Material Básico de Treinamento – PDPP 202210

www.pmgacademy.com

official course

Bem-vindo ao Material Básico de Treinamento (MBT)

- Esses slides contêm material básico na forma de apresentação para preparar os alunos para o exame EXIN Privacy & Data Protection Practitioner. Eles podem ser usados como base para um treinamento credenciado.
- O MBT refere-se a todas as especificações de exame e conceitos básicos deste módulo.
- O instrutor pode incluir notas adicionais.
- Um bom treinamento requer exemplos de experiência prática, aprofundamento de especificações de exames e conceitos básicos, exercícios, elaboração de temas de especial interesse do público.
- No caso de uma duração mínima de treinamento, os candidatos devem estudar a literatura (compare a duração do treinamento com a carga de estudo no Guia de Preparação)
- A ordem de apresentação das disciplinas segue a ordem das especificações do exame.
- Este MBT não é um conjunto completo de material didático. Para se credenciar, você precisará aprimorar e enriquecer este material.
- Ao usar este BTM, sua organização ainda precisará passar pelo procedimento normal de credenciamento no EXIN. Você pode encontrar os requisitos de acreditação no Manual de Acreditação.
- Este MBT é um serviço para provedores de treinamento, nenhum direito pode ser derivado dele.

Visão Geral do Programa

Plano do Treinamento

Exam requirements	Exam specifications	Weight
1. Data protection policies		**10%**
	1.1 Purpose of data protection and privacy policies within an organization	5%
	1.2 Data protection by design and by default	5%
2. Privacy information management system (PIMS)		**32.5%**
	2.1 Privacy information management system (PIMS) basics	12.5%
	2.2 Benefits of a privacy information management system (PIMS)	10%
	2.3 Privacy information management system (PIMS) relationships	10%
3. Roles of the controller, processor and data protection officer (DPO)		**17.5%**
	3.1 Roles of the controller and processor	10%
	3.2 Role and responsibilities of a DPO	7.5%
4. Data protection impact assessment (DPIA)		**27.5%**
	4.1 Criteria for a DPIA	15%
	4.2 Steps of a DPIA	12.5%
5. Data breaches, notification, and incident response		**12.5%**
	5.1 GDPR requirements with regard to personal data breaches	2.5%
	5.2 Requirements for notification	10%
	Total	**100%**

Objetivos do curso e grupo alvo

O EXIN Privacy & Data Protection Practitioner é uma certificação que valida o conhecimento e compreensão de um profissional sobre a legislação europeia de privacidade e proteção de dados e sua relevância internacional, bem como a capacidade do profissional de aplicar esse conhecimento e compreensão à prática profissional diária.

Esta certificação de nível Practitioner será particularmente útil para Data Protection Officers (DPOs) / Privacy Officers, Legal / Compliance Officers, Security Officers, Business Continuity Managers, Data Controllers, Auditores de Proteção de Dados (internos e externos), Analista de Privacidade e gerentes de RH.

Requisitos para a Certificação

• Conclusão bem sucedida do exame EXIN Privacy & Data Protection Practitioner.
• Treinamento credenciado de EXIN Privacy & Data Protection Practitioner, incluindo exercícios práticos aplicados pelo instrutor.

Conceitos Básicos

• A lista de conceitos básicos nas notas do aluno abaixo será considerada compreendida para o exame
• Aconselha-se que o aluno pesquise e compreenda os conceitos

Formato do Exame

Tipo de Exame	Questões de múltipla escolha
Número de questões:	40
Mínimo para aprovação	65% (26/40 quetões)
Com consulta:	As fontes de literature A e B não podem ser usadas. O texto do GDPR pode ser consultado durante todo o exame. Ele é fornecido como um apêndice no exame digital. Os candidatos devem trazer suas próprias cópias para exames em papel.
Equipamentos eletrônicos permitidos:	Não
Duração do Exame:	120 minutos

As Regras e Regulamentos dos exames EXIN aplicam-se a este exame.

Literatura do exame

A. IT Governance Privacy Team
EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide
IT Governance Publishing (4th edition, 2020)
ISBN 97811787782495 (pdf)
ISBN 97811787782501 (e-book)
ISBN 97811787782518 (Kindle)
ISBN 97811787782488 (hardcopy)
ISBN 97811787782495 (audiobook)

B. Alan Shipman & Steve Watkins.
ISO/IEC 27701:2019: An introduction to privacy information management
IT Governance Publishing (2020)
ISBN: 97811787781993 (hardcopy)
ISBN: 97811787782013 (e-book)

Literatura adicional

C. Comissão Europeia
General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)
Regulamento do Parlamento Europeu e do Conselho da União Europeia. Bruxelas, 27 de abril de 2016

D. Grupo de Trabalho do Artigo 29.º Para a Proteção de Dados
Orientações sobre os encarregados da proteção de dados (EPD), wp 243rev.01, 5 de abril de 2017

E. Grupo de Trabalho do Artigo 29.º Para a Proteção de Dados
Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679, wp248rev.01, 4 de abril de 2017

Literatura adicional

F. A. Cavoukian
Privacy by Design - The 7 Foundational Principles
Information & Privacy Commissioner, Ontario, Canada
https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

G. ISO/IEC 27701:2019 (EN)
Security Techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management - Requirements and Guidelines
Switzerland, ISO/IEC, 2019
https://www.iso.org/home.html

1. POLÍTICAS DE PROTEÇÃO DE DADOS

1.1 PROPÓSITO DAS POLÍTICAS DE PROTEÇÃO DE DADOS / PRIVACIDADE DENTRO DE UMA ORGANIZAÇÃO

1.1.1 políticas e procedimentos necessários em uma organização para conformidade com a legislação de proteção de dados

- O GDPR cita (parte do Preâmbulo 78)
  - "Para poder comprovar a conformidade com o presente regulamento, o controlador deverá **adotar orientações internas** e implementar medidas que atendam em especial, aos princípios da proteção de dados desde a concepção e da proteção de dados por padrão."
  - Essas políticas são "internas" da organização
- Tipos mencionados no GDPR
  - **Políticas gerais;** a organização declara e tem visões consistentes sobre como pretende atender aos requisitos do GDPR.
  - **Políticas de proteção de dados pessoais**
- Outras a considerar
  - Política de privacidade (disponível ao público)
  - Política de segurança da informação
- Políticas precisam ser suportadas por processos e procedimentos, estar ligadas às operações da organização, e precisam auditáveis (para demonstrar conformidade)

1.1.2 Conteúdo das políticas

Políticas devem conter

- Justificativa; explanação de porque é necessária
- Escopo; quais tópicos e aspectos estão cobertos pela política
- Definições dos contatos (papéis) e suas responsabilidades (RACI)
- Objetivo; no mínimo um objetivo descrevendo o que se pretende alcançar e como se relaciona com os objetivos de negócio mais amplos
- Tratamento de violações; procedimento

Para ter sucesso, as políticas precisam ser

- explícitas (e portanto documentadas) e concisas
- suportadas por processos e procedimentos que produzem "evidência" de conformidade
- auditáveis (capaz de provar conformidade) e executável
- capaz de ser implementada e fácil de entender

1.1.2 Conteúdo das políticas - Exemplos

Política de Proteção de Dados
Objetivo: O objetivo principal desta Política de Proteção de Dados é fornecer diretrizes gerais para as questões de privacidade de dados relacionadas à coleta, uso, processamento, divulgação, monitoramento, etc., dos dados pessoais de uma empresa (Nota 1).

Conteúdo (parcial):

- Propósito desta política
- Compromisso
- Oportunidade de recusar
- Coleta de informações pessoais
- Uso da informação
- Proteção da informação

1.2 PROTEÇÃO DE DADOS DESDE A CONCEPÇÃO E POR PADRÃO

1.2.1 O conceito de proteção de dados desde a concepção (by design) e por padrão (by default)

· *"Para poder comprovar a conformidade com o presente regulamento, o controlador deverá adotar políticas internas e implementar medidas que atendam, em especial, aos princípios da proteção de dados desde a concepção e da proteção de dados por padrão"* (GDPR)

- Alguns exemplos de medidas: minimização de processamento, pseudonimização, criação de transparência com relação ao processamento

- **Desde a concepção e por padrão;**
  - "Privacidade **desde a concepção (by design)** defende a visão de que o futuro da privacidade não pode ser garantido apenas pelo cumprimento das estruturas regulatórias; em vez disso, a garantia de privacidade deve se tornar idealmente o modo de operação **padrão** de uma organização"

- Ao desenvolver e projetar produtos, serviços e aplicativos, devem ser observados os princípios de proteção de dados desde a concepção (by design) e por padrão (by default)

1.2.1 O conceito de proteção de dados desde a concepção (by design) e por padrão (by default)

Exemplo de um framework de privacidade by design

https://www.privacycompany.eu/files/Privacy%20by%20Design%20Framework%20-%20English.pdf

PRIVACY COMPANY

Privacy by Design Framework

Governance:
Consists of privacy awareness within the organisation, internal policies, accountability measures, transparency to data subjects, cooperation with third parties and data processors (including data processing agreements)

Subjects / Actions	Anonymisation	1. Data minimisation (art. 5(1)c)	2. Pseudonymisation (art. 4(5))	3. Encryption (art. 6(4)e, 32(1)a)	4. Access control (art. 32(1), 5(1)f)	5. Data protection by default (art. 25(2))	6. Deletion / retention terms (art. 5(1)e)	7. Facilitate rights of data subject (artt. 12-22)
Technical	Anonymise and aggregate (e.g. differential privacy)	Gather only data that is strictly necessary. Delete unnecessary data immediately	Removal of all directly identifying elements, hashing, polymorphic pseudo-id	E.g. public key encryption, disk encryption	Digital data vault, physical access controls, logical access controls, authentication and authorisation	Privacy friendly settings as default setting, transparent user interface, permission management	Automated deletion, 'flagging' of data after end of retention term, sticky policies, data fading	Privacy dashboard, communication / support (art. 5(1)a)
Supportive Documents	No extra measures needed, no personal data involved	Description of purpose of data processing and list of necessary data	Policy for separation of identifying data and other data, agreements	Information security standards (art. 32(1)) and policies	Authorisation matrix and logging, based on need to know and need to access	Registration opt-in / opt-out and permissions	Policy and overview of retention terms, management of e-waste (old documents and devices)	Privacy statement, policy for access requests, correction and deletion of personal data
Alternative	If data is not anonymised follow the scheme	When possible anonymise / aggregate part of the data set, data fading	Other security measures	Other security measures (e.g. stand-alone server)	Access logs, with checks	No alternative, just comply	Anonymise and aggregate (archive if allowed)	No alternative legal obligation

Privacy Audit

A data protection impact assessment can test the requirements and make clear what needs to be done.

The mentioned article numbers refer to the articles of the General Data Protection Regulation (Regulation 2016/679 (GDPR))

www.privacycompany.eu

Fonte: www.privacycompany.eu

1.2.2 Os Sete princípios da proteção de dados desde a concepção (by design) e por padrão (by default)

1. Proativo não Reativo; Preventiva não Corretiva
2. Proteção de dados como configuração padrão
3. Privacidade Incorporada ao Design
4. Funcionalidade Total - Soma Positiva, Não Soma Zero
5. Segurança de ponta a ponta - proteção total do ciclo de vida
6. Visibilidade e transparência— Manter aberta
7. Respeito à privacidade do usuário— Manter centrada no usuário

1.2.3 Implementação dos Sete Princípios

Exemplos dos desafios de implementação

•Preventiva não Corretiva;
A abordagem tradicional é reativa. Mudar isso requer liderança e mudança cultural. A introdução da arquitetura corporativa pode apoiar este processo.

• Proteção de dados como configuração padrão;
Por exemplo. emitindo políticas especializadas como "privilégio mínimo", "necessidade de saber", "menos confiança ".

• Privacidade Incorporada ao Design;
Em hardware (por exemplo, TPM), e / ou software (por exemplo, SAMM, CLASP)

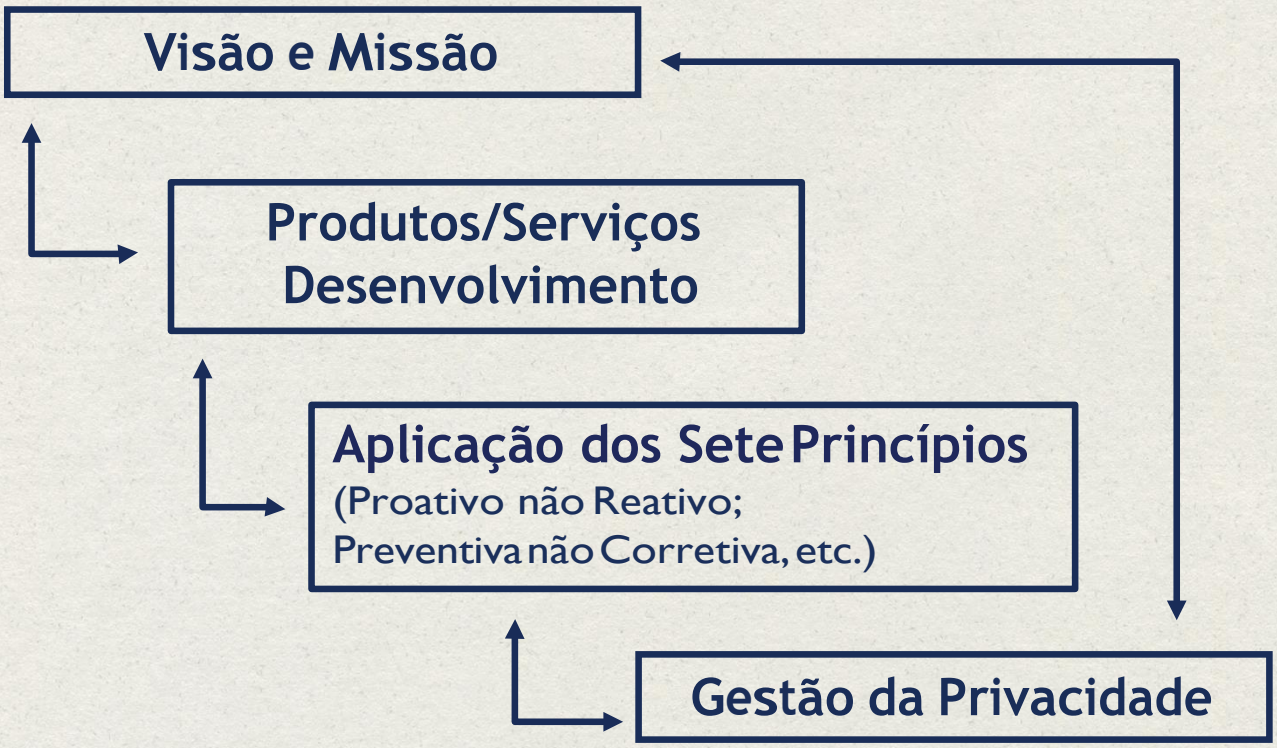
• Soma Positiva, Não Soma Zero;
Conflitos a serem resolvidos: acesso fácil versus acesso seguro, conveniência do usuário versus segurança, simples de implementar versus seguro de usar.

• Proteção Total do Ciclo de Vida (de ponta a ponta);
Requer uma estratégia de segurança voltada para a empresa como um todo. Principais áreas: DBSec e IAM.

• Manter aberta (visível e transparente);
Pode ser alcançado por exemplo, por padrões abertos, avaliação externa e validação como auditoria ISO / IEC 27001 e / ou publicação de políticas de segurança

• Manter centrada no usuário (respeito à privacidade do usuário);
Precisa ser alcançado um equilíbrio entre a proteção dos dados corporativos e os direitos do titular dos dados.

Proteção de Dados Desde a Concepção (by design) e por Padrão (by default)



Framework de Governança Corporativa

Fonte: J.Kyriazoglou

2. Privacy Information Management Systems (PIMS)

2.1 Básico do Privacy Information Management Systems (PIMS)

2.1.1 Diferentes termos usados no PMIS

Questões internas

- Relacionam-se com a gestão de pessoal (incluindo consultores e subcontratados) e relatórios

Questões externas

- Demonstrar como os requisitos legais e regulamentares relacionados ao gerenciamento de informações pessoais são cumpridos

Partes interessadas

- Por exemplo. diretores de empresas, reguladores e clientes/consumidores (entre outros)

2.1.2 Quais mídias devem ser consideradas ao implementar um sistema de gerenciamento de informações de privacidade (PIMS)

Todos os formatos e mídias em uso

Versões eletrônicas

Versões em papel

2.1.3 O que é uma declaração de aplicabilidade (SoA)

A ISO/IEC 27701 exige a produção de um documento que detalhe quais controles são aplicados dentro do PIMS e quais não são. Esta é a Declaração de Aplicabilidade (SoA), que estende a SoA produzida em relação a um sistema de gerenciamento de segurança da informação (SGSI) em conformidade com a ISO/IEC 27001.

	Compliance	Assessment	Results
Stan	Section		Findings
A.5	Information Security Policies		
A.5.1	Management direction for information		
A.5.1.1	Policies for information security		
		Do Security policies exist?	
		Are all policies approved by management?	
		Are policies properly communicated to	
A.5.1.2	Review of the policies for information		
		Are security policies subject to review?	
		Are the reviews conducted at regular	
		Are reviews conducted when	
A.6	Organisation of Information Security		
A.6.1	Internal organization		
A.6.1.1	Information security roles and		
		Are responsibilities for the protection of individual assets, and for carrying out specific security processes, clearly identified and defined and communicated	
A.6.1.2	Segregation of duties		
		Are duties and areas of responsibility separated, in order to reduce opportunities for unauthorized modification or misuse of	
A.6.1.3	Contact with authorities		

2.1.4 O objetivo da documentação em um sistema de gerenciamento de informações de privacidade (PIMS)

Demonstrar como as políticas corporativas, procedimentos operacionais e instruções de trabalho foram formuladas:

1. Registros de desenvolvimentos e atividades
2. Registros de atividades operacionais, ou seja, dados de trilha de auditoria
3. Procedimentos operacionais: quem faz o quê, onde e quando as instruções de trabalho

Lembrando que a documentação deve ser aprovada pelas pessoas certas e apenas as versões aprovadas mais recentes estão disponíveis.

2.1.5 O propósito das revisões gerenciais em um sistema de gerenciamento de informações de privacidade (PIMS)

A alta administração é: pessoa ou grupo de pessoas que dirige e controla uma organização no mais alto nível

- Iniciar o desenvolvimento do sistema de gestão
- Aprovar o recurso necessário
- Aprovar políticas corporativas que definam os objetivos do sistema de gestão
- Revise o progresso do PIMS em intervalos regulares:
    - Relatórios de auditoria
    - Mudanças na legislação/regulamentos
    - Incidentes relacionados à privacidade
    - Sugestões da equipe operacional
    - Medidas de eficácia
    - Oportunidades para melhoria contínua.

2.2 Benefícios do Privacy Information Management Systems (PIMS)

2.2.1 O objetivo

O objetivo das auditorias: monitorar a conformidade entre os requisitos do sistema de gestão e as práticas de trabalho.

Além disso, você deve demonstrar que o sistema de gestão:

- Está em conformidade com os requisitos da organização
- Está em conformidade com os requisitos do padrão internacional apropriado
- É efetivamente implementado e mantido

Atenção: Os relatórios de auditoria identificam não conformidades e oportunidades de melhoria.

2.2.2 Como determinar os requisitos específicos de um sistema de gerenciamento de informações de privacidade (PIMS) à luz das regras locais apropriadas e dos requisitos contratuais

Os requisitos específicos de um sistema de gestão de informações de privacidade (PIMS) precisam ser determinados à luz das regras locais apropriadas e dos requisitos contratuais

Estes requisitos terão de ser concebidos pela organização, utilizando todos os recursos disponíveis: gestão de topo, responsável pela proteção de dados, pessoal operacional, recursos humanos, pessoal de segurança da informação, pessoal de TI, etc.

2.2.3 Como determinar os requisitos específicos de um sistema de gerenciamento de informações de privacidade (PIMS) à luz das regras locais apropriadas e dos requisitos contratuais

A auditoria de um PIMS tem o objetivo de demonstrar que o sistema de gestão está em conformidade com os requisitos da norma internacional apropriada.

A organização precisará revisar quaisquer não conformidades identificadas e fazer os ajustes apropriados, seja nas práticas de trabalho ou, quando for de sua competência, no requisito.

2.2.4 Como um sistema de gerenciamento de informações de privacidade (PIMS) pode ajudar na seleção de fornecedores

A certificação ISO/IEC 27701 demonstra que a organização/fornecedor possui um PIMS em vigor.

A garantia de uma certificação acreditada é mais rentável do que a realização de auditorias a fornecedores e proporciona a confiança necessária.

2.3 Relacionamentos do sistema de gerenciamento de informações de privacidade (PIMS)

2.3.1 Diferença entre um sistema de gerenciamento de informações de privacidade (PIMS) e um sistema de gerenciamento de segurança da informação (ISMS)

- ISO/IEC 27701 é uma extensão da ISO/IEC 27001
- O SGSI (ISMS) em conformidade com a ISO/IEC 27001 deve ter um escopo que cubra pelo menos o escopo do PIMS.

Requisitos adicionais da ISO/IEC 27701 que estão alinhados aos controles documentados na ISO/IEC 27001:

- compreender o papel legal e/ou regulatório da organização como controladora de dados e/ou processadora de dados
- compreender as necessidades e expectativas das partes interessadas, incluindo os titulares de dados apropriados
- o processamento de informações de privacidade no âmbito do sistema de gestão de informações de privacidade (PIMS)
- uma avaliação de impacto na privacidade (PIA) em quaisquer processos de avaliação e tratamento de riscos

2.3.2 A relação entre o princípio de proteção de dados de acordos apropriados de segurança da informação e a norma ISO/IEC 27701

Controles na ISO/IEC 27701 além do Anexo A da ISO/IEC 27001. Existem 31 controles no Anexo A e 18 controles no Anexo B: cada um dividido em 4 categorias idênticas:

1. Condições de recolha e processamento
2. Obrigações com os princípios de PII
3. Privacidade desde o design e por padrão
4. Compartilhamento, transferência e divulgação de PII

2.3.3 A utilidade da norma ISO/IEC 27002 para a implementação de um sistema de gestão de informações de privacidade (PIMS)

Um dos seis princípios de proteção de dados é um requisito para disposições adequadas de segurança da informação. Este requisito é tratado na ISO/IEC 27701 por um requisito de conformidade com a ISO/IEC 27001, apoiado pela orientação da ISO/IEC 27002.

O Capítulo 5 da ISO/IEC 27701 pega os requisitos da ISO/IEC 27001 e, quando apropriado, os estende levando em consideração os requisitos do PIMS.

Da mesma forma, o Capítulo 6 segue as orientações da ISO/IEC 27002 e, quando apropriado, amplia-as levando em consideração as orientações do PIMS. Assim, está implícito ao implementar um PIMS baseado na ISO/IEC 27701 que a ISO/IEC 27001 também deve ser implementada.

2.3.4 Como aplicar os controles do sistema de gerenciamento de informações de privacidade (PIMS)

1. Projete um conjunto de controles para gerenciar o risco
2. Compare esta lista de controles com aqueles no Anexo A (para controladores de dados) ou Anexo B (para processadores de dados) da ISO/IEC 27701
3. Crie uma declaração de aplicabilidade (SoA)
4. Estender a SoA produzida em relação a um sistema de gerenciamento de segurança da informação (ISMS) em conformidade com a ISO/IEC 27001.

3. PAPÉIS DO CONTROLADOR, PROCESSADOR E DATA PROTECTION OFFICER (DPO)

Controlador, Processador e Data Protection Officer

3.1 PAPÉIS DO CONTROLADOR E PROCESSADOR

3.1.1 As responsabilidades do controlador

"Controlador", a pessoa física ou jurídica, autoridade pública, agência ou outro organismo que, sozinho ou em conjunto com outros, determina os fins e os meios de processamento dos dados pessoais (extrato) O controlador é o responsável final por garantir que os dados pessoais sejam processados de acordo com o GDPR.

- Determinar a finalidade das atividades de processamento
- Implementar medidas técnicas e organizacionais para garantir a proteção de dados e demonstrar que o processamento é realizado de acordo com o GDPR
- Implementar políticas apropriadas
- Implementar os princípios de proteção de dados desde a concepção (by design) e por padrão (by default) e realizar análises de impacto sobre proteção de dados
- Garantir que qualquer processador terceirizado obedeça às regras
- Notificar violações de dados pessoais à autoridade supervisora independente
- Legalmente responsável e prestador de contas não são o mesmo que o responsável e prestador de contas (accountable) em uma matriz RACI
- GDPR Artigo 5 (2) declara
  - **"O controlador deve ser responsável por, e ser capaz de demonstrar conformidade com o parágrafo 1 ("prestação de contas")."**
  - Assim, de acordo com o princípio da prestação de contas, o Controlador é responsável e prestador de contas pela legalidade do processamento de dados.
- A autoridade supervisora vai manter o controlador como responsável e prestador de contas pelos dados sob seus cuidados.
- Se for imposta uma multa, o controlador será multado, mesmo que existam contratos por escrito entre o controlador e o processador
  - O controlador pode solicitar compensação do processador se o processador não cumpriu o contrato.

3.1.2 As responsabilidades do processador

"Processador", uma pessoa física ou jurídica, autoridade pública, agência ou outro organismo que trata dados pessoais em nome do controlador;

- Apenas executar atividades de processamento "sob o controle" de um controlador (veja também o próximo slide)
- Garantir que as pessoas autorizadas a processar os dados pessoais se comprometeram com a confidencialidade ou estão sob uma obrigação legal de confidencialidade adequada
- Tomar todas as medidas prescritas pelo artigo 32 "Segurança de processamento"
- Se um processador infringir o regulamento ao determinar as finalidades e meios de processamento, o processador será considerado um controlador em relação a esse processamento.
- Determinar aspectos técnicos de processamento, como os sistemas usados para processamento, como os dados são armazenados, medidas de segurança, mecanismos de transferência, etc.

3.1.3 O relacionamento entre o controlador e o processador

O processador deve

- Não envolver outro processador sem autorização prévia específica ou geral por escrito do controlador
- Apenas efetuar o processamento governado por um **contrato** ou outro ato jurídico sob os termos da lei da União ou dos Estados-Membros, que vincule o processador em relação ao controlador
- Apenas processar dados pessoais segundo **instruções** documentadas do controlador
- **Auxiliar** o controlador a tomar as medidas apropriadas
- À escolha do controlador, **excluir ou devolver** todos os dados pessoais ao controlador após o fim da prestação dos serviços relacionados ao processamento
- Disponibilizar ao controlador todas as informações necessárias para **demonstrar conformidade**

Controlador e processador

- Ambos devem cooperar com a autoridade supervisora, suporte ao data protection officer (DPO)

3.2 PAPEL E RESPONSABILIDADES DE UM DPO

3.2.1 Quando um DPO é obrigatório?

Artigo 37 Designação do data protection officer
O processamento é **realizado por uma autoridade ou órgão público**, exceto para os tribunais que atuam na sua capacidade judicial (cláusula 1a)
As principais atividades do controlador ou do processador consistem em operações de processamento que, em virtude de sua natureza, seu escopo e / ou seus objetivos, requerem monitoramento regular e sistemático dos titulares dos dados em grande escala (cláusula 1b)
As principais atividades do controlador ou do processador consistem no processamento em grande escala de categorias especiais de dados nos termos do artigo 9.º e de dados pessoais relativos a condenações penais e infrações referidas no artigo 10.º (cláusula 1c)
Outros casos além dos mencionados acima ... Quando exigido pela legislação da união ou do estado-membro ... (cláusula 4)

Um único DPO (se facilmente acessível) é permitido para "um grupo de empresas" e para "um grupo de autoridades ou organismos públicos". (cláusulas 2 e 3); portanto, um DPO pode ser "compartilhado"

Outros requisitos; o DPO:

- deve ser designado com base nas qualidades profissionais
- pode ser um membro da equipe do controlador ou processador
- pode ser uma pessoa externa trabalhando sob um contrato de serviço.

Casos: Quando um DPO é obrigatório?

Caso 1:
Hospital. Por exemplo, a atividade essencial de um hospital é fornecer serviços de saúde. No entanto, um hospital não poderia fornecer serviços de saúde com segurança e eficácia sem processar dados de saúde, como registros de saúde dos pacientes. Portanto, o processamento desses dados deve ser considerado uma das atividades principais de qualquer hospital e os hospitais **devem, portanto, designar DPOs.**

Caso 2:
Empresa de segurança privada. Como outro exemplo, uma empresa de segurança privada realiza a vigilância de uma série de centros comerciais privados e espaços públicos. A vigilância é a atividade principal da empresa, que por sua vez está intimamente ligada ao processamento de dados pessoais. **Portanto, essa empresa também deve designar um DPO.**

Caso 3:
Uma **pequena empresa familiar** ativa na distribuição de eletrodomésticos em uma única cidade usa os serviços de um processador cuja atividade principal é fornecer serviços de análise de sites e assistência com publicidade e marketing direcionados. As atividades da empresa familiar e dos seus clientes não geram processamento de dados em "grande escala", considerando o pequeno número de clientes e as atividades relativamente limitadas. No entanto, as atividades do processador, tendo muitos clientes como esta pequena empresa, em conjunto, está realizando **processamento em larga escala**. O **processador** deve, portanto, designar um DPO nos termos do artigo 37.°, n.° 1, alínea b). Ao mesmo tempo, a própria empresa familiar não tem a obrigação de designar um DPO.

3.2.2 Papel e responsabilidades de um DPO

O data protection officer é independente (não recebe instruções sobre o exercício de suas funções), e

- Está envolvido em todas as questões relacionadas à proteção de dados pessoais
- Aconselha o controlador com relação à avaliação do impacto sobre a proteção de dados
- Deve manter seu conhecimento especializado
- Reporta-se ao mais alto nível de gestão do controlador
- Está acessível aos titulares dos dados
- Está sujeito a sigilo ou confidencialidade.

No entanto, o DPO pode executar outras tarefas, desde que não resultem em conflito de interesses.

Tarefas (primárias / obrigatórias)

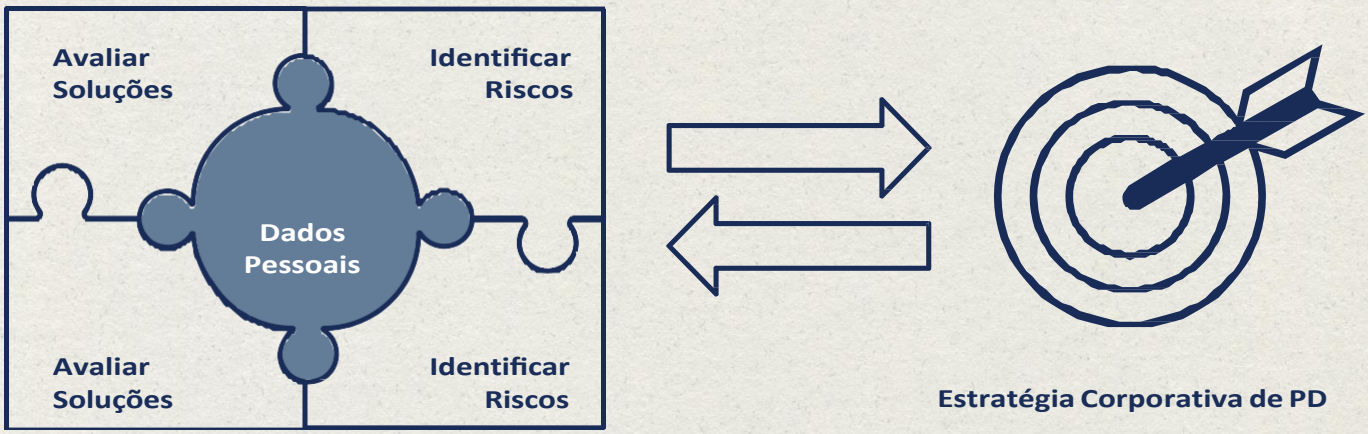
1. Informar e aconselhar o controlador ou o processador e os empregados que realizam o processamento sobre suas obrigações
2. Monitorar a conformidade com o GDPR (e qualquer legislação nacional adicional relacionada)
3. Fornecer aconselhamento quando solicitado; no que diz respeito à avaliação do impacto sobre a proteção de dados
4. Cooperar com a autoridade supervisora
5. Atuar como ponto de contato para a autoridade supervisora

3.2.3 A posição do DPO em relação às autoridades de proteção de dados

- O DPO é a ligação imediata com a autoridade supervisora (PUC)
- Obrigações
  - Cooperar com a autoridade supervisora
  - Atuar como ponto de contato para a autoridade supervisora , por exemplo
    - em todos os assuntos de processamento
    - consulta prévia

4. AVALIAÇÃO DE IMPACTO SOBRE A PROTEÇÃO DE DADOS (DPIA)

Avaliação de Impacto sobre a Proteção de Dados



REQUISITOS DO GDPR UE

Fonte: J. Kyriazoglou

official course

4.1 CRITÉRIOS PARA UMA DPIA

4.1.1 APLICAÇÃO DOS CRITÉRIOS PARA CONDUÇÃO DE UMA DPIA

Condições primárias: (GDPR)

- No caso de uma avaliação sistemática e extensa de aspectos pessoais relativos a pessoas físicas, que se baseia em processamento automatizado, incluindo criação de perfis
- Em caso de processamento em grande escala de categorias especiais de dados ou dados pessoais relativos a condenações criminais e infrações
- No caso de monitoramento sistemático de uma área acessível ao público em grande escala

Devem ser considerados os seguintes critérios:

1. Avaliação ou pontuação
2. Tomada de decisão automatizada com efeito legal ou significativo semelhante
3. Monitoramento sistemático
4. Dados sensíveis
5. Dados processados em grande escala
6. Conjuntos de dados que foram comparados ou combinados
7. Dados sobre titulares de dados vulneráveis
8. Uso inovador ou aplicação de soluções tecnológicas ou organizacionais
9. Transferência de dados através das fronteiras fora da União Europeia
10. Quando o próprio processamento "impede que os titulares dos dados exerçam um direito ou utilizem um serviço ou contrato"

CASOS: APLICAÇÃO DOS CRITÉRIOS PARA CONDUÇÃO DE UMA DPIA

- DPIA REQUERIDA -

Caso 1:
Um hospital que processa os dados genéticos e de saúde de seus pacientes (sistema de informações do hospital).
Critérios: (1) Dados sensíveis, (2) Dados relativos a titulares de dados vulneráveis

Caso 2:
O uso de um sistema de câmeras para monitorar o comportamento de direção nas rodovias. O controlador pretende usar um sistema de análise de vídeo inteligente para selecionar carros e reconhecer placas de licença automaticamente.
Critérios: (1) Monitoramento sistemático, (2) Uso inovador ou aplicação de soluções tecnológicas ou organizacionais

Caso 3:
Uma empresa que monitora as atividades de seus empregados, incluindo o monitoramento da estação de trabalho, atividade na Internet, etc.
Critérios: (1) Monitoramento sistemático, (2) Dados relativos a titulares de dados vulneráveis

- DPIA NÃO REQUERIDA -

Caso 1:
Uma revista online que usa uma lista de mala direta para enviar um resumo diário genérico a seus assinantes.
Critérios: Nenhum

Caso 2:
Um site de comércio eletrônico exibindo anúncios de peças de carros antigos envolvendo criação limitada de perfis com base no comportamento de compras anteriores em certas partes de seu site.
Critérios: Avaliação ou pontuação, mas não sistemática ou extensa

4.1.2 OBJETIVOS E RESULTADOS DE UMA DPIA

Objetivos

DPIAs são usadas para identificar riscos específicos para dados pessoais como resultado de atividades de processamento; o foco está na privacidade e proteção de dados.

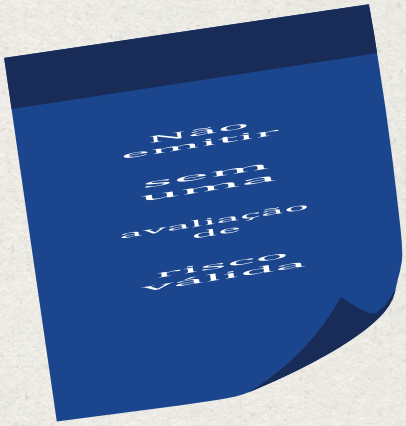
- Analisar como os programas, funções, sistemas e processos coletam, usam, compartilham e mantêm dados pessoais para garantir a conformidade com as leis e políticas aplicáveis de privacidade / proteção de dados; e
- Determinar os riscos aos dados pessoais inerentes aos programas, sistemas, funções, projetos e processos.

Resultados

- Uma descrição do processamento e seus propósitos
- Os interesses legítimos que você busca com este processamento
- Uma avaliação da necessidade e proporcionalidade do processamento
- Uma avaliação dos riscos para os direitos e liberdades dos titulares dos dados
- As medidas previstas para enfrentar os riscos
- Todas as salvaguardas e medidas de segurança para demonstrar a conformidade com o Regulamento
- Indicações de prazos se o processamento incluir o apagamento de dados pessoais
- Uma indicação de qualquer medida de proteção de dados desde a concepção (by design) e por padrão (by default)
- Uma lista dos destinatários dos dados pessoais
- Conformidade com códigos de conduta aprovados
- Detalhes sobre se os titulares dos dados foram consultados e consentiram

4.2 ETAPAS DE UMA DPIA

4.2.1 OS PASSOS DE UMA DPIA



1. Identificar a necessidade de uma DPIA
2. Descrever os fluxos de informação
3. Identificar a privacidade e os riscos relacionados
4. Identificar e avaliar soluções de privacidade
5. Assinar e registrar os resultados
6. Integrar os resultados em um plano de projeto
7. Consultar as partes interessadas internas e externas

Fonte: enisa.europa.eu

4.2.1 AS ETAPAS DE UMA DPIA

Alguns exemplos de riscos aos dados pessoais:
Hacking, vírus, malware, invasores, phishing, falta de treinamento, portadores de dados não criptografados , controle de acesso deficiente, senhas fracas, etc.

Quatro possíveis respostas a riscos:

1. Tratar (também conhecido como: controle, modificação de risco)
2. Tolerar (também conhecido como: aceitação de risco, retenção de risco)
3. Encerrar (também conhecido como: prevenção de risco)
4. Transferência (também conhecida como: compartilhamento de risco)

4.2.2 EXECUÇÃO DE UMA DPIA EM UMA SITUAÇÃO ESPECÍFICA

As sete etapas

1. Identificar a necessidade de uma DPIA
2. Descrever os fluxos de informação
3. Identificar riscos para a privacidade e relacionados
4. Identificar e avaliar soluções de privacidade
5. Dar encerramento, assinar e registrar os resultados
6. Integrar os resultados em um plano de projeto
7. Consultar partes interessadas internas e externas

} Cinco "Estágios principais"

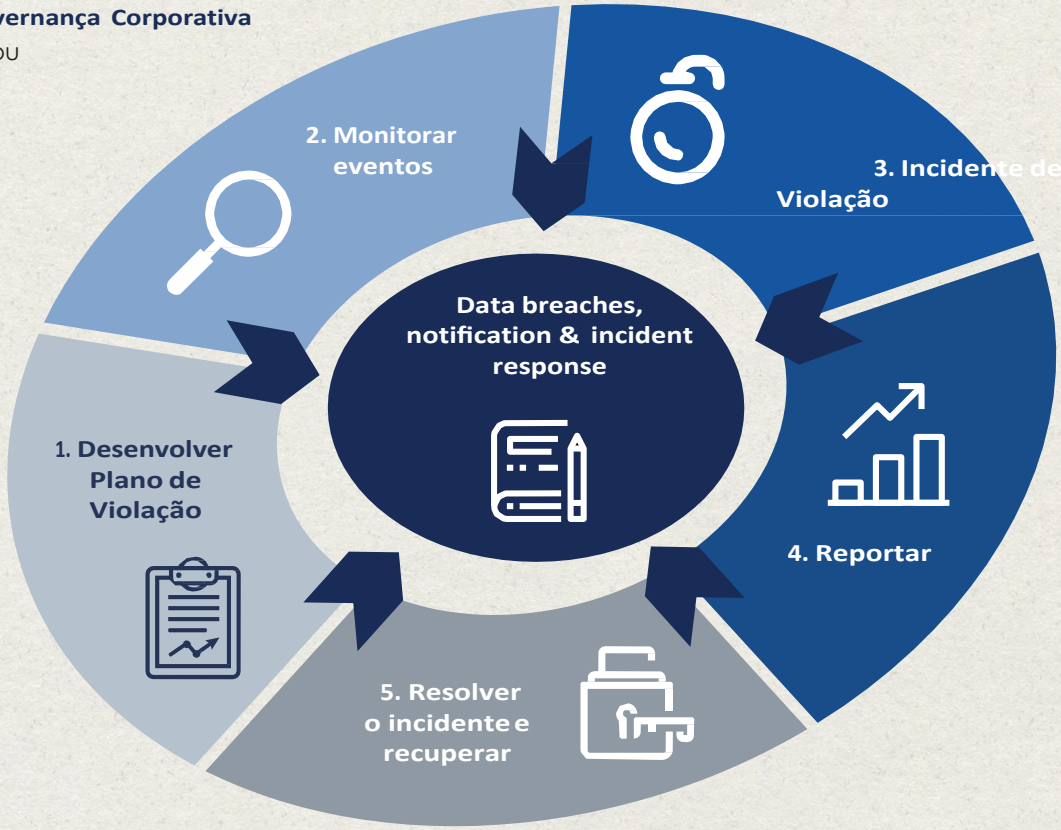
Consulta de partes interessadas

- Partes interessadas internas; por exemplo, equipes de projeto, DPO, jurídico, compras, equipe de TI, etc.
- Partes interessadas externas; por exemplo, titulares de dados, autoridade supervisora, etc.

5. VIOLAÇÕES DE DADOS, NOTIFICAÇÃO E RESPOSTA A INCIDENTE

CICLO DE VIDA DA VIOLAÇÃO DE DADOS

Framework de Governança Corporativa
Fonte: J. Kyriazoglou



5.1 REQUISITOS GDPR COM RELAÇÃO A VIOLAÇÕES DE DADOS PESSOAIS

5.1.1 UMA VIOLAÇÃO DE DADOS NOS TERMOS DO GDPR

1. Incidente → Incidente de segurança
(evento de segurança de informação → Violação de dados)

2. **Violação de dados pessoais** significa uma violação de segurança que leva
   Destruição acidental
   Destruição ilegal
   Perda
   Alteração
   Divulgação não autorizada
   Acesso não autorizado
   ... de / a **dados pessoais** transmitidos, armazenados ou processados de outra forma.

5.2 REQUISITOS PARA NOTIFICAÇÃO DE VIOLAÇÕES DE DADOS

5.2.1 NOTIFICAÇÃO DA AUTORIDADE SUPERVISORA

O que?

- O controlador deve documentar todas as **violações de dados pessoais,** compreendendo os fatos relacionados à violação de dados pessoais, seus efeitos e as medidas corretivas tomadas. cláusula 5)

Quando?

- **O processador** deve, sem atraso injustificado depois de tomar conhecimento da violação de dado pessoal, notificar o controlador. (Cláusula 2)
- **O controlador** deve, sem atraso injustificado depois de tomar conhecimento da violação de dado pessoal, notificar a **autoridade supervisora.**; e NÃO depois de 72 horas após ter tomado conhecimento da violação. (cláusula 1)

Quando não?

- Quando é improvável que a violação de dados pessoais resulte em risco para os direitos e liberdades das pessoas físicas. (cláusula 1)

Como? Notificação contém:

1. Natureza da violação de dados pessoais, incluindo: categorias e número aproximado de titulares de dados e registros de dados afetados;
2. Nome e detalhes de contato do DPO (ou outro contato);
3. As prováveis consequências da violação de dados pessoais;
4. Medidas tomadas e/ou propostas (incluindo aquelas para mitigar possíveis efeitos adversos).

5.2.2 NOTIFICAÇÃO DO TITULAR DOS DADOS

Quando?

- A violação de dados pessoais pode resultar em um **alto risco** para os direitos e liberdades das pessoas físicas

Quando não?

- Se o controlador implementou medidas que evitam que os dados pessoais sejam lidos por pessoas não autorizadas (por exemplo, criptografia)
- Se o controlador tiver tomado medidas para garantir que "alto risco" provavelmente não se materialize.
- Se a notificação do titular dos dados exigir um esforço desproporcional (por exemplo, um grande número de titulares dos dados; neste caso, uma comunicação pública seria considerada uma "forma igualmente eficaz")

Como?

- Em linguagem clara e simples
- Em estreita cooperação com a autoridade supervisora

Notificação contém:

1. Nome e detalhes de contato do DPO (ou outro contato);
2. As prováveis consequências da violação de dados pessoais
3. As medidas tomadas ou propostas para lidar com a violação de dados pessoais (incluindo aquelas para mitigar possíveis efeitos adversos).

CASO: NOTIFICAÇÃO DO TITULAR DOS DADOS VIOLAÇÃO DE DADOS E MEDIDAS PROPOSTAS

Violação de dados

Ataque via ransomware.
Efeitos aos dados pessoais: Nenhum dado pessoal foi danificado, roubado ou prejudicado.

Medidas correntes

1. Backup em 2 locais
2. Anti-malware
3. Monitoração da segurança
4. Firewalls

Propostas de novas medidas a serem tomadas

1. Treinar a equipe em técnicas de engenharia social.
2. Bloquear endereços IP e sites maliciosos conhecidos (Nota 1).

5.2.3 OS ELEMENTOS DA OBRIGAÇÃO DE DOCUMENTAÇÃO DO GDPR EM RELAÇÃO A VIOLAÇÕES DE DADOS

- Existe uma obrigação geral de manter registros das atividades de processamento
- O controlador deve documentar quaisquer violações de dados pessoais, incluindo
    1. Os fatos relativos à violação de dados pessoais; natureza, categorias e número de dados e titulares de dados
    2. O nome e detalhes de contato do DPO
    3. Seus efeitos (consequências)
    4. As medidas e ações corretivas tomadas

- O controlador deve documentar quaisquer violações de dados pessoais
  Essa documentação deve permitir à autoridade supervisora verificar o cumprimento do artigo 33: *Notificação de uma violação de dados pessoais à autoridade supervisora*

- O certificado impulsiona **oportunidades de carreira**
- O certificado contribui para a **produtividade**
- Treinamento e certificação são motivadores de **satisfação**

- **Economize 25% dos custos** treinando o talento que você já possui (Gartner).
- **Defesa** contra o **envelhecimento da força de trabalho de TI**
- **Autoestima do empregado** aprimorada
- Melhor **qualidade** em processos e infraestrutura de TI
- O desenvolvimento de habilidades da equipe reduz as falhas, diminui os custos, aumenta a **eficácia**
- **Retenção de pessoal**
- **Vencer a concorrência**

EXIN. THE MOST RENOWNED EXAMINATION INSTITUTE FOR IT PROFESSIONALS

- Complete portfolio of Information Management
- Exams in 165 countries
- Exams in 20 languages
- 2 million EXIN-certified professionals
- International network of accredited partners

SOBRE EXIN

Publicado e projetado pelo EXIN. EXIN é o instituto de certificação independente global para profissionais no domínio de TI. Com mais de 30 anos de experiência na certificação das competências de mais de 2 milhões de profissionais de TI, EXIN é a autoridade líder e confiável no mercado de TI. Com mais de 1000 parceiros credenciados, o EXIN facilita exames e avaliações de competência eletrônica em mais de 165 países e 20 idiomas. EXIN é o co-iniciador da Estrutura de e-Competence, que foi criada para fornecer princípios de medição de certificação de TIC inequívocos dentro e fora da Europa.