisão de Adequação"

Até o momento a Comissão Europeia forneceu a decisão de adequação aos seguintes países:

Andorra, Argentina, Canadá (nem todo tipo de processamento), Ilhas Faroé, Guernsey, Israel, Ilha de Man, Jersey, Nova Zelândia, Suíça e Uruguai.

TRANSFERÊNCIA DE DADOS PARA FORA DO EEE

3. Salvaguardas

No caso de o país de destino dos dados pessoais não possuir uma decisão de adequação , será necessário aplicar garantias adequadas, conforme o Artigo 46º, 2 :

- Um instrumento juridicamente vinculativo e com força executiva entre autoridades ou organismos públicos;
- **Regras vinculantes aplicáveis às empresas** em conformidade com o artigo 47º
- **Cláusulas contratuais padrões** de proteção de dados adotadas pela Comissão
- **Cláusulas contratuais padrão** de proteção de dados adotadas por uma autoridade supervisora
- Um código de conduta, aprovado nos termos do artigo 40.o, acompanhado de compromissos vinculativos e com força executiva assumidos pelos controladores ou processadores no país terceiro
- Um procedimento de certificação, aprovado nos termos do artigo 42.o, acompanhado de compromissos vinculativos e com força executiva assumidos pelos controladores ou processadores no país terceiro

Nota : Cláusulas contratuais padrões são utilizadas por empresas não pertencentes ao mesmo grupo .

TRANSFERÊNCIA DE DADOS PARA FORA DO EEE

Acordo EUA e EU

Em 2016, a Comissão Europeia e os Estados Unidos fecharam um marco jurídico sobre a transferência dos dados pessoais com fins comerciais.

O acordo, chamado de "Privacy Shield" (Escudo de Privacidade) protege os direitos fundamentais de qualquer pessoa na UE cujos dados pessoais sejam transferidos para os Estados Unidos para fins comerciais. Ele permite a transferência gratuita de dados para empresas certificadas nos EUA pelo Privacy Shield. Inclui:

- fortes obrigações de proteção de dados para empresas que recebem dados pessoais da UE
- salvaguardas sobre o acesso do governo dos EUA aos dados
- proteção e reparação eficazes para os indivíduos
- uma revisão anual conjunta da UE e dos EUA para monitorizar a correta aplicação do acordo

TRANSFERÊNCIA DE DADOS PARA FORA DO EEE

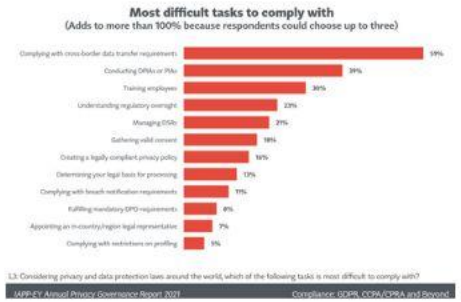
Acordo EUA e EU

Nota: Atualização na estrutura do Privacy Shield:

"Em 16 de julho de 2020, o Tribunal de Justiça Europeu emitiu uma sentença declarando inválida a Decisão 2016/1250 / EC da Comissão Europeia de 12 de julho de 2016 sobre a adequação da Estrutura de Escudo de Privacidade UE-EUA. Continuamos esperando que as empresas cumpram suas obrigações contínuas com relação às transferências feitas sob a Estrutura do Privacy Shield. Também encorajamos as empresas a continuarem a seguir princípios de privacidade robustos, como os subjacentes à Estrutura do Privacy Shield, e a revisar suas políticas de privacidade para garantir que descrevam suas práticas de privacidade com precisão, inclusive com relação a transferências internacionais de dados. Atualizado em 21 de julho de 2020".

Tarefas mais difíceis de cumprir na adequação à Proteção de Dados e Privacidade

Pesquisa direcionada a profissionais de privacidade, com participação de 473 pessoas de diferentes países revelou que as tarefas mais difíceis de cumprir são:



IAPP-EY Annual Privacy Governance Report 2021

TOP 10:

1) Cumprir os requisitos de transferência internacional de dados pessoais;

2) Elaboração de Relatórios de Impacto de Proteção de Dados Pessoais;

3) Treinamento e conscientização de colaboradores;

4) Compreender os impactos jurídicos de proteção de dados e demais leis;

5) Gerenciando solicitações de direitos dos titulares de dados;

6) Obter e formalizar consentimentos válidos;

7) Criação de uma política de privacidade legalmente válida e compatível com a realidade do negócio;

8) Cumprir os requisitos para a notificação de uma violação envolvendo dados pessoais;

9) Nomeação de DPO (interno e/ou consultoria – DPO as a Service);

10) Obedecer às restrições de criação de perfil e compatibilizá-las à viabilidade para a atividade empresarial.

https://www.linkedin.com/posts/adrianneclima_dpo-dpoaas-lgpd-activity-6868616945416110080-lCq6

2.4 REGRAS CORPORATIVAS VINCULANTES E PROTEÇÃO DE DADOS EM CONTRATOS

REGRAS CORPORATIVAS VINCULANTES

Regras Corporativas Vinculante (Binding Corporative Rules – BCR)

Acordos corporativos, processos e procedimentos sobre o processamento de dados pessoais dentro da própria organização (grupo de empresas) que permitam a transferência de dados pessoais para países que não tenham um nível adequado de proteção.

REGRAS CORPORATIVAS VINCULANTES

Conteúdo Regra corporativa vinculante – Artigo 47º, 2

- as transferências de dados, categorias de dados, tipos de processamento e suas finalidades
- tipos de titulares de dados afetados e identificação do país ou países terceiros
- a aplicação dos princípios gerais de proteção de dados e os requisitos relativos a transferências subsequentes para organismos não vinculados pelas regras vinculantes das empresas
- os direitos das pessoas em causa em relação ao processamento e os meios para exercer esses direitos
- a aceitação, pelo controlador ou pelo processador estabelecido no território de um Estado-Membro, da responsabilidade por eventuais violações das regras vinculantes da empresa por parte de um membro que não tenha sido estabelecida na União.
- o mecanismo de cooperação com a Autoridade Supervisora para assegurar o cumprimento por qualquer membro do grupo (...)

CONTRATOS ESCRITOS ENTRE CONTROLADOR E PROCESSADOR

Artigo 28º, 3 : O processamento em subcontratação é regulado por contrato ou outro ato normativo ao abrigo do direito da União ou dos Estados-Membros, que

- vincule o processador ao controlador,
- estabeleça o objeto e a duração do processamento,
- a natureza e finalidade do processamento,
- o tipo de dados pessoais e as
- categorias dos titulares dos dados, e as
- obrigações e direitos do responsável pelo processamento.

CONTRATOS ESCRITOS ENTRE CONTROLADOR E PROCESSADOR

Esse contrato estipula no mínimo que, o processador:

- Trata os dados pessoais apenas mediante instruções documentadas do controlador
- Assegura que as pessoas autorizadas a tratar os dados pessoais assumiram um compromisso de confidencialidade ou estão sujeitas a adequadas obrigações legais de confidencialidade;
- respeita as condições para contratar outro processador
- Auxilia o controlador, por meio de medidas técnicas e organizacionais apropriadas
- A escolha do controlador, suprime ou devolve todos os dados pessoais ao controlador após o termino da prestação de serviços
- Disponibiliza ao controlador todas as informações necessárias para demonstrar o cumprimento das obrigações

2.5 EXERCÍCIOS

Exercício 1

De acordo com o GDPR, ocorrendo uma violação de dados sensíveis, a quem o incidente deve ser reportado pelo controlador ?

a. Ao judiciário
b. Ao Data Protection Officer (DPO)
c. Ao gerente de Segurança
d. À Autoridade Supervisora 

PORTAL DO TREINAMENTO!

Exercício 2

Na ocorrência de uma violação de dados pessoais, quando os titulares devem ser sempre notificados?

a. Os dados pessoais foram processados em uma instalação do Processador que não está localizada dentro UE

b. Existe uma probabilidade significativa de que a violação conduza a alto risco para a privacidade dos titulares dos dados

c. Os dados pessoais foram processados por uma parte que concordou com um contrato de processamento enviada pelo Controlador, mas ainda não o assinou

d. Os dados pessoais foram processados por uma parte que ainda não assinou um contrato compulsório com o Controlador

PORTAL DO TREINAMENTO!

Exercício 3

A Comissão Europeia autorizou a transferência de dados pessoais entre empresas no EEE e na Argentina. Em linhas gerais, que tipo de disposição é essa?

a. Decreto de exceção

b. Contrato compulsório padrão

c. Decisão de adequação 

d. Tratado que substitui o GDPR

PORTAL DO TREINAMENTO!

Exercício 4

Processador somente trata os dados pessoais baseado em instruções documentadas do controlador.
O que contrato entre o processador e o controlador **não** deve definir:

a. Objeto do processamento

b. A duração do processamento

c. A natureza e o objetivo dos processamentos, como definido pela Autoridade Supervis

d. O tipo de dados pessoais envolvidos

Exercício 5

Cada controlador e, sendo o caso, o seu representante conserva um registro de todas as atividades de processamento sob a sua responsabilidade.

O que deve conter este registro ?

a. O nome e detalhes de contato do (s) controlador (es) ou seus representantes e DPO

b. Nome do processador

c. Descrição das categorias de dados organizacionais

d. Categorias de titulares de dados a quem tenham sido ou venham a ser divulgados os dados pessoais,

Exercício 6

A principal responsabilidade de uma Autoridade Supervisora é

a. Entender as necessidades dos titulares dos dados
b. Monitorar e fazer cumprir a aplicação do GDPR 
c. Responder a questões dos estados membros
d. Criar comissões de análise das leis sobre privacidade

PORTAL DO TREINAMENTO!

Exercício 7

Em caso de violação dos princípios básicos de processamento, incluindo as condições de consentimento, o que se aplica ?

a. Multa de € 10.000.000 ou 2% do faturamento mundial, o que for maior
b. Somente sanção administrativa
c. Multa de € 20.000.000 ou 4% do faturamento mundial, o que for maior 
d. Não é passível de multa ou sanção

PORTAL DO TREINAMENTO!

Exercício 8

Regras Corporativas Compulsórias (Regras Corporativas Globais) constituem um meio para facilitar a carga administrativa das organizações no cumprimento do GDPR.

Como essas regras podem ajudar?

a. Elas evitam a necessidade de abordar separadamente cada autoridade supervisora na UE.
b. Elas permitem que as organizações tenham contratos de apoio com todas as partes envolvidas no exterior.

c. Elas previnem que as organizações precisem pedir permissão a uma autoridade supervisora para o processamento dos dados após suas Regras Corporativas Compulsórias serem aprovadas.
d. Elas permitem que as organizações deixem terceiros fora da Área Econômica Europeia processarem os dados pessoais.

3. PRÁTICAS DE PROTEÇÃO DE DADOS

3 PRÁTICAS DE PROTEÇÃO DE DADOS

Tópicos

- Proteção de dados desde a concepção (by design) e por padrão (by default)
- Avaliação de Impacto sobre a Proteção de Dados (DPIA)
- Gestão do Ciclo de Vida de Dados
- Uso de Dados, Marketing e Mídias Sociais

3.1 PROTEÇÃO DE DADOS DESDE A CONCEPÇÃO (BY DESIGN) E POR PADRÃO (BY DEFAULT)

PROTEÇÃO DE DADOS “BY DESIGN” e “BY DEFAULT”

O GDPR exige que se coloque em prática medidas técnicas e organizacionais apropriadas para implementar os princípios de proteção de dados de maneira eficaz e salvaguardar os direitos individuais. Isso é 'proteção de dados por design e por padrão'.

Em essência, isso significa que você deve integrar ou "proteger" a proteção de dados em suas atividades de processamento e práticas de negócios, desde o estágio de design e através do ciclo de vida.

A proteção de dados “by Design” consiste em considerar antecipadamente os problemas de proteção e privacidade de dados em tudo o que você faz. Isso pode ajudar a garantir que você cumpra os princípios e requisitos fundamentais do GDPR e faz parte do foco na responsabilidade.

BY DESIGN

A proteção de dados por design é, em última análise, uma abordagem que garante que você considere questões de privacidade e proteção de dados na fase de design de qualquer sistema, serviço, produto ou processo e, em seguida, ao longo do ciclo de vida.

O GDPR , em seu artigo 25 nos traz o princípio de proteção de dados desde a concepção (by design) como um requisito legal, e não somente uma forma eficaz de cumprir as obrigações relacionadas à proteção dos dados, sendo o controlador responsável pela implementação de um conjunto completo de medidas técnicas e organizacionais apropriadas.

BY DEFAULT

A proteção “by defaul”, por padrão, exige que você processe apenas os dados necessários para atingir seu objetivo específico. Ele se vincula aos princípios fundamentais de proteção de dados, como minimização e limitação de objetivos.

Ou seja, por padrão (by default) :

- se coleta a menor quantidade de dados pessoais necessário
- se utiliza o escopo de processamento mais restrito possível
- Se utiliza o menor período de armazenamento
- Que os dados sejam acessíveis ao menor número de pessoas possíveis na organização .

OS 7 PRINCÍPIOS DE PROTEÇÃO DE DADOS DESDE A CONCEPÇÃO (BY DESIGN)

Ann Cavoukian, PhD., ex-Comissária de Privacidade e Informações de Ontário, Canadá, desenvolveu o conceito de proteção de dados desde a concepção (by design) e escreveu :

"A privacidade deve ser incorporada aos sistemas e tecnologias de dados em rede, por padrão. A privacidade deve se tornar parte integrante das prioridades organizacionais, objetivos do projeto, processos de design e operações de planejamento. A privacidade deve ser incorporada a todos os padrões, protocolos e processos que afetam nossas vidas.", apresenta Cavoukian, em seu documento : "Privacy by Design - The 7 Foundational Principles Implementation and Mapping of Fair Information Practices"

OS 7 PRINCÍPIOS DE PROTEÇÃO DE DADOS DESDE A CONCEPÇÃO (BY DESIGN)

Em outubro de 2010, foi aprovada, na Conferência Internacional de Autoridades de Proteção de Dados e Comissários de Privacidade, uma Resolução reconhecendo a Privacidade por Design como um componente essencial da proteção fundamental da privacidade.

Isso foi seguido pela inclusão da Privacidade por Design pela Comissão Federal de Comércio dos EUA como uma das três práticas recomendadas para proteger a privacidade online.

Desde então, o PbD foi traduzido para 39 idiomas, dando-lhe uma verdadeira presença global

Fonte: https://gpsbydesigncentre.com/about-us/ . Cavoukian, Ann «Cavoukian, Ann. "7 Foundational Principles"» (PDF). "Privacy by Design The 7 Foundational Principles". "Information and Privacy Commissioner of Ontario".

Dra. Ann Cavoukian apresenta o que a motivou a criar o conceito de PbD:

https://www.youtube.com/watch?v=v2s7_hFmZN0

PROTEÇÃO DE DADOS DESDE A CONCEPÇÃO (BY DESIGN)

REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO

de 27 de abril de 2016

relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)

(Texto relevante para efeitos do EEE)

Artigo 25.º

Proteção de dados desde a conceção e por defeito

1. Tendo em conta as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento, de uma forma que este cumpra os requisitos do presente regulamento e proteja os direitos dos titulares dos dados.

2. O responsável pelo tratamento aplica medidas técnicas e organizativas para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento. Essa obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade. Em especial, essas medidas asseguram que, por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares.

Fonte https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN

OS 7 PRINCÍPIOS DE PROTEÇÃO DE DADOS DESDE A CONCEPÇÃO (BY DESIGN)

1. Proativo não reativo; Preventivo, não corretivo

O “Privacy by design” não espera que os riscos de privacidade se materializem, nem oferece remédios para resolver infrações de privacidade depois que elas ocorrerem - **ele visa impedir que elas ocorram**. Em resumo, o Privacy by Design vem antes do fato, não depois.

2. Privacidade como padrão

O Privacy by Design procura oferecer o máximo grau de privacidade, **garantindo que os dados pessoais sejam protegidos automaticamente em qualquer sistema de TI ou prática comercial**. Se um indivíduo não faz nada, sua privacidade ainda permanece intacta. Nenhuma ação é necessária por parte do indivíduo para proteger sua privacidade - ela é incorporada ao sistema, por padrão.

OS 7 PRINCÍPIOS DE PROTEÇÃO DE DADOS DESDE A CONCEPÇÃO (BY DESIGN)

3. Privacidade incorporada ao design

O Privacy by Design é **incorporado ao design e arquitetura dos sistemas de TI e práticas de negócios**.

Não é inserido como um complemento, após o fato. O resultado é que a **privacidade se torna um componente essencial da funcionalidade principal que está sendo entregue.**

4. Funcionalidade total

soma positiva, não soma zero

Privacy by Design procura acomodar todos os interesses e objetivos legítimos de maneira positiva em termos de "ganho", não através de uma abordagem datada de soma zero, onde são feitas compensações desnecessárias. **A privacidade do Design evita a pretensão de falsas dicotomias, como privacidade versus segurança, demonstrando que é possível e muito mais desejável ter as duas.**

OS 7 PRINCÍPIOS DE PROTEÇÃO DE DADOS DESDE A CONCEPÇÃO (BY DESIGN)

5. Segurança de ponta a ponta - Proteção do ciclo de vida

Privacy by Design, **incorporada ao sistema antes do primeiro elemento de informação ser coletado, se estende com segurança por todo o ciclo de vida dos dados envolvidos** - fortes medidas de segurança são essenciais para a privacidade, do início ao fim (*do berço ao túmulo*).

6. Visibilidade e Transparência

Privacy by Design procura garantir a todos os interessados que, **independentemente da prática ou tecnologia comercial envolvida, ela esteja de fato operando de acordo com as promessas e objetivos declarados, sujeita a verificação independente.**

OS 7 PRINCÍPIOS DE PROTEÇÃO DE DADOS DESDE A CONCEPÇÃO (BY DESIGN)

7. Respeito pela privacidade do usuário

Acima de tudo, Privacy by Design **exige que arquitetos e operadores mantenham os interesses do indivíduo em primeiro plano, oferecendo medidas como padrões de privacidade fortes, aviso apropriado e opções poderosas para o usuário**. Mantenha o **foco no usuário!**

Benefícios

- **Identificar possíveis problemas em um estágio inicial,** quando resolvê-los, geralmente será mais simples e menos dispendioso
- **Maior conscientização** sobre questões de privacidade e proteção de dados
- **Capaz de atender aos requisitos legais, o que leva a uma chance reduzida de qualquer violação da proteção de dados**
- **O projeto não ser interrompido posteriormente**, ao produzir protocolos / acordos de compartilhamento de informações

PORTAL DO TREINAMENTO!

OS 7 PRINCÍPIOS DE PROTEÇÃO DE DADOS DESDE A CONCEPÇÃO (BY DESIGN)

BENEFÍCIOS AO IMPLEMENTAR O PRIVACY BY DESIGN:

https://www.youtube.com/watch?v=v2s7_hFmZN0

3.2 AVALIAÇÃO DE IMPACTO SOBRE A PROTEÇÃO DE DADOS

AVALIAÇÃO DE IMPACTO SOBRE A PROTEÇÃO DE DADOS

Avaliação de Impacto sobre a Proteção de Dados - DPIA é um processo concebido para :

- Descrever o processamento,
- Avaliar a necessidade e a proporcionalidade de um processamento
- Gerir os riscos para os direitos e liberdades das pessoas físicas resultantes do processamento de dados pessoais

Se antecipar aos eventos e agir com antecedência de forma a garantir a privacidade do titular - 1º princípio by design

AVALIAÇÃO DE IMPACTO SOBRE A PROTEÇÃO DE DADOS

O Artigo 35º , Avaliação de impacto sobre a proteção de dados, nos traz em seu paragrafo 1.

Quando um certo tipo de processamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas físicas,
o controlador procede, antes de iniciar o processamento,
a uma avaliação de impacto das operações de processamento previstas sobre a proteção de dados pessoais.

Se um conjunto de operações de processamento que apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação.

AVALIAÇÃO DE IMPACTO SOBRE A PROTEÇÃO DE DADOS

OBRIGATORIEDADE

O Artigo 35º, 3 , indica

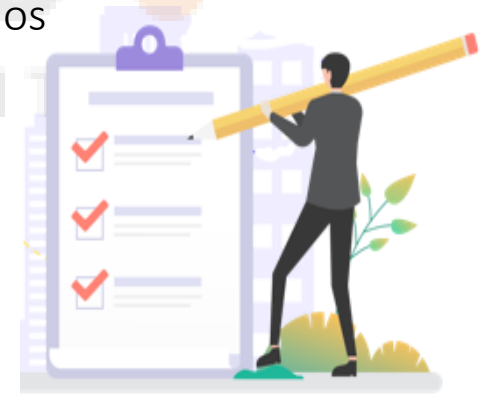
- Avaliação sistemática e completa dos aspectos pessoais relacionados com pessoas físicas, baseada no processamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa física ou que a afetem significativamente de forma similar
- Operações de processamento em grande escala de categorias especiais de dados a que se refere o artigo 9.o, n.o 1, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10.o
- Controle sistemático de zonas acessíveis ao público em grande escala.

AVALIAÇÃO DE IMPACTO SOBRE A PROTEÇÃO DE DADOS

TÓPICOS

Uma Avaliação de Impacto sobre a Proteção de Dados deve conter no mínimo :

- uma descrição das operações de processamento previstas e as finalidades do processamento
- uma avaliação da necessidade e proporcionalidade do processamento
- uma avaliação dos riscos para os direitos e liberdades dos titulares de dados
- as medidas previstas para:
  - abordar os riscos
  - demonstrar o cumprimento com o Regulamento



AVALIAÇÃO DE IMPACTO SOBRE A PROTEÇÃO DE DADOS

PROCESSO ITERATIVO GENÉRICO PARA A REALIZAÇÃO DE UMA AVALIAÇÃO DE IMPACTO SOBRE A PROTEÇÃO DE DADOS

conforme o WP 248 rev.01

AVALIAÇÃO DE IMPACTO SOBRE A PROTEÇÃO DE DADOS

BENEFÍCIOS

- Evitar mudanças custosas em processos, sistemas ou projetos
- Atenuar as consequências de uma fiscalização
- Melhorar a qualidade dos dados
- Melhorar a prestação de serviços e a imagem da empresa
- Melhorar a tomada de decisão
- Aumentar a conscientização sobre privacidade em uma organização
- Reforçar a confiança dos titulares de dados na forma como os dados pessoais são processados e a privacidade é respeitada

PORTAL DO TREINAMENTO!

AVALIAÇÃO DE IMPACTO SOBRE A PROTEÇÃO DE DADOS

EXEMPLOS

Exemplo de Processamento	Critérios	DPIA ?
Utilização de um sistema de câmaras para controlar o comportamento dos condutores nas autoestradas. O responsável pelo processamento pretende utilizar um sistema inteligente de análise através de vídeo para selecionar carros específicos e reconhecer automaticamente as matrículas.	- Controle sistemático. - Utilização de soluções inovadoras ou aplicação de novas soluções tecnológicas ou organizacionais.	
Revista em linha que utilize uma lista de endereços de correio eletrônico para enviar fascículos diários genéricos da revista para os seus assinantes.	- Dados processados em grande escala.	

AVALIAÇÃO DE IMPACTO SOBRE A PROTEÇÃO DE DADOS

EXEMPLOS

Exemplo de Processamento	Critérios	DPIA ?
Uma instituição que crie uma base de dados a nível nacional de notação de crédito ou de fraude.	- Avaliação ou classificação. - Decisões automatizadas que produzam efeitos jurídicos ou afetem significativamente de modo similar. - Impede os titulares dos dados de exercer um direito ou de utilizar um serviço ou um contrato. - Dados sensíveis ou dados de natureza altamente pessoal.	
Processamento de «dados pessoais de pacientes ou clientes de um determinado médico, profissional de cuidados de saúde, hospital ou advogado» (considerando 91).	- Dados sensíveis ou dados de natureza altamente pessoal. - Dados relativos a titulares de dados vulneráveis.	

3.3 GESTÃO DO CICLO DE VIDA DE DADOS (GCVD)

GESTÃO DO CICLO DE VIDA DE DADOS

FINALIDADE

A Gestão do Ciclo de Vida do Dado (GCVD) é um processo que visa atuar no gerenciamento do fluxo de dados em todo o seu ciclo de vida: da criação, uso, compartilhamento, arquivamento e exclusão, dentro de uma organização.

Rastrear os dados com precisão em todo o ciclo de vida da informação é a base de uma estratégia de proteção de dados pessoais e do suporte para determinar onde aplicar os controles de segurança

GESTÃO DO CICLO DE VIDA DE DADOS

É necessário que uma organização saiba:

- exatamente onde seus dados e, em particular, os dados pessoais estão
- para quais finalidades os dados devem ser coletados ou criados
- por quais razões os dados devem ser retidos
- em que data ou em que situação os dados devem ser excluídos

A Gestão do Ciclo de Vida do Dado

- fornece as ferramentas para gerenciar o fluxo de dados em um sistema de informações
- mantém rastreamento dos dados a partir do momento em que são coletados ou gerados até o momento em que são excluídos, porque não há motivo para retê-los.

GESTÃO DO CICLO DE VIDA DE DADOS

FLUXO DE DADOS – ATIVIDADES BÁSICAS

Mapeamento de Dados

O mapeamento de dados identifica e registra o caminho percorrido pelo dado pessoal dentro da empresa, incluindo os processos e procedimentos pelos quais o dado transita

Estrutura das permissões

Definir de forma clara e direta quem na organização, devido sua participação no processamento terá acesso a quais dados pessoais

Coleta de dados

Desde o início, é importante ter em mente quais dados pessoais são necessários para os fins do processamento pretendido.

Regras de retenção e exclusão

A coleta e guarda de dados pessoais em quantidades e tempo além do necessário as finalidades previstas, acarreta a organização um risco

CICLO DE VIDA DE DADOS

3.4 PRÁTICAS RELACIONADAS A APLICAÇÕES DO USO DE DADOS, MARKETING E MÍDIAS SOCIAIS

USO DE DADOS, MARKETING E MÍDIAS SOCIAIS

A economia atual é movida a partir de um importante ativo : Informações

Obter informações sobre uma quantidade grande de possíveis clientes tornou-se atividade diárias dentro de várias organizações

- Que tipo de produto ou serviços o potencial consumidor está mais propenso a comprar ?
- Como se comporta nas mídias sociais ?
- Como se comporta na internet ou em lojas físicas ?
- Quanto estão dispostos a gastar ?
- Que tipo de propaganda mais o atrai ?

A construção destes perfis necessita de muitos dados sobre pessoas e seu comportamento.
Como obter essas informações?

USO DE DADOS, MARKETING E MÍDIAS SOCIAIS

COOKIES

Um cookie, no âmbito da Internet, é um pequeno arquivo texto de computador ou pacote de dados enviados por um site da Internet para o navegador do usuário, quando esta visita o site.

Cada vez que o usuário visita o site novamente, o navegador envia o cookie de volta para o servidor para notificar atividades prévias do usuário.

USO DE DADOS, MARKETING E MÍDIAS SOCIAIS

Tipos mais comum de Cookies

Cookies de sessão

Ao sair do site, e fechar o navegador, o cookie da sessão é apagado da memória do computador do usuário e, como resultado, ele é apagado

O exemplo mais comum é o recurso de carrinho de compras de qualquer loja virtual. Sempre que os itens são selecionados, a seleção é armazenada no cookie da sessão

Cookies persistentes

Os cookies persistentes permanecem no disco rígido do usuário até serem apagados pelo usuário ou até expirarem..

Por exemplo, para manter a seleção de idioma do usuário.

Cookies de rastreamento

Geralmente é chamado de cookie de terceiros. Ele é colocado no disco rígido de um usuário por um site de um domínio diferente daquele que o usuário está visitando.

Definidos por redes de publicidade nas quais um site pode se inscrever.

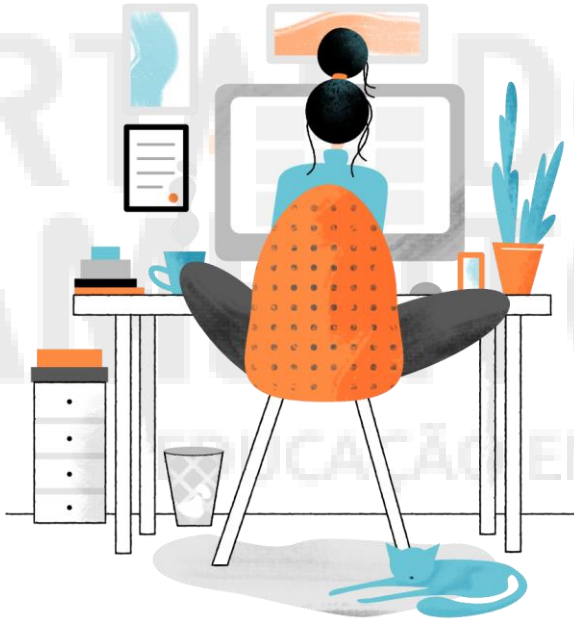
USO DE DADOS, MARKETING E MÍDIAS SOCIAIS

CRIAÇÃO DE PERFIL

O GDPR prevê o direito de oposição ao processamento de dados pessoais com finalidade de marketing direto, inclusive definição de perfis, bem como define que a criação de perfis pelas organizações também está sujeita as regras do regulamento.

De forma a garantir o consentimento informado e esclarecido, e evitar que os titulares dos dados de seu consentimento sem realmente ter lido a declaração de consentimento, o GDPR proíbe a declaração longa e ilegível e requer uma linguagem simples e clara, explicando para que os dados pessoais coletados devem ser usados.

3.5 EXERCÍCIOS



PORTAL DO TREINAMENTO!

Exercício

Em seu artigo 25º o GDPR nos traz o _____ como um requisito legal, e não somente uma forma eficaz de cumprir as obrigações relacionadas à proteção dos dados

a. Limitação de Finalidade
b. Minimização
c. Princípio de proteção de dados desde a concepção (by design)
d. Subsidiariedade

Exercício

A privacidade do Design evita a pretensão de falsas dicotomias, como privacidade versus segurança, demonstrando que é possível e muito mais desejável ter as duas.

Qual princípio é este ?

a. Seja proativo
b. Privacidade como padrão
c. Funcionalidade total - soma positiva, não soma zero 
d. Privacidade incorporada ao design

Exercício

Avaliação de Impacto sobre a Proteção de Dados - DPIA é um processo concebido para?

a. Descrever o processamento,
b. Avaliar a necessidade e a proporcionalidade de um processamento
c. Gerir os riscos para os direitos e liberdades das pessoas físicas
d. Todas as anteriores 

Exercício

Considerando os requisitos do GDPR, é necessário que uma organização saiba:

a. para quais finalidades as organizações existem
b. exatamente onde seus dados e, em particular, os dados pessoais estão 
c. por quais razões os dados devem ser conhecidos
d. em que data ou em que situação os titulares nasceram

PORTAL DO TREINAMENTO!

Exercício

Qual do tipo de cookie deixa de existir ao fechar o navegador ?

a. Cookie de Visita
b. Cookie de Sessão 
c. Cookie de Chocolate
d. Cookie de persistência

Exercício

Uma organização de assistência social pretende projetar uma nova base de dados para administrar seus clientes e os cuidados de que necessitam.

Para solicitar a permissão junto à autoridade supervisora, qual seria uma das primeiras medidas importantes a serem tomadas?

a. Coletar dados sobre os clientes e a quantidade e tipo de cuidados necessários e fornecidos.

b. Conduzir uma Avaliação de Impacto sobre a Proteção de Dados (AIPD) para determinar os riscos do processamento pretendido.

c. Obter o consentimento dos clientes para o processamento pretendido de seus dados pessoais.

Exercício

Que tipo de declaração de consentimento o GDPR proíbe?

a. Clara e direta
b. Longa e ilegível 
c. Curta e legível
d. Nenhum tipo

PORTAL DO TREINAMENTO!

Exercício

Um dos objetivos de uma Avaliação de Impacto sobre a Proteção de Dados (AIPD) é “fortalecer a confiança dos clientes ou cidadãos no modo como os dados pessoais são processados e a privacidade é respeitada”.

Como uma AIPD pode “fortalecer a confiança”?

a. A organização minimiza o risco de ajustes dispendiosos dos processos ou remodelamento dos sistemas em um estágio mais tardio.
b. A organização previne a não conformidade com o GDPR e minimiza o risco de multas.
c. A organização demonstra que considera a privacidade com seriedade e visa à conformidade com o GDPR.

RECAPITULAÇÃO

GDPR

QUANDO E ONDE É APLICÁVEL

PAPÉIS E RESPONSABILIDADES

DIREITOS DO TITULAR DOS DADOS

BASES LEGAIS

VIOLAÇÃO DE DADOS PESSOAIS

PRIVACY BY DESIGN E BY DEFAULT

CICLO DE VIDA DOS DADOS

AVALIAÇÃO DE IMPACTO DE PROTEÇÃO

AUTORIDADE SUPERVISORA

PRINCÍPIOS PARA TRATAMENTO

SANÇÕES

TRANSFERÊNCIA PARA PAÍSES TERCEIROS

DPO

PORTAL DO TREINAMENTO!

Recapitulando

1. FUNDAMENTOS E REGULAMENTAÇÃO DE PRIVACIDADE E PROTEÇÃO DE DADOs

Tópicos

- Contexto Histórico e Escopo PD&P
- Definições (responsável pelo tratamento/controlador; processador/subcontratante/operador, destinatário, terceiro)
- Dados pessoais
- Bases legais e princípios
- Direitos dos titulares dos dados
- Violação de dados pessoais

PORTAL DO TREINAMENTO!

Recapitulando

2. ORGANIZANDO A PROTEÇÃO DE DADOS

Conteúdo

- Importância da proteção de dados para a organização
- Autoridade supervisora
- Transferência de dados pessoais transfronteiriços
- Regras corporativas vinculantes
- Proteção de dados em contratos

PORTAL DO TREINAMENTO!

Recapitulando

3 PRÁTICAS DE PROTEÇÃO DE DADOS

Tópicos

- Proteção de dados desde a concepção (by design) e por padrão (by default)
- Avaliação de Impacto sobre a Proteção de Dados (DPIA)
- Gestão do Ciclo de Vida de Dados
- Uso de Dados, Marketing e Mídias Sociais

PORTAL DO TREINAMENTO!

Infos adicionais

- Material oficial EXIN
- Todo suporte possível pelo Portal do Treinamento
- Simulado durante o treinamento
- DICAS IMPORTANTES:
  - organizar-se para estudar este material + suas anotações ao longo do treinamento + fazer a leitura dos dispositivos legais do GDPR comentados em aula + realizar os simulados mais “caprichados” do Portal do Treinamento – ESTUDE!
  - Adquira o exame (online ou presencial) quando se sentir bem e confiante na compreensão do tema, pois só depende de você – há apenas 1 tentativa

Muito obrigada, Adrianne Lima

@profadrianne

Clique nos ícones!

PORTAL DO TREINAMENTO!

EDUCAÇÃO EM TI

Agradecemos sua presença em mais este treinamento

PORTAL DO TREINAMENTO!
EDUCAÇÃO EM TI

@Portaldotreinamento

Telegram

portaldotreinamento

Portal do Treinamento

+55 11 92004-3018

Clique nos ícones!

PORTAL DO TREINAMENTO!

EDUCAÇÃO EM TI