PDPF

Foundation

Curso Preparatório Para o Exame de Certificação

PDPF - EXIN Privacy and Data Protection Foundation

www.pmgacademy.com

Design: By Freepik & Flaticon.com

Módulo 01

Fundamentos da Privacidade

Boas-vindas!

GDPR e LGPD

Mas... Será que uma lei europeia é importante para você, que vive e trabalha aqui no Brasil?

- **Neste mundo globalizado, vai ser raro você não fazer negócios com empresas da UE.**

- **A nossa lei LGPD nasceu com base na GDPR.**

- Visa atestar o conhecimento sobre proteção de dados pessoais, e visa também uma compreensão das regras e regulamentos da União Europeia (UE) se tratando de proteção de dados.

- GDPR - General Data Protection Regulation, ou em português, Regulamento Geral de Proteção de Dados.

- No Brasil, tivemos a aprovação da Lei Geral de Proteção de Dados (LGPD) como consequência da GDPR da união europeia.

Sobre o Exame

Tipo de exame:	Questões de múltipla escolha
Número de questões:	40
Marca de Aprovação:	65% (28 questões)
Não pode usar livro ou fazer anotações	
Não será permitido equipamentos eletrônicos	
Duração do exame:	60 minutos

Objetivos do Módulo

- Definir corretamente o termo privacidade, relacionar privacidade a dados pessoais e proteção dos dados e vai descrever o contexto da legislação da União e do Estado-Membro.

- Definir dados pessoais de acordo com o GDPR distinguir dados pessoais e categorias especiais de dados, como dados pessoais sensíveis.

- Descrever os direitos do titular dos dados com relação aos dados pessoais, definirá processamento de dados pessoais que se enquadre no escopo do GDPR, listar os papéis, responsabilidades e partes interessadas conforme o GDPR.

- Listar os seis fundamentos legítimos para processamento, descrever o conceito e a limitação de finalidade e descrever proporcionalidade e subsidiariedade.

Objetivos do Módulo

- Descrever os requisitos para processamento legítimo de dados, descrever a finalidade do processamento de dados e explicar os princípios relacionados ao processamento de dados pessoais.
- Entender sobre os direitos relacionados à portabilidade de dados e direito de inspeção e vai saber descrever o direito ao esquecimento.
- Descrever o conceito de violação de dados pessoais, vai saber explicar os procedimentos sobre como agir quando ocorre uma violação de dados pessoais.
- Listar as partes interessadas relevantes que devem ser informadas no caso de uma violação de dados pessoais.

Por Que Proteção e Privacidade São Assuntos Tão Importantes?

Não é só porque agora existe uma regulamentação rigorosa da União Europeia não, mas porque essa imensa massa de dados está criando diversos desafios na segurança da informação, principalmente quando se trata de dados pessoais.

Qualquer empresa que processa dados pessoais de pessoas que moram ou apenas visitem um dos Estados-Membros da Área Econômica Europeia (AEE) devem cumprir com o GDPR. Isso mesmo, até as organizações que não fazem parte da AEE, mas que fazem negócios Europa devem aderir ao regulamento GDPR.

O GDPR poderá te prevenir de pagar multas e com certeza vai aumentar a confiança de seus clientes.

HERANÇA DAS REGULAMENTAÇÕES E LEIS

PRIVACIDADE

DUDH

PRIVACIDADE

Carta da UE

PROTEÇÃO DE DADOS

Directive/46/CE
Regulamento 2016/679

Cronologia

1948 - foi assinado a Declaração Universal dos Direitos Humanos DUDH (UHDR)

1950 - Convenção Europeia sobre Direitos Humanos CEDH (ECHR)

1981 - Convenção para Proteção de Indivíduos relativamente ao Processamento Automático de Dados Pessoais, ou Tratado de Estrasburgo

1995 - Diretiva 95/46/CE relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, conhecida como a Diretiva de Privacidade, que foi válida até 25/5/2018.

2002 - Carta dos Direitos Fundamentais da União Europeia CEDH

2016 - Regulamento Geral de Proteção de Dados.

2016 - Diretiva 2016/680 (cooperação judiciário e polícia para assuntos criminais)

2016 - Diretiva 2016/681 (sobre o uso de dados de registro de nome de passageiros - PNR

Cronologia

"Diretiva de Proteção de Dados" 95/46/EC.

Carta dos Direitos Fundamentais da União Europeia

ARTIGO 7: RESPEITO À VIDA PRIVADA E FAMILIAR

1. Toda pessoa tem o direito à sua vida privada e familiar, sua casa e sua correspondência.

ARTIGO 8: PROTEÇÃO DE DADOS PESSOAIS

1. Toda pessoa tem direito à proteção dos dados pessoais que lhe digam respeito.
2. Esses dados devem ser tratados de forma justa para fins específicos e com base no consentimento da pessoa em causa ou em qualquer outra base legítima estabelecida por lei. Todos têm o direito de acessar os dados coletados sobre ele e o direito de retificá-los.
3. O cumprimento destas regras está sujeito ao controle de uma autoridade independente.

Legislações Relacionadas da UE.

Constituição

Código Civil

Lei policial

Lei de imposto

Arquivos e registros de ato

Lei das telecomunicações

- Ao contrário de uma diretiva que deve ser assimilada dentro da legislação nacional de cada Estado-Membro, uma Regulação é vinculante e diretamente aplicável a todos os Estados-Membros. O GDPR é "Texto com Relevância EEE", o que significa que se aplica a todos os países do Espaço Econômico Europeu (EEE) ou da Área Econômica Europeia (AEE), composto por todos os Estados-Membros da UE, Islândia, Liechtenstein e Noruega.

CONSIDERAÇÕES, EXPLICAÇÕES OU PREÂMBULOS

- **Artigo 8 (1) da Carta dos Direitos Fundamentais da União Europeia (a 'Carta')** - proteção das pessoas físicas em relação ao tratamento de dados pessoais é um direito fundamental.

- **Artigo 16 (1) do Tratado sobre o Funcionamento da União Europeia (TFUE)** prevê que toda pessoa tem direito à proteção dos dados pessoais que lhe digam respeito.

Os princípios e regras relativos à proteção das pessoas físicas em relação ao tratamento dos seus dados pessoais devem, qualquer que seja a sua nacionalidade ou residência, respeitar os seus direitos e liberdades fundamentais, nomeadamente o direito à proteção de dados pessoais.

Privacidade e Proteção de Dados

Tratado sobre o Funcionamento da Europa ('Tratado de Roma de 1957') :

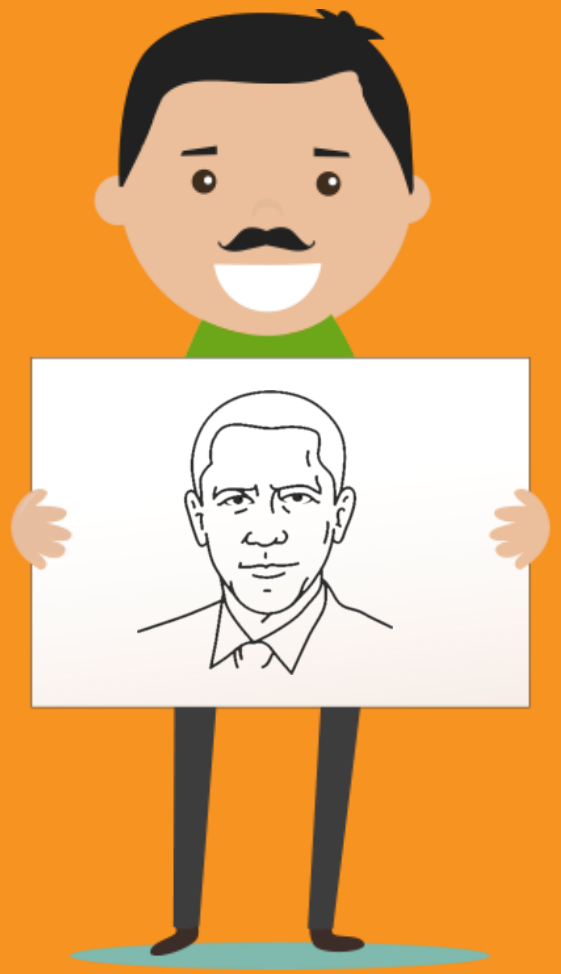
"Toda pessoa tem direito à proteção dos dados pessoais que lhes dizem respeito."

Carta dos Direitos Fundamentais da União Europeia (2000):

"Toda pessoa tem direito à proteção dos dados pessoais que lhe dizem respeito.". São iguais!

- **PRIVACIDADE** é definida como o direito a respeitar a vida privada e familiar de uma pessoa, sua casa e correspondência.
- **PROTEÇÃO DE DADOS** diz respeito à proteção de dados pessoais, não de todos os dados.

Dados Pessoais



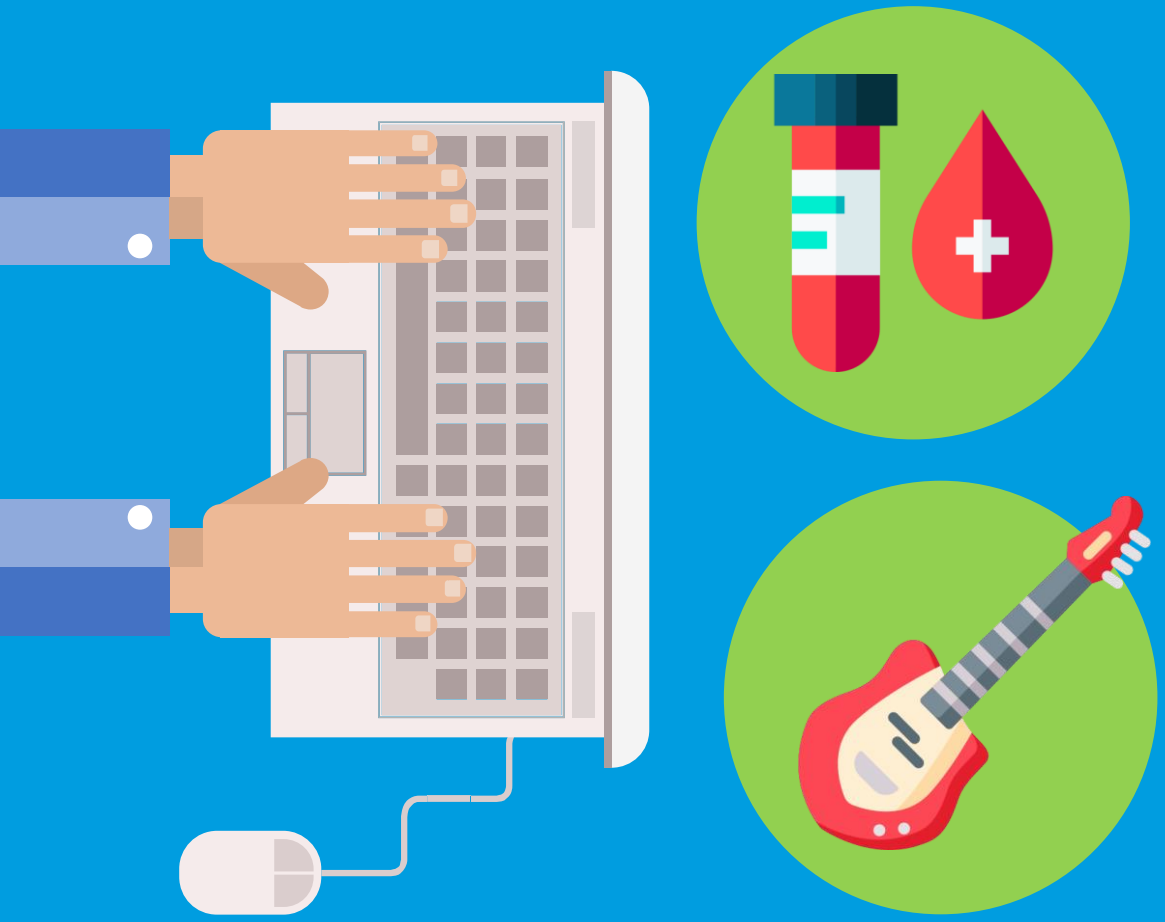
Barak Obama é havaiano, foi o 44.º presidente dos Estados Unidos. Casado com Michelle Obama, desde 1992. Coleciona gibis do Homem Aranha. Sancionou uma lei que passou a considerar os crimes motivados por identidade de gênero ou orientação sexual. Joga basquete pra caramba e é viciado em cigarros.

“Titular dos dados”

É identificado como uma pessoa física, que pode ser identificado, direta ou indiretamente com um identificador, tal como um nome, um número de identificação, dados de localização, um identificador on-line, como o IP, ou ainda como algo mais específicos da sua identidade física, fisiolologia, genética, mental, econômica, cultural ou social.

Definição de Dados Pessoais

Um dado de qualquer informação relacionada a uma pessoa física identificada ou identificável, ou seja, de um "titular dos dados".



- Para que as informações sejam "dados pessoais", elas não precisam ser verdadeiras ou comprovadas. Mentiras ou dados incorretos sobre uma pessoa ainda são dados pessoais.
- O conceito de dados pessoais inclui informações disponíveis em qualquer forma: texto, figuras, gráficos, fotografias, vídeo, acústico ou qualquer outra forma possível.
- E quando falamos de Pessoa Natural, estamos nos referindo legalmente a um ser humano, um indivíduo capaz de assumir obrigações e de ter direitos. Portanto, o GDPR não se aplica a pessoas falecidas (ver item 27).

Exemplos de Privacidade e Proteção de Dados

DADOS PESSOAIS

PRIVACIDADE

Proteção de Dados

ACEITAR

RECUSAR

Tipos de Dados Pessoais

Dados Pessoais Direto

Quando você lê em um blog: “O fundador da Microsoft faliu”. Isso é um dado direto, ou seja, é de uma pessoa conhecida, no caso sabemos que a referência é direta ao Bill Gates.

Dados Indiretos

São aqueles dados que não podem ser atribuídos a um objeto sem a utilização de informação adicional..

Dados Pseudonimizados

Significa o processamento de dados pessoais de forma que não possam mais ser atribuídos a um titular de dados específico sem o uso de informações adicionais.

Pseudo significa mentira, coisa falsa. Anonimização significa que nenhuma informação da qual a pessoa, a quem os dados se relacionam, pode ser identificada. De qualquer forma dados de uma mensagem anônima ou os dados de uma pessoa anônima NÃO são considerados dados pessoais.

Dados Pessoais Especiais

Artigo 9 do GDPR

Os dados pessoais especiais se diferenciam de outras categorias de dados pessoais, por serem mais sensíveis.

- dados que revelam origem racial ou étnica
- dados que revelam opiniões políticas
- dados que revelam crenças religiosas ou filosóficas
- dados que revelam adesão sindical
- dados genéticos
- dados biométricos processados com a finalidade de identificar unicamente uma pessoa natural
- dados relativos à saúde
- dados relativos à vida sexual ou orientação sexual de uma pessoa natural

Controlador dos Dados

O responsável pelo tratamento ou o responsável por definir os critérios específicos para a sua nomeação, poderá ser previsto pela legislação da União ou do Estado-Membro, mas geralmente, são as entidades "públicas" que os próprios titulares ou donos dos dados que fornecem suas informações escolhem.

Processamento de Dados

Processadores de dados

- Em muitos casos, o controlador de dados e o processador de dados serão a mesma entidade.

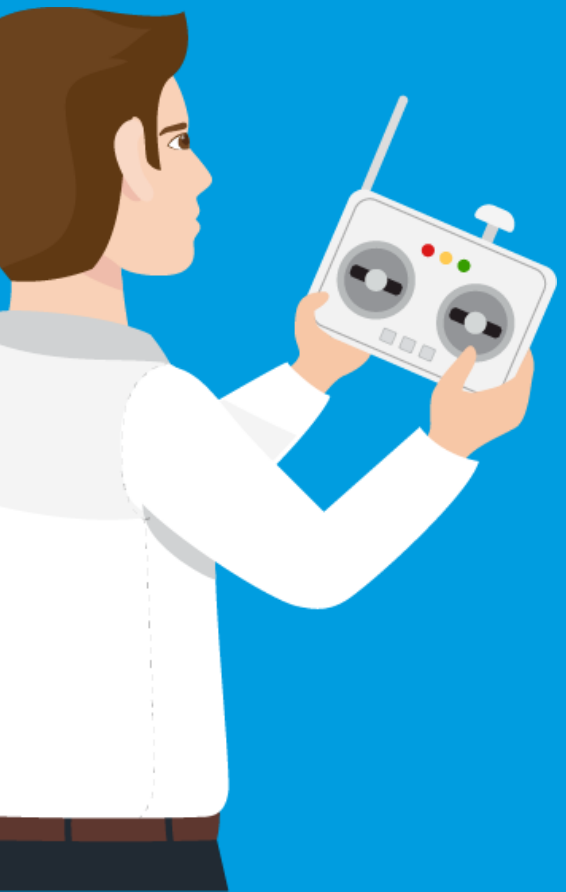
- Só lembrando que um único controlador de dados pode ter vários processadores de dados.

- **Processar é toda operação que envolve algum tipo de manuseio de dados pessoais, seja ela a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, edição, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.**

- O termo correto na LGPD brasileira é **TRATAMENTO DE DADOS** e não processamento de dados.

Controlador e Processador de Dados

- O **CONTROLADOR** define os meios de como será tratado os dados pessoais. No exemplo do Hospital, é ele que será responsável por definir quais serão as medidas técnicas de proteção, conforme o GDPR dos dados cadastrados, coletados, armazenados, etc., do formulário online dos pacientes.

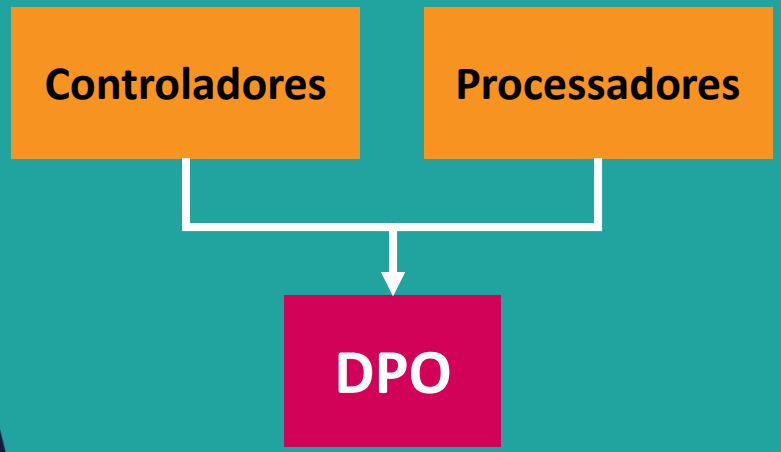


- O **PROCESSADOR DE DADOS**, que em muitos casos, acaba sendo a mesma entidade do controlador de dados.

De qualquer forma, basta lembrar que o processador de dados processa os dados conforme regras estipuladas pelo Hospital, ou seja, pelo controlador.

Necessidade de um Data Protection Officer (DPO)

1. Se os dados forem tratados por uma autoridade ou organismo público, exceto órgãos do Estado, como aqueles que atuam com ordens judiciais.
2. Se o processamento requer um monitoramento regular, sistemático e em grande escala dos dados dos titulares.
3. Se as atividades do controlador ou processador consistirem em processar grandes quantidades de categorias especiais de dados e dados pessoais relacionados a condenações e ofensas criminais.



Um **DPO**, segundo o artigo 9.º, n.º 6, pode ser contratado sob um contrato de prestação de serviço onde tal empresa ofereça este tipo de serviços. Semelhante com o que ocorre com o serviço de contabilidade, ou seja, se tiver verba, contrata um contador, caso contrário, um escritório de contabilidade.

Responsabilidades de um Data Protection Officer (DPO)

- Precisam ser mais do que especialistas em direito - eles precisam de uma mistura de qualificações que lhes permitam lidar, efetivamente, tanto com os requisitos legais, quanto com as operacionais.

- Deve se reportar diretamente à alta gerência para ajudar a garantir que a proteção de dados continue sendo uma preocupação importante para o conselho e para os gerentes seniores.

- O DPO deve oferecer aconselhamento e monitorar os DPIAs (Avaliação de Impacto sobre a Proteção de Dados).

- O DPO será o contato imediato com a autoridade supervisora. Portanto, seus detalhes de contato devem ser incluídos em vários relatórios e publicados pelo controlador de dados ou processador de dados.

Destinatário e Terceiros

Se os dados forem disponibilizados para autoridades públicas, cujo processo de inquérito esteja rolando, eles não serão considerados destinatários, porque inicialmente não eram os destinatários.

Leitores que costumam ver este conteúdo serão os **DESTINATÁRIOS** dos dados processados.

O processamento desses dados por essas autoridades públicas deve estar em conformidade com as regras de proteção de dados.

EX.: Pesquisa salarial publicada em um site da UE

O **TERCEIRO** é aquele que não tem interesse ou autorização para processar os dados, mas acabou vendo os dados. EX.: Alguém que vê a folha de pagamento dos funcionários largada em uma impressora. Ou aquele que acessar inadvertidamente esses mesmos dados, sem autorização, é considerado terceiros também.

ISO/IEC 27001 e GDPR

“medidas técnicas e organizacionais apropriadas para garantir e poder demonstrar que o processamento é realizado de acordo com o regulamento”.

Com base na abordagem de risco da norma ISO 27001, é possível implementar controles técnicos e organizacionais apropriados para:

- Garantir a confidencialidade, integridade, disponibilidade e resiliência contínuas dos sistemas e serviços de processamento;
- Garantir a segurança dos dados pessoais; e
- Garanta a capacidade de restaurar a disponibilidade após um incidente.

Processamento de Dados Pessoais

5° do GDPR

- São descritos os princípios relacionados ao processamento de dados pessoais desde a sua criação até a minimização dos dados. Ele nos ajuda bastante porque até institui um ciclo de vida dos dados.

- Quais os princípios e limites que o tratamento de dados pessoais deve seguir, de maneira que a licitude, a lealdade, a transparência, a finalidade, o limite, a proporcionalidade, a exatidão, a integridade e a confidencialidade são algumas das principais características que o tratamento de dados deve seguir.

- O artigo trata dos princípios porque eles serão expressos, depois, nas notificações da Autoridade Fiscalizadora, quando houver algum tipo de denúncia ou autuação.

Princípios no Processamento de Dados

Legalidade, justiça e transparência

Limitação de finalidade

Minimização de dados

Exatidão ou Precisão

Limitação de Armazenamento

Integridade e Confidencialidade

Prestação de Contas

Motivos Legítimos e Limitação de Finalidade

- **Artigo 6 -** é necessário o consentimento, geralmente quando esta permissão gira em torno de requisitos legais, como a conformidade com outra lei ou em conformidade com algo que visa proteger os direitos de um titular de dados, ou ainda onde o consentimento do titular de dados é fornecido através de um contrato que eles têm com terceiros.

- Os controladores são responsáveis por garantir que os dados pessoais sejam processados de forma legal, justa e transparente.

- Este artigo esclarece que o titular dos dados deve ter garantias que, a partir do seu consentimento, seus dados serão processados apenas para determinadas tarefas da qual consentiu.

Limitação de Finalidade e Especificação de Finalidade

GDPR - “Dados pessoais sejam recolhidos para fins específicos, explícitos e legítimos”.

https://www.pmgacademy.com/termos-de-uso/

https://www.pmgacademy.com/politica-de-privacidade/

Proporcionalidade e Subsidiariedade

SUBSIDIARIEDADE

- Apoio, colaboração, e no contexto da UE, ele é tratado como um princípio. Este princípio visa a descentralização do poder. E isso acontece através da intervenção da União Europeia. Então, algumas decisões são tomadas, primeiramente, a nível político de seus países membros, e depois sim, da UE.

- Significa que os dados pessoais só podem ser processados se não existir outra forma.

PROPORCIONALIDADE

- Significa que não podemos coletar mais informações do que o estritamente necessário.

Direitos dos Titulares dos Dados

Segundo o GDPR, é proibido processar quaisquer dados pessoais.

- Vai coletar informação de seu cliente, avise-o.
- Vai processar seus dados, informe como será feito.
- O silêncio ou a omissão não são considerados formas de consentimento.
- O titular dos dados pessoais tem a liberdade de escolha ante o consentimento, sendo que a sua recusa ou revogação não lhe causem nenhum prejuízo.

Então a ordem do dia é, garanta que essas pessoas ou usuários tenham ciência de que devem consentir o uso dos dados, e tenham o direito de saber qual a finalidade da coleta e acesso ao seu conteúdo, seja agora ou no futuro. É essencial assegurar a liberdade e a privacidade do titular dos dados.

Transparência

- Deve ser transparente no processamento de dados. Você deve deixar claro a exposição dos dados e o fácil acesso relativo à finalidade do processamento.
- Deve ainda mostrar ao titular a forma, duração, além das informações acerca dos agentes que realizam o processamento dos dados.
- Não cobre do titular pela consulta dessas informações, assim como informações de como são processados os dados.
- Somente os dados reais e estritamente necessários devem ser coletados, já que temos que buscar sempre garantir o direito a proteção à privacidade do titular, da mesma forma, que uma autoridade governamental deve garantir a proteção e transparência.
- Os dados anonimizados não são considerados dados pessoais, então, é importante que o método escolhido pelo processo de anonimização demonstre a impossibilidade de reversão dos dados que foram classificados como anônimos.

Direto de Acesso (Inspeção) pelo Titular dos Dados

O **TITULAR DOS DADOS** tem o direito de livre acesso às informações relativas ao processamento de seus dados, porque ele quer garantias que seus dados sejam tratados de forma segura e que estejam cumprindo com a sua finalidade. Da mesma forma, ele quer ter a liberdade de revogar o consentimento e requerer a eliminação de seus dados, por isso que é importante não só deixar claro no site o consentimento, mas o processo de revogação também.

Direito de retificação

Direito a ser esquecido

EX.: Imagine que você queira alterar as informações profissionais do seu perfil pessoal no **LinkedIn**, talvez queira inserir o seu certificado de aprovação no exame internacional do PDPF, queira determinar que somente esta informação seja pública, mas, que possibilite também no futuro mudar de opinião e colocar essa informação como restrita ao público.

Retificação e Apagamento

Artigos 16 e 17 do GDPR

- O GDPR assegura que os dados sejam retificados caso o titular detecte alguma inconsistência ou erro em seus dados. Esse direito é conhecido como **“DIREITO DE RETIFICAÇÃO”.**

- O GDPR fala ainda sobre o prazo. Isso quer dizer que o tratamento não deve ser realizado por tempo indeterminado. O término do tratamento de dados deve seguir alguns requisitos básicos, como a finalidade do processo, o término do prazo e a revogação do consentimento do titular, ou seja, depois de um período os dados deverão ser apagados. Esse direito ao apagamento é conhecido como o **“DIREITO AO ESQUECIMENTO”.**

Direito à Limitação do Processamento

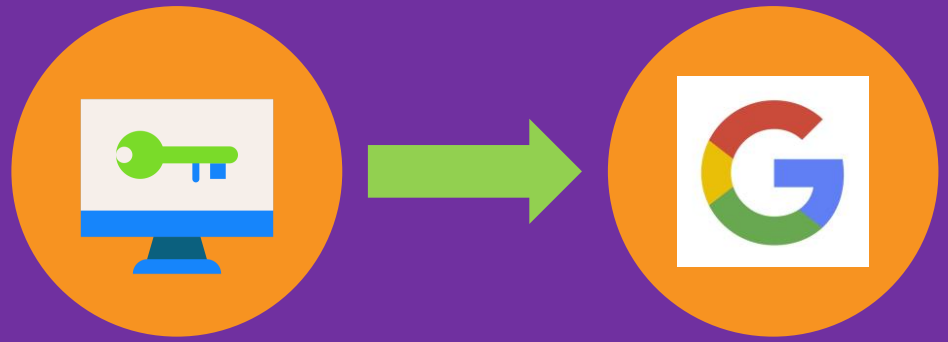
O GDPR não se limita apenas ao prazo, mas foca também na importância da limitação, ou seja, qual a finalidade do processamento e até onde pode se chegar.

Por exemplo, os dados coletados da sua seguradora podem ser processados por um banco ou qualquer outra instituição financeira? Ou vice-versa? Qual seria a real necessidade deste processamento?

Os titulares têm o direito de restringir o processamento de seus próprios dados pessoais quando tiverem um motivo específico. Isso pode ocorrer quando os titulares têm problemas com o conteúdo coletado ou pode restringir devido a forma que você processou seus dados.

Obrigação de Notificação

- **Além de retificar, restringir ou apagar os dados, você, como controlador também tem o dever de tomar "medidas razoáveis" para informar outros controladores de que o titular dos dados**



O **Artigo 19** do **GDPR** cria uma espécie de cadeia de avisos e deveres de notificação quando os dados foram transferidos para outras partes. Isso se aplica a todo o processo de big data. As regras adicionais do artigo 19 do regulamento exigem que o responsável pelo processamento notifique os destinatários dos dados a serem apagados e informe também o titular dos dados sobre esses destinatários.

Direito à Portabilidade dos Dados

- Foi projetada principalmente para aqueles que criam perfis sociais e interage com empresas online, já que aos titulares tem o direito de **“receber os dados pessoais a seu respeito, que ele forneceu a um controlador”** e o direito de **“transmitir esses dados para outro controlador sem impedimento do controlador ao qual os dados pessoais foram fornecidos”.**

“Formato estruturado, normalmente utilizado e legível por máquina"

- A interoperabilidade é incentivada, mas os controladores não são obrigados a criar sistemas compatíveis com os de seus (potenciais) concorrentes.

- A portabilidade de dados pode ser usada para mudar para um controlador diferente, mas isso não força automaticamente o controlador inicial remover os dados e parar de processá-los, porém, o titular dos dados poderia combinar sua demanda de portabilidade de dados com uma solicitação de apagamento com base no artigo 17 do GDPR, mas tenha claro que o objetivo dos dados portabilidade não é o apagamento, mas a transferência dos dados pessoais.

Direito de Contestar

- **O titular dos dados ainda terá o direito de se opor ao processamento de seus dados, mesmo se para fins estatísticos.**

Direito de Objetar

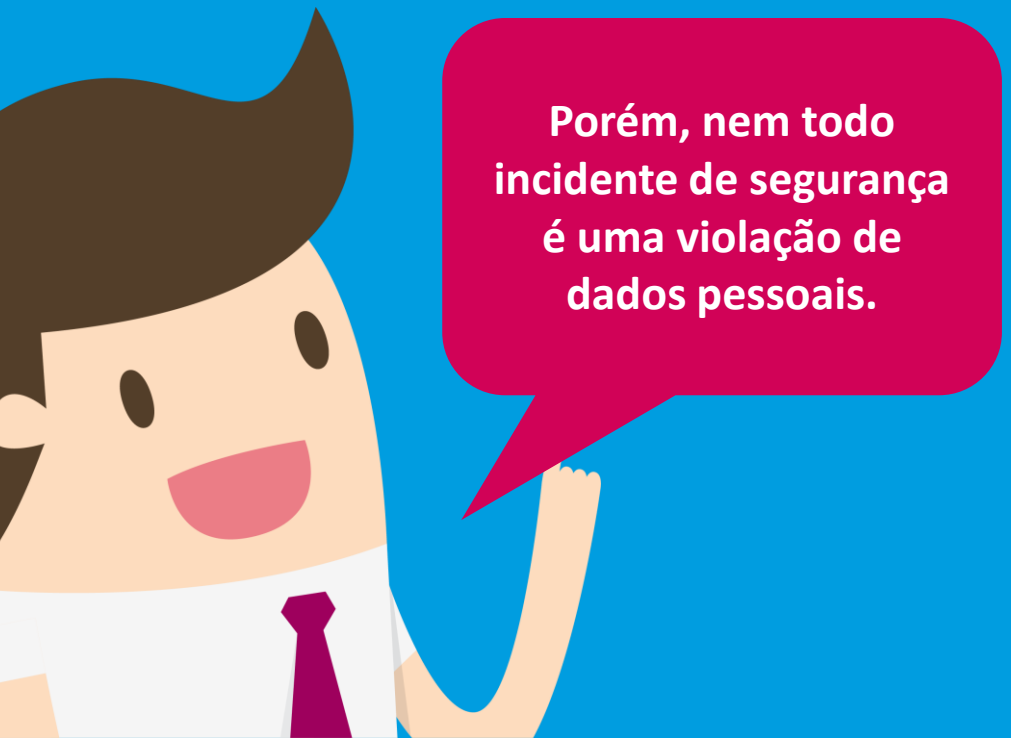
Se o controlador não apresentar motivos convincentes, que não seja do interesse do titular, ou que afete seus direitos e liberdades, o responsável pelo processamento deve atender à solicitação do titular e deixar de processar os dados pessoais.

- Os titulares dos dados têm o direito de obter uma solução judicial eficaz quando as autoridades de supervisão não tratarem de suas reclamações ou não as informarem dentro de três meses sobre o andamento ou o resultado das reclamações. Esse recurso judicial deve ser obtido nos tribunais dos Estados-Membros da UE onde as autoridades de supervisão estão localizadas.

Violação de Dados

INCIDENTE DE SEGURANÇA

Qualquer evento prejudicial, seja ele confirmado ou sob suspeita, que esteja relacionado à segurança de sistemas de informação e que pode levar a algum tipo de perda



VIOLAÇÃO DE DADOS PESSOAIS

Significa uma violação da segurança que leva à destruição acidental ou ilegal, perda, alteração, divulgação não autorizada ou acesso a dados pessoais.

Incidente de segurança que afetou a confidencialidade, integridade ou disponibilidade de dados pessoais.

A VIOLAÇÃO DE DADOS sempre será considerada um INCIDENTE DE SEGURANÇA.

Procedimento de Violação

- **O controlador deve notificar o ocorrido sem demora injustificada e sempre que possível, em até 72 horas após ter conhecimento do ocorrido.**
- **A notificação deve conter pelo menos, uma descrição da natureza da violação, a categoria e quantidade de indivíduos e dados afetados.**
- **No momento da notificação, o controlador indicará o nome e o contato do responsável pela proteção de dados que vai lidar com o evento.**
- **A notificação deve contar com as consequências prováveis da violação e as medidas adotadas para mitigar os possíveis efeitos da violação dos dados pessoais do titular.**

EXCEÇÕES

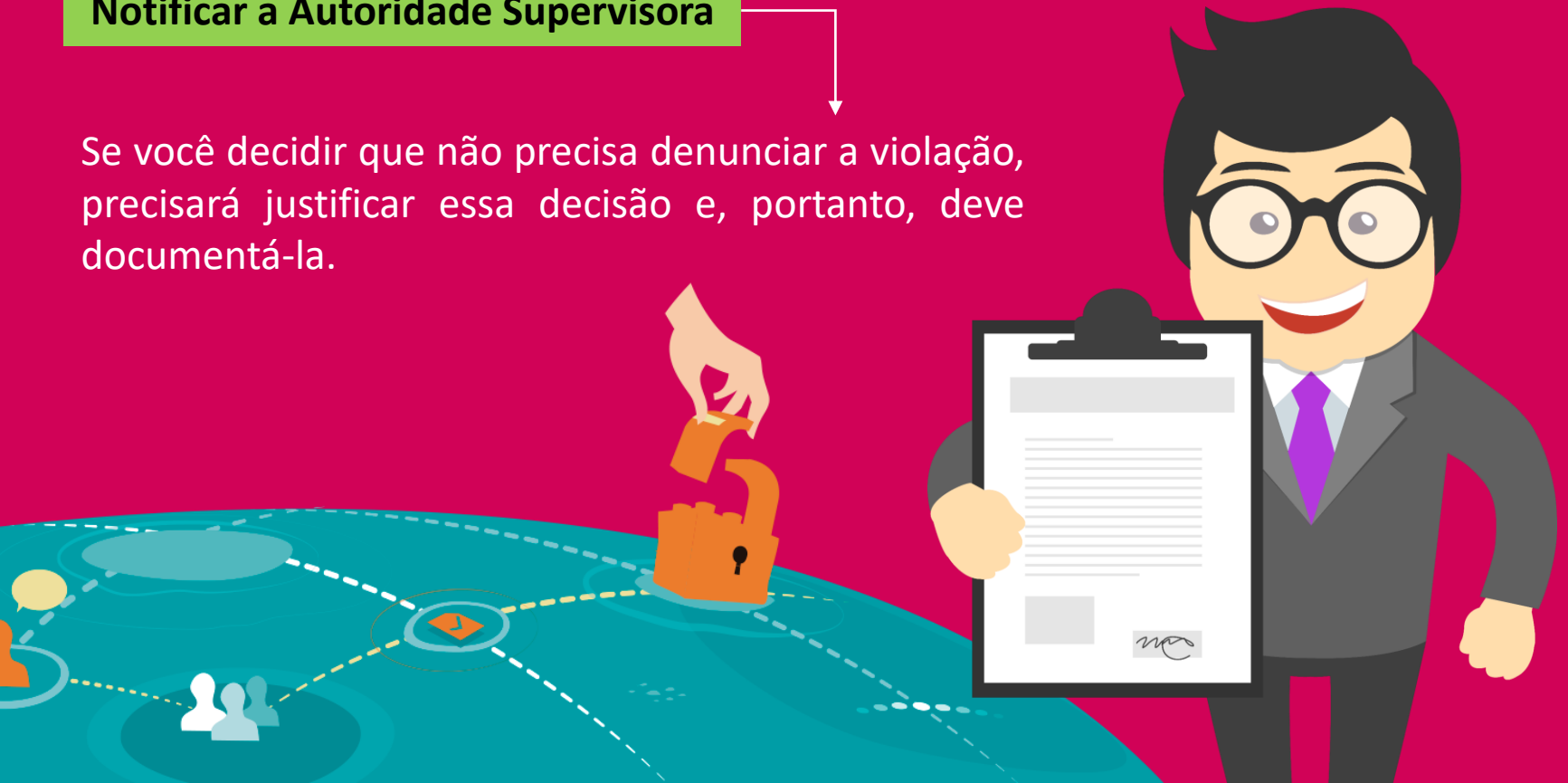
- quando os dados estiverem ilegíveis
- quando outras medidas são tomadas para minimizar o risco
- quando o processo de notificação é um esforço desproporcional.

Notificando uma Violação

Quando uma violação de dados pessoais ocorre, você precisa estabelecer a probabilidade e a gravidade do risco resultante.

Notificar a Autoridade Supervisora

Se você decidir que não precisa denunciar a violação, precisará justificar essa decisão e, portanto, deve documentá-la.



Ao avaliar o risco de direitos e liberdades, é importante focar nas possíveis consequências negativas para os indivíduos afetados. Isso significa que uma violação pode ter uma série de efeitos adversos sobre os afetados, incluindo danos emocionais, físicos e materiais. Você precisa avaliar caso a caso, observando todos os fatores relevantes.

O Papel dos Controladores na Notificação

- Se sua organização usa um processador de dados e esse processador sofre uma violação, ele deve informar assim que possível, logo após tomar conhecimento do ocorrido.

- Se você usa um processador, os requisitos de comunicação de violações devem ser detalhados no contrato entre você e seu processador. O GDPR reconhece que nem sempre será possível investigar uma violação completamente dentro de 72 horas para entender exatamente o que aconteceu e o que precisa ser feito para mitigá-la.

O **ARTIGO** 33 permite que você forneça as informações necessárias em fases, desde que isso seja feito sem demora.

Notificação de uma Violação ao Titular Afetado

- **Se uma violação provavelmente resultar em alto risco para os direitos e liberdades das pessoas, o GDPR diz que você deve informar diretamente as pessoas envolvidas e sem demora injustificada. Em outras palavras, isso deve ocorrer o mais rápido possível.**

'ALTO RISCO'

Significa que você deve informar primeiro as pessoas do que para notificar a à Autoridade Supervisora. Novamente, você precisará avaliar a gravidade do impacto potencial ou real sobre os afetados como resultado de uma violação e a probabilidade de isso ocorrer novamente.

Se você decidir não notificar as pessoas, ainda precisará notificar a Autoridade Supervisora, a menos que possa demonstrar que é improvável que a violação resulte em risco aos direitos e liberdades do titular de dados.

Você chegou ao fim deste módulo. PARABÉNS!

Módulo 02

Organizando a Proteção dos Dados

Proteção de dados para a organização

- Vai aprender os diferentes tipos de administração; indicar quais atividades são necessárias para estar em conformidade com o GDPR; definir a proteção de dados desde a concepção (by design) e por padrão (by default); dar exemplos de violação de dados pessoais; descrever a obrigação de notificação de violação de dados pessoais, conforme estabelecido no GDPR e descrever a execução das regras mediante a emissão de sanções, incluindo multas administrativas.

Autoridade Supervisora

- Saberá descrever as responsabilidades gerais de uma autoridade supervisora, descrever seu papel e responsabilidades em relação à violações de dados pessoais e, por fim, saberá descrever como ela contribui para a aplicação do GDPR.

Cumprindo Com os Requisitos do GDPR

Consentimento do titular na coleta de dados é primordial

Controlador ou processador

Garantir que o titular esteja ciente da finalidade do processamento de seus dados.

Por isso que o GDPR também garante que as empresas tenham a liberdade de utilizar os dados de maneira transparente e ética em troca de um serviço ou acesso.

Estrutura Legal

- O GDPR pretende oferecer as pessoas mais controle sobre como seus dados pessoais serão utilizados, e também, fornece às empresas uma estrutura legal clara e padronizada em toda a UE.

- O regulamento se aplica a TODAS as organizações que coletam e processam dados pessoais de indivíduos residentes na UE, independentemente da localização física da empresa.

O GDPR torna contratos escritos entre CONTROLADORES e PROCESSADORES um requisito.

- Os contratos entre controladores e processadores garantem que ambos compreendam suas obrigações, responsabilidades e responsabilidades.

- Os contratos também os ajudam a cumprir o GDPR e auxiliam os controladores a demonstrar aos indivíduos e reguladores sua conformidade, conforme exigido pelo princípio da responsabilidade.

Avaliações de Impacto na Proteção de Dados

DPIA (Avaliações de Impacto na Proteção de Dados)

É uma maneira de analisar sistematicamente e de forma abrangente o processamento de dados além de ajudar a identificar e minimizar os riscos da proteção de dados.

O processo de DPIA, pode ajudar a identificar e minimizar os riscos de proteção de dados de qualquer outro projeto importante que exija o processamento de dados pessoais.

O DPIA deve descrever a natureza, escopo, contexto e objetivos do processamento, assim, como avaliar a necessidade, proporcionalidade e medidas de conformidade.

Se você identificar um alto risco que não pode mitigar, deverá consultar a Autoridade Supervisora antes de iniciar o processamento, mas lembre-se, essa obrigatoriedade é apenas para situações onde o DPIA indicou um alto risco para a privacidade ou direitos e liberdades das pessoas

Registros Detalhados

As empresas que processam dados precisarão registrar os detalhes do que estão fazendo com os dados.

1. Os detalhes da sua organização e os detalhes de contato do seu responsável pela proteção de dados. Além disso, se sua empresa não estiver na UE, você deverá fornecer detalhes do seu representante designado na EU.

2. Uma descrição das medidas de segurança que você possui para proteger os dados. Isso inclui medidas de segurança técnica, como criptografia e segurança organizacional, por exemplo, restrições internas sobre quem tem acesso a quais partes da rede

3. Para transferências de dados para fora do EEA, as organizações precisarão documentar para onde os dados estão sendo transferidos. e as salvaguardas em vigor para proteger esses dados.

Registro do Controlador

- Determinar o objetivo do processamento de dados.
- Registrar os tipos de pessoas com os quais você está trabalhando e os tipos de dados também, que inevitavelmente diferem dependendo da natureza da sua empresa.
- Registrar os tipos de destinatários para os quais estará divulgando dados.
- Documentar por quanto tempo você planeja manter cada categoria de dados antes de serem apagados.

Registro do Processador

- **Os nomes e detalhes de contato do controlador para quem você está processando dados.**

- **Os detalhes do DPO do controlador (se eles tiverem um) e seu representante se eles não estiverem na UE.**

Agência de Marketing

Se sua organização é pequena, com menos de 250 pessoas, existe uma exceção no regulamento. Você não é obrigado a manter registros de todas as atividades de processamento, caso o processamento não cause algum risco para os direitos e liberdades dos titulares de dados, o processamento não seja ocasional ou o processamento inclui categorias especiais de dados ou dados pessoais relativos a condenações e infrações penais.

Desafios nos Registros

- Realize um inventário de análise dos dados que processa. O conhecimento dos dados que você processa o ajudará a identificar as lacunas no seu programa de conformidade com o GDPR e abrirá o caminho para a conformidade com muitos dos requisitos do GDPR.

- Você deve ter um registro de todo o processamento de dados, independentemente de os dados estarem no formato escrito ou eletrônico e estar disponível para a autoridade supervisora local quando necessário.

Registro de Violações de Dados Pessoais

Incidente de Segurança — **CONFIDENCIALIDADE** — **INTEGRIDADE** → **DISPONIBILIDADE**

- Você precisa estabelecer a probabilidade e a gravidade do risco resultante para os direitos e liberdades das pessoas. Se é provável que exista um risco, você deve notificar a Entidade Supervisora. Porém, se for improvável, não será necessário. No entanto, se você decidir que não precisa denunciar a violação, precisará justificar essa decisão e, portanto, deve documentá-la.

- No geral, você deve garantir a existência de procedimentos robustos de detecção de violações, investigação e relatórios internos. Isso facilitará a tomada de decisões sobre se você precisa ou não notificar a autoridade supervisora e as pessoas afetadas.

- Você também deve manter um registro de qualquer violação de dados pessoais, independentemente de ser ou não obrigado notificar.

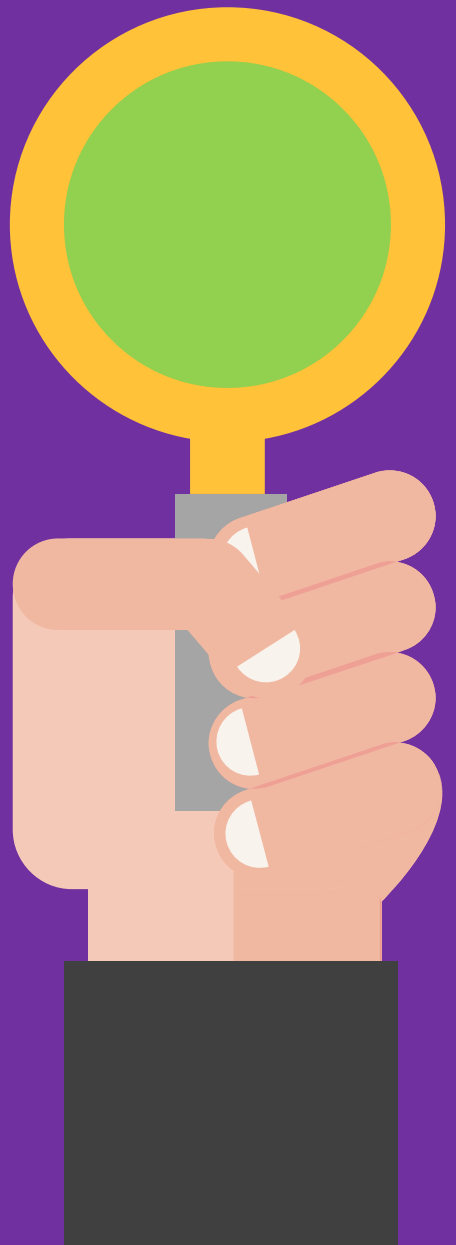
Autoridades Supervisoras

Também comumente chamadas de **DPAs – Data Privacy Authority (Autoridade de Proteção de Dados)** é autoridade pública independente criada por um Estado-Membro nos termos do artigo 51 do GDPR.

- As autoridades supervisoras também podem fornecer consultoria especializada em questões de proteção de dados e lidar com reclamações apresentadas contra violações do GDPR s e das leis nacionais. Existe um DPA em cada Estado-Membro da UE.

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

DPA no Estado-Membro da UE em que sua empresa está sediada.



Responsabilidades das Autoridades Supervisoras

- Aconselhar as empresas sobre o GDPR
- Realizar auditorias sobre conformidade com o GDPR
- Abordar reclamações dos titulares dos dados e
- Emitir multas quando as empresas deliberadamente não estiverem cumprindo o GDPR.

AUTORIDADE DE PROTEÇÃO DE DADOS

Embora uma Autoridade Supervisora seja responsável dentro de um país, as empresas que operam em vários países podem optar por nomear uma Autoridade Supervisora Líder para fins de geração de relatórios.

Tarefas de Uma Autoridade Supervisora

- Controlar e executar o próprio GDPR, pois assim cria-se legitimidade.
- Aconselhar de forma preventiva em relação à defesa dos direitos e liberdades das pessoas quanto ao processamento de dados.
- Incentivar a elaboração de códigos de conduta, incentivar o estabelecimento de procedimentos de certificação de proteção de dados, e de selos e marcas de proteção de dados, assim como fazer uma revisão periódica dessas certificações emitidas.
- Publicar os critérios de acreditação e conduzir o processo

Mas a Autoridade Supervisora não atende apenas as organizações que processam dados.

Poderes de Uma Autoridade Supervisora

Poder de investigação

- Ela tem o poder de realizar investigações como uma forma de auditorias sobre a proteção de dados, da mesma forma que pode rever as certificações que ela emitiu. E se houver uma violação do GDPR, é a autoridade supervisora que irá notificar o responsável pelo processamento de dados.

Poder de correção

- Por meio de advertências, caso o processamento esteja suscetível a violações, ela pode repreender o responsável pelo processamento...

Poder de ordenar algo

- Ela tem o poder de impor limitações temporárias ou definitivas no processamento de dados, ou até mesmo a sua proibição. Tem ainda o poder de ordenar a deleção, bem como a notificação dessas medidas. Felizmente, ela pode retirar a certificação caso a organização descumpra com o regulamento.

Poder consultivos e de autorização

- Ela presta aconselhamento, emite pareceres e aprovar projetos de códigos de conduta.

Mecanismos de Consistência

É através deste mecanismo que as autoridades supervisoras cooperam entre si e, quando for relevante, com a Comissão.

O mecanismo de consistência entra em ação quando uma autoridade supervisora toma uma decisão que afeta o processamento de dados em vários estados membros e que impactaria substancialmente um número significativo de titulares de dados, ou seja, causando algum efeito legal relacionado às operações de processamento de dados.

AEPD - Autoridade Europeia para a Proteção de Dados ou em inglês: EDPS – European Data Protection Supervisor

"balcão único" ou “One-Stop Shop”.

Cooperação Entre Autoridades

O objetivo repetido do mecanismo de consistência é garantir a "aplicação consistente" do GDPR.

CONSELHO EUROPEU DE PROTEÇÃO DE DADOS

Definido no GDPR como o órgão responsável pelo mecanismo de consistência. Esta é uma escolha óbvia, já que o Conselho é composto pelo chefe de cada autoridade supervisora e da AEPD Autoridade Europeia para a Proteção de Dados ou em inglês: EDPS – European Data Protection Supervisor.

Papéis e Responsabilidades Relacionadas a Violações de Dados Pessoais

Autoridade Supervisora

- Supervisionar os controladores e processadores para ajudá-las a serem exemplares.

E como funciona?

- As controladoras ou processadoras a consultam para aconselhamento através dos seus responsáveis pela proteção de dados (DPOs).

- Ela realiza auditorias de proteção de dados dos controladores e processadores para verificar a conformidade.

Princípio da Responsabilidade

Os controladores e processadores são responsáveis pelo cumprimento das regras de proteção de dados, porém o apoio por parte da Autoridade Supervisora é essencial, pois são eles que fornecerão orientações sobre como estarem em conformidade.

Condições Gerais Para a Imposição de Multas Administrativas

As autoridades supervisoras são responsáveis por garantir que as multas administrativas sejam efetivas e proporcionadas em cada caso individual.

Artigo 84 do GDPR

Aponta que cabe aos Estados-Membros o estabelecimento de regras para a aplicação de sanções, que devem ser efetivas, proporcionais aos danos sofridos e dissuasivas

As multas relacionadas à violação de dados pessoais podem alcançar multas de € 10.000.000 ou 2% do volume de negócios mundial da empresa no ano financeiro anterior, o que for maior; ou multas de € 20.000.000 ou 4% do faturamento mundial da empresa no exercício financeiro anterior, o que for maior.

One-Stop-Shop

One-Stop-Shop - “Balcão Único”: significa que apenas uma Autoridade Supervisora principal lidera as atividades de processamento quando é envolvido cidadãos de mais de um país da EU.

Conselho de Proteção de Dados da UE

- Esse é o mecanismo de **“balcão único”,** que visa reduzir a carga burocrática envolvida no tratamento de questões potencialmente complexas sobre proteção de dados, sobre anonimato e assim por diante.

- Cada estado também determina uma autoridade supervisora principal ou autoridade de proteção de dados, que nomeia um membro do Conselho de Proteção de Dados da EU.

Processamento Transfronteiriço

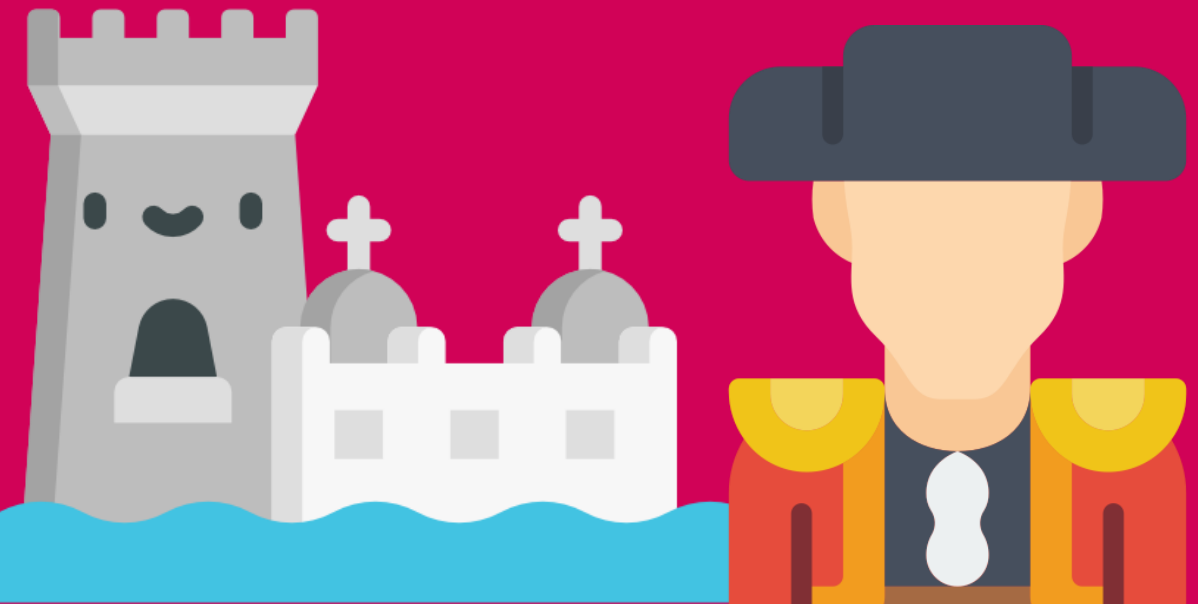
O processamento de dados pessoais que tem uma conexão com mais de um estado membro da UE é chamada então de processamento transfronteiriço.

- O **CONTROLADOR** ou **PROCESSADOR DE DADOS,** que processa dados pessoais em vários estados membros da UE, precisa saber com qual autoridade supervisora deve entrar em contato.
- O **TITULAR DOS DADOS** sempre poderá escolher com qual **AUTORIDADE SUPERVISORA** do país deseja entrar em contato.
- O local que esteja acontecendo o processamento de dados pessoais que tenha conexão com mais de um estado membro da UE deve ser examinado conjuntamente pelas autoridades de supervisão envolvidas no processamento de dados pessoais.

Afetar Substancialmente

O que se entende por **“AFETAR SUBSTANCIALMENTE”** dependerá da natureza das atividades de processamento em que sua organização está envolvida. Se necessário, sua autoridade supervisora principal determinará o que constitui um efeito substancial, caso a caso.

REGULAMENTO SOBRE O PROCESSAMENTO TRANSFRONTEIRIÇO



Depois de confirmar que sua organização está envolvida no processamento transfronteiriço, sua próxima etapa será determinar a localização do seu estabelecimento principal. A chave para determinar o seu estabelecimento principal, se você é um controlador de dados, é identificar qual dos estabelecimentos da sua organização tem o poder de tomar decisões sobre os propósitos e os meios do processamento de dados pessoais

Transferência de Dados

- A proteção oferecida pelo GDPR continuam sendo aplicadas independentemente de onde os dados estiverem. Isto também se aplica quando os dados são transferidos para um país que não é membro da EU, denominado como um "país terceiro".

- o GDPR considera qualquer transferência de dados pessoais que esteja em processamento ou para serem processados após a transferência para um país terceiro ou para uma organização internacional.

- O GDPR restringe a transferência de dados pessoais para fora do Espaço Econômico Europeu (EEE), a menos que os direitos dos titulares em relação a seus dados pessoais estejam protegidos de alguma maneira.

Enquadramento da Transferência de Dados

DECISÃO DE ADEQUAÇÃO

Significa que os dados podem ser transferidos para a empresa daquele país terceiro sem que o país de origem seja obrigado a fornecer outras salvaguardas ou estar sujeito a condições adicionais. Em outras palavras, as transferências para um país “terceiro adequado" serão comparáveis a uma transmissão de dados dentro da UE.

- Na ausência de uma decisão de adequação, uma transferência pode ocorrer mediante o fornecimento de salvaguardas apropriadas e sob a condição legais.

- Se prevista uma transferência de dados pessoais para um país terceiro que não seja objeto de uma decisão de adequação e se houver salvaguardas adequadas, poderá ser feita uma transferência com base em várias situações específicas.

Condições de Transferência de Dados

Parta do princípio que todas as transferências de dados pessoais são ilegais, a menos que sejam permitidas.

A Comissão Europeia chegou a uma “decisão de adequação” sobre o país em que o destinatário está sediado?

A transferência é coberta por “salvaguardas apropriadas”?

A transferência de dados pessoais para países terceiros ou organizações internacionais está coberto conforme algumas condições?

Regras Corporativas Vinculantes (BCR)

Imagine que sua empresa esteja localizada no território da EU e tenha uma filial fora do Espaço Econômico Europeu (EEE).

As BCRs foram projetadas para permitir que empresas multinacionais transfiram dados pessoais do Espaço Econômico Europeu (EEE) para suas afiliadas localizadas fora do EEE.

A principal vantagem das BCRs sobre outros meios de fornecer salvaguardas adequadas é que, uma vez desenvolvidas e operacionais, as BCRs podem fornecer uma estrutura para uma variedade de transferências intragrupo para atender aos requisitos da sua organização.

As BCRs também devem ajudá-lo a lidar com questões de privacidade e aumentar a conscientização sobre a proteção de dados em sua organização.

Você chegou ao fim deste módulo. PARABÉNS!

Módulo 03

Práticas de Proteção dos Dados

Objetivos do Módulo

- Entender sobre proteção de dados desde a concepção (by design) e por padrão (by default).
- Ver o que um DPIA aborda e quando um DPIA deve ser realizado
- Aprender sobre os dados pessoais em uso.

Proteção de Dados Por Concepção e Padrão

- O GDPR exige que você implemente medidas técnicas e organizacionais apropriadas para implementar os princípios de proteção de dados e proteger os direitos individuais. Essa exigência significa então “proteção de dados por concepção e por padrão”.

- Isso significa que você deve integrar a proteção de dados em suas atividades de processamento e práticas de negócios, desde o estágio de concepção ao longo do ciclo de vida.

A PRINCIPAL MUDANÇA COM O GDPR É QUE AGORA É UM REQUISITO LEGAL.

Proteção de Dados Por Design

É necessário que você ponha em prática medidas técnicas e organizacionais adequadas, destinadas a implementar os princípios de proteção de dados, e integre salvaguardas ao seu processamento para atender aos requisitos do GDPR, além de proteger os direitos individuais.

Você deve integrar a proteção de dados em suas atividades de processamento e práticas de negócios.

EX.: desenvolver novos sistemas, serviços, produtos e processos de TI que envolvam o processamento de dados pessoais, desenvolver políticas, processos, práticas de negócios e / ou estratégias organizacionais que tenham implicações de privacidade, desenho físico e encabeçar iniciativas de compartilhamento de dados.

Proteção de Dados Por Default

A proteção de dados por padrão, exige que você processe apenas os dados necessários para atingir seu objetivo específico. Ele está vinculado aos princípios fundamentais de proteção de dados, como minimização e limitação de objetivos.

Você precisa especificar esses dados antes do início do processamento, informar adequadamente as pessoas e processar apenas os dados necessários para o seu propósito.

- O GDPR não exige que você adote uma solução padrão.

- O GDPR quer que você comprove que não processará dados adicionais, a menos que o titular permita e que garanta que os dados pessoais não sejam automaticamente disponibilizados ao público e a terceiros, a menos que o indivíduo decida fazê-lo.

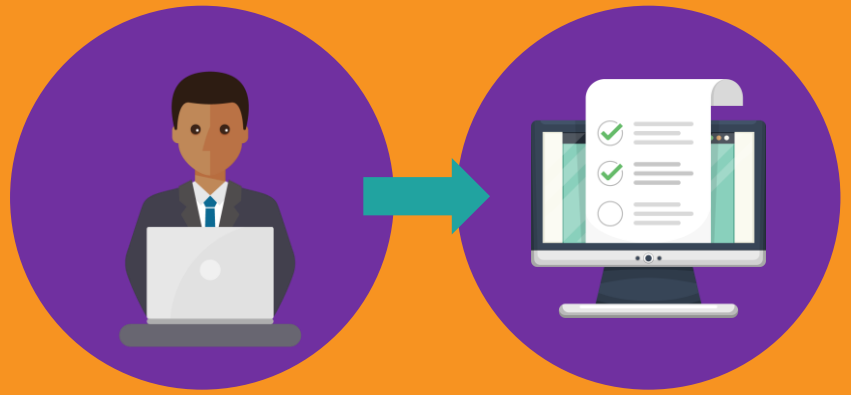
Envolvidos na Proteção de Dados

Afinal, quem é o responsável pelo cumprimento da proteção de dados por design e por default?

- **Você deve garantir que seja incorporado a proteção de dados por design em todos os seus processos e procedimentos internos, mas isso não significa que seja aplicado a todos na organização.**

- **A proteção de dados não se aplica apenas se você for o tipo de organização que possui seus próprios desenvolvedores de software e arquitetos de sistemas, mas também se terceirar esses recursos.**

Processando os Dados



Processador de Dados

- Usar apenas processadores que forneçam garantias suficientes para aplicar medidas técnicas e organizacionais, de modo que o tratamento cumpra com os requisitos do GDPR.

- A proteção de dados por DESIGN e por PADRÃO também podem afetar outras organizações além de controladores e processadores.

O artigo 78 do GDPR

- Ao desenvolver, projetar, selecionar e usar aplicativos, serviços e produtos baseados no processamento de dados pessoais, os desenvolvedores de soluções, serviços e aplicativos devem ser incentivados a levar em consideração o direito de proteção de dados ao desenvolver e projetar esses produtos, serviços e aplicativos e, no que diz respeito ao estado da arte, garantir que controladores e processadores possam cumprir suas obrigações de proteção de dados.

7 Princípios de Proteção de Dados Desde a Concepção (by design)

Proativo não reativo; preventivo não remediador

Privacidade de dados como configuração padrão

Privacidade incorporada ao Design

Funcionalidade total - Soma positiva, não soma zero

Segurança de ponta a ponta - proteção total do ciclo de vida

Visibilidade e transparência – Abertura:

Respeito pela privacidade do usuário

Benefícios da Aplicação dos Princípios

De acordo com o GDPR, o controlador ou processador têm uma obrigação geral de implementar medidas técnicas e organizacionais para mostrar que elas consideraram e integraram a proteção de dados em suas atividades de processamento.

- Problemas potenciais são identificados em um estágio inicial.
- Maior conscientização sobre privacidade e proteção de dados em toda a organização.
- É mais provável que a empresa cumpra suas obrigações legais e violem menos o GDPR.
- É menos provável que as ações sejam intrusivas na privacidade e tenham um impacto negativo nas pessoas.

Contratos Escritos Entre Controlador e Processador

Nos casos em que um controlador contrate um processador para processar dados pessoais, esse processador deve ser capaz de fornecer "garantias suficientes para implementar medidas técnicas e organizacionais apropriadas", que o processamento esteja em conformidade com o GDPR e que a proteção dos direitos dos titulares de dados esteja garantida.

Você deve garantir que as disposições contratuais sejam revisadas e atualizadas.

Garanta que as responsabilidades entre o controlador e o processador sejam estipuladas.

Documente as responsabilidades dos dados com muita clareza para garantir que não haja confusão.

Avaliação de Impacto Sobre a Proteção de Dados (DPIA)

Uma DPIA é uma maneira de analisar sistematicamente e de forma abrangente seu processamento e ajudá-lo a identificar e minimizar os riscos de proteção de dados.

- Devem considerar os riscos de conformidade, mas também riscos mais amplos para os direitos e liberdades dos indivíduos;
- Devem considerar a probabilidade e a gravidade de qualquer impacto sobre os indivíduos;
- Uma DPIA pode cobrir uma única operação de processamento ou um grupo de operações de processamento semelhantes.

Objetivos da DPIA

- Avalie se você realmente precisa fazer uma DPIA em sua organização
- Decida, por exemplo, se em qualquer projeto importante que deve envolver o uso de dados pessoais;
- Considere fazer uma DPIA se você está planejando realizar uma avaliação de risco, se precisa melhorar sua tomada de decisão, se precisa iniciar um monitoramento sistemático, se quer melhorar o tratamento de dados sensíveis ou de natureza altamente pessoal.

O propósito da DPIA é processar dados pessoais que vise melhorar a qualidade dos dados, a viabilidade de seu projeto, aumentar a confiança dos titulares e estar protegido em eventuais auditorias e fiscalizações, pois é sabido que é melhor prevenir do que remediar.

Fases de Um Processo DPIA

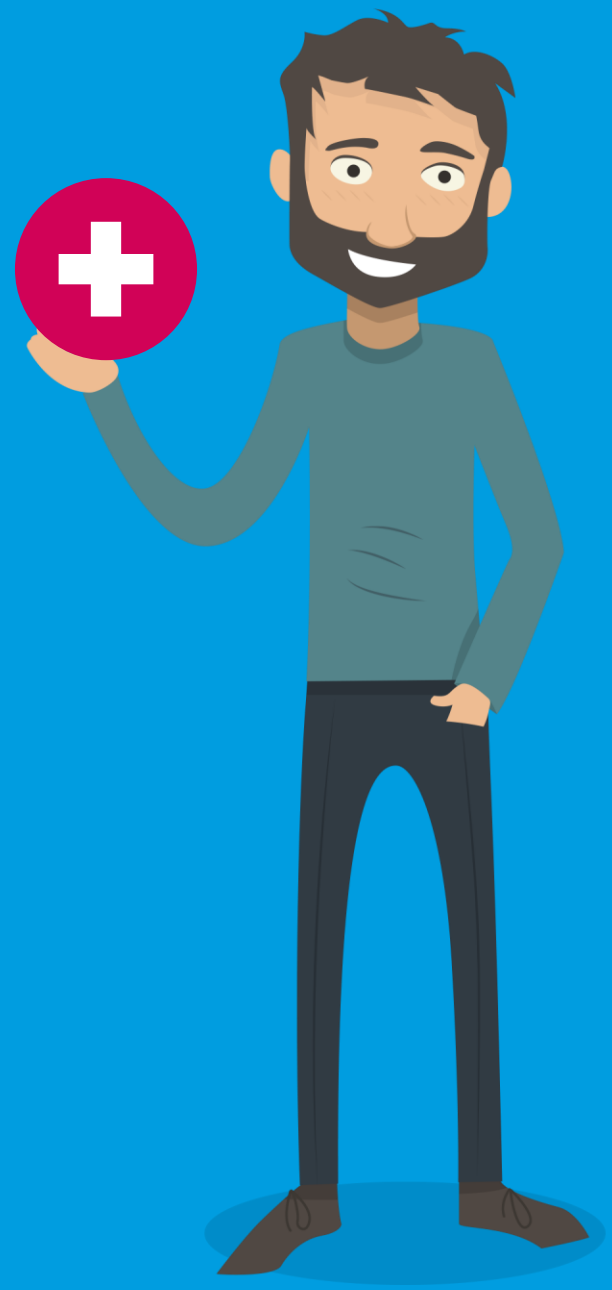
- Uma DPIA deve começar no início da vida de um projeto, antes de você iniciar o processamento, e acompanhar o processo de planejamento e desenvolvimento, mas esteja ciente que a realização de uma DPIA é um processo contínuo, não uma tarefa única.

GDPR

- Descreva as operações de processamento previstas e os objetivos do processamento
- Faça a avaliação da necessidade e proporcionalidade do processamento
- Faça uma avaliação dos riscos para os direitos e liberdades dos titulares dos dados
- Aplique medidas previstas para enfrentar os riscos e demonstrar conformidade com o GDPR

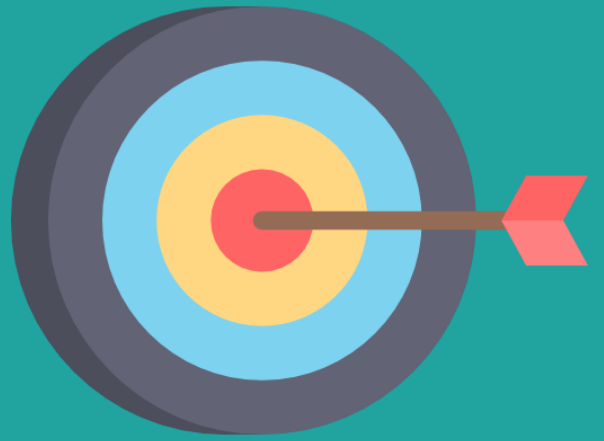
Benefícios de Uma DPIA

- Garantir e demonstrar que sua organização está em conformidade com o GDPR, consequentemente, evitar sanções.
- Inspirar confiança no público, melhorar as comunicações sobre questões de proteção de dados.
- Garantir que seus usuários não corram o risco de violar seus direitos de proteção de dados.
- Permitir que sua organização incorpore “proteção de dados por design” a novos projetos.
- Reduzir custos de operação, otimizando os fluxos de informações dentro de um projeto e eliminar a coleta e o processamento desnecessários de dados.
- Reduzir riscos relacionados à proteção de dados para sua organização.
- Reduzir o custo e a interrupção das salvaguardas de proteção de dados, integrando-as ao design do projeto desde o início.



Gestão do Ciclo de Vida de Dados (GCVD)

O objetivo de uma gestão do ciclo de vida de dados é gerenciar com segurança o ciclo de vida completo dos dados (criação, armazenamento, transferência, processamento e exclusão de dados).



E qual o resultado disso?

Resposta: Diferentes políticas de proteção de dados.

1. A criação ou geração de novo conteúdo ou a atualização do conteúdo existente.
2. O armazenamento, que serve para confirmar que os dados estejam em um repositório de armazenamento.
3. O uso dos dados significa que os dados são visualizados, processados ou usados em uma atividade específica.
4. A fase de compartilhamento diz respeito as informações que são acessíveis a vários atores ou organizações.
5. Arquivamento, que significa que os dados não são usados ativamente e entram no armazenamento de longo prazo.
6. A de destruição, onde os dados são excluídos permanentemente.

Como Melhorar o Gerenciamento do Ciclo de Vida de Dados

1. Coleta de dados.
2. Crie uma estrutura de permissões para evitar o uso indevido ou o acesso inadequado.
3. Defina limites para compartilhamento seguro.
4. Crie regras de retenção / exclusão com base no seu esquema de classificação.

BOA PRÁTICA

Compreenda a diferença entre o que pode ser compartilhado e o que deve ser compartilhado.

Auditoria de Proteção de Dados

Aborda aspectos mais amplos da proteção de dados, como os mecanismos para garantir que as informações sejam obtidas e processadas de maneira justa, legal e com base adequada, para garantir a qualidade das informações. Ou seja, garantir que sejam precisas, completas, atualizadas, adequadas, relevante e não excessivas.

Foco da Auditoria de Proteção de Dados

É determinar se a organização implementou as políticas e procedimentos adequadamente.

Detectar violações de dados ou possíveis violações cibernéticas, avaliar e adequar os controles internos, recomendar mudanças em controles, políticas, procedimentos e plataformas de TI.

Alguns Benefícios

- Ajuda a aumentar a conscientização sobre proteção de dados.
- Pode garantir um “de acordo” formal com o compromisso da gerência em reconhecer o valor da proteção de dados.
- O resultado gerado de uma auditoria pode ser uma lista de recomendações específicas para automatizar a conformidade.

Benefícios de Uma Auditoria

- Facilita a conformidade com o GDPR.
- Mede e ajuda a melhorar a conformidade com o sistema de proteção de dados da organização.
- Aumenta o nível de conscientização sobre proteção de dados entre a gerência e a equipe.
- Fornece informações para revisão do sistema de proteção de dados.
- Melhora a satisfação do cliente, reduzindo a probabilidade de erros que levam a uma reclamação.

Métodos de Auditoria

AUDITORIA DE ADEQUAÇÃO

É verificar se quaisquer Políticas, Códigos de Prática, Diretrizes e Procedimentos documentados atendem aos requisitos do GDPR. Essa parte da auditoria é realizada primeiro e é feita dentro da empresa e com todos os terceiros envolvidos, como processadores.

AUDITORIA DE CONFORMIDADE

É verificar se a organização está de fato operando de acordo com suas Políticas, Códigos de Prática, Diretrizes e Procedimentos documentados, no entanto, o detalhamento da auditoria vai depender dos riscos percebidos para a empresa.

Contexto do Marketing e Mídias Sociais

- O tratamento de quaisquer dados pessoais sempre deve ser levado a sério, especialmente porque o GDPR traz consequências significativas para o não cumprimento, incluindo as multas.

- As organizações devem ter uma base legal para o processamento de dados pessoais sob o GDPR.

Plataformas de Mídia Social

Ferramentas e Técnicas do Marketing e das Mídias Sociais

Retargeting ou Redirecionando de Anúncios

É possível usar anúncios de redirecionamento nas plataformas de mídia social postadas no GDPR. O redirecionamento permite veicular anúncios para pessoas que visitaram seu site.

- As empresas podem gerar relatórios de mídia social para acompanhar o desempenho em relação aos seu KPIs (indicadores de performance), fornecendo assim, informações para campanhas futuras.

- Essas postagens se enquadram na definição de dados pessoais no GDPR, e estão disponíveis publicamente para visualização na plataforma de mídia social.

Prosumidores

Os “prosumidores” ativos, ou seja, são os consumidores produtores, que não apenas interagem com as empresas, mas também podem advogar a favor ou contra as marcas, ajudando-a a gerar negócios, dinheiro, conteúdo, etc.

- A jornada do consumidor está evoluindo. O número de pontos de contato ou os estágios aumentaram muito!
- O prosumidor está tirando o poder de compra e escolha da mão do produtor, mas não só porque ele se tornou mais exigente, mas porque ele força a indústria a construir aquilo que ele deseja.
- O termo prosumidor também pode ser usado para descrever aquelas pessoas que pagam por um serviço digital com ativos não monetários.
- Em termos de proteção de dados, o GDPR adota alguns regulamentos no uso de informações de mídia social em atividades de marketing.

Cookies

Um cookie é um arquivo pequeno, geralmente de letras e números, baixado para um dispositivo quando o usuário acessa determinados sites. Os cookies permitem que um site reconheça o dispositivo de um usuário.

Cookies de sessão

- Permitem que os sites vinculem as ações de um usuário durante uma sessão do navegador.

Cookies persistentes

- São armazenados no dispositivo do usuário entre as sessões do navegador, o que permite que as preferências ou ações do usuário em um site (ou em alguns casos em sites diferentes) sejam lembradas.

Cookies de rastreamento

- Cookies primários em termos básicos são cookies definidos por um site visitado pelo usuário - o site exibido na janela do URL. Cookies de terceiros são definidos por um domínio diferente daquele que está sendo visitado pelo usuário.

Criação de Perfil

A criação de perfil e o enriquecimento de dados podem ser muito úteis para o marketing direto e geralmente existem benefícios comerciais claros.

- Você deve garantir que qualquer perfil ou enriquecimento que você faça ou compre de terceiros esteja em conformidade com o GDPR. As atividades de criação de perfil devem ser realizadas de maneira justa, legal e transparente.

- Se você usar dados não pessoais para enriquecer os detalhes que você possui sobre um indivíduo, eles se tornarão dados pessoais, por exemplo, um dado não pessoal seria: o tipo de pessoa que vive em uma determinada região, mas, ao atrelar aos seus prospectos ou clientes, tornam-se dados pessoais.

Big Data

Refere-se a ativos de alto volume, alta velocidade e alta variedade. A big data usa uma técnica chamada de mineração de dados, ou seja, estamos falando de coleta de dados. Posteriormente haverá o processamento destes dados.

Big data e a proteção de dados se envolvem de duas maneiras principais:

- **Aplicação de técnicas de proteção de dados**
- **Aumento na quantidade de criação de "dados pessoais"**

=

E como resultado, aumenta muito a nossa capacidade de extrair e analisar conjuntos de dados de grande volume, variabilidade e velocidade.

Chegamos ao Fim

Módulo 04

Inteligência Artificial e Cibersegurança

O Que é Inteligência Artificial (IA) para o GDPR?

Segundo a **Comissão Europeia**, a Inteligência Artificial refere-se a sistemas que exibem um comportamento inteligente.

Pode ser puramente baseada em **SOFTWARE**

EX.: Siri ou a Alexa

Também pode estar embutida em **HARDWARES**

EX.: Robôs, drones

Machine Learning (Aprendizado de Máquina)

Subdivisão da Inteligência Artificial. → **Big Data**

1. • Categorizar ou catalogar coisas ou pessoas.
2. • Prever resultados ou ações prováveis com base nesses padrões.
3. • Identificar padrões e relacionamentos que até então eram desconhecidos.
4. • Detectar comportamentos anômalos ou inesperados.

Algoritmos e Dados

Algoritmos

São os processos matemáticos e lógicos que as máquinas usam para aprender.

Quanto mais **dados** são fornecidos (os ingredientes do bolo) e quanto **mais rápido** os computadores conseguem processar essa receita, **melhor a máquina aprende.**

A máquina não é autonomamente criativa.

'entra lixo, sai lixo' (Garbage in, Garbage out)

EX.: Imagine que uma grande empresa decida usar uma IA para selecionar currículos e contratar novos diretores.

O Perigo do Viés (O Exemplo do Policiamento Preditivo)

bias

O que é o viés na Inteligência Artificial?

O que acontece quando você usa esse tipo de dado sujo, enviesado e preconceituoso para treinar um sistema de IA?

Em 2019, pesquisadores da Universidade de Nova York analisaram sistemas de IA

'Policiamento Preditivo'

Princípio da Fairness

Imprevisibilidade Desde a Concepção

'Imprevisibilidade desde a concepção' (ou unpredictability by design).

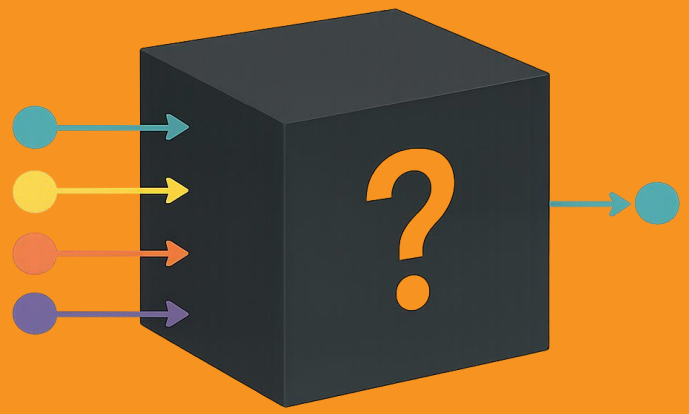
Conformidade com o GDPR

Três tipos de dados:

- Dados observados;
- Dados derivados;
- Dados inferidos.

Essas características da IA entram em choque direto com os princípios fundamentais do GDPR:

- Limitação de Finalidade;
- Minimização de Dados.



"Caixa Preta" (Black Box)

O Duplo Fardo Regulatório (GDPR + AI Act)

AI Act – Lei de Inteligência Artificial

'Duplo Fardo Regulatório' - Double regulatory burden

Quando uma organização cria ou utiliza um cenário que combina o processamento de Dados Pessoais com um sistema de Inteligência Artificial, ela tem que cumprir duas leis pesadas ao mesmo tempo!

GDPR

- INDIVÍDUO - "Você tem base legal para usar o dado dessa pessoa? Você garantiu os direitos dela? O processamento é justo?".

AI Act

- SISTEMA - Classifica as IAs em níveis de risco.

Os 6 Grandes Desafios da IA no GDPR

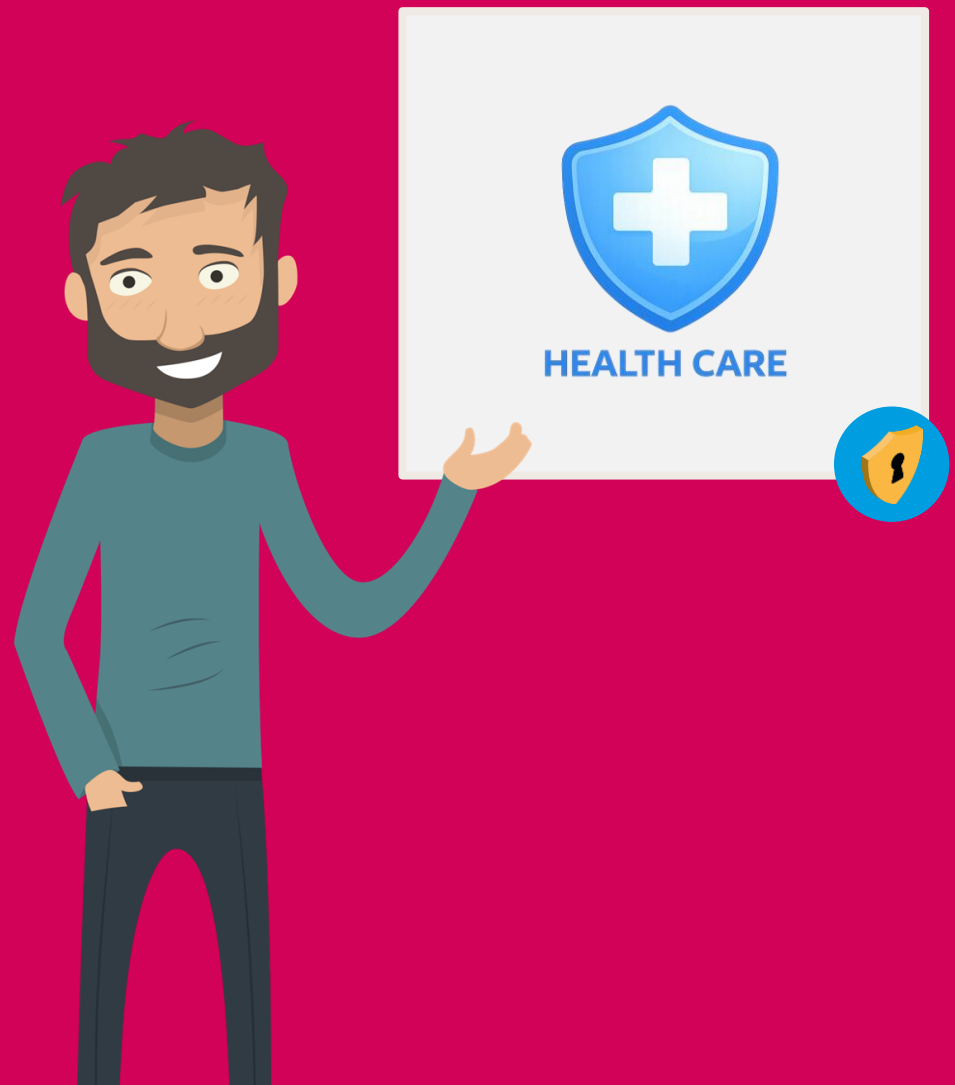
E por que é tão difícil juntar Inteligência Artificial e proteção de dados na prática?

1. A falta de transparência.
2. Dificuldade em garantir a limitação de finalidade e a minimização de dados.
3. Riscos de profiling (definição de perfis) e decisões automatizadas.
4. Garantir uma base legal para o processamento.
5. Honrar os direitos dos titulares.
6. Riscos de Viés e Discriminação, o famoso Bias.

Estudo de Caso Oficial: Detecção de Fraudes

Imagine uma grande empresa de seguro de saúde...

Como essa seguradora garante a conformidade com o GDPR e com o AI Act usando essa IA?



A ideia é que a IA analise os pedidos de reembolso passados, cruze com padrões de comportamento, histórico de consultas do cliente, frequência de exames e valores solicitados para sinalizar atividades suspeitas em tempo real.

Garantindo a Conformidade na Prática

A seguradora precisa seguir rigorosamente estas 6 condições:

Limitação de Finalidade: A empresa tem que definir e documentar que o uso daquela IA é *exclusiva e estritamente* para detecção de fraude.

Minimização de Dados: A IA não pode ter acesso irrestrito a toda a vida do paciente.

Transparência: Não pode haver surpresas.

Direito de Oposição e Supervisão Humana: Se a IA sinalizar uma fraude e bloquear o reembolso do cliente automaticamente, a empresa tem que permitir que o cliente conteste essa decisão.

Avaliação de Risco (DPIA): IA; *profiling* e dados de saúde (que são dados de categoria especial).

Responsabilidade (Accountability): O princípio da prestação de contas.

Conclusão da IA

A IA pode e deve ser usada pelas empresas para inovar, mas isso precisa ser feito de forma responsável e ética.

As salvaguardas de proteção de dados precisam ser construídas dentro do código e da arquitetura do sistema desde o primeiro dia de planejamento.

Princípio de Privacy by Design (Proteção de Dados desde a Concepção) e **Privacy by Default** (Privacidade por Padrão).

Se a IA for desenhada com a privacidade em mente, minimizando dados por padrão e garantindo a transparência, ela estará em conformidade.

O Novo Ecossistema de Leis Europeias

- **CYBERSECURITY ACT (LEI DE CIBERSEGURANÇA):** Estabelece uma estrutura europeia para certificações de segurança cibernética de produtos, serviços e processos de TI.

- **NIS2 (DIRETIVA DE SEGURANÇA DE REDES E INFORMAÇÃO):** É uma lei focada em proteger infraestruturas críticas.

- **DORA (DIGITAL OPERATIONAL RESILIENCE ACT):** Essa é focada especificamente no setor financeiro (bancos, seguradoras, cripto).

GDPR - 2018

Transferências Internacionais (Europa - EUA)

O GDPR proíbe a transferência de dados pessoais para fora do Espaço Econômico Europeu (EEE),

***Safe Harbor* ou o *Privacy Shield*.**

PARA O EXAME:

- A regra atual adotada em 2023 - o EU-U.S. **Data Privacy Framework (DPF)**, ou **Estrutura de Privacidade de Dados UE-EUA.**
- Essa decisão de adequação não vale para os Estados Unidos como um todo.
- A transferência só é livre e legal se a empresa americana for certificada e estiver inscrita na lista oficial do **Data Privacy Framework.**

E SE A EMPRESA AMERICANA NÃO FOR CERTIFICADA NO DPF? A transferência é proibida?

A mais comum, são as **Cláusulas Contratuais Padrão (SCCs - Standard Contractual Clauses).**

O Top 5 Causas de Violação de Dados

Vulnerabilidade ≠ **Incidente de Segurança** ≠ **Violação de Dados Pessoais**

Ex.: Um funcionário tem o péssimo hábito de levantar e deixar o computador desbloqueado.

Ex.: Um hacker consegue invadir a rede da empresa através de uma falha no firewall.

Após a investigação confirmar que o incidente afetou dados pessoais (destruição, perda, alteração ou acesso não autorizado) .

1. Phishing e Engenharia Social.
2. Senhas fracas ou falta de autenticação multifator (MFA).
3. Ameaças internas (Insider Threats).
4. Malware e Ransomware.
5. Software desatualizado.

1. Prevenir/Monitorar (ter segurança antes de acontecer),
2. Investigar (descobrir se dados pessoais foram afetados),
3. Mitigar (conter o dano, fechar a brecha) e, por fim,
4. Notificar (avisar a autoridade em 72 horas).

Atualização da ISO 27701 e Novas Siglas

ISO/IEC 27701 versão 2025

- Atuar como uma extensão da **ISO 27001** (que cuida da segurança da informação) para estabelecer um **PIMS** (Privacy Information Management System. Em português, **SGPI** (Sistema de Gestão de Privacidade da Informação).

Siglas das autoridades europeias

- **Conselho Europeu de Proteção de Dados:** EDPB (European Data Protection Board).

- **Autoridade Europeia para a Proteção de Dados** (que atua como a autoridade supervisora para as próprias instituições e órgãos da União Europeia) é o EDPS (European Data Protection Supervisor).

Compliance Audit (Auditoria de Conformidade)

A Armadilha da LGPD (Aviso Final)

- Desligue a chave da LGPD na sua cabeça.

- O exame PDPF é 100% focado no GDPR europeu.

- Se vir alguma alternativa citando a ANPD (Autoridade Nacional de Proteção de Dados), ou prazos exclusivos da lei brasileira, não marque!

- Para a prova, a autoridade que manda é a **Autoridade Supervisora (a Supervisory Authority ou DPA).**

Chegamos ao Fim

- Reveja o conteúdo e repita os exercícios.
- Realize os simulados atualizados até conseguir atingir 100% da pontuação.
- Evite avançar para o exame enquanto ainda tiver dúvidas sobre os temas abordados.
- Crie o seu próprio mapa mental com os principais conceitos e relações entre os tópicos.
- Inclua no mapa temas como princípios, bases legais, direitos dos titulares, controlador, IA e transferências.
- Leia sempre a apostila obrigatória.

Boa sorte!