PDPP

Módulo 1 - Introdução

Boas-Vindas

PDPP - EXIN Privacy & Data Protection Practitioner

Este curso faz parte do programa de qualificação EXIN Privacy & Data Protection

Para se tornar um Data Protection Officers (DPO), precisa ser aprovado em:

- **PDPF** - Privacy & Data Protection Foundation
- **ISFS** - ISO 27001 Foundation

PRATICTIONER

FOUNDATION

ESSENTIALS

GDPR e LGPD

PDPF - EXIN Privacy & Data Protection Foundation

e PDPP - EXIN Privacy & Data Protection Practitioner

- Foco exclusivamente no **GDPR** – Lei Europeia
- Neste mundo globalizado, vai ser raro não fazer negócios com empresas da União Europeia.

PDPE - EXIN Privacy & Data Protection Essentials

- Certificação baseada na **LGPD** – Lei totalmente Brasileira.
- “Essentials” é mais genérico e é voltado exclusivamente para conscientização de todo mundo na empresa.

Visão Geral do Curso PDPP

- Explosão cada vez maior de informações na internet, apps e redes sociais gerenciar e proteger a privacidade das pessoas e seus dados
- Novas leis na UE, assim como nos EUA e em muitas outras regiões
- Implementação de políticas e procedimentos para o cumprimento da legislação
- Estabelecimento de um Sistema de Gestão de Proteção de Dados (SGPD)
- Norma ISO/IEC 27701:2019 Técnicas de Segurança – Extensão da ISO/IEC 27001 e 27002 para Gestão de Informações de Privacidade – Requisitos e Diretrizes

Objetivos e Público-alvo da Certificação PDPP

A certificação EXIN Privacy & Data Protection Practitioner (PDPP) visa

- Valida o conhecimento e a compreensão de um profissional em relação à legislação de privacidade e proteção de dados europeia e sua relevância internacional.
- Aplicar esse conhecimento e compreensão à sua prática profissional diária.

Público-Alvo

- Data Protection Officers (DPOs)
- Escritório de Privacidade (Privacy Office)
- Legal / Compliance officers
- Security officers
- Gerentes de Continuidade de Negócios
- Controladores de Dados
- Auditores de Proteção de Dados (internos e externos)
- Analistas de Privacidade
- Gerentes de RH

Atividades Práticas

A realização das atividades práticas faz parte dos requisitos da certificação para EXIN Privacy & Data Protection Practitioner (PDPP).:

- ✔ Ao final do treinamento serão propostas três atividades práticas, a serem desenvolvidas e avaliadas por instrutor credenciado.
- ✔ Caso tenham sido cumpridos um mínimo de 9 dos 14 (65%) critérios, o candidato terá concluído com sucesso os trabalhos práticos.
- ✔ As atividades práticas e instruções aparecem ao final deste curso.

Sobre o Exame PDPP

Tipo de exame:	40 - Questões de múltipla escolha
Número de questões:	65% (26 questões)
Pontos para aprovação:	90 minutos
Duração do exame:	Não
Anotações :	Não
Equipamentos eletrônicos:	O texto do GDPR pode ser consultado durante todo o exame;
Consulta:	Será fornecido como um apêndice no exame digital.

Exige compreensão dos conceitos, aplicação do conhecimento e análise de situações.

PDPP

Módulo 2: Políticas de proteção de dados

Relembrando as Principais Definições

O propósito geral do GDPR é, através de uma lei unificada, proteger os direitos, a privacidade e as liberdades das pessoas físicas na UE

- Dados Pessoais: qualquer informação relativa a uma pessoa física identificada ou identificável
- Processamento: qualquer operação ou conjunto de operações efetuadas em dados pessoais, ou em conjuntos de dados pessoais, por meios automatizados ou não
- Controlador: pessoa física ou jurídica, autoridade pública, agência ou outro organismo que, individualmente ou em conjunto com outros, determina os fins e os meios de processamento de dados pessoais
- Processador: pessoa física ou jurídica, autoridade pública, agência ou outro organismo que processa dados pessoais em nome do controlador
- Autoridade Supervisora: representa uma organização governamental que será responsável por reforçar a aplicação do GPDR

Políticas e GDPR

O Regulamento indica várias práticas e documentos que qualquer organização deve ser capaz de oferecer.

O controlador deve adotar políticas internas e aplicar medidas que respeitem os princípios da proteção de dados. Esses princípios são aqueles referentes à proteção desde a concepção (*by design*) e por padrão (by *default*)

Por políticas internas devemos entender que a organização declara de forma transparente e consistente de que forma ela atende aos requisitos do regulamento.

Políticas e Conformidade

- O Controlador deve desenvolver uma política explícita, documentada, de proteção de dados pessoais totalmente aderente à conformidade da organização ao GDPR.

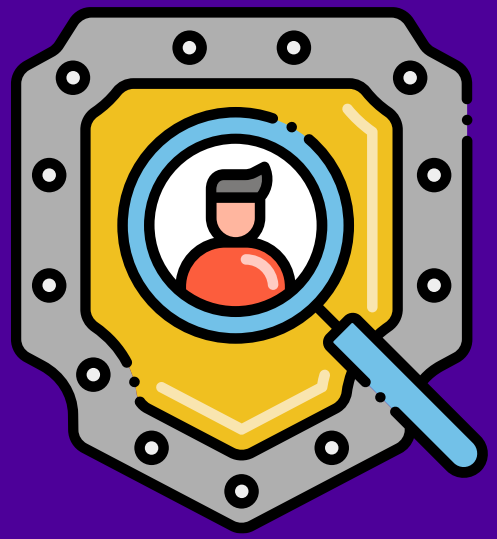
- Os DPOs devem monitorar de perto a aderência às políticas como parte da garantia de conformidade da organização às leis e regulamentações apropriadas.

- Uma política formal e auditável de privacidade e proteção de dados pessoais é de total interesse de potenciais parceiros e clientes.

- Tornar pública indica transparência, permite que os parceiros e clientes avaliem a política e oferece para as autoridades supervisoras e outros reguladores uma posição clara que pode ser avaliada por eles.

Elementos da Política

Uma política deve incluir certas informações logo na coleta dos dados (Artigo 13 do GDPR):



- Identidade e detalhes de contato do DPO e do Controlador, e se o Controlador pretende transferir dados para outro país ou outra empresa internacional, entre outros.
- Informações adicionais sobre como o processamento é transparente e justo, como prazo de retenção e os direitos dos titulares dos dados.
- Texto mais específico ou genérico como “o período de armazenamento dos dados pessoais será determinado pelo contrato celebrado com o titular dos dados”.

Disponibilização da Política

A sua política deve estar acessível, no mesmo lugar onde os dados pessoais são coletados:

WEBSITE

LOJA FÍSICA

QUALQUER OUTRO MECANISMO

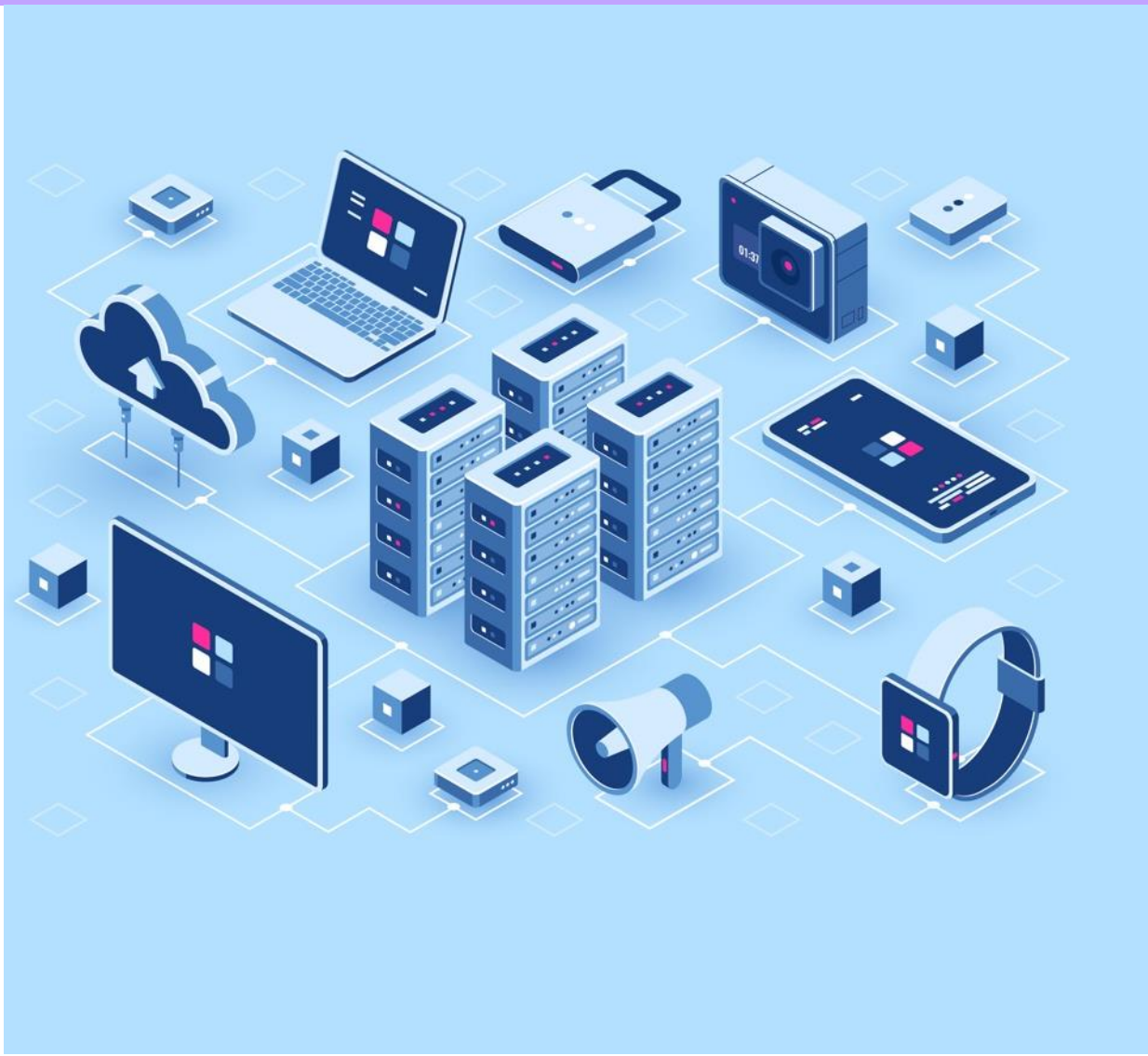
Exemplo de Tópicos de Política de Proteção de Dados

1. Propósito
2. Compromisso
3. Oportunidade de recusa
4. Coleta de informações pessoais
5. Uso da informação
6. Verificação de referências de crédito
7. Divulgação da informação
8. Proteção da informação
9. Acesso à Internet
10. Monitoração das comunicações
11. Solicitação de acesso do titular dos dados
12. Violações de proteção de dados
13. Contato

Política de Segurança da Informação

A política de segurança da informação pode ser um único documento, ou aparecer na forma de um conjunto de políticas de segurança (Normas ISO 27000)

- Controle de acesso
- Classificação da informação
- Backup
- Transferência de informação
- Antivírus e anti-malware
- Gerenciamento de vulnerabilidade
- Criptografia
- Comunicações
- Relações com fornecedores



Conteúdo de Políticas de Segurança da Informação

Uma boa política reflete os objetivos da organização e, ao mesmo tempo, direciona as ações.

Além disso, elas deveriam também:

- Esclarecer por que a política é necessária
- Descrever o escopo, ou o que é coberto pela política
- Definir contatos e responsabilidades
- Incluir pelo menos um objetivo
- Explicar como as violações serão tratadas

Políticas Efetivas

- Para que uma política realmente funcione, é necessário que ela seja suportada por processos e procedimentos aderentes aos parâmetros definidos dentro da própria política.
- Os processos e procedimentos devem ser criados com a visão de produzir evidência de que foram implementados de forma correta.
- Suítes de ferramentas de suporte à documentação, com seus vários modelos e templates, podem ser muito práticas e efetivas em custo como ponto de partida para o desenvolvimento da documentação de conformidade ao GDPR da forma mais apropriada.

Proteção de Dados Desde a Concepção (by design)

O GDPR estabelece que o Controlador deve adotar políticas e implementar medidas que atendam, em especial, aos princípios de proteção de dados desde a concepção (by design) e por padrão (by default).

Proteção de dados desde a concepção (by design)

Abordagem que garante que você vai considerar as questões de privacidade e proteção de dados durante a fase de desenho ou de projeto de qualquer sistema, serviço, produto ou processo, e ao longo de todo o ciclo de vida.

Aplicação da Proteção de Dados Desde a Concepção (by design)

Quer dizer que você integrou ou "embutiu" a proteção de dados nas suas atividades de processamento e práticas de trabalho:

- Desenvolver novos sistemas de TI, serviços, produtos e processos que envolvem dados pessoais
- Desenvolver políticas e processos organizacionais, e práticas de negócio ou estratégias que possuem implicações de privacidade
- Executar projetos físicos
- Se envolver em iniciativas de compartilhamento de dados
- Utilizar dados pessoais para novos propósitos.

Proteção de Dados por Padrão (by default)

O princípio de proteção de dados desde a concepção foi expandido no GDPR para incluir a proteção de dados por padrão (by *default*)

- Exige de você a garantia de apenas processar os dados necessários para atingir um propósito específico.
- Especificar que dados são esses antes do início do processamento.

Aplicação da Proteção de Dados por Padrão (by default)

Depende das circunstâncias de seu processamento e dos riscos aos indivíduos. De uma forma geral, no entanto, você deve considerar coisas como:

- Abordagem de privacidade em primeiro lugar com quaisquer configurações de sistemas e aplicativos;
- Não forneça uma escolha ilusória ou enganosa aos indivíduos em relação aos dados que você vai processar;
- Não processar dados adicionais, a menos que a pessoa decida que você pode;
- Dados pessoais não sejam automaticamente disponibilizados publicamente a terceiros;
- Fornecer às pessoas controles e opções suficientes para exercer seus direitos.

Responsáveis Pela Proteção Desde a Concepção e Por Padrão

O Artigo 25 do GDPR especifica que, como controlador, você tem a responsabilidade pela conformidade com a proteção de dados desde a concepção e por padrão.

- Altos executivos, por exemplo, atuando no desenvolvimento de uma cultura de “consciência de privacidade”
- Engenheiros de software, arquitetos de sistema e desenvolvedores de aplicativos, e todos aqueles que projetam sistemas, produtos e serviços, devem levar em conta os requisitos de proteção de dados;
- Nas suas Práticas comerciais e de negócio, você deve garantir que elas incorporem a proteção de dados desde a concepção em todos os seus processos e procedimentos internos;

É isso que o Regulamento ordena: que as medidas para garantir que os direitos e liberdades dos titulares dos dados sejam preservados, funcionem.

Processadores e a Proteção de Dados

Desde a Concepção (by design) e por Padrão (by default)

> O Artigo 28 menciona os cuidados que você deve ter sempre que estiver selecionando um processador. Por exemplo, você só deve usar processadores que oferecem garantias suficientes para implementar medidas técnicas e organizacionais adequadas, para que o processo cumpra os requisitos do regulamento e assegure a proteção dos direitos do titular dos dados.

> Seu Processador não pode, necessariamente, ajudar você nas obrigações de proteção de dados desde a concepção (*by design*) ao contrário das medidas de segurança.

Organizações Terceiras e a Proteção de Dados

Desde a Concepção (by design) e por Padrão (by default)

O Preâmbulo 78 estende os conceitos de proteção de dados desde a concepção a outras organizações. Mas atenção! Não há imposição para que essas outras empresas cumpram os princípios.

Empresas terceiras que desenvolvem produtos, serviços e aplicativos devem ser incentivadas a levar em consideração o direito de proteção de dados nos seus desenvolvimentos e projetos e na aplicação das técnicas.

Deve-se considerar os princípios e técnicas aplicáveis da proteção de dados desde a concepção e por padrão, conforme aparece no Artigo 47 (2d).

O Que Deve Ser Feito na Prática

Considere as questões de proteção de dados desde o início de qualquer atividade de processamento, e adote as políticas e ações apropriadas que atendam aos requisitos da proteção de dados desde a concepção e por padrão.

- Minimizar o processamento dos dados pessoais
- “Pseudonimização” de dados pessoais assim que possível
- Garantir a transparência com relação aos papéis e processamento de dados pessoais
- Permitir que os indivíduos monitorem o processamento
- Criação e aperfeiçoamento de recursos da segurança

Quando As Ações Devem Ser Tomadas

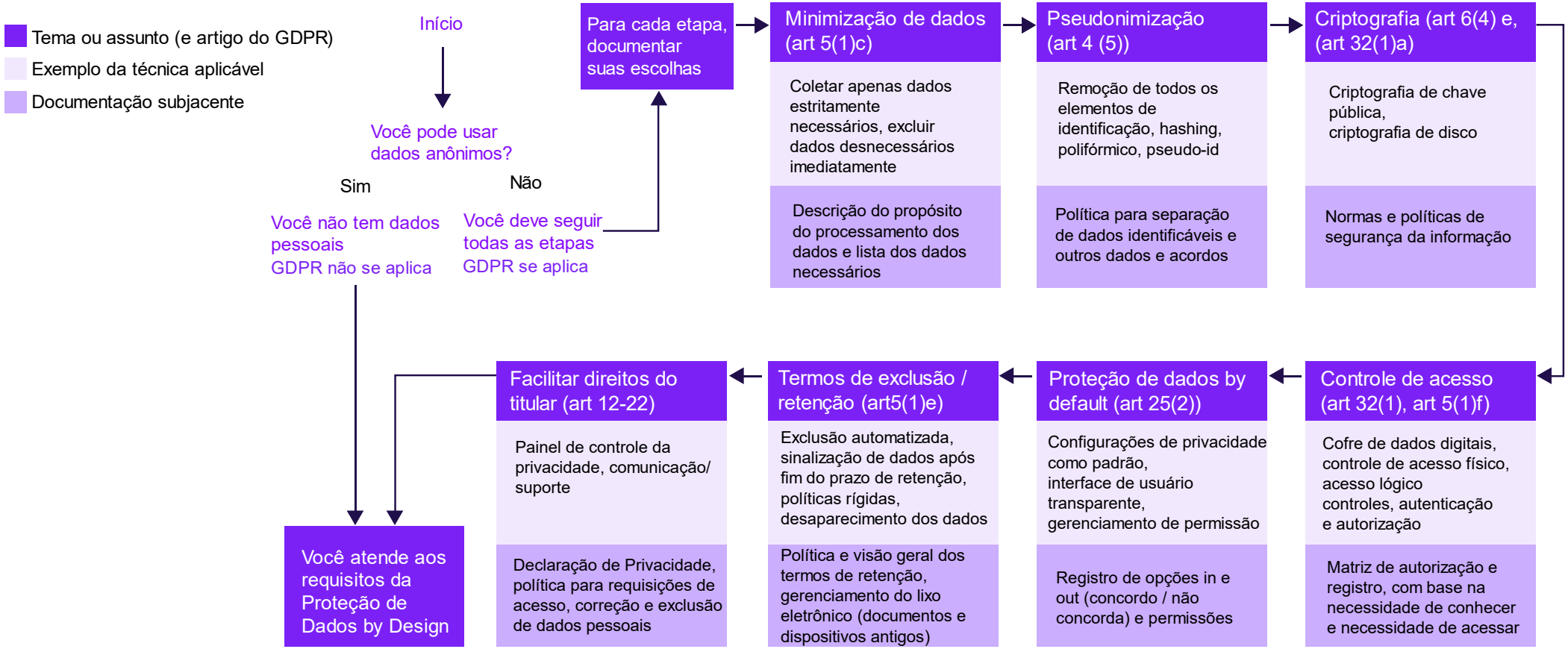
Você deve começar com as ações de proteção de dados na fase inicial de qualquer sistema, serviço, produto ou processo.
Considerações:

- Envolver o que existir de melhor, o estado da arte em termos de medidas
- Custos envolvidos
- Natureza, escopo, contexto e propósitos do seu processamento
- Riscos que o seu processamento impõe aos direitos e liberdades das pessoas

"No momento da determinação dos meios de processamento".

"No momento do processamento em si", ou seja, durante todo o ciclo de vida.

Framework de Proteção de Dados by Design



https://uploads-ssl.webflow.com/5d5d0a0090052fec16249aaab/5e3038105251e1325b280818_Privacy%20by%20Design%20framewor

Os 7 Princípios Fundamentais da Proteção de Dados

- Foram desenvolvidos por Ann Cavoukian, Ph.D, como *Information and Privacy Commissioner* de Ontario, na década de 1990, e atualizados desde então.
- O futuro da privacidade não pode ser garantido apenas pela conformidade com marcos regulatórios; em vez disso, a garantia de privacidade deve, idealmente, se tornar o padrão
- Se estende aos elementos de sistemas de TI (inclusive no uso de algoritmos, big data e inteligência artificial), práticas responsáveis de negócio, projeto físico e infraestrutura de rede
- Podem ser aplicados a todos os tipos de informações pessoais, mas com maior força para dados confidenciais
- A força das medidas de privacidade tendem a ser proporcionais à sensibilidade dos dados.

1: Proativo, não reativo; preventivo, não corretivo

Os objetivos da privacidade desde a concepção ou *by design* são garantir a privacidade e controle sobre as informações pessoais; e para as organizações, garantir uma vantagem competitiva sustentável

- Comprometimento por parte dos níveis mais altos da empresa
- Compartilhar o comprometimento com a privacidade abertamente entre as comunidades de usuários e acionistas
- Estabelecimento de métodos para reconhecer desenhos não tão bons com relação à privacidade, antecipar práticas não adequadas de privacidade e suas consequências

Desafio e Implementação

- Liderança e mudança cultural
- Introdução de arquitetura corporativa

2: Privacidade como Configuração Padrão

Nenhuma ação é necessária por parte da pessoa para proteger sua privacidade – a proteção está integrada ao sistema, por padrão.

- Especificação do propósito
- Limitação da coleta
- Minimização dos dados
- Limitação no uso, retenção e divulgação de informações pessoais

Desafio e Implementação

Publicação de políticas especializadas como "privilégio de acesso mínimo", "necessidade de saber", “menor confiança”.

3: Privacidade Incorporada ao Desenho

Proteção de Dados desde a concepção está incorporada ao projeto, à arquitetura de sistemas de TI e práticas de negócio. Mas não pendurada como um complemento, depois que alguma coisa acontece.

- Holística, pois contextos adicionais e mais amplos devem sempre ser considerados
- Integrada, porque todas as partes interessadas precisam ser consultadas
- Criativa, pois incorporar privacidade pode significar reiventar as suas escolhas

Desafio e Implementação

TPM (Trusted Platform Module): um chip microcontrolador que pode armazenar com segurança artefatos usados para autenticar uma plataforma.

SAMM (Software Assurance Maturity Model), um framework aberto que auxilia as organizações a formular e implementar uma estratégia de segurança de software sob medida para os riscos específicos.

CLASP (Comprehensive, Lightweight Application Security Process), uma metodologia de desenvolvimento seguro de software orientada a atividades e papéis.

4: Funcionalidade Total - Soma Positiva, Não Soma Zero

A Proteção de Dados "*by design*" busca acomodar todos os interesses e objetivos legítimos de uma maneira positiva para todos.

- Evitar a pretensão de falsos conflitos como privacidade versus segurança, demonstrando que é possível usufruir dos benefícios de ambas.
- Deve ser feito de uma forma que não comprometa a plena funcionalidade e que permita que todas as exigências sejam otimizadas tanto quanto possível.

Desafio e Implementação

Os conflitos a serem resolvidos:

- Facilidade de acesso versus acesso seguro
- Conveniência do usuário versus segurança
- Simples para implementar versus simples para usar.

5: Segurança de Ponta a Ponta e Proteção Durante Todo o Ciclo de Vida dos Dados

- A Proteção de Dados “by design” tendo sido incorporada ao sistema antes que o primeiro elemento da informação seja coletado, se estende com segurança durante todo o ciclo de vida dos dados envolvidos;
- Garante que todos os dados sejam retidos com segurança e, depois, destruídos com segurança no final do processo, em tempo hábil.
- Garantir a confidencialidade, integridade e a disponibilidade dos dados pessoais ao longo de todo o ciclo de vida, incluindo métodos seguros e fortes de destruição, criptografia e controle de acesso.

Desafio e Implementação

- **DBSec** – conferência anual internacional que cobre pesquisas abrangentes em segurança e privacidade de dados e de aplicações.
- **IAM** (Gerenciamento de Gestão e Acesso) - framework desenvolvido para processo de negócios que garante maior controle para o registro e segurança de identidades digitais ou eletrônicas.

6: Visibilidade e Transparência

Assegurar a todas as partes interessadas que, seja qual for a prática ou tecnologia de negócio envolvida, ela está, de fato, operando de acordo com as promessas e objetivos declarados, sujeito a verificação independente.

- Componentes e operações permanecem visíveis e transparentes
- Políticas e procedimentos relacionados à privacidade devem ser documentados e comunicados conforme for apropriado, e então, designados a um indivíduo específico
- Ao transferir informações pessoais para terceiros, devem ser asseguradas medidas equivalentes de proteção à privacidade
- Monitorar, avaliar e verificar a conformidade com as políticas e procedimentos de privacidade

Desafio e Implementação

- Utilização de padrões abertos
- Avaliação e validação externas como auditorias ISO/IEC 27001
- Publicação de políticas de segurança

7: Respeito à Privacidade do Usuário

Exige que as empresas prezem ao máximo pelos interesses do indivíduo. Isso é feito por meio de medidas.

- Consentimento específico, dado livre e espontâneo para a coleta, uso e divulgação de seus dados pessoais, exceto em casos permitidos pela lei.
- Quanto maior for a sensibilidade do dado, mais claro e específico deve ser o consentimento exigido
- Acurácia ou precisão das informações pessoais
- Os indivíduos precisam ter acesso a seus dados pessoais, e serem informados de seus usos e divulgações
- Pedir e conseguir as correções
- Mecanismo para reclamações e remediações sobre privacidade

Desafio e Implementação

Equilíbrio entre proteção dos dados da empresa e os direitos do titular de dados

Framework de Governança Corporativa

Visão e Missão

Desenvolvimento dos Produtos/Serviços

Desenvolvidos seguindo o que é preconizado pelos Sete Princípios da Proteção de Dados *By Design*

Gestão da Privacidade

Fonte: J.Kyriazolou

PDPP

Módulo 3: Sistema de Gestão de Informações de Privacidade (PIMS)

Introdução

Segurança da Informação e norma ISO 27001

A segurança da informação é um dos principais elementos que devemos considerar ao desenvolver ou aprimorar um sistema de gerenciamento de informações de privacidade (PIMS).

Por que é importante aprender sobre o PIMS?

- É pelo PIMS que as pessoas saberão como fazer toda a gestão da privacidade;
- Muitas empresas estão considerando o uso da norma ISO/IEC 27701:2019.

O que esperar deste módulo?

- Compreender o gerenciamento de informações de privacidade.
- Aprender a gerenciar informações de privacidade usando um PIMS alinhado com a ISO/IEC 27701
- Entender as principais áreas de investimento para um PIMS voltado para negócios
- Compreender como sua organização pode demonstrar garantia na gestão de informações de privacidade

FASES DO GERENCIAMENTO DE INFORMAÇÕES DE PRIVACIDADE:

Tomada de decisão → Iniciação do projeto → Conscientização contínua

O que é Gerenciamento de Informações Privadas?

Privacidade:

- Habilidade de uma pessoa em controlar a exposição e a disponibilidade de informações acerca de si mesmo.

O PMIS é baseado na ISO/IEC 27701

- Concentrado em aspectos 'informacionais' da privacidade.

Exemplos de Problemas Relacionados às Informações Pessoais

EXEMPLOS

1

- Sua empresa não quer que outras pessoas usem suas informações pessoais sem permissão.
- Porém, a restrição total pode impedir o uso benéfico das informações.

2

- Imagine que você queira compartilhar suas informações pessoais com uma organização quando for vantajoso.
- Para isso, deve-se garantir o equilíbrio entre confidencialidade e disponibilidade.

3

- Ao fornecer informações pessoais, valorizamos o fato de ter confiança ao lidar com uma organização, mas nem sempre a reputação é suficiente.

Princípios da GDPR

O processamento de informações pessoais é subdividido em seis princípios de proteção de dados (GDPR):

1. O processamento deve ser justo e legal, e para propósitos específicos.
2. O processamento não deve ser usado para nenhum outro propósito.
3. As informações pessoais devem ser adequadas e relevantes para os propósitos especificados, e devem ser limitadas ao necessário para os propósitos.
4. As informações pessoais devem ser precisas e, quando necessário, atualizadas.
5. As informações pessoais não devem ser retidas por mais tempo do que o necessário.
6. As informações pessoais devem ser processadas de maneira segura.

Envolvidos na Privacidade

Titulares de dados:

- Precisam ter garantias que suas informações pessoais estão sendo gerenciadas e protegidas adequadamente

Organizações:

- Devem cumprir requisitos legais e regulatórios e permanecer competitivas no mercado.

País de Atuação

Nem todos os países têm os mesmos níveis de proteção de privacidade

- União Europeia: **GDPR**
- Reino Unido: **Lei de Proteção de Dados de 2018**

Os indivíduos precisam saber em que país suas informações pessoais estão sendo processadas

Gerenciamento do Processamento com Terceiros

As organizações precisarão ter políticas para qualquer processamento subcontratado de informações pessoais

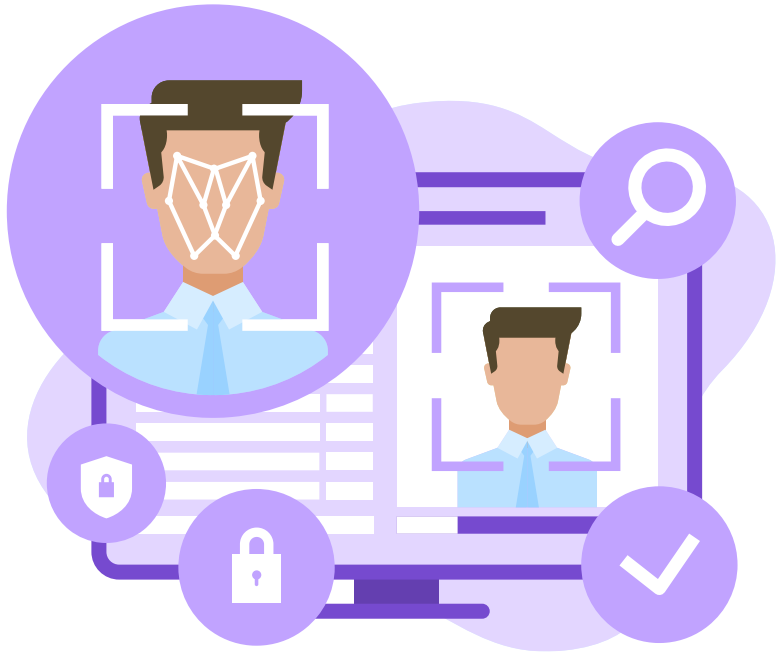
Especialmente provedores de serviços baseados em nuvem

A terceirização e outros contratos agora estão especificando cada vez mais a conformidade

O que é 'Informação Pessoal'

Vários termos são usados para se referir a “Informação Pessoal”:

- Na GDPR da UE usa-se o termo “dados pessoais”.
- Nos EUA, usam “informações pessoalmente identificáveis”



GDPR

Informação pessoal é "qualquer informação relacionada a uma pessoa natural identificada ou identificável”.

- **Nome;**
- **Endereço;**
- **Data de Nascimento etc.**

Motivo das Informações Pessoais serem Processadas

Por que as informações pessoais são processadas?

- Necessidade de fornecer serviços de forma apropriada.
- A quantidade de informações pessoais processadas dependerá dos serviços oferecidos.
- Manter uma vantagem competitiva frente aos concorrentes
- Melhorias no atendimento ao cliente.
- Construir uma boa estratégia de gerenciamento do conhecimento.
- Setor público: justiça e segurança nacional.

O que Precisa ser Considerado

Como um PIMS pode atender às necessidades de uma organização?

- Clientes, staff, fornecedores e cultura?

O gerenciamento de informações privadas vai além da tecnologia!!!

- Até as informações em papel precisam estar no PIMS.
- Seria ideal se o PIMS abrangesse a organização toda.

Questões Internas e Externas

A ISO/IEC 27701 fala sobre considerar “questões externas e internas".

- Questões externas: leis e regulamentos (GDPR, DPA etc.)
- Questões internas: gerenciamento de pessoal e emissões de relatórios.

Partes Interessadas

Quem são as partes interessadas?

- Diretores da empresa;
- Reguladores (como o ICO no Reino Unido);
- Clientes da organização.

Fatores externos e internos:

- Leis e regulamentos aplicáveis;
- Decisões judiciais;
- Contexto organizacional;
- Requisitos contratuais.

As necessidades e expectativas das partes interessadas precisam ser entendidas pela organização!!!

Equilíbrio entre Organizações e Indivíduos

A intenção da organização e a permissão dos titulares podem entrar em conflito no processamento de dados!

- As organizações precisam equilibrar suas próprias necessidades com os desejos das pessoas e a conformidade com as leis.
- Para isso, dependências e interfaces de todos os aspectos do gerenciamento e informações pessoais precisam ser consideradas.
- Em particular, é necessário desenvolver e implementar medidas de segurança da informação necessárias.

Formato e Meio de Armazenamento

O PIMS deve considerar os formatos e meios em uso e garantir que os mecanismos adequados estejam em vigor

- Documentos físicos merecem o mesmo nível de proteção que as versões eletrônicas.
- Se informações forem acessadas de forma não autorizada, não importa seu meio ou formato: a violação de privacidade ocorreu.

Quando tal violação afeta negativamente o titular dos dados, pode-se resultar em:

- Sanções legais;
- Pedidos de compensação;
- Perda de confiança na organização.

Subcontratado

Ao lidar com subcontratados (processadores de dados), é preciso considerar:

- Partes internas e externas;
- Partes interessadas;
- Equilíbrio entre os desejos da organização e os dos indivíduos;
- Formato e meio de armazenamento.

Subcontratados são extensões da organização!

ISO/ IEC 27701

A ISO/IEC 27701:2019 é a norma internacional para o gerenciamento de informações de privacidade

- Segue a mesma estrutura da ISO/IEC 27001
- Cobre desde o estabelecimento do PIMS até a sua revisão e adaptação.
- Avaliação de desempenho e melhoria

Desafio: variação na definição de processamento de informações de privacidade ao redor do mundo

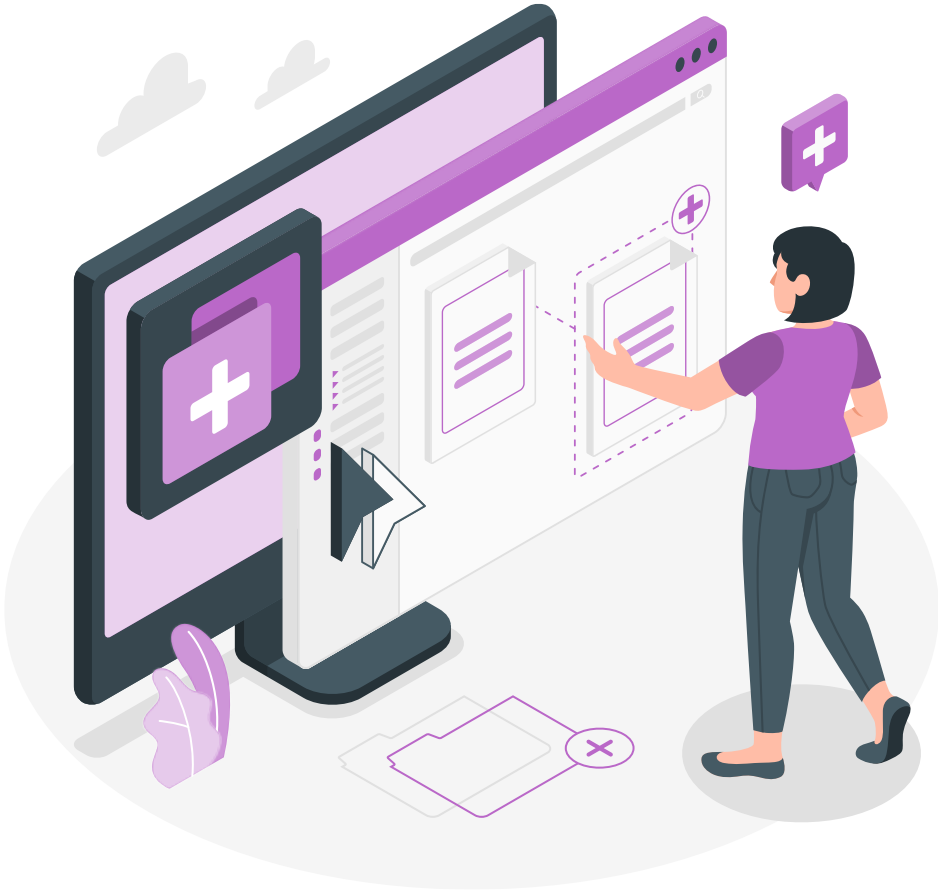
Comitê ISO/IEC: “informações pessoalmente identificáveis”.

Ao implementar um PIMS com base na ISO/IEC 27701, a ISO/IEC 27001 também precisa ser implementada.

Documentação

É útil manter registros de desenvolvimentos e atividades:

- Registrar e manter registros apropriados pelo tempo necessário.
- Criar registros de atividades operacionais
- Uma vez criados, esses registros precisam ser protegidos.
- Os procedimentos operacionais precisam descrever os processos que apoiam as políticas corporativas e explicar quem faz o quê, onde e quando.
- Toda a documentação precisa ser escrita e aprovada.



Auditoria

As auditorias podem ocorrer tanto dentro da empresa quanto fora.

- Em um PIMS, o objetivo é mostrar que o sistema de gestão está alinhado com os requisitos da organização.
- Podem ser internas ou externas.
- Os relatórios de auditoria vão apontar qualquer desvio entre a prática real e os requisitos.
- **São uma oportunidade de melhoria**: atualizações nas políticas, nos procedimentos operacionais e/ou instruções de trabalho.

Revisão do Sistema de Gestão

A alta direção tem um papel importante no controle de sistemas de gestão como o PIMS.

- Iniciam o desenvolvimento do sistema de gestão, aprovam os recursos necessários e as políticas corporativas.
- É interessante realizar essas revisões de gestão em intervalos regulares
- A revisão também pode analisar as medidas de eficácia e oportunidades de melhoria.
- A ISO/IEC 27701:2019 pede para a organização revisar a eficácia do PIMS referenciando as seções apropriadas da ISO/IEC 27001.

Recursos Disponíveis

O trato com informações pessoais é regulado na maioria dos países por leis e/ou regulamentações.

Os requisitos específicos de um SGIP precisam ser determinados à luz das leis e regras locais:

- Alta direção;
- Oficial de proteção de dados (DPO);
- Equipe operacional Sênior;
- Gerenciamento de registros;
- Recursos humanos;
- Segurança da informação e/ou TI;
- Expertise técnica em TI;
- Gestão de riscos;
- Vendas e marketing.

Avaliação de Impacto à Privacidade (PIA)

Avaliação de Impacto de Privacidade (PIA): Antes de começar qualquer projeto, fazemos uma PIA para identificar e minimizar os riscos de informações pessoais.

- É recomendada para qualquer processamento de informações pessoais.
- Deve antecipar tudo que pode dar errado com as informações pessoais.
- A PIA não é só sobre máquinas, também é sobre as pessoas.

A PIA é para Todos!

Riscos à Privacidade

Para fazer uma PIA: estimar a probabilidade de risco e seu impacto potencial sobre o indivíduo.

Os riscos para a privacidade devem ser identificados e estimados com base nos **6 princípios de proteção de dados**

- Cada risco de privacidade tem suas próprias consequências.
- Perda de Privacidade: spam, martketing massivo, perda de confiança.

Risco de privacidade = Probabilidade × Impacto

Avaliação de Riscos de Privacidade

A avaliação de risco de privacidade considera o impacto na organização.

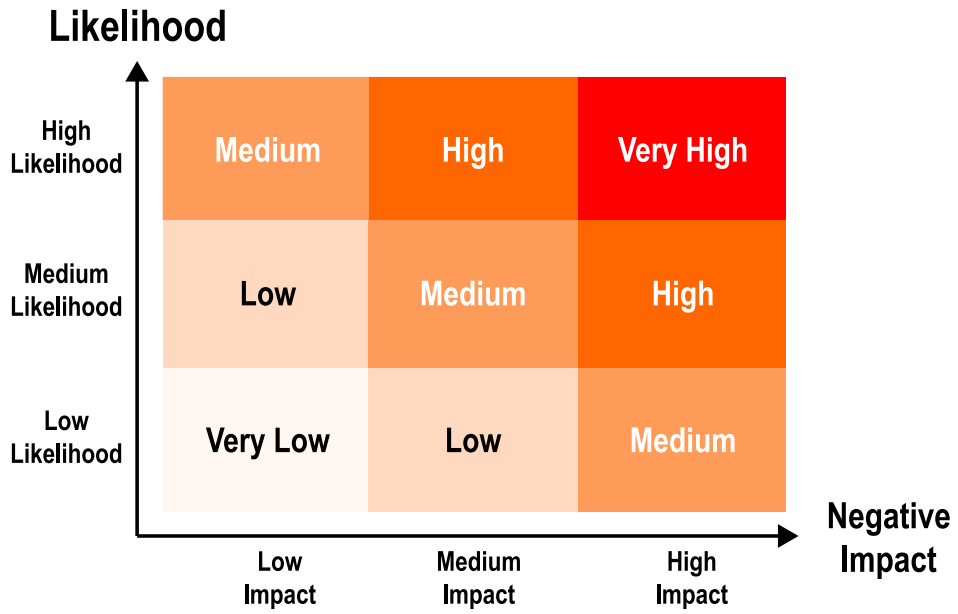


Figure 1: Relationship between likelihood, impact and risk

- **Probabilidade:** Sobre quão provável é que algo dê errado.
- **Impacto:** Se algo der errado, o quanto isso vai afetar as pessoas e a organização?

Perspectivas por Quantidade de Informações Processadas

Objetivo final: administrar todos os riscos de privacidade em um nível que seja aceitável para a organização.

- **Grandes Processadores de Dados:** Empresas que lidam com muitas informações pessoais querem manter o risco o mais baixo possível.
- **Pequenos Processadores de Dados:** Empresas com menos dados sensíveis podem achar que medidas extras são exageradas. Elas aceitam mais riscos.
- **Proprietários de riscos:** devem acompanhar os riscos e reduzi-los quando necessário.

É importante existir processos para identificar, avaliar o impacto e lidar com violações de privacidade.

Aplicando Controles PIMS

Primeiro passo:

Criar um conjunto de controles para controlar os riscos.

Os controles devem cumprir as obrigações legais, regulatórias e contratuais

Declaração de Aplicabilidade (SoA - Statement of Applicability)

A SoA deve ser um guia mestre, não apenas uma burocracia.

Determinar os controles certos demanda uma coordenação central.

Controles de Gestão da Informação de Privacidade

Temos 31 controles no Anexo A e mais 18 no Anexo B da Norma Internacional, divididos em quatro categorias:

- Condições para coleta e processamento.
- Obrigações aos princípios de Informação Pessoal Identificável (PII).
- Privacidade por design e por padrão.
- Compartilhamento, transferência e divulgação de PII.

Uma organização pode escolher e moldar esses controles para atender às suas necessidades exclusivas.

Inicia-se com requisitos específicos do setor da empresa e requisitos contratuais. Depois explora-se outras opções.

Extensão dos Controles da ISO/IEC 27001

CAPITULO 5

da ISO/IEC 27701:

Requisitos adicionais alinhados aos controles documentados na ISO/IEC 27001.

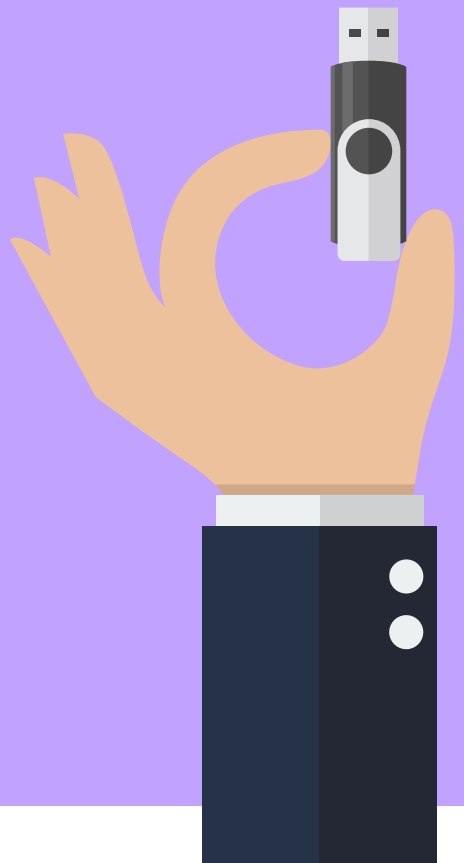
1. Entendendo o Papel Legal e/ou Regulatório da Organização
2. Atendendo às Necessidades e Expectativas das Partes Interessadas:
3. Inclusão do Processamento de Informações de Privacidade no Escopo do PIMS:
4. PIA: Ferramenta Essencial para Avaliação de Impacto à Privacidade:

Orientações Adicionais Alinhadas à ISO/IEC 27002

CAPITULO 6

da ISO/IEC 27701:

Orientações suplementares que estão alinhadas àquelas incluídas na ISO/IEC 27002.
Diretrizes específicas de SGPI relacionadas à ABNT NBR ISO/IEC 27002



1. Desenvolvimento de Políticas de Privacidade.
2. Identificação e Designação de Funções e Responsabilidades no PIMS:
3. Treinamento de Conscientização para Funcionários.
4. Classificação e Rotulagem de Informações.
5. Proteção de Informações em Mídias Removíveis
6. Procedimentos Adequados para Mídias Removíveis.

Orientações Adicionais Alinhadas à ISO/IEC 27002

7. Transferência Segura de Informações em Mídias Removíveis
8. Mecanismos Adequados de Registro de Usuários
9. Controles Criptográficos Adequados (se exigido por legislação/regulamentação)
10. Garantia de Procedimentos Adequados para Descarte de Equipamentos
11. Restrição do Uso de Materiais Impressos que Contêm Informações Pessoais (especialmente cópias de informações digitais)
12. Uso e Gerenciamento Adequado de Sistemas de Backup
13. Garantia da Disponibilidade, Uso e Proteção de Mecanismos de Monitoramento e Registro
14. Uso de Acordos de Confidencialidade e Sigilo para Funcionários e Outros Envolvidos (como processadores de dados) com Acesso a Informações Pessoais

Orientações Adicionais Alinhadas à ISO/IEC 27002

15. Uso Seguro de Redes Públicas (como sistemas de e-mail), Incluindo o Uso de Criptografia
16. Desenvolvimento de Sistemas (Internos e Terceirizados)
17. Uso e Proteção de Dados de Teste
18. Uso de Contratos e Outros Acordos com Fornecedores quando Envolvem Informações Pessoais
19. Responsabilidade e Tratamento Subsequente de Incidentes Relacionados à Privacidade com Informações Pessoais
20. Demonstração de Como as Exigências Legais e/ou Regulatórias são Atendidas
21. Proteção de Todos os Registros Relacionados ao Processamento de Informações Pessoais
22. Tratamento de Solicitações de Avaliações Independentes por Parte dos Titulares de Dados

Condições para Coleta e Processamento de Dados

Existem condições que precisamos respeitar antes de coletar dados:

- Controles em nível corporativo relacionados a como e por que as informações pessoais são coletadas e processadas.
- Identificação e documentação dos propósitos legítimos para os quais as informações pessoais são coletadas
- Registro do consentimento e as informações fornecidas pelo titular.
- Gestão do relacionamento com o processador de dados e como o processamento é gerenciado.
- Gestão do relacionamento com o controlador de dados.

Obrigações para os Titulares dos Dados

Obrigações dos Controladores de Dados:

- Documentar todas as regras legais e obrigações que têm com os titulares dos dados.
- Fornecer as informações que o titular dos dados requer.
- Documentação de suas obrigações legais e regulatórias.

Obrigações dos Processadores de Dados:

- Trabalhar em parceria com os controladores para garantir que eles cumpram suas obrigações legais.
- Lidar com solicitações de titulares dos dados ou encaminhá-las para o controlador.

Privacidade desde a Concepção e por Padrão

Para Controladores de Dados:

- Coletar apenas as informações pessoais mínimas necessárias para o propósito pretendido.
- Retirar apenas as informações pessoais necessárias para o propósito pretendido.
- Garantir que as informações pessoais processadas sejam precisas e estejam atualizadas.
- Após a conclusão do propósito, eliminar todas as cópias das informações pessoais mantidas para esse propósito.
- Garantir que quaisquer arquivos temporários que incluam informações pessoais sejam excluídos o mais rápido possível.
- Assegurar que a integridade de qualquer informação pessoal enviada a outra organização seja protegida.

Privacidade desde a Concepção e por Padrão

Para Processadores de Dados:

- Seguem as regras dos controladores.
- Apagar tudo quando a missão termina.
- Seguir o acordo com o controlador de dados.

Compartilhamento, Transferência e Divulgação de Informações Pessoais

Para Controladores de Dados:

- Seguir as leis e regulamentos.
- É essencial ter essas políticas e procedimentos para garantir a conformidade.

Para Processadores de Dados:

- Seguir as leis e regulamentos.
- Garantir que os subcontratados estão cientes e obter a aprovação quando houver qualquer mudança para o subcontratante.

Anexos na ISO/IEC 27701

- **Anexo A:** lista controles. Útil para organizações que atuam como controladores de dados.
- **Anexo B:** semelhante ao Anexo A, mas específico para processadores de dados.
- **Anexo C:** mapeamento com a ISO/IEC 29100.
- **Anexo D:** mapeamento com a GDPR.
- **Anexo E:** Mapeamento com a ISO/IEC 27018 e 29151.
- **Anexo F:** Fornece informações sobre como aplicar a ISO/IEC 27701 à ISO/IEC 27001 :2013 e ISO/IEC 27002:2013.

Lidando com Vazamentos de Informações Privadas

A ISO/IEC 27701 é muito útil para reduzir o risco de vazamentos de informações privadas.

Vazamentos podem ocorrer de várias formas.

- Acesso indevido a informações pessoais.
- Armazenamento de informações indevido ou dados desatualizados.

Vazamentos podem requerer a aplicação de um plano de continuidade de negócios.

- Se a causa for um incidente, precisamos revisar o plano de continuidade de negócios.
- Nem todos os incidentes são graves, mas todo o pessoal deve estar alerta

Conformidade e Auditoria

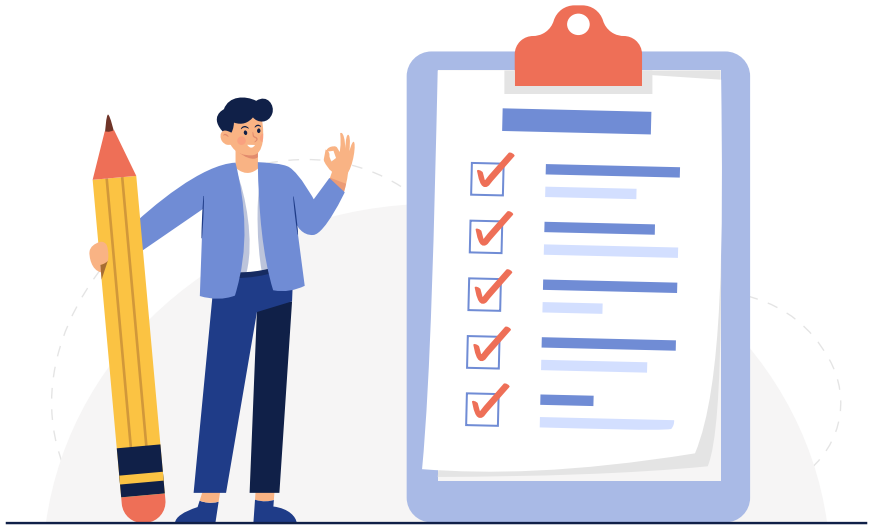
A organização precisa ficar atenta e seguir as obrigações legais e requisitos contratuais.

A avaliação técnica do PIMS deve relatar como estão:

- Os equipamentos de TI;
- Sistemas;
- Software;
- Processos relacionados.

A programação pode incluir verificações e até testes de penetração.

Certificação



A certificação da ISO/IEC 27701 não segue a ISO/IEC 17065 e, portanto, não é uma "certificação GDPR da UE".

- A certificação na ISO/IEC 27701 só fornece a garantia de que os processos de gestão estão em vigor para proteger a privacidade.
- Obtê-la requer auditoria por um organismo certificador independente e um certificado acreditado.
- A acreditação é como um acordo internacional entre órgãos do mundo todo.
- A acreditação depende da implementação de uma série de controles.

Certificação no Horizonte

A questão da certificação acreditada está em análise por organizações relevantes.

- Já existe um esquema de certificação acreditada para Sistemas de Gestão de Segurança da Informação (ISMS) conformes com a 27001 há anos
- Uma certificação acreditada para a 27701 pode surgir mais rápido do que imaginamos.
- O processo de auditoria para a certificação ISO/IEC 27701 provavelmente será semelhante ao da auditoria de um ISMS para a ISO/IEC 27001.

A certificação ISO/IEC 27701 está a caminho!

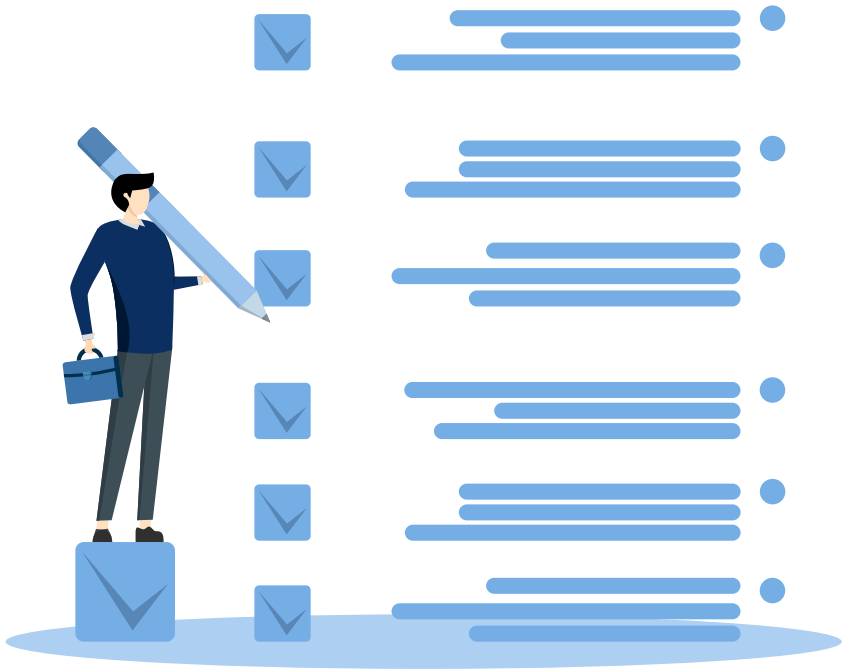
Auditoria da Certificação

Um ou mais auditores são designados pela instituição de certificação.

- Os auditores vão atrás de evidências da conformidade com os critérios de auditoria.
- O auditor precisa documentar tudo, classificando como uma não conformidade maior ou menor
- Se a não conformidade for algo sério, a instituição de certificação vai validar a correção e a eficácia da ação corretiva.
- A instituição de certificação precisa fazer um acompanhamento na auditoria subsequente

A ISO/IEC 27701 oferece garantias sobre o gerenciamento específico de uma disciplina pela organização!

Aplicações Adicionais de Auditoria



Auditorias de fornecedores = auditorias de segunda parte

- Os compradores podem utilizar a Norma como um framework reconhecido e disponível para conduzir auditorias de fornecedores.
- Essas auditorias ajudam a assegurar que o gerenciamento de informações de privacidade esteja alinhado com o contrato.
- Também podem impulsionar a melhoria contínua em toda a cadeia de suprimentos.

Para saber se um certificado acreditado é equivalente aos emitidos sob o esquema descrito, verifique se o órgão de acreditação é membro do Fórum Internacional de Acreditação (www.iaf.nu).

PDPP

Módulo 4: Papéis do Controlador, Processador e Data Protection Officer (DPO)

Definição do Papel de Controlador de Dados

Controlador de Dados

Responsável pela garantia de que os dados pessoais são processados de acordo com o Regulamento.

Diz o GDPR: “Controlador de Dados significa a pessoa física ou jurídica, autoridade pública, agência ou outra entidade que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais” - Artigo 4 (7).

- Determina os propósitos das atividades de processamento, mesmo que não seja ele quem efetivamente processa os dados.
    - Quais dados serão coletados, quem vai fazer a coleta e de onde, se existem justificativas para não notificar os titulares dos dados ou buscar o seu consentimento, por quanto tempo os dados serão retidos, e outros aspectos.

Detalhes Sobre o Controlador de Dados

- *"**O Controlador*** só deve utilizar Processadores que forneçam garantias suficientes para implementar medidas técnicas e organizacionais de forma que o processamento atenda aos requisitos do Regulamento, e assegurem a proteção dos direitos do Titular dos Dados".
- É uma entidade voltada para o público, para quem os titulares fornecem suas informações. Por exemplo: um hospital pode ter um formulário on-line para informações de saúde.
- Se o formulário é gerenciado por um terceiro que tem certa autonomia sobre o desenho do formulário e as categorias dos dados que ele coleta, então esse terceiro pode se tornar o que é chamado de ***joint controller***, ou controlador conjunto, ou co-controlador.

Mais Tarefas do Controlador de Dados

- Proteger os dados pessoais pela implementação de medidas técnicas e organizacionais.

- Medidas também podem ser chamadas de controles, e devem ser aplicadas em resposta a riscos calculados, claramente documentados.

- Medidas ou controles devem ser monitoradas e verificadas quanto à sua efetividade.

- “Tanto no momento da determinação dos meios de processamento quanto no momento do próprio processamento”, segundo GDPR Artigo 21 (1).

Mais adiante, neste curso:

- Avaliação de Impacto Sobre a Proteção de Dados (DPIA);

- O Controlador deve consultar os Processadores que podem ser afetados para garantir que a DPIA seja completa;

- É possível para dois ou mais Controladores determinar, em conjunto, os propósitos e meios de processamento;

- Se a sua organização precisa estabelecer uma relação de co-controladora em parceria com outra organização, você vai precisar que “sejam estabelecidas as respectivas responsabilidades para conformidade com o Regulamento”.

Papel do Processador de Dados

- Segundo o GDPR, “Processador significa a pessoa física ou jurídica, autoridade pública, agência ou outra entidade que processa dados pessoais em nome do Controlador” – Artigo 5 (8).
- O processamento devem estar dentro de parâmetros fornecidos pelo Controlador de Dados e de acordo com o Regulamento.
- Os contratos entre Controladores e Processadores tem uma quantidade específica de requisitos, que estão listados no Artigo 28.
- Para escolher um terceiro para ser um Processador, você precisa executar uma Avaliação de Risco de Proteção de Dados.

Tarefas do Processador de Dados

O Controlador não tem que definir cada elemento individual de como o dado é processado, e frequentemente ele confia na garantia do Processador.

O Processador deve ainda ser responsável pela determinação dos seguintes elementos:

- Sistemas de TI e outros métodos usados para coletar os dados pessoais;
- Como os dados são armazenados;
- Segurança relacionada aos dados pessoais;
- Como os dados pessoais são transferidos de uma organização para a outra;
- Como os dados pessoais sobre um indivíduo específico são recuperados;
- Métodos para garantir que a retenção siga uma programação;
- Como os dados são excluídos e descartados.

Exemplo:

- Se uma organização contrata uma agência de marketing para fazer uma pesquisa, a organização deve determinar o propósito do processamento dos dados.
- Pode deixar a cargo da especialização da agência de marketing em como atingir esse resultado.

Mais detalhes Sobre o Processador de Dados

- Os Processadores não podem se associar ou engajar com outro Processador nas atividades sem que “o Controlador tenha dado, previamente e por escrito, autorização específica ou geral” – Artigo 28 (2).
- Isso garante que o Controlador mantenha a supervisão da cadeia de custódia dos dados pessoais.
- Em muitos casos, o Controlador e o Processador serão a mesma entidade.
- Como a definição de processamento pode ser muito ampla, ou seja, abrange todas as ações sobre os dados pessoais, da coleta ao descarte completo, é improvável um Controlador não participar de alguma parte do processamento dele mesmo.

Controladores e Processadores fora da UE

Controladores e Processadores com base na UE estão sujeitos ao GDPR.

Qualquer organização que fornece serviços na União precisa obedecer o regulamento ou encarar as multas.

O Regulamento exige que todas as organizações tenham um Representante designado dentro da União, estabelecido em um dos Estados-Membros, onde se encontram os titulares dos dados.

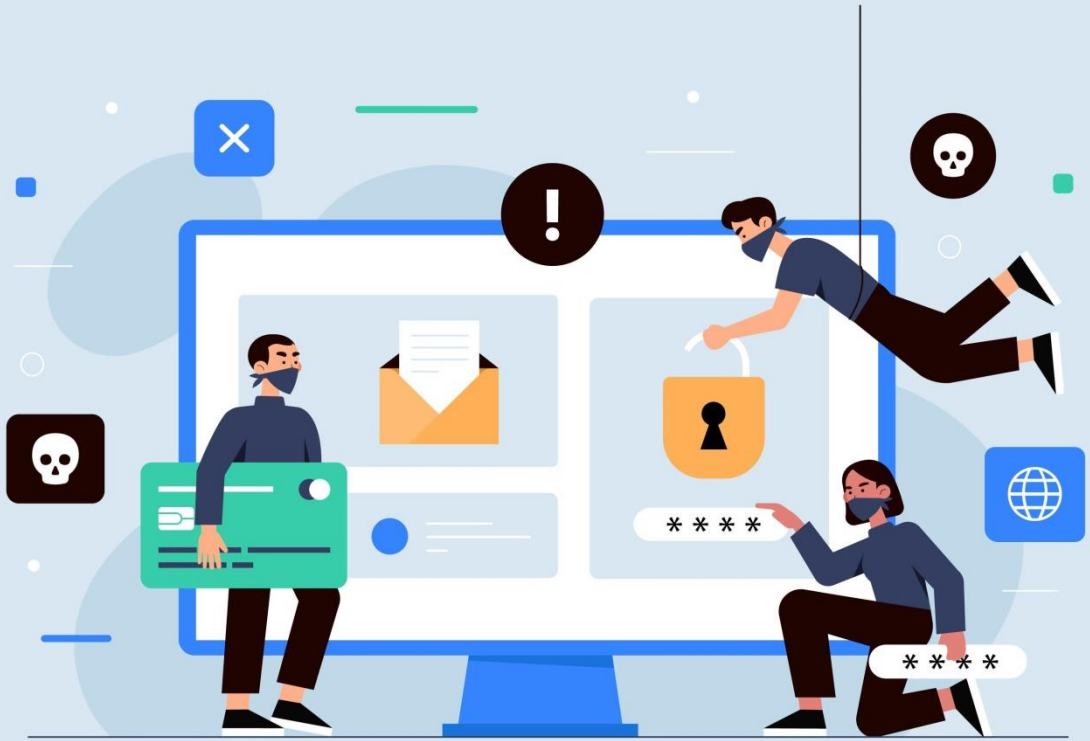
Exceções:

- Se o processamento for ocasional e não incluir larga escala e nem processamento de categorias especiais de dados – Artigo 9 (1); e processamento de dados pessoais relacionados a condenações criminais e ofensas que aparecem no Artigo 10, e quando não é provável que o processamento resulte em um risco aos direitos e liberdades de pessoas físicas;

- Processamento por uma autoridade ou entidade pública – Artigo 27 (2).

Responsabilidades do Representante do Controlador

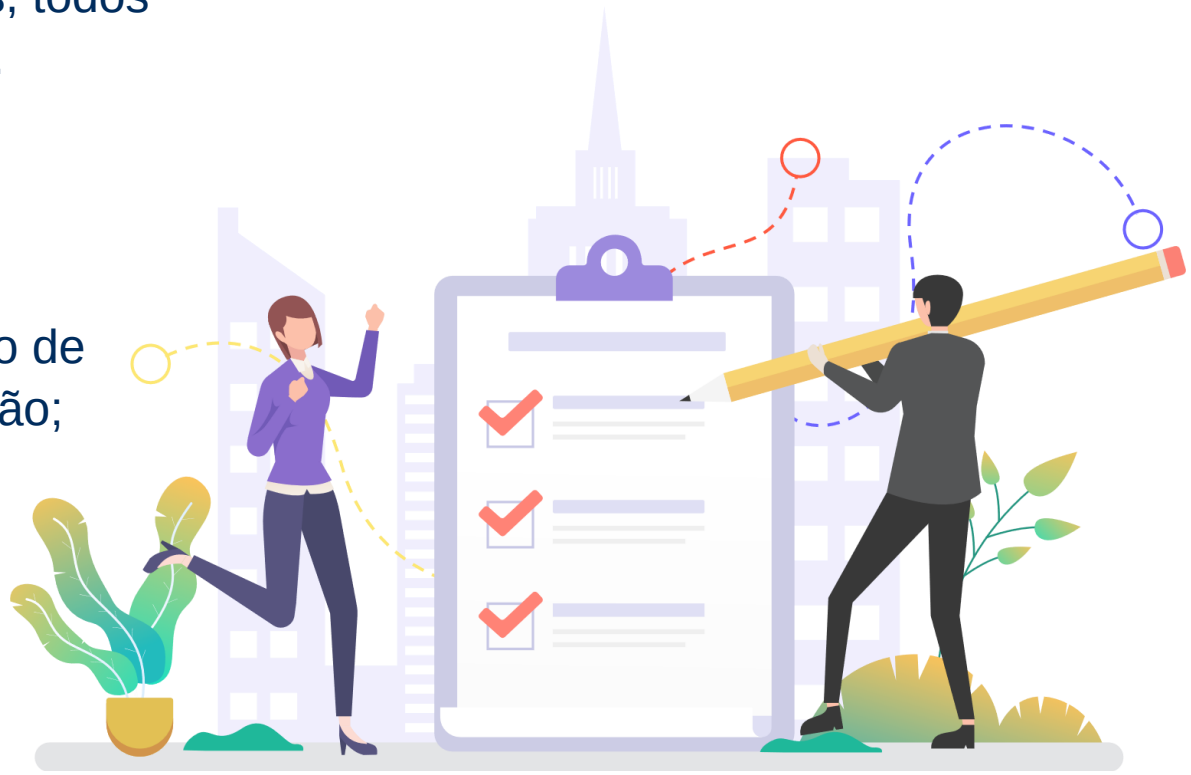
- Operar como uma conexão local com a Autoridade Supervisora do Estado-Membro.
- Pode assumir alguma prestação de contas ou responsabilização a respeito das falhas do Controlador ou do Processador em atender aos requisitos do Regulamento.
- Ter um Representante não absolve o Controlador ou o Processador das suas responsabilidades.
- Se você precisa de um Representante na UE, você deve garantir isso por escrito para a Autoridade Supervisora relevante no Estado Membro onde o Representante está estabelecido.



Registros de Processamento

As organizações precisam manter registros que comprovem a conformidade, caso a Autoridade Supervisora solicite evidências.

- Registros como avisos de processamento, políticas de retenção, evidência de consentimento, relatórios de DPIA, e outros, todos podem ser usados como comprovação de conformidade.
- Você vai precisar de uma combinação de registros para demonstrar a sua conformidade.
- Orientações e manuais operacionais para o pessoal que processa os dados, módulos de treinamento em proteção de dados; registros de risco; registros de ativos de informação; estruturas de governança e controles.
- Documentação do seu framework de conformidade de privacidade, avaliações de riscos e controles.



Registros como Evidências

Tipos de registro :

- Política de proteção de dados ou segurança da informação;
- Política de retenção e descarte;
- Registros de destruição de ativos de informação;
- Acordos de nível de serviço e de não divulgação;
- Aviso de processamento justo e ou da política de privacidade;
- Documentação de gerenciamento de risco, plano de tratamento de riscos, declarações de aplicabilidade, relatórios DPIA;
- Monitoração e medição de controles para gerenciamento de riscos;
- Registros de treinamento e conscientização;
- Relatórios de auditorias internas;
- Registros de melhoria contínua;
- Políticas, procedimentos e registros de gerenciamento de incidente.

O GDPR também exige que muitos Controladores e Processadores mantenham um registro específico das suas atividades de processamento.

As obrigações relacionadas aos registros não se aplicam às empresas ou organizações com menos de 250 trabalhadores, a menos que:

- O tratamento efetuado possa implicar um risco para os direitos e liberdades;
- Não seja ocasional;
- Envolvam as categorias especiais de dados ou dados pessoais relativos a condenações penais.

Deve ser algo simples.

Registros de Controladores e de Processadores

REGISTROS DO CONTROLADOR DE DADOS	REGISTROS DO PROCESSADOR DE DADOS
Nome e detalhes de contato do Controlador, do Co-controlador e/ou Representante do Controlador e do DPO.	Nome e detalhes de contato do(s) Processador(es) e de cada Controlador para quem o Processador trabalha, do Representante do Controlador ou Processador e do DPO.
Propósito do processamento.	Categorias do processamento executado em nome de cada Controlador.
Descrição das categorias de Titulares de dados e categorias de dados pessoais.	Detalhes de quaisquer transferências de dados pessoais para um país terceiro ou organização internacional.
Categorias dos destinatários para quem os dados são divulgados, incluindo destinatários fora da EU.	Descrição geral das medidas de segurança técnicas e organizacionais.
Detalhes de quaisquer transferências de dados pessoais para um país terceiro ou organização internacional	
Limites de tempo para apagamento das diferentes categorias de dados pessoais.	
Descrição geral das medidas de segurança técnicas e organizacionais.	

Introdução ao Papel Data Protection Officer (DPO)

O Controlador e o Processador devem designar um DPO em qualquer caso em que:

- O processamento é executado por uma autoridade ou entidade pública, exceto tribunais agindo judicialmente;
- As atividades essenciais do Controlador ou do Processador consistem em operações de processamento que, devido à sua natureza, seu escopo ou seus propósitos, exigem monitoração regular e sistemática dos titulares de dados em larga escala;
- As atividades essenciais do Controlador ou do Processador consistem de processamento em larga escala de categorias especiais de dados.

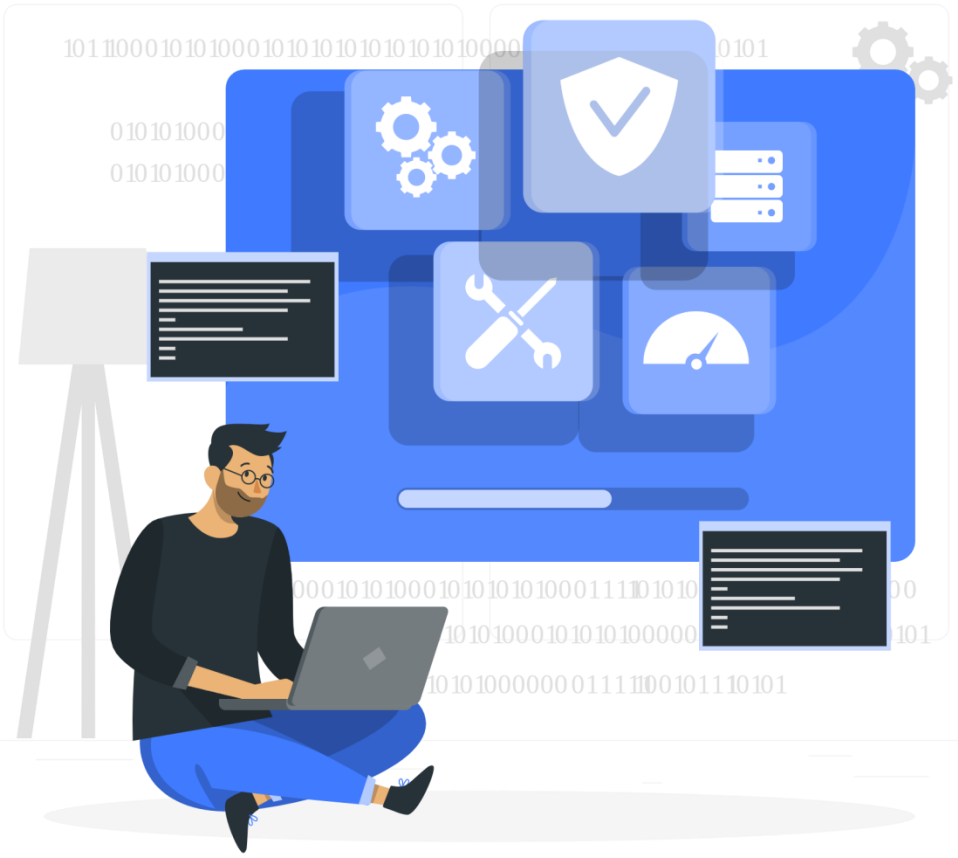
Requisitos do Papel Data Protection Officer (DPO)

Atividades essenciais

Podem ser consideradas como as principais operações necessárias para atingir os objetivos do Controlador ou Processador.

Exemplos que exigem um DPO:

- ✓ A atividade principal de um hospital é fornecer cuidados de saúde. No entanto, um hospital não poderia fornecer cuidados de saúde com segurança e eficácia sem processar os registros de saúde dos pacientes;
- ✓ 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 tratamento de dados pessoais.



Requisitos do Papel Data Protection Officer (DPO)

O artigo 37 do GDPR exige que a designação de um DPO se torne obrigatória quando o tratamento de dados pessoais for realizado em grande escala.

Fatores:

- Número de titulares de dados afetados, número absoluto ou percentual da população em causa;
- Volume de dados e/ou o escopo dos diferentes elementos dos dados;
- Duração, ou permanência, da atividade de processamento de dados;
- Extensão geográfica da atividade de processamento.

Exemplos de processamento considerados em grande escala:

- Dados de pacientes durante as atividades normais de um hospital;
- De Viagem das pessoas que utilizam os transportes públicos;
- De geolocalização de clientes de uma rede de fast-food;
- De uma companhia de seguros ou de um banco;
- Pessoais para fins de publicidade comportamental por um mecanismo de busca;
- Operadoras de telefonia ou provedores de internet.

Não constituem tratamento em grande escala: processamento de dados de pacientes por um médico; e dados pessoais relacionados a condenações e infrações por um advogado.

Requisitos do Papel Data Protection Officer (DPO)

Monitoramento Regular e Sistemático

Regular: contínuo ou que ocorre a intervalos específicos num determinado período.

Sistemático: o que ocorre de acordo com um sistema.

Exemplos:

- Prestação de serviços de telecomunicações;
- Roteamento de e-mails;
- Criação de perfil e pontuação para efeito de avaliação de risco;
- Acompanhamento de localização;
- Programas de fidelização;
- Publicidade comportamental;
- Monitoramento de dados de bem-estar, condição física e de saúde através de dispositivos vestíveis;
- Televisão em circuito fechado;
- Dispositivos conectados (IoT).

Designação Voluntária de um DPO

Podem existir empresas que, por sua conta e sem pressão do Regulamento, decidem designar um DPO.

Cada organização deve fazer uma avaliação racional, levando em consideração:

- Tamanho, complexidade e diversidade das operações de negócio;
- Nível aceitável de risco;
- Riscos aos direitos e liberdades dos titulares de dados.

Quando uma organização decide nomear voluntariamente um DPO, são aplicáveis todos os requisitos do GDPR relacionados a essa designação.

O Artigo 29 recomenda que os Controladores e Processadores documentem a análise interna que determinou se um DPO será ou não nomeado.

Empresas que Compartilham um DPO

- **O GDPR permite que um grupo de empresas tenha um único DPO compartilhado, desde que esse DPO esteja "facilmente acessível a partir de cada estabelecimento" – Artigo 37 (2).**

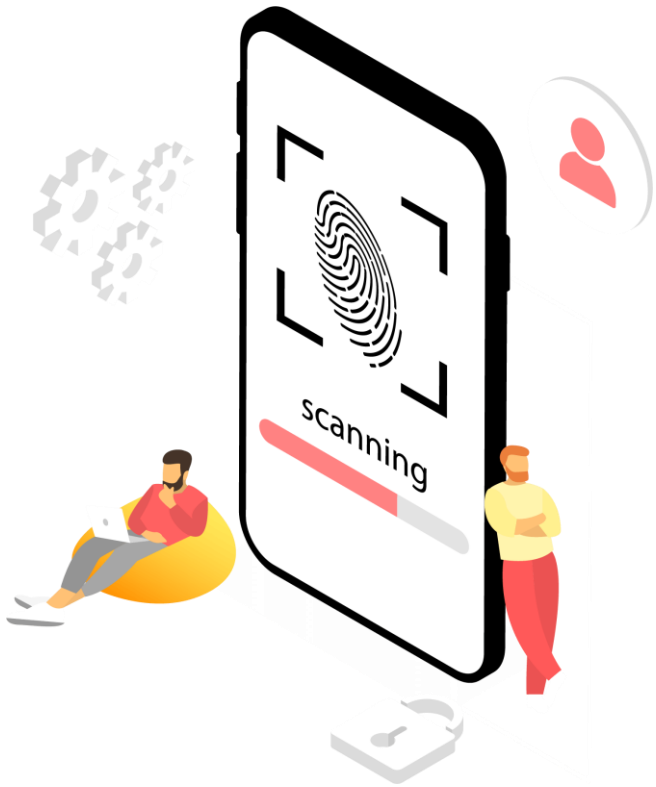
- **O Controlador deve estar certo de que um único DPO pode dar conta, de forma eficiente, mesmo atendendo a várias autoridades e entidades.**

- Essa situação de estar acessível se refere ao papel do DPO como o ponto de contato com relação aos titulares de dados e Autoridades Supervisoras.
- "Informar e aconselhar o Controlador, o Processador e os empregados que processam os dados, sobre suas obrigações nos termos do presente regulamento e de outras disposições de proteção de dados da União ou dos Estados-Membros" – Artigo 39 (1).
- Garantir a visibilidade dos detalhes de contato de acordo com os requisitos do GDPR.
- Pelo Artigo 37 (7), o Controlador ou o Processador deve publicar os contatos do DPO e comunicar a Autoridade Supervisora.
- A comunicação deve acontecer nos idiomas dos titulares de dados e das Autoridades Supervisoras.

DPO em Contrato de Serviço

- A função de DPO também pode ser exercida através de um contrato de prestação de serviço de um terceiro individual ou uma empresa terceirizada, ou seja, pode ter um contrato tipo *“DPO-as-a-Service”.*
- É essencial que cada membro dessa organização que exerce a função de DPO atenda a todos os requisitos relevantes do GDPR.
- Muito importante que essa pessoa nesta função seja protegida pelo GDPR.
- Pontos fortes e especializações individuais podem ser combinadas e assim uma equipe pode atender seus clientes de forma mais eficiente.
- A alocação de tarefas deve ser muito clara dentro dessa equipe.
- Um único indivíduo indicado como líder da equipe para contato.
- Uma única pessoa “encarregada” de cada cliente.
- Seria muito bom e útil você especificar esses pontos no contrato de serviço.

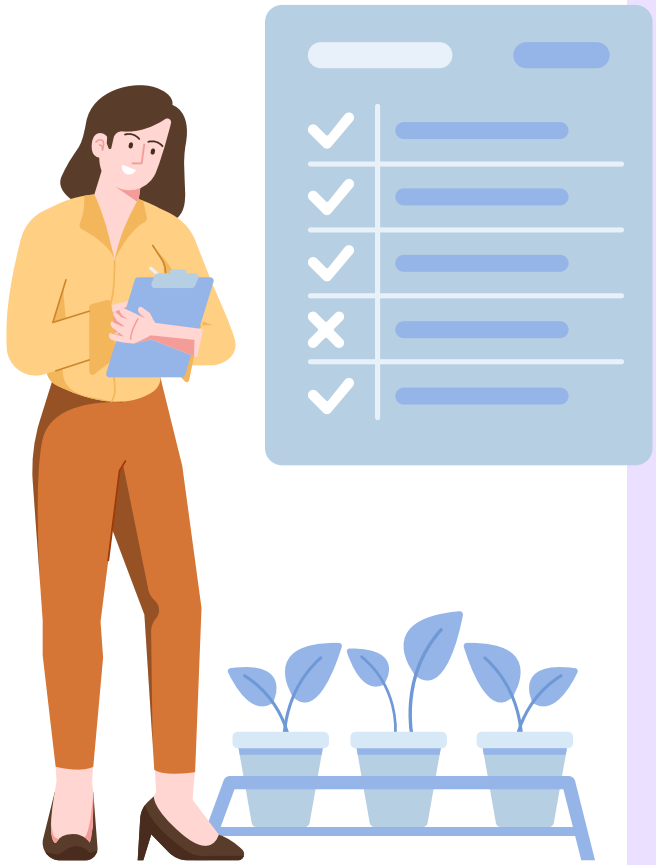
Publicação do Contato do DPO



- O GDPR exige que o Controlador ou o Processador publiquem os detalhes de contato do DPO e comunicar esses detalhes de contato para as Autoridades Supervisoras.
- Garantir que Titulares de dados, dentro e fora da organização, e as Autoridades Supervisoras possam fazer contato com o DPO, direta e confidencialmente.
- Endereço postal, número de telefone dedicado ou endereço de e-mail dedicado.
- O GDPR não exige que os detalhes de contato incluam o nome do DPO, mesmo que isso seja uma boa prática.
- É uma boa prática divulgar o nome e detalhes de contato do DPO para a Autoridade e pessoal interno via Intranet.

Posição do DPO

O GDPR, no Artigo 38, determina que o Controlador e o Processador devem ter certeza que o DPO esteja envolvido, adequadamente e em tempo hábil, em todas as questões relacionadas à proteção dos dados pessoais.



É crucial que o DPO:

- Se envolva desde o início, o quanto antes possível, no desenvolvimento do modelo de conformidade de privacidade e em todas as questões de proteção de dados;
- O DPO deve ser envolvido desde o início nas Avaliações de Impacto de Proteção de Dados (AIPD) – Artigo 35 (2);
- Seja visto como alguém importante e crítico e que tem o que dizer em todas as atividades de processamento de dados;
- Seja convidado a participar regularmente de reuniões da gerência sênior e media;
- Esteja presente na tomada de decisões sobre implicações de proteção de dados;
- Todas as informações relevantes passem pelo DPO em tempo hábil;
- A opinião do DPO sempre seja levada em conta;
- Seja prontamente consultado nas violação de dados.

Disponibilização de Recursos

“A organização deve prover os recursos necessários para o DPO executar suas tarefas e acessar os dados pessoais e operações de processamento, e ainda manter seu conhecimento especializado” – Artigo 38 (2) do GDPR.

- Suporte ativo à função de DPO por parte do comitê executivo ou diretoria;
- Tempo suficiente para o DPO completar suas tarefas;
- Recursos financeiros, infraestrutura, instalações, equipamentos e equipe;
- Comunicação oficial da nomeação do DPO para toda a equipe;
- Acesso que for necessário a outros serviços, como RH, jurídico, TI, segurança etc.;
- Treinamento continuado. O DPO tem que ter a oportunidade de se manter atualizado;
- Pode ser necessário criar um time, ou seja, um DPO e sua equipe.

Quanto mais complexas e sensíveis forem as operações de processamento, mais recursos devem ser disponibilizados para que o DPO possa trabalhar.

Atuação Independente do DPO

- O GDPR no Artigo 38 (3), Citação 97, estabelece claramente certas garantias de proteção para que o DPO seja capaz de desempenhar suas tarefas com suficiente autonomia.
- Controladores e Processadores precisam estar certos de que o DPO não receba qualquer instrução relacionada ao exercício das suas funções.
- Isso não quer dizer que a autonomia do DPO o autoriza a ter poderes de decisão além dos seus deveres nos termos do GDPR.
- O Controlador ou Processador continuam responsáveis pela conformidade com o Regulamento de proteção de dados.

Proteção do Papel do DPO

- O GDPR oferece proteção para o papel do DPO quando cita no Artigo 38 (3), que o DPO não deve ser dispensado ou penalizado pelo Controlador ou Processador por executar as suas tarefas.
- Esse requisito também reforça a autonomia do DPO e ajuda a garantir que ele possa agir de forma independente.
- O Controlador ou o Processador podem não concordar com a opinião do DPO, mas nem por isso podem dispensar ou penalizar o DPO por esse conselho.
- Como qualquer outro empregado ou contratado, um DPO pode ser demitido ou dispensado de forma legítima por outras razões que não a execução de suas tarefas.

Conflito de Interesse

O GDPR prevê que o DPO desempenhe suas tarefas e deveres, exigindo que as organizações garantam que as tarefas e deveres do DPO não resultem em conflito de interesse – Artigo 38 (6).

Mesmo que o DPO possa exercer outras funções, ele só pode fazer isso desde que não provoque a situação de conflito de interesse.

Pode ser uma boa prática para o Controlador / Processador:

- Identificar as posições incompatíveis com a função de DPO;
- Traçar regras internas para evitar conflito de interesse;
- Incluir uma explicação geral sobre conflito de interesse;
- Declarar que o DPO não tem conflito de interesse;
- Incluir salvaguardas nas regras da organização e garantir que o anúncio de uma vaga para a posição de DPO ou contrato de serviço seja suficientemente preciso e detalhado.

Designando um DPO

O DPO deve ser designado com base nas suas qualidades profissionais e, em particular, conhecimento especializado na lei e práticas de proteção de dados, e a habilidade de realizar as tarefas.

O principal requisito de um DPO é o cumprimento das suas tarefas, que exige um nível significativo de conhecimento e experiência prática sobre implementação e operação de um modelo de conformidade de privacidade.

Alguns dos atributos e conhecimento que podem ser exigidos de um DPO:

- Formação em Direito, idealmente com especialização em lei de privacidade GDPR;
- Qualificações e certificações profissionais relacionadas a proteção de dados;
- Qualificações e certificações profissionais relevantes à indústria ou setor no qual está trabalhando;
- Experiência em implementação de medidas e ou frameworks, modelos de proteção de dados;
- Experiência em gerenciamento de sistemas e processos envolvidos em proteção de dados pessoais;
- Experiência com normas e modelos de gerenciamento de risco;
- Experiência e conhecimento em gerenciamento de segurança da informação e certificações relevantes em garantia de segurança *cyber security.*

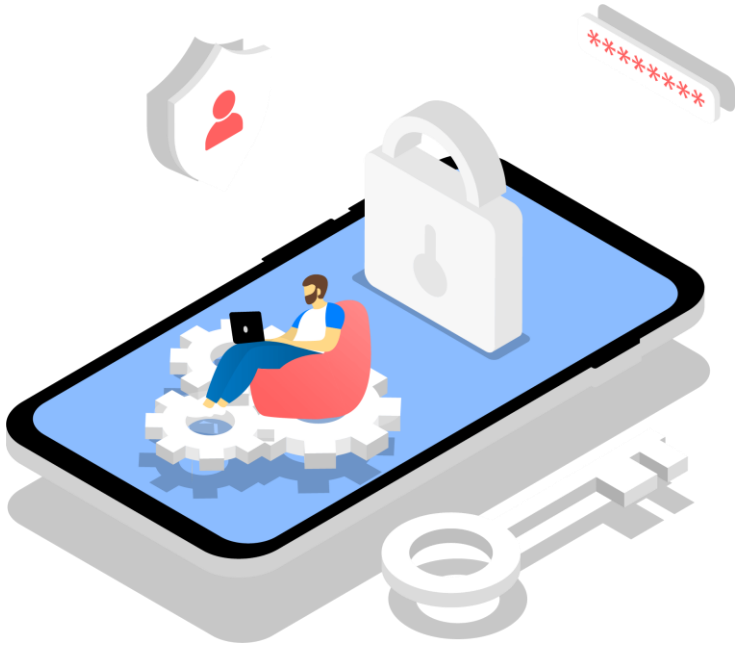
Primeira Tarefa do DPO

A primeira tarefa do DPO é informar e avisar o Controlador ou o Processador, e os empregados que executam o processamento, sobre suas obrigações em proteção de dados nos termos do GDPR e outros da União ou Estado Membro.

- **O DPO é responsável por garantir** que o Controlador, Processador e empregados que processam dados pessoais entendam suas obrigações, e aconselhar sobre como cumprir com elas.
- **O DPO deve aconselhar** Controladores e Processadores em como implementar programas de conscientização e treinamento da equipe.
- **Orientar** quanto às novas legislações incluindo penalidades e multas relacionadas, tanto para o Controlador, Processador e Equipe.

Segunda Tarefa do DPO

Monitorar a conformidade com o Regulamento, com outras provisões da União e dos Estados Membros, e com as políticas do Controlador e do Processador em relação à proteção de dados pessoais, incluindo a designação de responsabilidades, aumento da conscientização e treinamento da equipe.



- **O DPO deve supervisionar** o modelo de conformidade de privacidade.
- **O DPO também deve ser capaz** de confirmar que os processos da organização atendem aos requisitos do Regulamento.
- **Cabe ao Controlador, Processador e DPO garantir a geração** de registros adequados e precisos através do modelo de conformidade de privacidade. Esses registros serão necessários para o DPO confirmar a eficácia do programa de conformidade da organização.

Terceira, Quarta e Quinta Tarefas do DPO

A **terceira grande tarefa do DPO** é aconselhar e dar seu parecer com relação à avaliação de impacto da proteção de dados nos termos do Artigo 35.

Vamos ver a **quarta e a quinta tarefas do DPO** juntas pois estão bem relacionadas:

- Cooperar com a Autoridade Supervisora;
- Atuar como ponto de contato para a Autoridade Supervisora.

O DPO, essencialmente, é a ligação imediata da organização com a Autoridade Supervisora.

O DPO deve prestar a devida atenção ao processamento de alto risco, levando em conta a natureza, escopo, contexto e propósitos.

O DPO deve garantir que tenha os processos adequados e documentados para responder às solicitações e reclamações para o Controlador ou Processador, e atuar como mediador em qualquer discussão.

O DPO e a Organização

- O DPO é um papel muito independente.
- Esse papel tem a ver com entrega de conformidade, e não pode haver conformidade sob a direção da equipe de entrega.
- Para garantir a autonomia e a capacidade de supervisão, o DPO deve ocupar uma posição no gerenciamento de risco, conformidade e na função de governança.
- O DPO deve poder conduzir as suas atividades com total confidencialidade e sigilo, sempre que necessário, o que faz surgir uma camada de separação entre o DPO e a organização na busca pela conformidade.
- Para ser um DPO eficaz, você deve garantir que a proteção de dados, privacidade e obrigações legais da organização estejam na agenda dos Diretores.
- O tamanho das multas em potencial e as ramificações das violações de dados impõem um dever fiduciário na alta administração.

O DPO e a Autoridade Supervisora

Em muitas situações, o DPO atua como uma espécie de intermediário, oferecendo um ponto único de contato, garantindo que qualquer comunicação entre a Autoridade Supervisora e o Controlador ou Processador seja muito clara.

- Os detalhes de contato do DPO têm que estar disponíveis para o público e para a Autoridade Supervisora. Ele deve responder diretamente às requisições da Autoridade Supervisora, e garantir que as solicitações da Autoridade Supervisora feitas à ele, e garantir que as solicitações da Autoridade Supervisora endereçada aos Controladores sejam reconhecidas.
- O DPO também tem que cooperar com a Autoridade Supervisora se ela pedir, por exemplo, para complementar as informações fornecidas em uma notificação, para verificar uma reclamação relacionada à organização do DPO.
- O DPO não somente deve responder a todas as solicitações dentro de um mês, como também garantir que as solicitações endereçadas aos Controladores sejam tratadas no mesmo prazo.

A mediação feita pelo DPO entre a Autoridade Supervisora e o Controlador ou Processador quando de uma violação de dados é de extrema importância.

Avaliação de Impacto de Proteção de Dados e Avaliação de Risco

- O DPO deve entender o gerenciamento de risco como um processo e como ele se encaixa no modelo de conformidade. Isso é especialmente se o DPO for um contratado externo.
- O DPO deve também garantir que entende o apetite ao risco da organização, e como isso interage com as expectativas da Autoridade Supervisora.
- Uma organização pode, por exemplo, estar disposta a aceitar certos riscos que a Autoridade Supervisora esperaria que fossem rejeitados.
- Muitas dessas questões devem ser resolvidas durante a fase de consulta, após um DPIA.
- O DPO precisa estar super preparado para dar conselhos ao Controlador e Processador e a responder a qualquer pergunta ou recomendação da Autoridade Supervisora.

DPO Interno ou Contratado

Organizações maiores provavelmente vão empregar um ou mais DPOs para se fortalecer e ter recursos adequados na equipe de proteção de dados para cobrir feriados, férias, problema de saúde e planejar promoções. Para organizações menores, o DPO pode na verdade nem representar uma atividade em tempo integral.

A organização tem duas opções: designar o papel de DPO para um membro da sua equipe, ou contratar de uma parte terceira.

- Designar o papel a um **membro do time atual** tem a vantagem de quase sempre o custo ser menor do que empregar uma nova pessoa.
- Apesar de parecer a opção mais custosa**, a contratação do papel em uma parte terceira** pode ser a melhor alternativa.

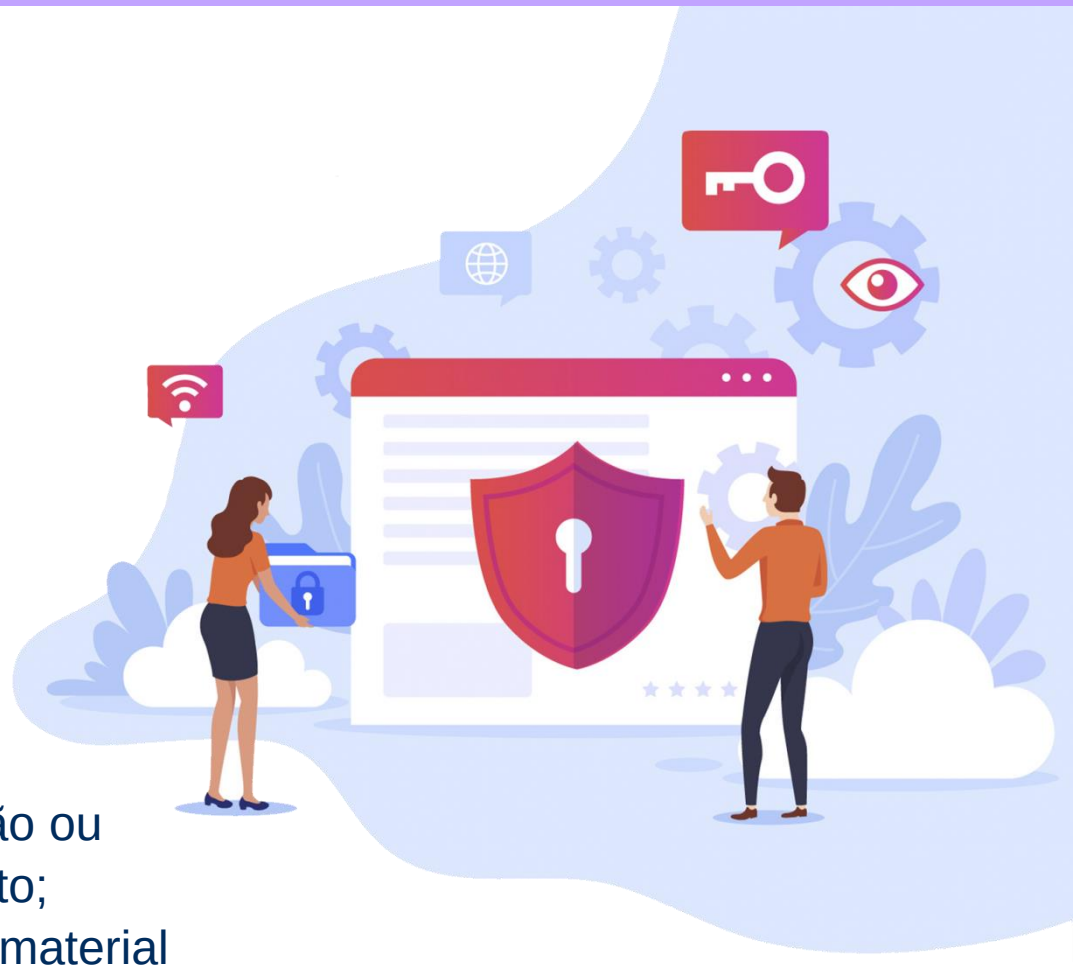
PDPP

Módulo 5: Avaliação de Impacto sobre a Proteção de Dados (DPIA)

Introdução à Avaliação de Impacto sobre Proteção de Dados

DPIA

- A Avaliação de Impacto sobre Proteção de Dados – DPIA é um dos processos obrigatórios no GDPR.
- DPIA é usada para identificar os riscos específicos aos dados pessoais por conta das atividades de processamento.
- Ela pode ser comparada à avaliação de risco de segurança da informação exigida pela ISO/IEC 27001 e descrita na ISO/IEC 27005. Mas as DPIAs, é claro, têm um foco maior em proteção de dados e privacidade.



Na avaliação devem ser considerados os riscos:

- Destruição acidental ou criminosa, perda, alteração, divulgação ou acesso não autorizados, além de transmissão, armazenamento;
- Qualquer outra atividade que pode levar a algum dano físico, material ou não material.

Resultados Esperados da DPIA

O GDPR também estabelece o que deve, minimamente, compor uma DPIA:

- Descrição do processamento e propósitos;
- Interesses legítimos perseguidos pelo Controlador;
- Avaliação da necessidade e proporcionalidade do processamento;
- Avaliação dos riscos aos direitos e liberdades dos Titulares dos Dados;
- Medidas previstas para tratar os riscos;
- Salvaguardas e medidas de segurança para comprovar conformidade;
- Indicação dos prazos se o processamento está relacionado ao apagamento;
- Indicação de qualquer medida de proteção de dados desde a concepção (*by design*) e por padrão (*by default*);
- Lista dos destinatários dos dados pessoais;
- Confirmação da conformidade com códigos de conduta aprovados;
- Detalhes se os titulares de dados foram consultados.

Podem existir resultados específicos que você determina como requeridos com base nas necessidades.

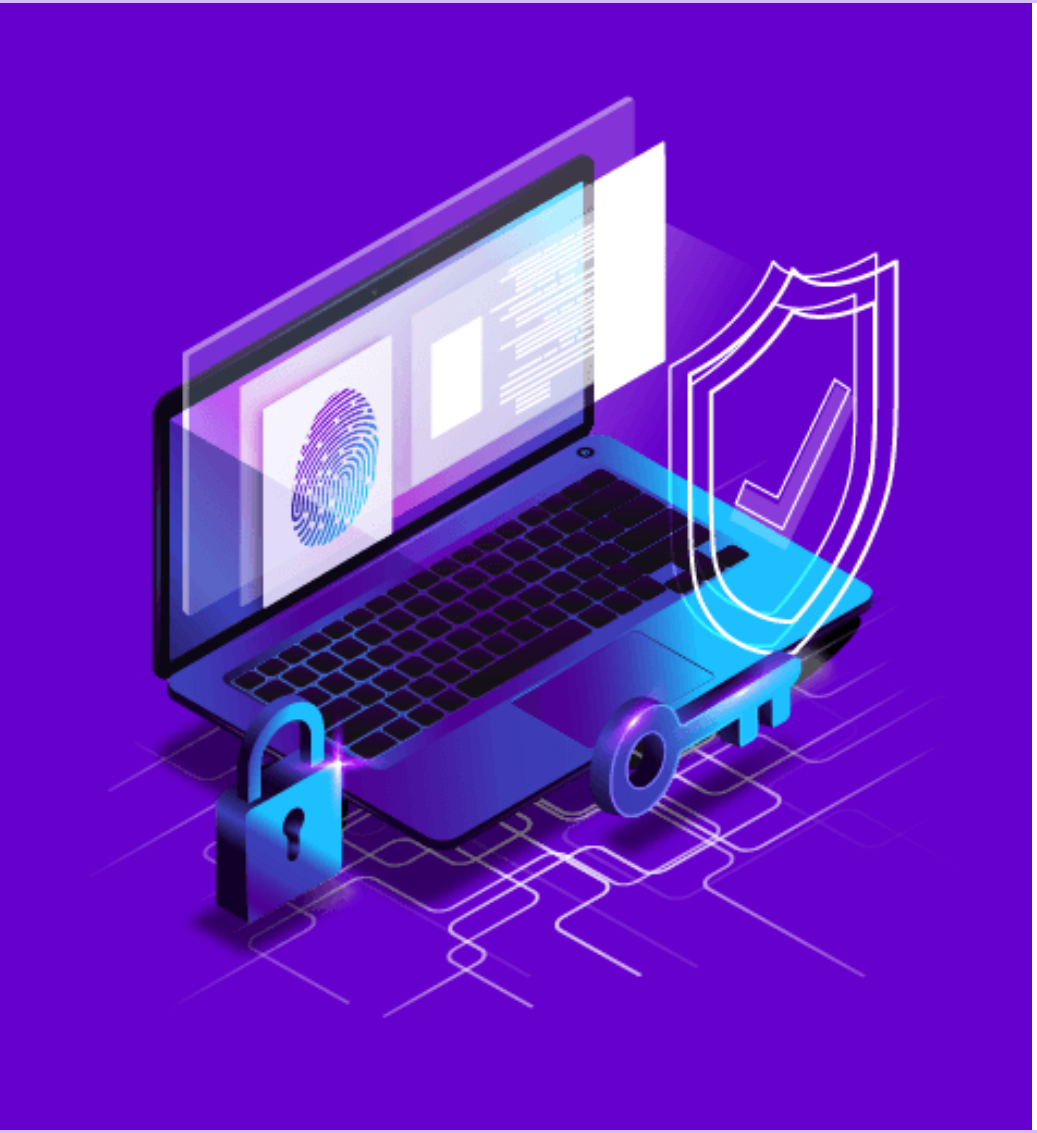
Benefícios da DPIA

- Uma DPIA constrói confiança.
- Publicar os resultados de uma DPIA para mostrar que a sua organização mantém os dados pessoais seguros. Para isso, você adota uma abordagem muito rigorosa.

- **Internamente, acaba se traduzindo em maior consciência dos deveres das pessoas.**
- **Externamente, a DPIA leva a uma melhor reputação e maior confiança.**

- A DPIA também ajuda a identificar problemas antecipadamente.
- Ajuda a estender a revisão dos dados que você coleta nos termos do princípio da minimização dos dados.
- O procedimento completo das avaliações de impacto pode ser longo, especialmente para as grandes organizações ou para aquelas que manuseiam grandes volumes de dados complexos.

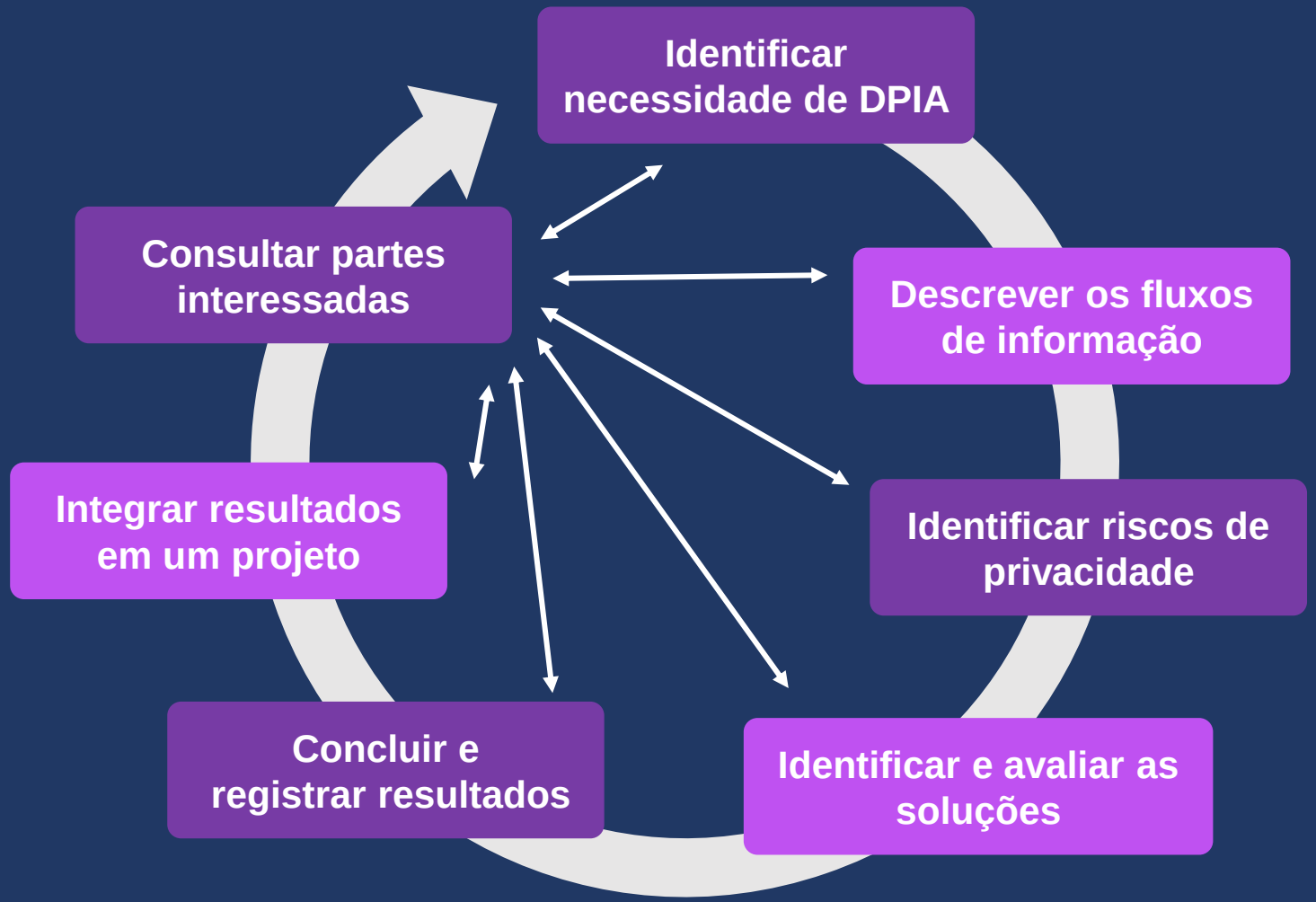
Fundamentos da DPIA



Antes do GDPR existia a Avaliação de Impacto sobre Privacidade (*Privacy Impact Analysis* – PIA), considerada por todos a melhor prática, incluindo os Reguladores. Devido a essa aceitação, a PIA pode ser usada como base para a DPIA.

- DPIA é um processo que auxilia as organizações a identificar e minimizar riscos de privacidade, e normalmente, é conduzida antes da implementação de novos processos, projetos ou políticas.
- Procurar problemas potenciais, para que possam ser mitigados antecipadamente.
- Permite o aperfeiçoamento de políticas, processos e sistemas.
- Várias agências Europeias desenvolveram um completo código de práticas e documentos para as avaliações de impacto.
- Consultar a Autoridade Supervisora local para orientação para saber se existe alguma orientação regional apropriada.

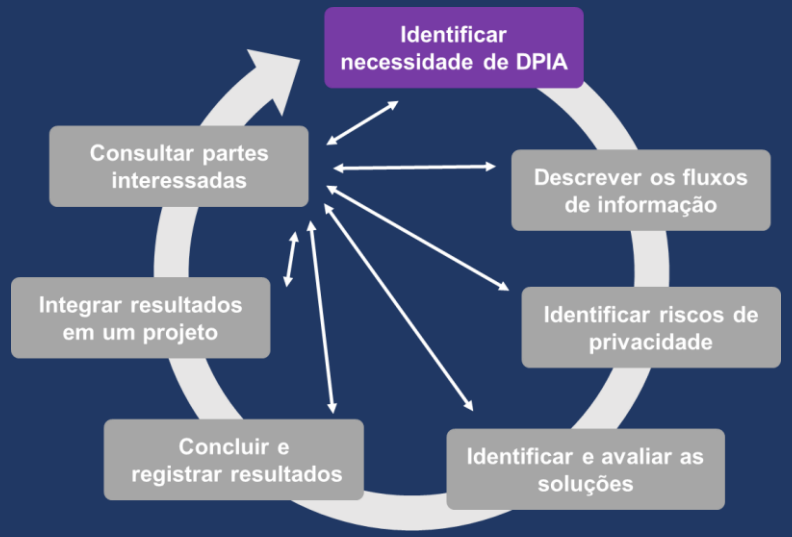
Etapas de uma DPIA



Identificar a Necessidade de DPIA

DPIA 1

Identificar necessidade de DPIA



- Uma DPIA é necessária quando as operações de processamento são suscetíveis de implicar um elevado risco.
- A sua empresa vai precisar determinar se, antes de mais nada, a lei exige, ou se a organização é quem deseja fazer essa avaliação.
- “O Controlador deve executar uma avaliação de impacto se o tipo de processamento em particular usando novas tecnologias, considerando a natureza, escopo, contexto e propósitos do processamento, tiver alguma chance de resultar em um alto risco, para os direitos e liberdades das pessoas. E ela deve acontecer antes de qualquer processamento”.

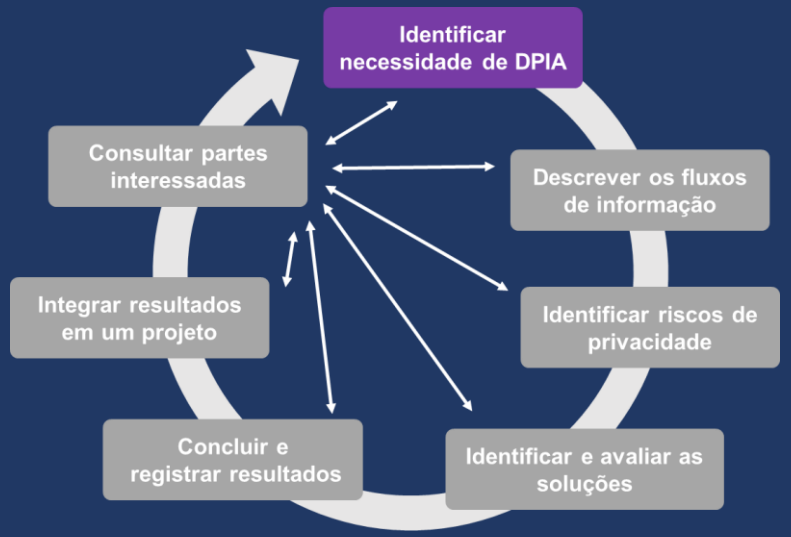
Condições para realização de DPIA no GDPR:

- Avaliação sistemática e extensiva de aspectos pessoais relacionados às pessoas naturais, baseada no tratamento automatizado;
- Processamento de categorias especiais de dados ou dados pessoais relacionados a condenações criminais e crimes em larga escala;
- Monitoramento sistemático de uma área de acesso público em larga escala.

Razões para conduzir uma DPIA

DPIA 1

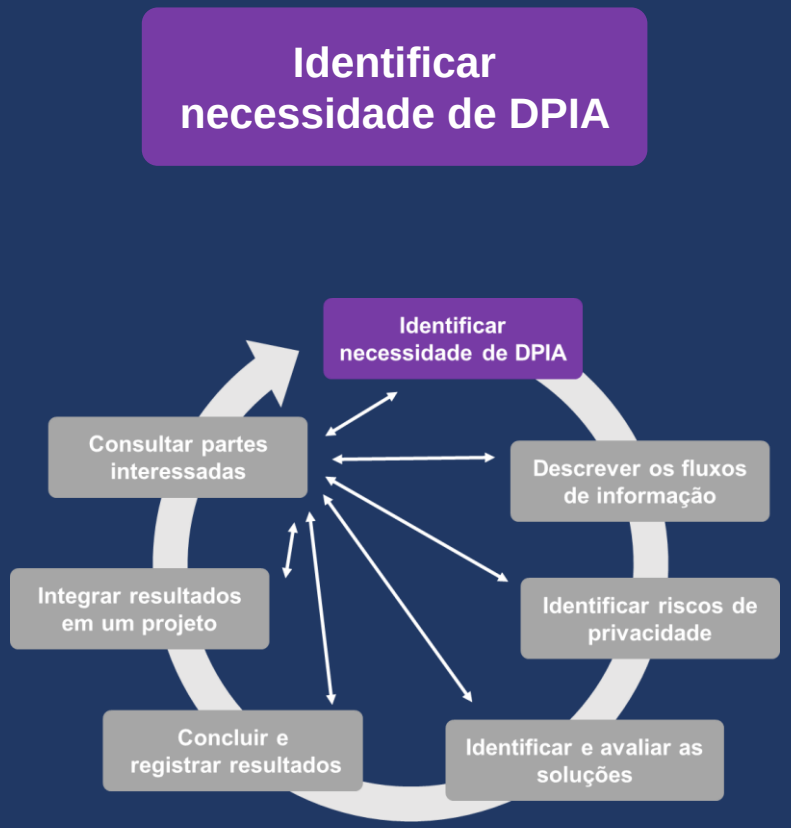
Identificar necessidade de DPIA



- O projeto envolve um conjunto de informações novas sobre indivíduos?
- O projeto obriga os indivíduos a fornecer informações pessoais sobre eles?
- As informações sobre os indivíduos serão divulgadas para novas organizações ou pessoas que não tinham acesso anteriormente?
- Você está usando informação sobre os indivíduos para um propósito que atualmente não existe ou de alguma forma que atualmente não é utilizada?
- O projeto envolve a utilização de novas tecnologias que podem ser percebidas como invasivas à privacidade?
- O projeto resulta em decisões ou ações relacionadas aos indivíduos que podem ter um impacto significativo sobre eles?
- A informação sobre os indivíduos é de um tipo que tem a chance de gerar preocupação ou expectativa com relação à privacidade?
- O projeto exige que você entre em contato com os indivíduos de uma maneira que eles possam considerar intrusiva?

Exemplos de Situações de DPIA

DPIA 1

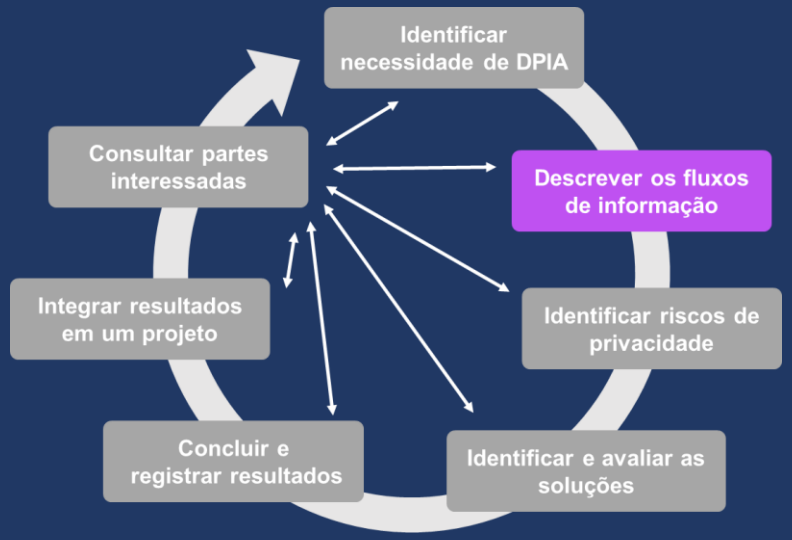


- Um hospital processando os dados genéticos e de saúde de seus pacientes.
- Arquivamento de dados sensíveis sob pseudônimo de projetos de pesquisa ou ensaios clínicos.
- Organização que utiliza um sistema inteligente de análise de vídeo para destacar veículos e reconhecer automaticamente os registros.
- Uma organização que monitora sistematicamente as atividades de seus empregados, incluindo suas estações de trabalhos e atividades na Internet.
- Coleta de dados de mídia social públicos para gerar perfis.
- Instituição que cria um banco de dados de classificação de crédito ou fraude em nível nacional.
- **Pode ser necessária para atender aos requisitos do gerenciamento de risco da própria empresa.**
- **Você deve documentar seus critérios ou definir um processo repetível para determinar se uma DPIA é necessária.**

Descrever os Fluxos de Informação

DPIA 2

Descrever os fluxos de informação



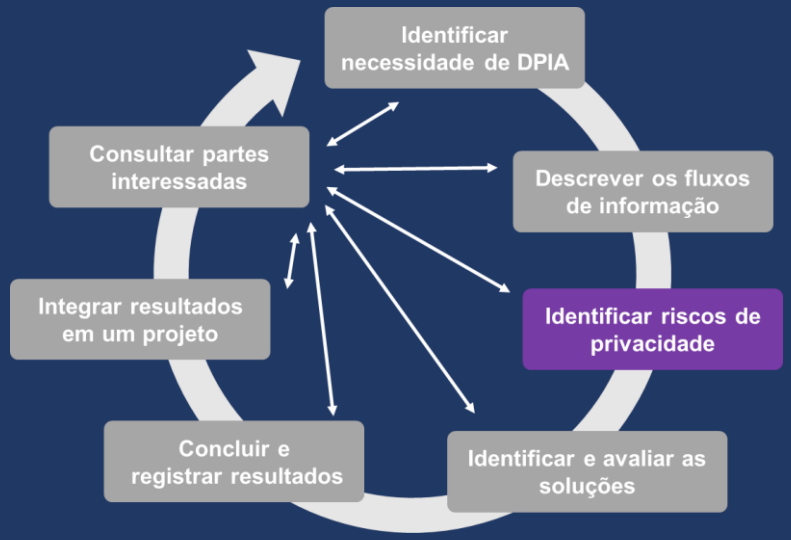
- É essencial conhecer os dados pessoais que você está coletando e os que você já detém.
- DPIA depende do entendimento completo do ciclo de vida dos dados.
- Não existe no Regulamento nenhum requisito explícito para **mapeamento dos dados**, mas seria extremamente difícil atender a todos os requisitos do GDPR sem estabelecer o ciclo de vida dos dados pessoais na sua organização.
- O mapeamento de dados pode ser um tanto desafiante para as organizações que nunca tenham examinado os seus processos antes.

- **O mapeamento de dados possui quatro elementos principais: itens de dados, formatos, métodos de transferência e locais.**
- **O mapeamento de dados é uma parte importante do processo de gerenciamento de risco.**
- **Fica bem óbvio quando se olha um mapa de dados quais áreas podem causar problemas de privacidade.**

Identificar os Riscos Relacionados à Privacidade

DPIA 3

Identificar riscos de privacidade

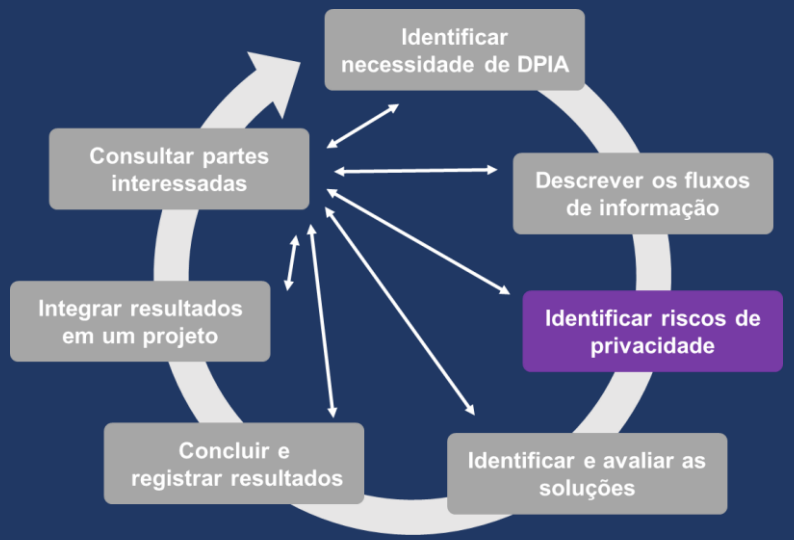


- Conhecer as ameaças e como elas podem explorar as suas vulnerabilidades.
- Catalogar toda a gama de ameaças e vulnerabilidades relacionadas aos direitos e liberdades dos titulares dos dados.
- **Riscos aos dados pessoais**: ação de hacker, vírus, malware, invasores, phishing, falta de treinamento e conscientização de segurança, dados não criptografados, controle de acesso inadequado, senhas fracas, etc.
- Você usa a DPIA para identificar riscos à privacidade dos titulares de dados, a segurança dos seus dados pessoais, e aos seus direitos e liberdades em relação aos dados.
- DPIA deve informar e fazer parte da atividade muito mais ampla que é o seu gerenciamento de risco corporativo.

Avaliação dos Riscos

DPIA 3

Identificar riscos de privacidade

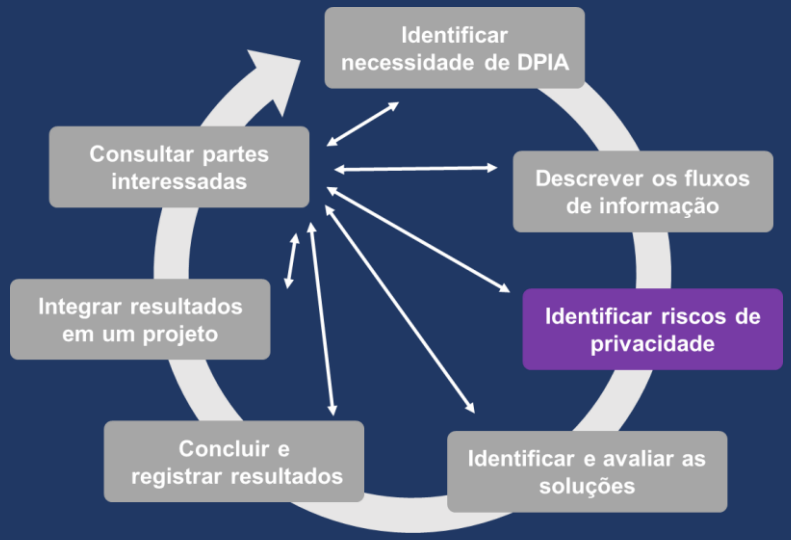


IMPACTO MUITO ALTO	RISCO MÉDIO	RISCO MÉDIO	RISCO ALTO	RISCO ALTO	CRÍTICO
IMPACTO ALTO	RISCO BAIXO	RISCO MÉDIO	RISCO ALTO	RISCO ALTO	RISCO ALTO
IMPACTO MÉDIO	RISCO BAIXO	RISCO BAIXO	RISCO MÉDIO	RISCO MÉDIO	RISCO ALTO
IMPACTO BAIXO	RISCO MUITO BAIXO	RISCO BAIXO	RISCO BAIXO	RISCO MÉDIO	RISCO MÉDIO
IMPACTO MUITO BAIXO	RISCO MUITO BAIXO	RISCO MUITO BAIXO	RISCO BAIXO	RISCO BAIXO	RISCO MÉDIO
	MUITO IMPROVÁVEL	IMPROVÁVE;	MODERADA-MENTE PROVÁVEL	PROVÁVEL	MUITO PROVÁVEL

Um Pouco Mais Sobre Riscos

DPIA 3

Identificar riscos de privacidade

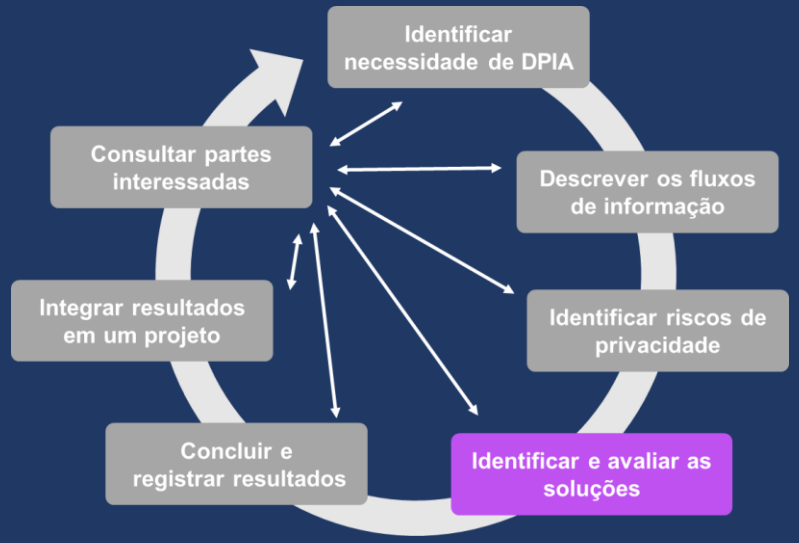


- É importante entender toda a gama de riscos reais e como essas várias formas de risco podem ter impactos significativos na privacidade.
- Você não pode esquecer que riscos físicos também podem representar riscos à privacidade.
- Riscos cibernéticos, ou seja, riscos relacionados às tecnologias de informação e comunicação, obviamente tem a maior intersecção com os riscos à privacidade.
- Os riscos de continuidade podem impedir uma organização de operar.
- Como o GDPR exige que você forneça aos titulares dos dados o acesso às informações deles, logo isso se torna um risco à privacidade.
- Uma perda de continuidade pode ainda trazer outros riscos como falha no trancamento de portas eletrônicas, que impõe um risco físico às instalações, e daí um risco potencial de privacidade.

Identificar e Avaliar as Soluções de Privacidade

DPIA 4

Identificar e avaliar soluções



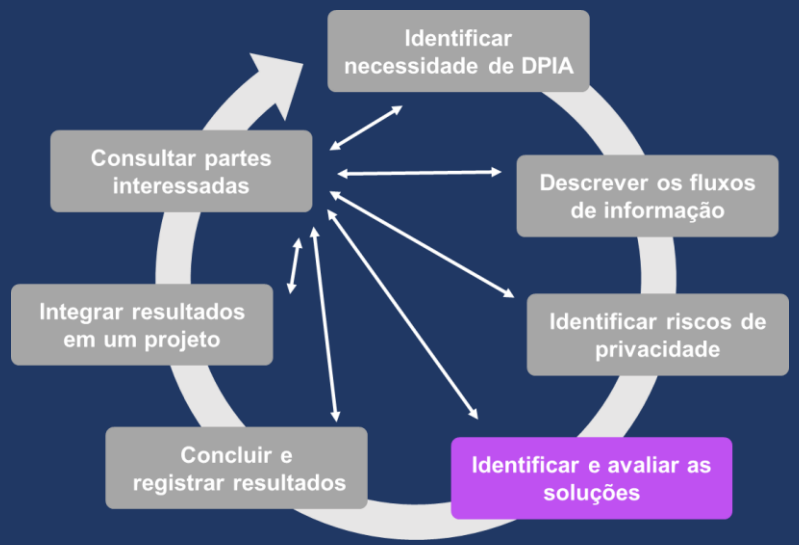
Para cada risco aos dados pessoais, você deve tomar o que chamamos "decisão de risco".

- **Tratar, controlar ou modificar o risco:** o objetivo aqui, é a aplicação de controle para reduzir o risco até um nível aceitável dentro dos seus critérios.
- **Tolerar, aceitar ou reter o risco:** é a resposta padrão aos riscos que estão dentro dos critérios de avaliação. Mas também pode ser aplicada aos riscos aonde o custo de tratamento ultrapassa os benefícios de negócio.
- **Mitigar, eliminar ou evitar o risco:** normalmente isso é feito pela remoção do alvo do risco, como encerrando o processo ou se livrando do ativo ou item em questão.
- **Transferir ou compartilhar o risco:** terceirizar o processo ou o ativo para outra empresa, assim elas teriam que encarar o risco. Mas veja bem! Transferir um risco de proteção de dados dessa forma não absolve você ou sua empresa da prestação de contas nos termos do GDPR.

Tratamento dos Riscos

DPIA 4

Identificar e avaliar soluções



Não é necessário eliminar todos os riscos de privacidade. A chave aqui é reduzir até em um nível aceitável.

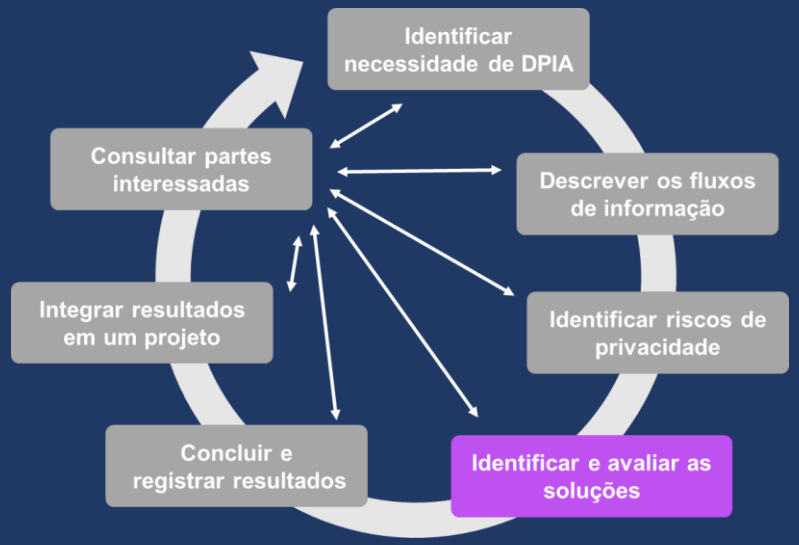
Ações de uma organização para tratar, transferir ou mitigar os riscos:

- Reduzir a quantidade de dados coletados;
- Desenvolver uma política de retenção para governar por quanto tempo e em qual formato os dados pessoais são armazenados;
- Destruir a informação de forma segura quando não for mais necessária;
- Minimizar acesso através de políticas e procedimentos de controle de acesso;
- Introduzir um programa de treinamento e conscientização;
- Anonimizar os dados pessoais;
- Redigir contratos ou acordos de compartilhamento de dados;
- Desenvolver um processo de solicitação de acesso para proteger os direitos dos titulares dos dados;
- Solicitar que os fornecedores conduzam avaliações de risco e disponibilizem os resultados.

Registro de Riscos

DPIA 4

Identificar e avaliar soluções



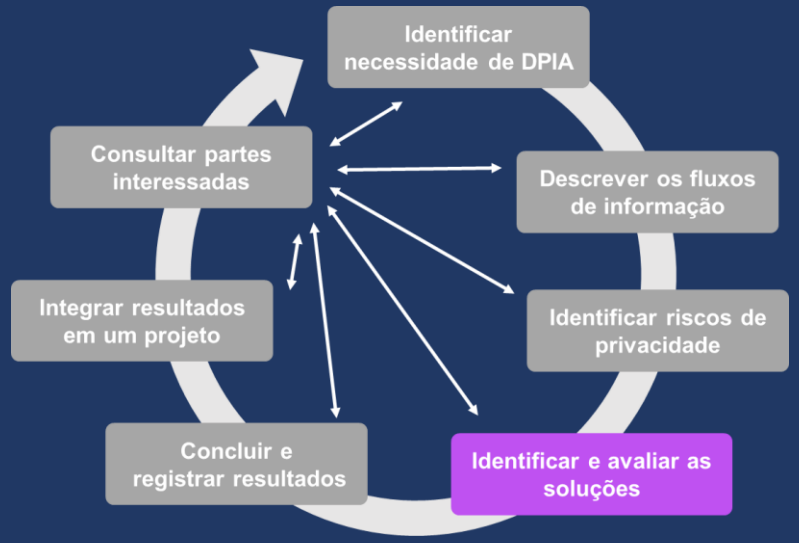
RISCO	IMPACTO	PROBAB.	RESPOSTA	AÇÃO	RESPONSÁVEL
Controle de divulgação inadequado	Alto	Alta	Tratar	Desenvolver, comunicar política de divulgação	Gerente de Segurança da Informação
Informação coletada e armazenada indefinidamente	Moderado	Baixa	Tratar	Desenvolver política de retenção	Gerente de Operações
Violação de dados por terceiros	Alto	Moderada	Tolerar	Cláusulas apropriadas nos contratos existentes	Gerente de Relacionamento e Jurídico
Apropriação ou perda acidental de dados	Alto	Moderada	Transferir	Apólice de seguro	CFO

Importante: o conteúdo desta tabela é um exemplo e não sugestão.

Gerenciamento de Risco e Dados Pessoais

DPIA 4

Identificar e avaliar soluções



- **Reconhecer que os riscos aos direitos e liberdades dos titulares de dados de qualquer atividade de processamento em particular pode ter um perfil diferente em relação à organização.**
- **A corrupção do dado de um indivíduo pode ter um impacto mínimo para uma organização que processa milhares de registros de dados, mas pode ter um impacto significativo para esse indivíduo.**
- O GDPR exige que as organizações considerem esse impacto no indivíduo e determinem os controles apropriados que vão reduzir esse impacto a níveis aceitáveis, para a lei e para as pessoas.
- Deve ser documentado e serve como evidência para comprovar que a empresa identifica e implementa os controles organizacionais e técnicos apropriados.

Concluir e Registrar os Resultados da DPIA

DPIA 5

Concluir e registrar resultados

- Os resultados da DPIA devem ser registrados e assinados por quem seja responsável pelas decisões.
- Um relatório formal vai delinear as medidas para tratar as questões de proteção de dados.
- Responsabilização e transparência.
- Permitindo que os indivíduos aprendam mais sobre como a privacidade afeta a todos e o seu trabalho.
- Garantir que o relatório final da sua DPIA seja adequado para distribuição externa.

O relatório da sua DPIA deve incluir uma visão geral do projeto que indica:

- Pessoal envolvido;
- O que você faz com ele e porquê;
- Quanto tempo os dados serão mantidos;
- Fornecer informação para demonstrar que você avaliou o impacto do projeto;
- “Higienizado” para proteger os titulares de dados e a própria organização;
- Deve ser assinado pela autoridade apropriada.

Integrar os Resultados da DPIA em Um Plano de Projeto

DPIA 6

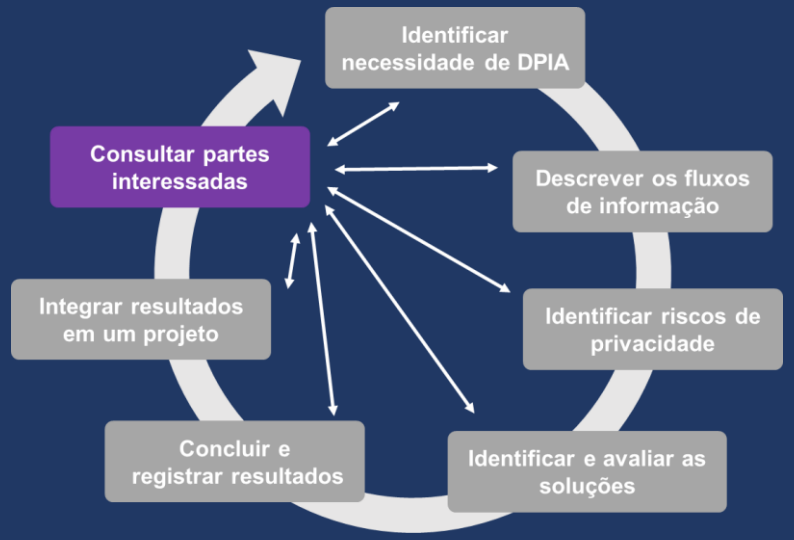
Integrar resultados em um projeto

- Nesta etapa as decisões que você tomou anteriormente se tornam ações definidas.
- Implementação real do plano de projeto, que estabelece as funções de processamento examinadas pela DPIA.
- Pode exigir mais ou menos trabalho técnico, como programação e codificação, e talvez você tenha que rever os prazos e dependências do projeto.
- Algumas medidas que você implementar podem exigir procedimentos operacionais relevantes para manutenção e observação periódicas.
- Definir métricas para medir a efetividade das respostas aos riscos.
- Garantir que o seu framework de conformidade de privacidade, qualquer que seja o modelo que você tenha adotado, tenha sido considerado.

Consultar as Partes Interessadas ao Longo da DPIA

DPIA 7

Consultar partes interessadas



Partes interessadas devem ser consultadas apropriadamente ao longo do processo.

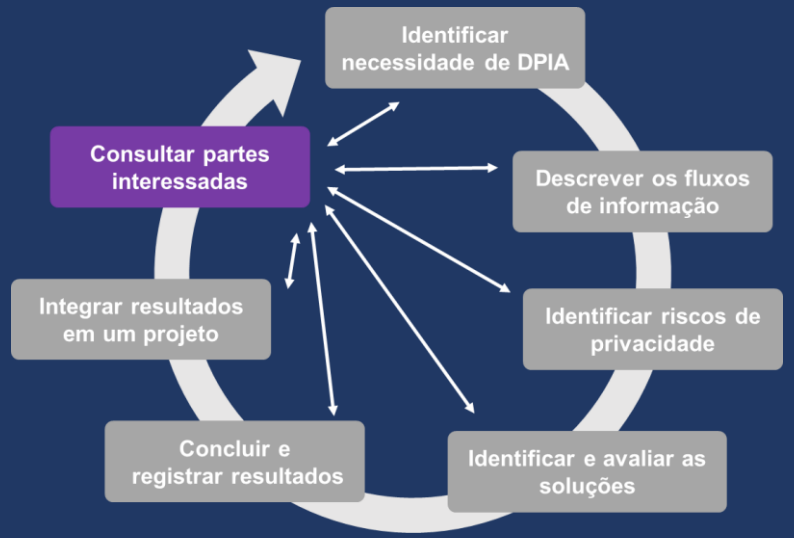
Partes interessadas internas provavelmente estão envolvidas no processamento ou no projeto de alguma forma, e devem ser consultadas para se ter uma ideia melhor dos riscos envolvidos.

- Incluir equipe de gerenciamento de projeto, DPO, engenheiros, equipe de TI, área de compras, suporte ao cliente, jurídico, e assim por diante.
- Externamente, pode ser um consultor especializado em proteção de dados e privacidade, ou um grupo de titulares de dados anônimos.
- O GDPR estipula que “onde for apropriado, os controladores dos dados devem buscar as visões dos titulares de dados e seus representantes no processo pretendido”.
- Consulta para conseguir os resultados que você possa usar na DPIA.

Consultando Partes Interessadas Externas

DPIA 7

Consultar partes interessadas



- A consulta deve ser oportuna - na etapa certa e dando às partes interessadas tempo suficiente para responder.
- A consulta deve ser clara e proporcional – apresentar informação necessária, nem mais nem menos.
- Consultar representantes apropriados, garantindo que aqueles que você abordar representem de forma justa quem for impactado, ou os que podem oferecer informações como autoridades locais e entidades regulatórias.
- Ser objetivo e realista, oferecendo a essas partes externas opções realistas e informação sem viés.
- Feedback tem duas mãos, ou seja, se você recebe feedback, esteja certo de oferecer feedback também.
- **A Autoridade Supervisora é a parte interessada externa mais importante a ser consultada.**
- **O Controlador de dados deve consultar a Autoridade Supervisora se a DPIA "indicar que o processamento poderia resultar em um alto risco na ausência de medidas tomadas pelo controlador para mitigar os riscos".**

Quem Precisa se Envolver na DPIA

- É responsabilidade do Controlador de Dados garantir que as DPIAs sejam conduzidas onde “as operações de processamento possam resultar em um alto risco aos direitos e liberdades das pessoas”.
- O Controlador de Dados deve buscar o conselho do DPO, quando existir um designado, ao executar uma “Avaliação de Impacto sobre Proteção de Dados”.
- Os donos ou proprietários de ativos e processos devem com certeza serem envolvidos.
- Poderia ser envolvida: gerenciamento de risco, entrega de serviço, infraestrutura e outras.
- Ter muita gente diretamente envolvida pode arruinar o processo.

PDPP

Módulo 6 - Violação de dados, notificação e resposta a incidentes

Módulo 6 - Falhas de Segurança de Dados

Organizações pequenas podem ser varridas do mapa simplesmente pela natureza da violação ou dos custos imediatos. Grandes corporações podem ser alvo de multas pesadas, ações judiciais e danos à reputação, tudo isso com enorme repercussão.

O Regulamento não proíbe explicitamente as violações de dados, e não faria sentido proibir porque é impossível cumprir. O GDPR declara que as organizações devem buscar formas de proteger todos os dados pessoais contra perdas e danos.

Target (EUA) - no final de 2013, os criminosos tiveram acesso a informações pessoais de cerca de 70 milhões de clientes e 40 milhões de cartões de crédito e cartões de pagamento:

- Não havia estabelecido um processo de verificação de segurança do fornecedor;
- A interface entre o sistema de gestão edifícios em uma das lojas da Target e os sistemas de pagamento não estavam protegidos;
- A Target ignorou vários avisos automáticos provenientes do seu software de detecção de intrusão (IDS);
- Se viu envolvida em multas e ações judiciais, o CIO e o CEO foram obrigados a se demitir.

O que é Violação de Dados Pessoais?

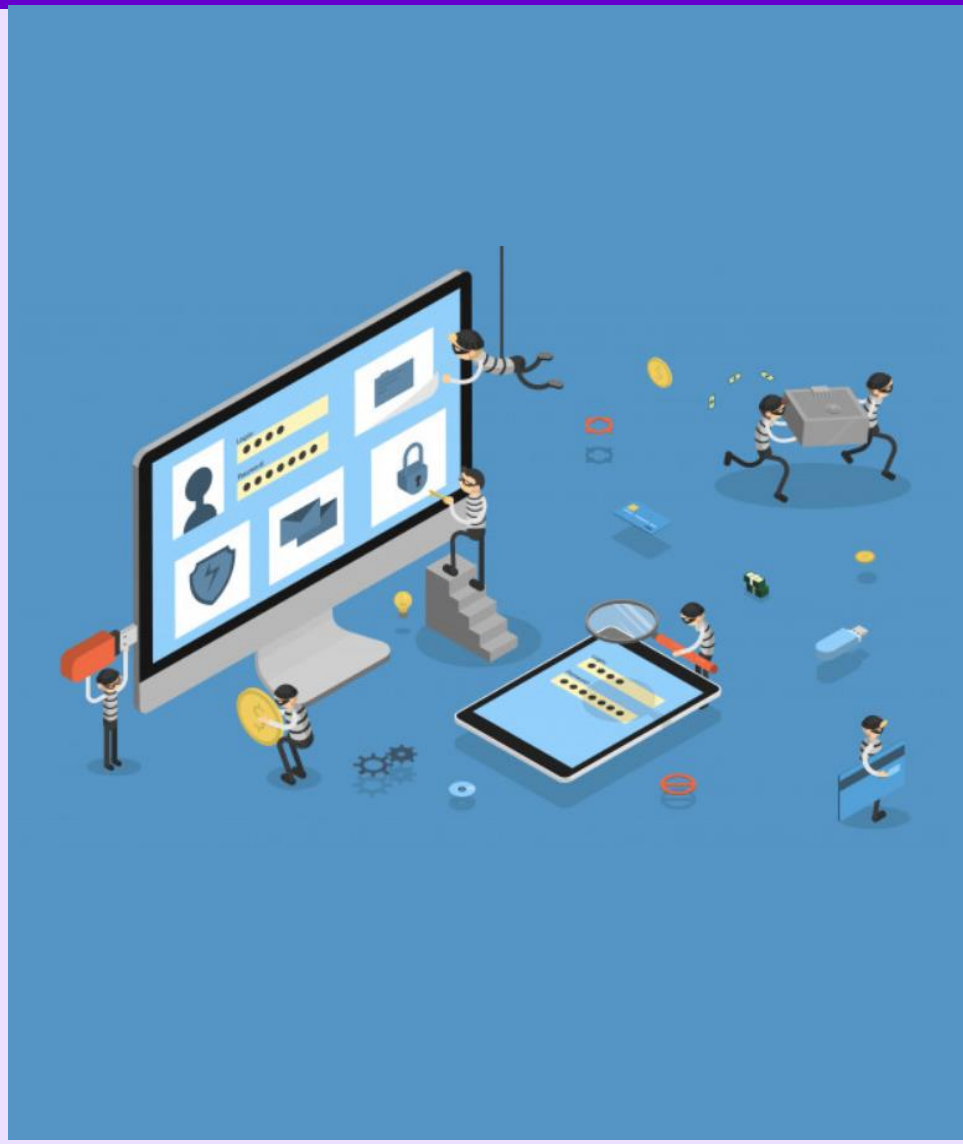
A violação de dados pessoais consiste em uma infração da segurança que tenha por efeito a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de processamento, seja acidental ou de modo ilícito.

- Um dos principais focos do GDPR.
- Regulamento não se preocupa com as demais violações, a menos que elas possam trazer algum impacto à segurança dos dados pessoais.
- Tudo o que a organização puder fazer para proteger suas informações, vai fortalecer a segurança dos dados pessoais daqueles que estão dentro e fora dos limites da empresa.

Formas de Violação de Dados

A informação pode ficar comprometida de muitas formas:

- Distribuída para fora da organização, por exemplo, através de roubo ou venda na *dark web;*
- Destruição ou deterioração da informação, por vandalismo;
- Informações podem ficar inacessíveis, por exemplo, por *ransomware* ou sequestro dos dados.
- Violações de confidencialidade, integridade ou disponibilidade são conhecidas pela sigla CID (“CIA”, para os termos em inglês);
- Ação ou inação que enfraquece a segurança de dados e abre as portas para as ameaças;
- Muitas ameaças estão associadas a certos personagens ou atores como um cyber criminoso, um informante interno malicioso, ou um membro desatento da equipe.



Vulnerabilidade e Violação de Dados

Uma vulnerabilidade, como você também já estudou, segundo a ISSO/IEC 27000, é "A fragilidade de um ativo ou controle que pode ser explorada por uma ou mais ameaças"

Uma violação de dados acontece quando uma ameaça consegue explorar com sucesso uma vulnerabilidade.

As vulnerabilidades são localizáveis, tem um local, e não somente no sentido físico. Uma aplicação web, por exemplo, pode ter uma vulnerabilidade no SQL localizada no ambiente virtual.

Sua organização possui várias fronteiras, que são definidas pelos pontos nos quais a empresa encontra o mundo exterior:

- Em termos físicos, elas representam os muros de um edifício ou as paredes do escritório;
- Em termos lógicos seria a sua rede e seus equipamentos nas pontas, como os laptops e celulares.

Protegendo a Informação

Controle é um processo ou ferramenta que evita o risco de uma ameaça explorar uma vulnerabilidade, pela redução da probabilidade da ocorrência ou do impacto se acontecer.

Dentre as medidas, também já exploradas anteriormente, a gente poderia destacar:

- Pseudonimização e criptografia de dados pessoais;
- Capacidade de manter a confidencialidade, a integridade, a disponibilidade e a resiliência dos sistemas e serviços de tratamento de dados;
- Restabelecimento da disponibilidade e acesso aos dados pessoais em caso de um incidente técnico ou físico;
- Realização regular de testes e avaliações em relação à efetividade das medidas técnicas e organizacionais para garantir a segurança do tratamento dos dados.

Proteção da informação não é algo que pode ser alcançado só com tecnologia.

Exige uma abordagem integrada e sistemática.

Respondendo a uma Violação de Dados

Mais cedo ou mais tarde, toda organização sofre uma violação de dados.

A questão não é “se”, mas “quando” a brecha vai ocorrer.

Quando existe uma violação de dados, você precisa ter um mecanismo implantado que permita responder de forma rápida e efetiva.

Gerenciamento de Incidente é um processo que visa minimizar o impacto de uma violação. Implica no reconhecimento de que um incidente aconteceu, na resposta às preocupações em curto e longo prazos, e no rastreamento do incidente para garantir que ações sejam efetivas.

Eventos e Incidentes

Evento de segurança da informação:
É uma ocorrência que indica uma possível violação da política da segurança da informação ou falha dos controles; ou uma situação previamente desconhecida, que possa ser relevante para a Segurança da Informação.

Incidente de Segurança da Informação:
É um evento único ou uma série de eventos de segurança da informação que têm probabilidade significativa de comprometer as operações de negócios e ameaçar a Segurança da Informação.

Gerenciamento de Incidente:
Deve deixar claro como distinguir entre um evento e um incidente, e deveria também garantir que os eventos sejam avaliados de forma apropriada para confirmar se configuram ou não um incidente.

Formas de Incidentes

Incidentes de segurança da informação podem aparecer em muitas formas, de interrupções físicas a intrusões eletrônicas.

Um incidente que impede acesso aos dados pessoais, significa que você não pode dar suporte ao direito que os titulares de dados têm de acessar ou de corrigir seus dados.

Incidentes representam o resultado de uma ameaça que explora com sucesso uma vulnerabilidade.

Sua avaliação de risco deve oferecer uma boa ideia da variedade de incidentes possíveis na sua organização.

Planos de resposta a incidentes

Processos e procedimentos de respostas incidentes cibernéticos aparecem em várias práticas e frameworks, muitos dos quais são excelentes ferramentas para a conformidade com o GDPR.

Uma das referências é um processo de gerenciamento de incidente desenvolvido pela **CREST.**

O modelo proposto tem três fases:

- **Preparar**: trata de conduzir uma avaliação de criticidade para sua organização e executar uma análise das ameaças, com cenários realistas;
- **Responder**: identificar os incidentes e investigar dentro dos seus objetivos de resposta, e daí tomar as ações necessárias para recuperar seus sistemas, dados e conectividade;
- **Follow-up**: dar prosseguimento investigando o incidente com mais detalhe, comunicar as partes interessadas relevantes e proceder em uma revisão para lições aprendidas e melhoria de informações, processos e controles.

Considere também as boas práticas de gerenciamento de incidente dos frameworks de gestão de serviço com o ITIL.

Papéis no Gerenciamento de Incidente

Apoio do nível mais alto de gestão para garantir os recursos necessários e que as pessoas compreendam que os processos envolvidos na preparação para incidentes, incluindo as medidas preventivas, fazem todo o sentido.

As pessoas que vão implementar qualquer medida preventiva precisam comprar a ideia, junto com aquelas que vão trabalhar com essas medidas.

Todos na organização devem entender suas obrigações de reporte e notificação.

Designação de um gerente para o processo de gerenciamento de incidente. Deve ser uma pessoa identificada com autoridade e responsabilidade.

Notificação da Autoridade Supervisora

O Controlador de Dados deve notificar a Autoridade Supervisora sobre uma violação o mais breve, sem demora injustificada, quando possível em até 72 horas depois, após o Controlador ficar ciente da ocorrência da violação.

A notificação precisa incluir várias informações específicas:

- Natureza da violação dos dados pessoais, incluindo as categorias e número aproximado de titulares de dados afetados, e as categorias e número aproximado de registros de dados pessoais;
- Nome e detalhes de contato do DPO ou outro contato para informações adicionais;
- Prováveis consequências da violação de dados pessoais;
- Medidas tomadas ou propostas para tratar a violação de dados pessoais, incluindo medidas para mitigar possíveis efeitos adversos.

Notificação dos Titulares de Dados

O Regulamento também exige que você notifique os titulares de dados se “For provável que a violação dos dados pessoais resulte em um alto risco aos direitos e liberdades dos titulares de dados”.

As notificações de violação devem ser feitas aos titulares de dados “em linguagem clara e simples” e com “Cooperação estreita com a Autoridade Supervisora”. E devem incluir:

- Nome e detalhes de contato do DPO ou outro contato para informações adicionais;
- Prováveis consequências da violação de dados pessoais;
- Medidas tomadas ou propostas para tratar a violação de dados pessoais, incluindo medidas para mitigar possíveis efeitos adversos.

Exceções para Notificação dos Titulares de Dados

- Se o Controlador de Dados implementou medidas, como criptografia por exemplo, significando que os dados não podem ser lidos por pessoas não autorizadas;
- Se o Controlador tomou ações para garantir que o alto risco não tem mais probabilidade de se materializar;
- Se a notificação para as pessoas afetadas poderia envolver um esforço desproporcional. Neste caso, o Controlador de Dados vai precisar fazer um comunicado público para informar os titulares de dados de uma “Forma igualmente efetiva”.

Considerações finais

A violação de dados pessoais é um incidente preocupante e que pode trazer consequências graves ao direito fundamental à proteção de dados pessoais, tais como o uso indevido dos dados, fraude, danos materiais e comprometimento da reputação dos indivíduos.

É de fundamental importância que os papéis envolvidos no tratamento de dados – seja como processador, seja como controlador – tenham agilidade e observem o GDPR em caso de violação de dados pessoais.

A Autoridade Supervisora deve ser informada o quanto antes e deve receber o maior número de informações possíveis sobre o ocorrido.

É fundamental que os Controladores e Processadores:

- Realizem um diagnóstico para verificar se o GDPR é aplicável ao processamento de dados;
- Em caso positivo, eles devem observar atentamente e respeitar suas normas, princípios e padrões (inclusive os referentes à segurança dos dados), adotar controles e medidas eficazes relacionadas à proteção de informações e cumprir com o dever de notificar e comunicar em caso de violação dos dados pessoais.


pmg
academy