White paper: Privacidade, Dados Pessoais e GDPR

Edição 202005

Sobre o autor

Leo Besemer
CertiQA
https://www.certiqa.nl/website/
Contato: leo.besemer@certiqa.nl

Copyright © EXIN Holding B.V. 2020. All rights reserved.
EXIN® is a registered trademark.

No part of this publication may be reproduced, stored, utilized or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written permission from EXIN.

Conteúdo

1.1 A História das Regulações de Proteção de Dados 8
1.1.1 Cronologia da Proteção de Dados 9
1.1.2 Regulação versus Diretiva 10

1.2 Escopo material e territorial do GDPR 10
1.2.1 Escopo material 10
1.2.2 Escopo territorial 10

1.3 Definições 11
1.3.1 Privacidade 11
1.3.2 Proteção de Dados 11
1.3.3 Dados Pessoais 11
1.3.4 Pessoa Natural 12
1.3.5 Dados pessoais diretos, indiretos e pseudonimizados 12
1.3.5.1 Dados pessoais diretos 12
1.3.5.2 Dados pessoais indiretos 12
1.3.5.3 Dados pessoais pseudonimizados 13
1.3.5.4 Dados pessoais especiais 13
1.3.6 Processamento 13

1.4 Papéis, Responsabilidade e Partes Interessadas (stakeholders) 14
1.4.1 Controlador 14
1.4.2 Processador 15
1.4.3 Data Protection Office (DPO) 15
1.4.3.1 Tarefas do DPO 16
1.4.4 Destinatário 16
1.4.5 Terceiro 16

2.1 Princípios de Processamento de Dados 18
2.1.1 Legalidade, Justiça e Transparência 18
2.1.2 Limitação de Finalidade 18
2.1.3 Minimização de Dados 18
2.1.4 Precisão 18
2.1.5 Limitação de Armazenamento 19
2.1.6 Integridade e Confidencialidade 19
2.1.7 Prestação de Contas 19

3.1 Motivos Legítimos para o Processamento 20
3.1.1 Limitação de Finalidade e Especificação de Finalidade 20
3.1.1.1 Especificado 21
3.1.1.2 Explícito 21
3.1.1.3 Legítimo 22
3.1.2 Proporcionalidade e Subsidiariedade 22
3.1.2.1 Subsidiariedade 22
3.1.2.2 Proporcionalidade 22

4.1 Informação Transparente, Comunicação e Modalidades 24

4.2 Informação sobre e acesso a dados pessoais 25
4.2.1 Informações fornecidas ao titular dos dados em qualquer caso 25
4.2.2 Informações a serem fornecidas ao titular dos dados ao transferir dados pessoais 25

4.2.3 Informações adicionais a serem fornecidas quando dados pessoais não forem obtidos diretamente do titular dos dados 26
4.2.4 Momento da informação a ser fornecida 26

4.3 Direto de Acesso (Inspeção) pelo Titular dos Dados 26

4.4 Retificação e Eliminação 27
4.4.1 Direito à retificação 27
4.4.2 Direito ao apagamento (direito de ser esquecido) 27
4.4.3 Direito à limitação do processamento 27
4.4.4 Obrigação de notificação (retificação/eliminação/limitação do processamento) 28
4.4.5 Direito à portabilidade dos dados 29

4.5 Direito de Contestar e Automatizar a Tomada de Decisão Individual 30
4.5.1 Direito a objetar 30
4.5.2 Tomada de decisão individual automatizada, incluindo criação de perfil 30

4.6 Direito de Apresentar queixa junto a uma Autoridade Supervisora 30

5.1 O Conceito de Violação de Dados Pessoais 31

5.2 Procedimento sobre como agir quando ocorre violação de dados pessoais 31
5.2.1 Notificação de uma violação de dados pessoais à Autoridade Supervisora 32
5.2.2 Notificação de uma violação de dados pessoais ao controlador 32
5.2.3 Notificação de uma violação de dados pessoais ao titular afetado 32
5.2.3.1 Criptografia, etc. 32
5.2.3.2 Medidas de mitigação 33
5.2.3.3 Esforço desproporcional 33

5.3 Categorias de violações de dados pessoais 33

6.1 Requisitos para cumprir com a o GDPR 34
6.1.1 Princípios relativos ao processamento de dados pessoais são cumpridos 34
6.1.2 Estrutura legal 34
6.1.3 Avaliação de Impacto 35
6.1.4 Controlador - contrato do processador 35
6.1.5 Consulta prévia 35

6.2 Tipos Requeridos de Administração 36
6.2.1 Registro de atividades de processamento 36
6.2.2 Registro de violações de dados pessoais 37

7.1 Responsabilidades Gerais de uma Autoridade Supervisora 38
7.1.1 Acompanhar e fazer cumprir a aplicação do regulamento 39
7.1.2 Aconselhar e promover a conscientização 39
7.1.3 Administrar violações de dados e outras violações 39
7.1.4 Estabelecer Padrões 39
7.1.4.1 Processamento que requer DPIA 39
7.1.4.2 Código de conduta e certificação 39
7.1.4.3 Cláusulas contratuais padrão e regras corporativas vinculativas e – contratos 40
7.1.5 Cooperação com outras autoridades supervisoras e a AEPD (EDPS). 40

7.2 Papeis e Responsabilidades Relacionadas a Violações de Dados Pessoais 41

7.3 Poderes da Autoridade Supervisora na aplicação do GDPR 41
7.3.1 Poderes de investigação da Autoridade Supervisora 41
7.3.2 Poderes corretivos da Autoridade Supervisora 42
7.3.3 Condições gerais para a imposição de multas administrativas 42
7.3.3.1 Proporcional 42

7.3.3.2 Dissuasivo 43

7.4 Transferência de Dados Transfronteiriça 43
7.4.1 'One-stop-shop' 43
7.4.2 Processamento transfronteiriço 44
7.4.3 Empresa multinacional 44
7.4.4 Empresa que opera internacionalmente 44
7.4.5 Afetar substancialmente 44

7.5 Regulamentos Aplicáveis à Transferência de Dados dentro da AEE 45
7.5.1 Identificar a Autoridade Supervisora principal 45

7.6 Regulamentos aplicáveis à transferência de dados fora do AEE 46
7.6.1 Transferências com base em uma decisão de adequação 46
7.6.2 Transferências sujeitas a salvaguardas apropriadas 46
7.6.3 Regras Corporativas Vinculantes (BCR) 47
7.6.4 Transferências ou divulgações não autorizadas pela lei da UE 47
7.6.5 Regulamentos aplicáveis à transferência de dados entre o AEE e os EUA 48

8.1 Proteção de Dados desde a Concepção (by design) e por Padrão (by default) 50
8.1.1 Os sete princípios de proteção de dados desde a concepção (by design) 50
8.1.1.1 Proativo não reativo; preventiva não remediadora 51
8.1.1.2 Proteção de dados como configuração padrão 51
8.1.1.3 Privacidade Incorporada ao Design 51
8.1.1.4 Funcionalidade Total - Soma Positiva, Não Soma Zero 51
8.1.1.5 Segurança de ponta a ponta - proteção total do ciclo de vida 51
8.1.1.6 Visibilidade e transparência - Abertura 51
8.1.1.7 Respeito à privacidade do usuário – Centrada no Usuário 51
8.1.2 Benefícios da aplicação dos princípios de Privacidade desde a Concepção (by design) e Privacidade por Padrão (by default) 52

8.2 Contratos Escritos entre Controlador e Processador 52
8.2.1 Cláusulas do contrato escrito 52
8.2.1.1 Exemplo 53

8.3 Avaliação de Impacto sobre a Proteção de Dados (DPIA) 54
8.3.1 Objetivos de uma DPIA 55
8.3.2 Tópicos de um relatório DPIA 56

8.4 Gestão do Ciclo de Vida de Dados (GCVD) 56
8.4.1 Finalidade do GCVD 56
8.4.2 Compreendendo os Fluxos de Dados 56
8.4.2.1 Coleta de dados 56
8.4.2.2 Estrutura das permissões 57
8.4.2.3 Construir regras de retenção e exclusão 57

8.5 Auditoria de Proteção de Dados 57
8.5.1 Finalidade de uma auditoria 58
8.5.1.1 Auditoria de adequação 58
8.5.1.2 Auditoria de Conformidade 58
8.5.2 Conteúdo de um plano de auditoria 59

8.6 Práticas Relacionadas a Aplicações do Uso de Dados, Marketing e Mídias Sociais 59
8.6.1 O uso de informações de mídia social em atividades de marketing 59
8.6.2 Uso da internet no campo do marketing 60
8.6.3 Cookies 60

8.6.3.1 Cookies de sessão 60
8.6.3.2 Cookies persistentes 61
8.6.3.3 Cookies de rastreamento 61
8.6.4 Outras informações de perfil: o preço dos serviços "gratuitos" 61
8.6.5 Perspectiva de proteção de dados 62
8.6.5.1 Cookies 62
8.6.5.2 Criação de Perfil 63

8.7 Big data 64

EXIN Privacy & Data Protection Foundation e Essentials

Introdução

Este white paper apresenta um resumo da literatura para os candidatos que estudam para os exames EXIN Privacy & Data Protection Foundation e Essentials (PDPF e PDPE). Para os requisitos mais recentes para o exame, consulte o Guia Oficial de Preparação do EXIN, que pode ser baixado em www.exin.com.

Em uma era digital, as informações sobre as pessoas estão se tornando cada vez mais valiosas. Facilitadas por novas tecnologias, as organizações coletam e armazenam dados em grande escala. Esta recente explosão de dados apresenta desafios específicos de segurança, especialmente quando se trata de dados pessoais, devido à regulamentação rigorosa da União Europeia em relação à proteção de dados.

Privacidade e proteção de dados pessoais devem ser uma prioridade para qualquer organização.

Organizações que processam dados pessoais de pessoas que residam ou visitem um dos Estados-Membros da Área Econômica Europeia (AEE) devem cumprir o Regulamento Geral de Proteção de Dados (GDPR - General Data Protection Regulation). As organizações fora da AEE também deverão observar o GDPR ao fazer negócios na Europa. A adesão ao regulamento GDPR previne multas e aumenta a confiança dos clientes.

Ter profissionais certificados com o nível certo de conhecimento pode ajudar a preparar uma organização para cumprir o GDPR e ajudá-la a ficar em conformidade com a regulamentação. O programa EXIN Privacy & Data Protection Foundation (PDPF) abrange o conhecimento necessário sobre proteção de dados e cumprimento do GDPR.

EXIN, outubro de 2019

Fundamentos de Privacidade

1 Definições e Contexto Histórico

Neste capítulo, veremos a história da privacidade e proteção de dados e a relação entre os dois conceitos. Com isso, analisaremos algumas definições básicas, já que elas são usadas no Regulamento Geral de Proteção de Dados (GDPR). Alguns dos termos e conceitos são explicitamente definidos no Artigo 4 do GDPR para o restante deste documento. Alguns dos termos usados em todo o GDPR são derivados do direito internacional.

1.1 A História das Regulações de Proteção de Dados

As recentes invenções e métodos de negócios chamam a atenção para o próximo passo que deve ser tomado para a proteção da pessoa e para assegurar ao indivíduo ... o direito de "estar sozinho" ... Vários dispositivos mecânicos ameaçam cumprir a previsão de que "o que é sussurrado no armário deve ser proclamado a partir dos telhados ".

Fonte: https://www.brandeis.edu/now/2013/july/privacy.html (acessado em 18 de março de 2017)

Enquanto alguém poderia pensar que este texto foi escrito recentemente, Louis D. Brandeis o escreveu em um artigo na revista Harvard Law Review, em 1890. Este direito de não ser incomodado ou sofrer invasões, acabou se tornando a base sobre a qual o Artigo 12 da Declaração Universal dos Direitos Humanos (DUDH), fundada em 1948.

Ninguém estará sujeito a interferências arbitrárias em sua privacidade, família, lar ou correspondência, nem a ataques à sua honra e reputação. Todos têm o direito de proteção da lei contra tais interferências ou ataques.

Fonte: https://www.un.org/en/universal-declaration-human-rights/ (acessado em 18 de março de 2017)

O rápido progresso no processamento de dados e o aumento das possibilidades no uso de telecomunicações na década de 1970 coincidiram com o desenvolvimento da União Europeia, que aumentou o comércio transfronteiriço. Como resultado, sentiu-se a necessidade de novos padrões que permitissem aos indivíduos exercer controle sobre suas informações pessoais. Ao mesmo tempo, o comércio internacional precisava de um fluxo internacional de informações livre. O desafio é encontrar um equilíbrio entre as preocupações com a proteção das liberdades pessoais e a possibilidade de apoiar o livre comércio em toda a Europa.

Os Estados-Membros da União Europeia assinaram na Convenção Europeia de Direitos Humanos (ECHR - European Convention of Human Rights, 1950) um tratado para defender os direitos humanos em toda a União Europeia, entre eles **o direito ao respeito pela vida privada e familiar**.

Um primeiro esforço para consolidar a **proteção da privacidade** e a **necessidade de fluxo internacional de dados pessoais livre** veio da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) em 1980: Diretrizes para a Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais (*Guidelines on the Protection of Privacy and Trans-border flows of Personal Data)*. Essas diretrizes foram formalizadas em 1981 pela Convenção para a Proteção de Indivíduos

no que diz respeito ao Processamento Automático de Dados Pessoais, também conhecido como Tratado de Estrasburgo.

Quando o desenvolvimento do comércio internacional e a necessidade de proteção aumentaram, sentiu-se a necessidade de harmonização da legislação europeia sobre privacidade. Isso resultou, em 1995, na "Diretiva de Proteção de Dados" 95/46/EC.

A Carta dos Direitos Fundamentais da União Europeia (a 'Carta', proclamada em dezembro de 2002) incluía os princípios gerais estabelecidos na CEDH. A Carta refere-se explicitamente à proteção da privacidade e à proteção de dados pessoais como um **direito** fundamental:

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.

Fonte: Carta dos Direitos Fundamentais da União Europeia.

Enquanto o progresso no processamento de dados aumentava a cada ano, o comércio internacional era dificultado por leis diferentes. As regras e regulamentos nos Estados-Membros, embora baseados na diretiva 95/46 / CE, ainda eram bastante diversas. Após anos de discussão, o GDPR foi publicado em 25 de maio de 2016. O GDPR é aplicável como lei em todos os países do AEE em 25 de maio de 2018. O regulamento revoga a Diretiva 95/46 / CE. Isso significa que todas as leis nacionais baseadas nesta diretiva são substituídas pelo GDPR.

Nos termos do artigo 94(2) do GDPR, as referências à diretiva revogada devem entender-se como sendo feitas ao presente regulamento. As referências ao Grupo de Trabalho sobre proteção de pessoas físicas, relativas ao tratamento de dados pessoais, estabelecido no artigo 29 da Diretiva 95/46 / CE, serão consideradas como referências ao Conselho Europeu de Proteção de Dados criado pelo GDPR. O artigo 94 deixa claro que, mesmo quando os Estados-Membros precisam de mais tempo para atualizar a lei nacional que de alguma forma complementa a lei com base na Diretiva 95/46 / CE, não pode haver confusão sobre qual lei se aplica.

1.1.1 Cronologia da Proteção de Dados

Ano	Nome	Sigla
1948	Declaração Universal dos Direitos Humanos	DUDH (UHDR)
1950	Convenção Europeia sobre Direitos Humanos	CEDH (ECHR)
1981	Convenção para Proteção de Indivíduos relativamente ao Processamento Automático de Dados Pessoais	ETS 108 = EU 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	Diretiva de Privacidade (válida até 25/5/2018)
2002	Carta dos Direitos Fundamentais da União Europeia	CEDH (EU Charter)
2016	Regulamento Geral de Proteção de Dados (EU - 2016/679)	'GDPR' (a partir de 25/5/2018)
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	

1.1.2 Regulação versus Diretiva

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.

1.2 Escopo material e territorial do GDPR

1.2.1 Escopo material

A regulação aplica-se ao tratamento de dados pessoais, no todo ou em parte, por meios automatizados e ao tratamento, com exclusão dos meios automáticos de dados pessoais que fazem parte de um sistema de arquivo ou se destinam a fazer parte de um sistema de arquivo.

Fonte: Regulamento Geral de Proteção de Dados – GDPR (EU) 2016/679; Artigo 2(1)

O GDPR se aplica a dados pessoais de forma estruturada, desde sistemas de banco de dados totalmente automatizados até arquivos baseados em papel, como os arquivos médicos clássicos ainda usados em alguns hospitais.

Existem algumas exceções. Em vez do GDPR, a Diretiva 2016/680 (legislação nacional com base nesta diretiva) aplica-se a atividades relacionadas com a política externa e de segurança comum, pelo tratamento pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou a execução de sanções penais.

O GDPR também não se aplica ao processamento de dados pessoais por uma pessoa natural "**no curso de uma atividade puramente pessoal ou doméstica**". O item 18 refere-se a isto como atividades sem ligação com atividades profissionais ou comerciais, como correspondência pessoal e um livro de endereços que é mantido para esse fim, redes sociais e atividades online nesse contexto.

1.2.2 Escopo territorial

1. Esta regulação se aplica ao tratamento de dados pessoais no contexto das atividades de um estabelecimento de um controlador ou um processador na União, independentemente de o tratamento ter lugar na União ou não.
2. Esta regulação se aplica ao tratamento de dados pessoais de titulares de dados que estejam na União por um controlador ou processador não estabelecidos na União, em que as atividades de tratamento estejam relacionadas com:
    a. a oferta de bens ou serviços, independentemente de ser ou não exigido o pagamento da pessoa em causa, a essas pessoas na União; ou
    b. o monitoramento do seu comportamento, desde que o seu comportamento ocorra na União.

Fonte: Regulamento Geral de Proteção de Dados – GDPR (EU) 2016/679; Artigo 3

Qualquer processamento de dados pessoais no contexto das atividades de um estabelecimento de um controlador ou de um processador na União Europeia deve ser efetuado em conformidade com o GDPR, independentemente do local (no mundo) em que se processe efetivamente.

O GDPR também se aplica ao processamento relacionado ao comércio ("a oferta de bens ou serviços") e ao "monitoramento do comportamento" de pessoas que estão na União Europeia (item 23). Isso tem consequências de longo alcance. Por exemplo o caso de uma empresa canadense

que processa dados pessoais de um cidadão argentino para uma compra online. Se esse cidadão argentino estiver visitando Paris (França) no momento da compra e a empresa canadense souber que está oferecendo bens ou serviços para a União Europeia (porque eles enviaram os produtos para a Europa, por exemplo), esse processamento está sujeito ao GDPR.

Além disso, o GDPR se aplica ao processamento de dados pessoais por um controlador não estabelecido na AEE, mas "em um local em que a lei do Estado-Membro se aplica por força do direito internacional público". O item 25 dá o exemplo da missão diplomática ou consulado de um Estado-Membro.

O GDPR também se aplica ao processamento a bordo de navios registrados em um Estado-Membro da UE, independentemente de qualquer lugar do mundo em que o navio realmente esteja.

1.3 Definições

Nos primeiros itens do GDPR, a definição de privacidade está explicitamente ligada à Carta dos Direitos Fundamentais da União Europeia.

1. A proteção das pessoas físicas em relação ao tratamento de dados pessoais é um direito fundamental. O Artigo 8(1) da Carta dos Direitos Fundamentais da União Europeia (a «Carta») e o Artigo 16(1), do Tratado sobre o Funcionamento da União Europeia (TFUE) estabelecem que todas as pessoas têm direito à proteção dos direitos fundamentais relativos a se dados pessoais.
2. 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. (…)

Fonte: Regulamento Geral de Proteção de Dados – GDPR (EU) 2016/679; explicações (1) e (2)

Nesse sentido, o direito à proteção de dados pessoais é um meio de proteger os direitos e liberdades fundamentais das pessoas, entre eles a sua privacidade.

1.3.1 Privacidade

De acordo com o acima exposto, a privacidade é definida como o **direito a respeitar a vida privada e familiar de uma pessoa, sua casa e correspondência**.

1.3.2 Proteção de Dados

A partir dos parágrafos anteriores, podemos concluir que o GDPR diz respeito à proteção de dados pessoais, não de todos os dados. O artigo 4 do GDPR define exatamente quais dados são incluídos na definição.

1.3.3 Dados Pessoais

O Artigo 4(1) do GDPR define dados pessoais como:

Dados pessoal significa qualquer informação relativa a uma pessoa natural identificada ou identificável (titular dos dados); uma pessoa natural identificável é aquela que pode ser identificada, direta ou indiretamente, em particular por referência a um identificador como um nome, um número de identificação, dados de localização, um identificador online ou a um ou mais fatores específicos de identidade física, fisiológica, identidade genética, mental, econômica, cultural ou social daquela pessoa natural;

Fonte: Regulamento Geral de Proteção de Dados – GDPR (EU) 2016/679; Artigo 4(1)

Qualquer informação pode ser tomada literalmente. Inclui informações objetivas, como coisas que podem ser medidas, por exemplo, tipo sanguíneo, tamanho do sapato ou a quantidade de álcool no sangue da pessoa. Também inclui informações subjetivas, tais como opiniões sobre uma pessoa (por exemplo, John é um bom treinador). 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 não se limita a informações que possam ser consideradas prejudiciais à vida privada e familiar do indivíduo. O meio em que as informações estão contidas também é irrelevante. O conceito de dados pessoais inclui informações disponíveis em qualquer forma: texto, figuras, gráficos, fotografias, vídeo, acústico ou qualquer outra forma possível.

1.3.4 Pessoa Natural

Legalmente, uma pessoa natural é 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). Os Estados-Membros, pelo contrário, podem prover regras relativas ao tratamento de dados pessoais de pessoas falecidas.

1.3.5 Dados pessoais diretos, indiretos e pseudonimizados

Na prática, há três tipos de dados pessoais.

1.3.5.1 Dados pessoais diretos

Dados pessoais diretos são dados que podem ser atribuídos diretamente a um indivíduo específico sem o uso de informações adicionais. Por exemplo, a foto do indivíduo, seu DNA, impressão digital. Os nomes podem ser dados pessoais diretos se forem muito raros, mas a maioria dos nomes não é considerada exclusiva e, portanto, não são dados pessoais diretos. Um título único, como "o atual primeiro-ministro da França", também é uma referência direta a um indivíduo, ou seja, dados pessoais diretos.

1.3.5.2 Dados pessoais indiretos

Os dados pessoais indiretos são dados que podem estar ou poderão estar no futuro vinculados a um indivíduo específico usando informações adicionais. Por exemplo, a placa numérica de um carro é um dado pessoal indireto, porque é possível rastrear o carro até seu proprietário usando informações adicionais (neste caso, as informações em um banco de dados eram as placas de matrícula relacionadas aos proprietários dos carros). O mesmo é válido para números exclusivos atribuídos a pessoas pelo governo (número de previdência social) ou por um provedor de serviços internet (endereço IP), que pode ser vinculado a um único indivíduo. O fato de nem todos os controladores poderem rastrear uma placa de carro, número de segurança social ou endereço IP associado a um indivíduo não é importante. O fato de que isso seja em teoria possível, faz com que sejam dados pessoais indiretos.

Os nomes são dados pessoais indiretos, em que o nome é comum o suficiente para não apontar para uma pessoa específica. Para distinguir "James Williams" de outros indivíduos com esse nome, são necessárias informações adicionais, como residência e data de nascimento.

1.3.5.3 Dados pessoais pseudonimizados

Pseudonimização de dados é o processo de disfarçar identidades. O objetivo desse processo é ser capaz de coletar dados adicionais relacionados ao mesmo indivíduo sem precisar conhecer sua identidade. Um exemplo pode ser uma câmera registrando quantos carros únicos passam por uma ponte em uma estrada. O número da placa é um dado pessoal indireto. O controlador substituiria cada número da placa por uma chave ou pseudônimo exclusivo, mantendo uma tabela separada vinculando cada chave à placa correspondente. O controlador pode enviar esses dados pseudônimos para um processador, mantendo a chave em um local seguro.

Dados pseudonimizados são um tipo de dados pessoais indiretos, onde os dados adicionais necessários para identificar os titulares dos dados ('a chave') estão disponíveis apenas para o controlador. O processo é reversível desde que a chave exista. Consequentemente, dados pseudonimizados de uma pessoa são considerados dados pessoais, porque a identificação ainda é tecnicamente possível.

Anonimização significa que nenhuma informação da qual a pessoa a quem os dados se relacionam possa ser identificada de qualquer forma. Dados anônimos em uma pessoa **não são mais** considerados dados pessoais. Dados pseudonimizados podem ser anonimizados destruindo a chave.

Por exemplo, para pesquisas sobre saúde e hábitos alimentares, é chamado um grupo selecionado de titulares de dados. Os nomes, números de telefone e outros dados dos titulares dos dados são conhecidos e mantidos em um banco de dados, para o qual os titulares dos dados deram sua permissão. Os titulares dos dados são chamados várias vezes durante a pesquisa. Depois que o período da pesquisa termina, todos os dados identificáveis são apagados após a coleta das informações necessárias para a pesquisa. Isso significa que os dados não podem mais ser vinculados aos titulares de dados específicos, porque não existe uma chave. Somente dados pessoais mais gerais, como sexo e categoria etária, estão vinculados aos dados sobre saúde e hábitos alimentares. Em outras palavras, os dados deixados após a pesquisa são anonimizados.

1.3.5.4 Dados pessoais especiais

O GDPR distingue várias categorias de dados pessoais que necessitam um tratamento especial. As categorias de dados pessoais especiais são:

- 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

É proibido processar dados pessoais especiais, exceto nos casos explicitamente mencionados no Artigo 9 do GDPR.

1.3.6 Processamento

No que diz respeito ao GDPR, os dados de processamento são sempre considerados como o processamento de dados pessoais. O GDPR não se aplica ao processamento de quaisquer outros dados. Dito isto, a definição de processamento é muito ampla:

Processamento significa qualquer operação ou conjunto de operações efetuadas em dados pessoais ou em conjuntos de dados pessoais, por meios automatizados ou não, como coleta, registro, organização, estruturação, armazenamento, adaptação ou alteração, recuperação, consulta, utilização, divulgação por transmissão, disseminação ou de outra forma tornar disponível, alinhamento ou combinação, restrição, apagamento ou destruição

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Artigo 4 (1)

Na verdade, é difícil pensar em algo que possa ser feito com dados pessoais, mas não estaria contido na definição.

A coleta de dados pessoais é processamento. O armazenamento de dados pessoais é processamento. Destruir dados pessoais também é processando. Mesmo fazer um backup de um servidor que não é seu, mas contém dados pessoais, seria considerado um tipo de armazenamento, incluído na definição de processamento.

1.4 Papéis, Responsabilidade e Partes Interessadas (stakeholders)

1.4.1 Controlador

Controlador significa a pessoa natural ou jurídica, autoridade pública, agência ou outro organismo que, individualmente ou em conjunto com outros, determina os fins e os meios do tratamento de dados pessoais.

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Artigo 4 (7)

O controlador é a pessoa natural ou jurídica responsável pela **determinação das finalidades e meios do processamento meios para o processamento**.

1. Tendo em conta a natureza, o âmbito, o contexto e os fins do processamento, bem como os riscos de variação da probabilidade e gravidade dos direitos e liberdades das pessoas físicas, o responsável pelo tratamento deve implementar medidas técnicas e organizacionais adequadas para garantir e poder demonstrar que o processamento é realizado em conformidade com o presente regulamento. Essas medidas devem ser revistas e atualizadas sempre que necessário.
2. Sempre que proporcionada em relação às atividades processamento, as medidas referidas no parágrafo 1 devem incluir a implementação de políticas adequadas em matéria de proteção de dados pelo responsável pelo controlador.

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Artigo 24

Em outras palavras, a responsabilidade e o papel do controlador é implementar medidas técnicas e organizacionais apropriadas para cumprir o GDPR, incluindo políticas apropriadas de proteção de dados.

O Artigo 24(1) indica que o nível das medidas técnicas pode variar de acordo com a situação específica e o nível de risco para as pessoas físicas envolvidas. Por exemplo, o convite para o churrasco de verão do clube de hóquei, apesar de processar dados pessoais, provavelmente não precisa do mesmo nível de segurança de dados que um convite para um grupo de pessoas que sofrem de uma doença crônica. Veja também o item 1.3.5.4-Dados pessoais especiais.

Observe que o papel do controlador não é apenas a implementação técnica dos procedimentos apropriados. O controlador é responsável e deve ser capaz de demonstrar que o processamento é executado de acordo com o GDPR.

1.4.2 Processador

Processador é uma pessoa natural ou jurídica, autoridade pública, agência ou outro organismo que processa dados pessoais em nome do controlador.

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Artigo 4 (8)

Às vezes, um processador pode ser chamado de "processador de dados". A definição indica que um processador sempre age 'em nome do controlador' e que o processador deve cumprir as instruções do controlador. As instruções podem ser escritas em um contrato. O contrato controlador-processador é discutido em 8.2.

1.4.3 Data Protection Office (DPO)

Controladores e processadores podem, e nos casos citados abaixo **devem** nomear um Data Protection Office (DPO). O DPO é uma pessoa que tem a tarefa formal de garantir que a organização esteja ciente e cumpra suas responsabilidades e obrigações de proteção de dados de acordo com o GDPR e as leis do Estado-Membro.

O controlador e o processador designarão um Data Protection Office (DPO) em qualquer caso em que:

(a) o tratamento for efetuado por uma autoridade ou organismo público, com exceção dos órgãos jurisdicionais que atuem no exercício das suas funções
(b) as atividades principais do controlador ou do processador consistem em operações de tratamento que, devido à sua natureza, âmbito e / ou finalidades, exigem monitoramento regular e sistemático em grande escala dos titulares dos dados ou
(c) as atividades principais do controlador ou do processador consistem no tratamento de uma grande variedade de categorias especiais de dados nos termos do Artigo 9 e dados pessoais relativos a condenações penais e infracções referidas no Artigo 10

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Artigo 37(1)

As organizações que não precisam nomear um DPO são livres para fazê-lo por vontade própria. Se uma organização designar voluntariamente um DPO, o DPO será mantido de acordo com os padrões do GDPR. Sempre que um DPO é nomeado, a organização deve comunicar isso à Autoridade Supervisora relevante e publicar os detalhes do DPO, para que os titulares dos dados possam chegar ao DPO. De acordo com o item (97), o DPO deve ser "uma pessoa com conhecimento especializado das leis e práticas de proteção de dados".

O Artigo 38 do GDPR exige explicitamente que o controlador e o processador garantam que o DPO esteja envolvido, de forma adequada e em tempo hábil, em todas as questões relacionadas à proteção de dados pessoais. Eles têm a obrigação de apoiar o DPO no desempenho de suas tarefas, fornecendo recursos necessários para realizar essas tarefas e acesso a dados pessoais e operações de processamento, e para manter seu conhecimento especializado. O DPO tem uma **posição independente** e é protegido pelo GDPR:

O controlador e o processador devem assegurar que o DPO não receba instruções sobre o exercício dessas tarefas. Ele não deve ser dispensado ou penalizado pelo controlador ou pelo processador por executar suas tarefas. O DPO deve reportar diretamente ao mais alto nível de gerenciamento do controlador ou do processador.

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Artigo 38 (3)

1.4.3.1 Tarefas do DPO

O DPO deve ter pelo menos as seguintes tarefas:

(a) informar e aconselhar o controlador ou o processador e os empregados que efetuam o processamento das suas obrigações nos termos do presente regulamento e de outras disposições em matéria de proteção de dados da União ou dos Estados-Membros;

(b) b) monitorar a conformidade com o presente regulamento, com outras disposições em matéria de proteção de dados da União ou dos Estados-Membros e com as políticas do controlador ou dos processadores no tocante à proteção dos dados pessoais, incluindo a atribuição de responsabilidades, a sensibilização e a formação do pessoal; envolvidos em operações de processamento e as auditorias relacionadas;

(c) c) prestar aconselhamento, se tal for solicitado, no que diz respeito à avaliação de impacto sobre a proteção de dados, e acompanhar o seu desempenho nos termos do Artigo 35;

(d) d) cooperar com a Autoridade Supervisora;

(e) e) servir de ponto de contato para a Autoridade Supervisora em questões relacionadas com o processamento, incluindo a consulta prévia referida no Artigo 36, e a consultar, se for caso, qualquer outra questão.

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Artigo 39(1)

1.4.4 Destinatário

Destinatário é uma pessoa natural ou jurídica, uma autoridade pública, uma agência ou outro organismo para o qual os dados pessoais são divulgados, terceiros ou não. No entanto, as autoridades públicas que possam receber dados pessoais no âmbito de um inquérito específico em conformidade com a legislação da União ou do Estado-Membro não são consideradas destinatários; o processamento desses dados por essas autoridades públicas deve estar em conformidade com as regras de proteção de dados aplicáveis, de acordo com os objetivos do processamento.

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Artigo 4 (9)

A definição diz principalmente o que o destinatário não é. O destinatário é uma parte interessada importante, sendo aquele para quem dados pessoais ou resultados de processamento de dados pessoais são divulgados. Em particular, quando o destinatário esteja fora do AEE, e ainda mais se o destinatário for uma instituição do Governo fora do AEE, existem regras estritas, que serão discutidas mais adiante (ver tópico 7.4).

1.4.5 Terceiro

Terceiro é uma pessoa natural ou jurídica, autoridade pública, agência ou organismo que não seja o titular dos dados, o controlador, o processador e as pessoas que, sob a autoridade direta do controlador ou do processador, estão autorizados a tratar dados pessoais;

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Artigo 4(10)

Um terceiro é uma pessoa natural ou jurídica, autoridade pública, agência ou organismo. Em qualquer caso, não é o titular dos dados, nem o controlador nem o processador, nem as pessoas que, sob a autoridade direta do controlador ou do processador, estão autorizadas a processar dados pessoais. Então, o que é um terceiro?

Em princípio, um terceiro é uma pessoa ou organização sem motivos legítimos específicos nem autorização para processar dados pessoais. Um exemplo é um contador, que na execução de suas funções pode, inadvertidamente, ver dados pessoais. Ou um gerente de sistemas verificando se o back-up de dados pessoais foi bem-sucedido e, ao fazer isso, vê alguns nomes e outros dados pessoais.

Um terceiro que recebe dados pessoais - seja legal ou ilegalmente - processa, por definição, dados pessoais. Quando o processamento não for executado sob a autoridade direta do controlador, este "terceiro" será, em princípio, considerado como um novo controlador.

2 Processamento de Dados Pessoais

De acordo com a definição de processamento, qualquer operação em dados pessoais está contida na definição de processamento. O capítulo II do GDPR (Artigos 5 a 11) detalha os princípios de processamento de dados.

2.1 Princípios de Processamento de Dados

O processamento de dados pessoais precisa sempre estar em conformidade com os princípios relativos ao processamento de dados pessoais. Esses princípios são:

- Legalidade, justiça e transparência
- Limitação de finalidade
- Minimização de dados
- Precisão
- Limitação de armazenamento
- Integridade e confidencialidade
- Prestação de contas

2.1.1 Legalidade, Justiça e Transparência

Os dados pessoais devem ser processados de forma legal, justa e transparente em relação ao titular dos dados. O titular dos dados pode perguntar como seus dados são processados, se não estiver claro para eles.

2.1.2 Limitação de Finalidade

Os dados pessoais devem ser coletados para fins especificados, explícitos e legítimos e **não devem ser processados** de maneira incompatível com esses fins.

Processamento adicional é permitido para:

- fins de arquivamento de interesse público,
- pesquisa científica ou histórica ou
- fins estatísticos,

desde que, de acordo com o GDPR, estejam em vigor as salvaguardas adequadas para os direitos e liberdades do titular dos dados.

2.1.3 Minimização de Dados

Os dados pessoais devem ser adequados, relevantes e **limitados ao necessário** em relação aos fins para os quais são processados.

2.1.4 Precisão

Os dados pessoais devem ser precisos e, se necessário, atualizados: todas as medidas razoáveis devem ser tomadas para garantir que os dados pessoais que são incorretos sejam retificados ou excluídos.

2.1.5 Limitação de Armazenamento

Os dados pessoais devem ser mantidos em um formato que permita a identificação dos titulares de dados por não mais do que o necessário para as finalidades para as quais os dados pessoais são processados; etc.

2.1.6 Integridade e Confidencialidade

Os dados pessoais devem ser processados de maneira a garantir a segurança apropriada dos dados pessoais, incluindo proteção contra processamento não autorizado ou ilegal e contra perda, destruição ou dano acidental, usando medidas técnicas ou organizacionais apropriadas.

2.1.7 Prestação de Contas

O controlador é responsável pelo processamento de dados. Isso significa que o controlador é responsável pela conformidade com os princípios mencionados acima, juntamente com o processador. O controlador também deve ser capaz de demonstrar conformidade com os princípios de processamento de dados.

3 Motivos Legítimos e Limitação de Finalidade

3.1 Motivos Legítimos para o Processamento

De acordo com o Artigo 6(1) do GDPR, o processamento só será lícito se, e na medida em que **ao menos um** dos seguintes motivos legítimos de processamento se aplicar:

- O titular dos dados **consentiu** com o processamento dos seus dados pessoais para um ou mais fins específicos
- O processamento é **necessário para a execução de um contrato** do qual o titular dos dados é parte ou para tomar medidas a pedido do titular dos dados antes de celebrar um contrato. No entanto, o processamento em relações pré-contratuais é legítimo, desde que seja para dar passos a pedido do titular dos dados antes de entrar num contrato.
- O processamento é necessário para o **cumprimento de uma obrigação legal** à qual o controlador está sujeito
- O processamento é necessário para proteger um **interesse vital** da pessoa em causa ou de outra pessoa natural
- O processamento é necessário para o desempenho de uma tarefa realizada no **interesse público** ou no exercício da autoridade oficial conferida ao controlador.
- O processamento é necessário para os **interesses legítimos** perseguidos pelo controlador ou por um terceiro,
    - exceto quando esses interesses são sobrepostos pelos interesses ou direitos e liberdades fundamentais do titular dos dados que exigem a proteção dos dados pessoais, em especial quando o sujeito dos dados é uma criança.

Esta lista de motivos é exaustiva. Não são possíveis outros motivos legítimos para o processamento de dados pessoais sob o GDPR.

3.1.1 Limitação de Finalidade e Especificação de Finalidade

Especificação de finalidade como um termo não está definido explicitamente no GDPR. No entanto, em abril de 2013, o Grupo de Trabalho do Artigo 29 (WP29), composto por representantes das autoridades europeias de supervisão, da Autoridade Europeia para a Proteção de Dados e da Comissão Europeia, publicou um parecer sobre o princípio da limitação de objetivos no processamento de dados pessoais. Os pareceres do WP29 fornecem orientações oficiais sobre as regras da UE de proteção de dados.

A partir de 25 de maio de 2018, o Grupo de Trabalho do Artigo 29 foi sucedido pelo Conselho Europeu de Proteção de Dados (EDPB), conforme definido no artigo 68 do GDPR. Em sua primeira reunião, o EDPB endossou as diretrizes e outros documentos sobre o GDPR publicados pelo WP29 para verificar a continuidade. Muitas das diretrizes e opiniões publicadas no WP29 antes de maio de 2018 são incorporadas ou referenciadas no GDPR.

Os dados pessoais devem ser coletados para finalidades especificadas. O controlador deve, portanto, considerar cuidadosamente para que finalidade ou fins os dados pessoais serão utilizados e não deve coletar dados pessoais que não sejam necessários, adequados ou relevantes para a finalidade ou finalidades que devem ser atendidas.

Fonte: Parecer do WP29 sobre limitação de finalidade, § III.1.1. (acessado em 29 de março de 2017)

O Artigo 5(1.b) do GDPR exige que os “dados pessoais sejam recolhidos para fins específicos, explícitos e legítimos”. Vamos ver os elementos dessa sentença:

3.1.1.1 Especificado

A fim de determinar se o processamento de dados está em conformidade com a lei e estabelecer quais as salvaguardas de proteção de dados que devem ser aplicadas, é uma pré-condição necessária para identificar a (s) finalidade (s) específica (s) para as quais é exigida a coleta de dados pessoais. A especificação de finalidade, portanto, estabelece limites para as finalidades para as quais os controladores podem usar os dados pessoais coletados e ajuda a estabelecer as salvaguardas de proteção de dados necessárias.

A especificação do objetivo requer uma avaliação interna realizada pelo controlador de dados e é uma condição necessária para a prestação de contas. É um primeiro passo fundamental que um controlador deve seguir para garantir a conformidade com a lei de proteção de dados aplicável. O controlador deve identificar quais são as finalidades e documentar e demonstrar que realizou essa avaliação interna.

Fonte: Parecer do WP29 sobre limitação de finalidade (acessado em 24 de julho de 2019)

Como a coleta de dados pessoais está processando dados pessoais, o objetivo deve ser especificado antes da coleta de dados pessoais.

A especificação de finalidade deve ser detalhada o suficiente para determinar que tipo de processamento está e não está incluído no objetivo especificado. Um objetivo vago ou geral, como "melhorar a experiência dos usuários", "fins de marketing" ou "pesquisas futuras", sem mais detalhes, geralmente não atende aos critérios de ser "específico". Uma mensagem para o titular dos dados de que "as informações de navegação são processadas para apresentar anúncios relacionados aos seus interesses" relacionaria exatamente qual é o objetivo e como é alcançado.

3.1.1.2 Explícito

Os dados pessoais devem ser coletados para fins explícitos. Os objetivos da coleta não devem ser especificados apenas na mente das pessoas responsáveis pela coleta de dados. Eles também devem ser explicitados. Em outras palavras, elas devem ser claramente reveladas, explicadas ou expressas de alguma forma inteligível. Segue-se da análise anterior que isso deve acontecer o mais tardar, no momento em que ocorra a coleta de dados pessoais.

O objetivo final deste requisito é garantir que os objetivos sejam especificados sem imprecisão ou ambiguidade quanto ao seu significado ou intenção. O que se entende deve ser claro e não deve deixar dúvida ou dificuldade de compreensão. A especificação dos fins deve, em particular, ser expressa de forma a ser entendida da mesma forma não apenas pelo controlador (incluindo todo o pessoal relevante) e por quaisquer terceiros processadores, mas também pelas autoridades de proteção de dados e os titulares de dados em causa. Deve-se tomar cuidado especial para assegurar que qualquer especificação do objetivo seja suficientemente clara para todos os envolvidos, independentemente de suas diferentes origens culturais / linguísticas, nível de compreensão ou necessidades especiais.

Fonte: Parecer do WP29 sobre limitação de finalidade, § III.1.1. (acessado em 30 de março de 2017)

A especificação da finalidade explícita torna transparente como os controladores pretendem usar os dados pessoais coletados. Ela ajuda todos aqueles que processam dados em nome do controlador, bem como os sujeitos de dados, Autoridades Supervisoras e outras partes interessadas a ter um entendimento comum de como os dados podem ser usados. Isso, por sua vez, reduz o risco de que as expectativas dos titulares de dados sejam diferentes das expectativas do controlador.

3.1.1.3 Legítimo

A exigência de legitimidade significa que as finalidades para o processamento de dados devem estar de acordo com a lei no sentido mais amplo (Artigo GDPR 6(3)). Isso inclui todas as formas de direito comum e escrito, legislação primária e secundária, decretos municipais, precedentes judiciais, princípios constitucionais, direitos fundamentais, outros princípios jurídicos, bem como jurisprudência, como tal lei seria interpretada e consideradas pelos tribunais competentes.

Além de qualquer outra lei, o Artigo 6 (1) do GDPR se aplica sempre ao processamento de dados pessoais. Para que o processamento seja legal, ele deve **sempre** ser baseado em pelo menos um dos seis motivos legítimos de processamento (ver 7.3.3).

3.1.2 Proporcionalidade e Subsidiariedade

3. Nos termos do princípio da subsidiariedade, nos domínios que não são da sua competência exclusiva, a União só deve atuar se e na medida em que os objetivos da ação proposta não possam ser suficientemente realizados pelos Estados-Membros, quer a nível central, quer a nível regional e local, mas, pelo contrário, podem, devido à escala ou aos efeitos da ação proposta, ser melhor alcançados ao nível da União. (...)

4. Ao abrigo do princípio da proporcionalidade, o conteúdo e a forma da ação da União não devem exceder o necessário para alcançar os objetivos dos Tratados.

Fonte: Tratado sobre o Funcionamento da União Europeia art. 5

Isso parece longe da prática de proteger a privacidade e os dados pessoais, mas não é. Esses princípios formam um fio condutor em todo o GDPR até o nível prático.

3.1.2.1 Subsidiariedade

Além deste tratado, a subsidiariedade também é encontrada na regra geral que exige que os dados pessoais só possam ser processados **se não houver outros meios para atingir esses objetivos**. Cinco das seis bases legais para o processamento exigem que o processamento seja absolutamente necessário. Quando existem outros meios para atingir esses objetivos, é difícil sustentar que o processamento de dados pessoais é necessário.

Por exemplo, suponha que se queira descobrir quantas pessoas andam numa rua comercial em uma tarde média de sábado. Para esse fim, não é necessário identificar os indivíduos. Seria possível contar indivíduos com um smartphone usando o sinal de seu smartphone (um endereço MAC, por exemplo). No entanto, como um endereço MAC pode ser rastreado até a pessoa que possui o smartphone, esse sinal é considerado dado pessoal. Definitivamente, existem outras maneiras de contar o número de pessoas que passam pela rua sem usar dados pessoais. Pode-se, por exemplo, postar observadores e simplesmente contar indivíduos. O princípio de subsidiariedade no GDPR significaria que o uso do endereço MAC é um uso ilegal de dados pessoais, porque seu interesse em contar o número de visitantes é anulado pelo direito fundamental à privacidade dos visitantes. Você terá que usar um método que mantenha os visitantes anônimos e não colete dados pessoais diretos ou indiretos.

3.1.2.2 Proporcionalidade

O princípio da proporcionalidade está intimamente relacionado à subsidiariedade. A proporcionalidade exige que qualquer ação da UE não ultrapasse o necessário para alcançar os objetivos dos Tratados. Quando aplicado ao processamento de dados pessoais, isso significa que não devem ser coletados mais dados do que o estritamente necessário. Achamos isso no nível prático, com o princípio de minimização de dados: 'os dados pessoais devem ser adequados, relevantes e limitados ao necessário em relação às finalidades para os quais são processados'. Isso parece óbvio, mas todos sabemos exemplos em que mais informações são coletadas do que o estritamente necessário para a finalidade especificada. Por exemplo, quando uma loja virtual

coleta dados sobre sexo em seu formulário de endereço de entrega, enquanto isso não é necessário para enviar seu produto ao cliente.

4 Direitos dos Titulares dos Dados

Desde o histórico de privacidade e proteção de dados, vimos que os direitos fundamentais do titular dos dados são considerados de extrema importância. O GDPR declara que o processamento de dados pessoais é proibido, exceto quando vários requisitos são atendidos. Deve haver uma razão legal para o processamento. O objetivo do processamento deve ser claramente especificado. E mesmo assim, se houver outros meios além do processamento de dados pessoais para atingir o objetivo especificado, esses outros meios deverão ser utilizados.

Mesmo quando todos os requisitos são atendidos, o responsável pelo tratamento deve sempre equilibrar os direitos fundamentais do titular dos dados com os objetivos do processamento. Não é de admirar que uma seção relativamente grande do GDPR seja dedicada aos direitos de um titular de dados.

4.1 Informação Transparente, Comunicação e Modalidades

Uma ideia básica no GDPR é que o titular dos dados deve ser **informado** sempre que seus dados pessoais forem processados. Se o processamento for baseado no consentimento, o titular dos dados deve saber e entender com o que está consentindo ('consentimento informado').

Quando o processamento é baseado em um ou mais dos outros motivos legítimos, o titular dos dados ainda deve ser informado sobre quais dados pessoais são processados, com que finalidade e quem é responsável. E por "saber" e "ser informado", o GDPR significa explicitamente "estar ciente" e "entendê-lo".

O controlador deve tomar as medidas adequadas para prestar as informações referidas nos Artigos 13 e 14 e qualquer comunicação nos termos dos Artigos 15 a 22 e 34 relativas ao processamento à pessoa em causa, de forma concisa, transparente, inteligível e facilmente acessível, utilizando linguagem clara e simples, em particular para qualquer informação dirigida especificamente a uma criança. As informações devem ser fornecidas por escrito ou por outros meios, incluindo, quando apropriado, por meios eletrônicos. Quando solicitado pelo titular dos dados, a informação pode ser fornecida oralmente, desde que a identidade do titular dos dados seja comprovada por outros meios.

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Artigo 12(1)

Os artigos citados acima são discutidos nos parágrafos seguintes. Eles detalham os vários direitos que os titulares de dados têm quando seus dados pessoais serem processados.

O responsável pelo tratamento facilita o exercício dos direitos dos titulares de dados nos termos dos artigos 15 a 22. Nos casos referidos no artigo 11(2), o responsável pelo tratamento não deve recusar-se a agir a pedido do titular dos dados no exercício dos seus direitos ao abrigo dos artigos 15 a 22, a menos que o controlador demonstre que não está em posição de identificar o titular dos dados.

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Artigo 12(2)

Existem duas exceções importantes para agir a pedido de um titular de dados.

- Em primeiro lugar, os controladores podem (e geralmente devem) exigir que os titulares de dados forneçam prova de identidade. Isso ajuda a limitar o risco de terceiros obterem acesso ilegal a dados pessoais.

- Em segundo lugar, o controlador está isento da sua obrigação de cumprir certos direitos dos titulares de dados se não conseguir identificar quais os dados relevantes em sua posse que se relacionam com o titular dos dados.

O segundo parágrafo do Artigo 12 é pelo menos tão importante. É ótimo ter o direito a algo, mas nem todo mundo se sente suficientemente empoderado para exercer seus direitos quando alguma empresa ou instituição governamental lhes diz que pretendem realizar processamento de seus dados.

De acordo com o Artigo 12 (2), um planejamento de processamento do controlador deve informar aos titulares dos dados sobre os direitos que eles têm e ajudá-los a exercer esses direitos. As informações sobre o processamento pretendido mencionadas anteriormente e a assistência ao titular dos dados devem ser fornecidas gratuitamente. Ao ignorar esta obrigação, um controlador corre riscos enormes (ver 7.3.3).

4.2 Informação sobre e acesso a dados pessoais

Para além das informações referidas no parágrafo 1, o controlador fornecerá ao titular dos dados, no momento da obtenção dos dados pessoais, as informações adicionais necessárias para garantir um processamento justo e transparente:

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Artigo 13(2)

4.2.1 Informações fornecidas ao titular dos dados em qualquer caso

Existem pequenas diferenças nas informações que devem ser fornecidas ao titular dos dados, dependendo se os dados pessoais a serem processados estão sendo coletados do titular dos dados (GDPR Artigo 13) ou de outras fontes (GDPR Artigo 14).

Em todos os casos, o controlador deve fornecer:

- a identidade e os dados de contato do controlador e do seu representante, se for o caso
- os detalhes de contato do DPO, quando aplicável
- as finalidades do processamento para o qual os dados pessoais se destinam
- a base jurídica para o processamento
- o período pelo qual os dados pessoais serão armazenados (período de retenção) ou, caso isso não seja possível, o critério usado para determinar o período
- a existência do direito de solicitar ao controlador:
    - o acesso aos seus dados pessoais
    - a retificação ou apagamento de seus dados pessoais
    - a restrição de processamento
    - a contestação do processamento bem como o direito de portabilidade dos dados
- caso o processamento se baseie no consentimento, a existência do direito de retirar o consentimento a qualquer momento, sem afetar a legalidade do processamento com base no consentimento antes de sua retirada
- o direito de apresentar uma reclamação a uma autoridade supervisora
- os interesses legítimos perseguidos pelo responsável pelo tratamento ou por terceiros (se houver)

4.2.2 Informações a serem fornecidas ao titular dos dados ao transferir dados pessoais

Caso o controlador pretenda transferir dados pessoais para um país terceiro ou organização internacional, devem ser fornecidos detalhes adicionais:

- Os destinatários ou categorias de destinatários dos dados pessoais

E caso esta transferência seja para um destinatário fora da EEA ou uma organização internacional:
- o fato de o controlador pretender transferir dados pessoais a um destinatário em um país terceiro ou organização internacional
- a existência de uma decisão de adequação por parte da Comissão ou, se não houver, as garantias apropriadas em vigor

4.2.3 Informações adicionais a serem fornecidas quando dados pessoais não forem obtidos diretamente do titular dos dados

Caso os dados pessoais não tenham sido obtidos diretamente do titular dos dados, algumas informações adicionais devem ser fornecidas:

- as categorias de dados pessoais em causa
- de qual fonte os dados pessoais se originam e, se aplicável, se vieram de fontes publicamente acessíveis

4.2.4 Momento da informação a ser fornecida

O controlador deve fornecer as informações acima referidas:

- num prazo razoável após a obtenção dos dados pessoais, mas o mais tardar no prazo de um
- tendo em conta as circunstâncias específicas em que os dados pessoais são tratados,
- se os dados pessoais devem ser utilizados para comunicação com a pessoa em causa, o mais tardar no momento da primeira comunicação a essa pessoa ou,
- se for prevista a divulgação a outro destinatário, o mais tardar quando os dados pessoais forem divulgados pela primeira vez.

Existem algumas obrigações extras para casos especiais e algumas exceções a essas regras. Veja o Artigo 15(4) do GDPR.

4.3 Direto de Acesso (Inspeção) pelo Titular dos Dados

O titular dos dados tem o direito de obter, a partir da confirmação do controlador, se os dados pessoais que lhe dizem respeito estão ou não a ser processados e, se for esse o caso, o acesso aos dados pessoais (...)

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Artigo 15(1).

Não obstante as regras sobre ser informado, como detalhadas anteriormente, o titular dos dados tem, a qualquer momento, o direito de obter informações do controlador sobre se os dados pessoais relativos a ele estão sendo processados.

E se os dados estiverem sendo processados, o controlador é obrigado a fornecer as informações mencionadas acima e uma cópia dos dados sendo processados gratuitamente. Cópias adicionais dos dados podem ser cobradas do titular dos dados, mas apenas a um preço razoável com base nos custos administrativos.

Uma restrição importante ao direito do titular dos dados de obter uma cópia dos dados pessoais processados ou a serem processados é que a solicitação não pode afetar adversamente os direitos e liberdades de terceiros.

4.4 Retificação e Eliminação

4.4.1 Direito à retificação

Naturalmente, quando um titular de dados recebe uma cópia dos dados pessoais do controlador, o titular dos dados pode achar que os dados estão incorretos. Nesse caso, o titular dos dados pode exigir uma correção:

O titular dos dados terá o direito de obter do controlador, sem demora injustificada, a retificação de dados pessoais incorretos que lhe digam respeito. Tendo em conta os fins do processamento, o titular dos dados tem o direito de fornecer dados pessoais incompletos, incluindo através de uma declaração suplementar.

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Artigo 16.

4.4.2 Direito ao apagamento (direito de ser esquecido)

Os titulares de dados têm o direito de ter seus dados "apagados" em certos casos. Esse caso geralmente ocorre quando o processamento falha em atender aos requisitos do GDPR. O direito pode ser exercido contra os controladores, que devem responder sem atrasos indevidos (e em qualquer caso dentro de um mês, embora isso possa ser estendido em casos difíceis)

O titular dos dados tem o direito de obter do controlador o apagamento de dados pessoais que lhe digam respeito sem demora injustificada e o controlador tem a obrigação de apagar os dados pessoais sem demora indevida (...)

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Artigo 17.

Motivos para ter dados pessoais apagados podem ser:

- os dados não são mais necessários para as finalidades de processamento
- retirada do consentimento
- os dados foram coletados para uma oferta de serviços de informação diretamente a uma criança menor de 16 anos.
- objeções ao processamento (veja abaixo)
- processamento Ilegal
- conformidade com a legislação da União ou do Estado-Membro aplicável ao controlador

O direito de apagar por esses motivos só tem efeito quando o motivo específico era o único motivo legítimo para processamento. Por exemplo, os titulares de dados que exigem que o governo apague os dados pessoais necessários para calcular seu imposto de renda porque eles não consentem mais não terão êxito, porque nesse caso 'consentimento' não era motivo para processamento legítimo.

4.4.3 Direito à limitação do processamento

Os titulares dos dados têm o direito de restringir o controlador ao processar seus dados em certos casos. Os motivos para restringir o processamento podem ser:

- A precisão dos dados é contestada pelo titular dos dados
    - o processamento dos dados pessoais é restrito pelo tempo necessário para verificar a reivindicação e retificar os dados
- o processamento é ilegal e o titular dos dados se opõe ao apagamento dos dados pessoais

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

O que significa o processamento restrito?

Quando o processamento tiver sido restringido pelo parágrafo 1, tais dados pessoais, com exceção do armazenamento, somente serão processados com o consentimento do titular dos dados ou para o estabelecimento, exercício ou defesa de reivindicações legais ou para a proteção dos direitos de pessoa jurídica ou por razões de interesse público importante da União ou de um Estado-Membro.

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Artigo 18(2).

O controlador deve notificar o assunto dos dados antes de levantar uma restrição.

4.4.4 Obrigação de notificação (retificação/eliminação/limitação do processamento)

O controlador comunicará a retificação ou o apagamento de dados pessoais ou a restrição de processamento efetuados nos termos do Artigo 16, do Artigo 17(1) e do Artigo 18 a cada destinatário a quem tenham sido divulgados dados pessoais, salvo se tal for impossível ou envolver esforços desproporcionais. O controlador deve informar o titular dos dados sobre esses destinatários, se o titular dos dados assim solicitar.

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Artigo 19.

Essa obrigação significa que, além de implementar sistemas e procedimentos para garantir os direitos do titular dos dados, os controladores precisam implementar sistemas e procedimentos para notificar terceiros afetados sobre o exercício desses direitos.

Cartoon © Pierre Kroll, derived with authorization from the leaflet 'Take Control of your Personal Data' (2012), ISBN 978-92-79-22654-0, Published by European Commission - Directorate-General for Justice

4.4.5 Direito à portabilidade dos dados

O titular dos dados tem o direito de receber os dados pessoais que lhe são fornecidos, que forneceu a um controlador, num formato estruturado, normalmente utilizado e legível por máquina, e tem o direito de os transmitir para outro controlador sem impedimento do controlador para o qual os dados pessoais foram fornecidos, (…).

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Artigo 20.

Se o processamento é baseado no consentimento ou em um contrato, **e** o processamento é realizado por meios automatizados, os titulares dos dados têm o direito de receber os dados pessoais ou transferir seus dados pessoais entre os controladores. Os titulares dos dados têm o direito de mover os detalhes da conta de uma plataforma online para outra.

Esse direito facilita a troca de clientes para outro fornecedor on-line, como lojas da web ou outros negócios on-line. A criação de uma nova conta deve se tornar mais fácil, porque o controlador deve permitir que as informações da conta sejam transferidas para um concorrente.

Note-se que o direito à portabilidade de dados **não** se aplica ao processamento necessário para o desempenho de uma tarefa realizada no interesse público ou no exercício da autoridade oficial conferida ao controlador.

4.5 Direito de Contestar e Automatizar a Tomada de Decisão Individual

4.5.1 Direito a objetar

Conforme estabelecido no 3.1, um controlador deve ter uma base legal para o processamento de dados pessoais. No entanto, quando essa base legal é ou 'interesse público' ou 'interesses legítimos' (incluindo a definição de perfis), os titulares de dados podem ter o direito de se opor a esse processamento.

O GDPR exige que a organização demonstre que possui bases convincentes para continuar o processamento ou que o processamento é necessário em conexão com seus direitos legais. Se não puder demonstrar que um desses dois fundamentos se aplicam, deve cessar essa atividade de processamento.

4.5.2 Tomada de decisão individual automatizada, incluindo criação de perfil

Quando dados pessoais são processados para fins de marketing direto, o titular dos dados deve ter o direito de se opor a tal processamento, incluindo o perfil na medida em que está relacionado a tal marketing direto, seja em relação ao processamento inicial ou posterior, em qualquer tempo e gratuitamente. Esse direito deve ser explicitamente levado à atenção do titular dos dados e apresentado de forma clara e separada de qualquer outra informação.

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Rec.70.

Os titulares dos dados têm o direito de se opor ao processamento de dados pessoais para fins de marketing direto, incluindo a criação de perfis.

O Artigo 22(1) acrescenta que o titular dos dados tem o direito de não ser objeto de uma decisão baseada exclusivamente no processamento automatizado. Este parágrafo, no entanto, não se aplica se a decisão for baseada no consentimento explícito e informado do titular dos dados.

4.6 Direito de Apresentar queixa junto a uma Autoridade Supervisora

Sem prejuízo de qualquer outra solução administrativa ou judicial, todos os titulares dos dados têm o direito de apresentar uma queixa a uma autoridade de controlo, em especial no Estado-Membro da sua residência habitual, local de trabalho ou local da alegada violação se o titular dos dados considera que o processamento de dados pessoais que lhe digam respeito viola o presente regulamento.

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Artigo 77(1).

Os titulares dos dados têm o direito de apresentar uma reclamação relativa ao processamento dos seus dados pessoais junto a Autoridade Supervisora do Estado-Membro onde residem ou no Estado-Membro em que a alegada violação ocorreu. O GDPR contém regras para garantir que o direito dos dados sujeitos a um recurso judicial efetivo seja mantido por todas as partes, incluindo controlador ou controladores, processador ou processadores ou Autoridades Supervisoras envolvidas.

5 Violações de Dados e Procedimentos Relacionados

5.1 O Conceito de Violação de Dados Pessoais

Violação de dados pessoais é uma violação da segurança que conduz à destruição acidental ou ilegal, perda, alteração, divulgação não autorizada ou acesso a dados pessoais transmitidos, armazenados ou tratados de outro modo;

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Artigo 15(1).

No GDPR, uma violação de dados pessoais é **sempre** um incidente de segurança. Não é apenas uma vulnerabilidade (risco à segurança) ou uma ameaça à segurança. O pesadelo do gerente de segurança acaba de se tornar realidade e alguém teve acesso aos dados.

Para uma violação de dados pessoais, o incidente de segurança deve ter levado a uma situação em que os dados pessoais foram ou podem ter sido processados ilegalmente. Isso significa que nem todo incidente de segurança é uma violação de dados pessoais. Lembre-se de que destruir, armazenar e copiar também é considerado processamento.

Os artigos sobre violações de dados pessoais geralmente dão exemplos de cenários que incluem hackers mal-intencionados ou benignos e terceiros obtendo acesso não autorizado a dados pessoais. No entanto, a definição do GDPR de violação de dados pessoais é muito mais ampla.

Um incêndio em um data center pode destruir os dados pessoais armazenados lá. Isso tornaria um incidente de segurança, porque os dados não estão mais disponíveis, e uma violação de dados pessoais, porque os dados pessoais foram processados, neste caso destruídos, sem autorização.

De maneira semelhante, quando um processador exclui acidentalmente um conjunto de dados pessoais, ele viola o artigo 29 do GDPR, o que torna o processamento ilegal:

O processador e qualquer pessoa que atue sob a autoridade do controlador ou do processador, que tenha acesso a dados pessoais, não devem processar esses dados, salvo instruções do controlador, a menos que tal seja exigido pela legislação da União ou do Estado-Membro.

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Artigo 29.

Na literatura, o termo "violação de dados" é frequentemente usado onde se entende por "violação de dados pessoais". A diferença é que uma 'violação de dados' também pode, dependendo do contexto, se referir a uma violação em que dados comerciais ou de outra empresa estão comprometidos. Uma violação de dados pessoais é sempre uma violação de dados. Uma violação de dados é apenas uma violação de dados pessoais quando dados pessoais estão envolvidos.

5.2 Procedimento sobre como agir quando ocorre violação de dados pessoais

O artigo 32 do GDPR exige que **tanto controladores quanto processadores** 'implementem medidas técnicas e organizacionais apropriadas para garantir um nível de segurança adequado ao risco'.

Normas de segurança da informação internacionalmente aceitas, como ISO / IEC 27001, geralmente estarão em vigor. Essas normas têm procedimentos para lidar com um incidente com o objetivo de reparar o dano e impedir a recorrência do incidente.

Uma violação de dados pessoais pode, se não tratada de maneira apropriada e oportuna, resultar em danos físicos, materiais ou imateriais a pessoas físicas, tais como perda de controle sobre seus dados pessoais ou limitação de seus direitos, discriminação, roubo de identidade ou fraude. Perda financeira, reversão não autorizada de pseudonimização, dano à reputação, perda de confidencialidade de dados pessoais protegidos pelo sigilo profissional ou por qualquer outra desvantagem econômica ou social significativa para a pessoa natural em causa.

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Recital (85).

5.2.1 Notificação de uma violação de dados pessoais à Autoridade Supervisora

No caso de uma violação de dados pessoais, os controladores de dados devem notificar a **Autoridade Supervisora**. O aviso deve ser fornecido "sem demora indevida e, quando possível, o mais tardar 72 horas após ter tomado conhecimento do mesmo".

Quando a violação de dados pessoais é relatada depois de 72 horas após a observação da violação de dados pessoais, um bom motivo para o atraso deve ser enviado com a notificação.

O Artigo 33(1), porém, contém uma exceção importante ao requisito de notificação de violação de dados: a notificação **não** é exigida se "for improvável que a violação de dados pessoais resulte em um risco para os direitos e liberdades das pessoas físicas".

5.2.2 Notificação de uma violação de dados pessoais ao controlador

Quando um processador de dados experimenta uma violação de dados pessoais, ele deve notificar o **controlador** ' sem atrasos indevidos após tomar conhecimento de uma violação de dados pessoais '.

O processador não tem outra obrigação de notificação ou relatório sob o GDPR. Todas as outras notificações e relatórios devem ser feitos pelo controlador.

5.2.3 Notificação de uma violação de dados pessoais ao titular afetado

Se o controlador determina que a violação de dados pessoais "pode resultar num risco elevado para os direitos e liberdades dos indivíduos", deve também comunicar informações relativas à violação de dados pessoais aos **titulares de dados** afetados. Isso deve ser feito de acordo com o Artigo 34, "sem demora indevida".

Existem três exceções à exigência adicional de notificar os titulares dos dados. A notificação ao titular dos dados **não** é obrigatória nas seguintes circunstâncias:

- quando os dados estiverem ilegíveis
- quando outras medidas são tomadas para minimizar o risco
- quando notificar é um esforço desproporcional

5.2.3.1 Criptografia, etc.

O controlador "implementou medidas apropriadas de proteção técnica e organizacional" que "tornam os dados ininteligíveis para qualquer pessoa que não esteja autorizada a acessá-los, como a criptografia".

5.2.3.2 Medidas de mitigação

O controlador toma as medidas subsequentes à violação de dados pessoais para «garantir que o elevado risco para os direitos e liberdades das pessoas em causa» não é provável que se materialize.

5.2.3.3 Esforço desproporcional

Quando a notificação para cada titular dos dados "envolveria um esforço desproporcional". Nesse caso, medidas alternativas de comunicação podem ser usadas, como uma notificação no site da empresa.

5.3 Categorias de violações de dados pessoais

É possível distinguir três categorias de violação de dados pessoais. Violações de dados pessoais que:

- Seja **improvável** que resultem em risco para os direitos e liberdades das pessoas singulares;
  - (notificação da violação não é obrigatória)
- **Pode** resultar em danos físicos, materiais ou não- materiais às pessoas
  - (a notificação à Autoridade Supervisora é obrigatória)
- **Provavelmente** resultará em um alto risco para os direitos e liberdades dos indivíduos
  - (a notificação à Autoridade Supervisora e
  - Notificação ao titular dos dados é obrigatória - se possível)

Organizando a Proteção de Dados

6 Importância da proteção de dados para a organização

Quase todas as organizações processam dados pessoais. Para uma organização que processa dados pessoais, a proteção de dados não é apenas "um requisito da lei" ou "importante para evitar multas". A reputação da organização está em risco.

O processamento de dados pessoais de maneira profissional significa garantia de qualidade, gerenciamento de segurança e governança.

Os parágrafos a seguir descrevem os requisitos para o processamento legal de dados pessoais.

6.1 Requisitos para cumprir com a o GDPR

De acordo com o GDPR, o processamento de dados pessoais é proibido, a menos que os requisitos do GDPR sejam atendidos. Os seguintes requisitos devem ser atendidos:

6.1.1 Princípios relativos ao processamento de dados pessoais são cumpridos

Em particular, os princípios de proteção de dados estabelecidos no parágrafo 2.1 devem ter sido satisfeitos. O objetivo deve ser claro, detalhado e especificado, e pelo menos um dos seis possíveis “fundamentos legais para o processamento” deve ser aplicado. Os direitos do titular de dados devem ser garantidos e medidas adequadas de proteção de dados devem estar em vigor.

6.1.2 Estrutura legal

O GDPR requer controladores, processadores e, na verdade, qualquer pessoa que, em um determinado momento, processe dados pessoais para cumprir com o GDPR. O controlador, como aquele que determina as finalidades e os meios de processamento, é obrigado a implementar medidas técnicas e organizacionais apropriadas para assegurar que o processamento seja realizado de acordo com o GDPR.

Como vimos no parágrafo 1.4.1, o controlador **também** é responsável por ter essas “medidas apropriadas” implementadas pelo processador para garantir que o processamento ocorra em conformidade com os princípios de processamento de dados estabelecidos no regulamento (ver também o parágrafo 2.1). Como consequência, um processador não pode terceirizar parte do processamento para um subprocessador sem autorização prévia específica ou geral por escrito do controlador.

O processador somente processa os dados pessoais baseado em instruções documentadas do controlador. É obrigatória a existência de um contrato legalmente vinculante entre o processador e o controlador e que defina:

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

Para poder **demonstrar conformidade** com os requisitos, o controlador e o processador devem documentar como eles estão em conformidade. Alguns dos documentos que mostram conformidade são obrigatórios e no formato prescrito. Os outros documentos são necessários quando algo der errado ou quando houver uma razão adicional para que a Autoridade Supervisora inspecione a conformidade com o regulamento.

6.1.3 Avaliação de Impacto

Quando um tipo de processamento, em especial utilizando novas tecnologias, e tendo em conta a natureza, âmbito, contexto e finalidades do processamento, possa resultar num risco elevado para os direitos e liberdades das pessoas singulares, o controlador processamento, proceder a uma avaliação do impacto das operações de processamento previstas na proteção de dados pessoais.

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Artigo 35(1)

Diretrizes publicadas estão disponíveis indicando em quais casos de processamento uma Avaliação de Impacto sobre a Proteção de Dados (DPIA) precisa ser realizada.

Em vez de DPIA, muitas vezes o termo PIA (avaliação do impacto na privacidade) é usado. No contexto do GDPR, os dois termos descrevem a mesma avaliação. O que uma DPIA compreende e seus objetivos são discutidos no tópico 8.3.

6.1.4 Controlador - contrato do processador

Quando o controlador quiser terceirizar parte da operação de processamento para outra parte, o qual se torna um processador, um contrato legal deve estar em vigor. Os detalhes de tal contrato são descritos no tópico 8.2.

6.1.5 Consulta prévia

O controlador deve consultar a Autoridade Supervisora antes do processamento quando a avaliação de impacto sobre a proteção de dados prevista no Artigo 35 indicar que o processamento resultaria num risco elevado, na ausência de medidas adotadas pelo controlador para atenuar o risco.

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Artigo 36(1).

Em contraste com os requisitos da diretiva 95/46 / EC, o GDPR declara que o responsável pelo tratamento não tem a obrigação de consultar previamente uma Autoridade Supervisora para todas as operações de processamento. A consulta prévia com a Autoridade Supervisora só é necessária se uma DPIA indicar um **alto risco** para a privacidade ou direitos e liberdades de pessoas físicas.

6.2 Tipos Requeridos de Administração

6.2.1 Registro de atividades de processamento

Cada controlador e, quando aplicável, o representante do controlador deve manter um registro das atividades de processamento sob sua responsabilidade.
Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Artigo 30(1).

O **registro do controlador** deve conter:

(a) O nome e detalhes de contato do (s) controlador (es) ou seus representantes e DPO
(b) as finalidades do processamento
(c) uma descrição das categorias de titulares de dados e categorias de dados pessoais
(d) as categorias de destinatários a quem tenham sido ou venham a ser divulgados os dados pessoais, incluindo destinatários em países terceiros ou organização internacional s
(e) quando aplicável, as transferências de dados pessoais para um país terceiro ou uma organização internacional, incluindo a identificação desse país ou organização internacional (...)
(f) sempre que possível, os prazos previstos para o apagamento das diferentes categorias de dados
(g) sempre que possível, uma descrição geral das medidas técnicas e organizativas de segurança

O Artigo 30 requer o controlador para manter um 'registro de atividades de processamento sob sua responsabilidade.

No caso de um processador realizar atividades de processamento na instrução do controlador, o processador também precisa manter registros:

Cada processador e, quando aplicável, o representante do processador deve manter um registro de todas as categorias de atividades de processamento realizadas em nome de um controlador, (...)

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Artigo 30(2).

O **registro do processador** deve conter:

(a) o nome e detalhes de contato do (s) processador (es) e de cada controlador em nome do qual o processador está agindo e, quando aplicável, do representante do controlador ou do processador e do Data Protection Officer (DPO)
(b) as categorias de processamento realizadas em nome de cada controlador
(c) se for caso, transferências de dados pessoais para um país terceiro ou uma organização internacional, incluindo a identificação desse país terceiro ou organização internacional (...)
(d) sempre que possível, uma descrição geral das medidas técnicas e organizativas de segurança

Os registros de controladores e processadores não são necessariamente os mesmos. O controlador pode usar vários processadores. Um processador pode estar sob contrato com vários controladores.

Há uma **exceção** à obrigação para pequenas empresas e organizações:

A obrigação de manter registos de todas as atividades de processamento não se aplica a organizações ou empresas que empreguem menos de 250 pessoas, a menos que o seu processamento possa resultar num 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 (...).

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Artigo 30(5).

Na prática, essa exceção ajuda apenas até certo ponto, uma vez que não isenta o controlador da obrigação de demonstrar conformidade.

6.2.2 Registro de violações de dados pessoais

O controlador deve documentar quaisquer violações de dados pessoais, incluindo os factos relacionados com a violação de dados pessoais, os seus efeitos e as medidas corretivas adotadas. Essa documentação deve permitir à Autoridade Supervisora verificar o cumprimento do presente Artigo.

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Artigo 33(5).

Os fatos relativos à violação de dados pessoais são:

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

7 Autoridades Supervisoras

Mesmo antes da introdução do GDPR, foi criado um sistema de “autoridades supervisoras” de cooperação estreita. Muitas vezes eles são chamados de 'Autoridade de Proteção de Dados' (DPA) ou uma tradução desse termo no idioma local.

O estabelecimento de Autoridades Supervisoras nos Estados-Membros, habilitadas a desempenhar as suas funções e a exercer os seus poderes com total independência, é uma componente essencial da proteção das pessoas singulares no que diz respeito ao processamento dos seus dados pessoais. Os Estados-Membros devem poder estabelecer mais do que uma Autoridade Supervisora para refletir a sua estrutura constitucional, organizacional e administrativa.

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; item 117.

Os membros da AEE podem estabelecer várias Autoridades Supervisoras. A Alemanha tem uma Autoridade Supervisora para cada um dos 16 estados. A maioria dos membros da AEE tem uma única Autoridade Supervisora nacional.

A independência das Autoridades Supervisoras é uma parte importante da estrutura:

1. As autoridades de controlo agem com total independência no desempenho das suas funções e no exercício das suas competências em conformidade com o presente regulamento.
2. O membro ou os membros de cada autoridade de controlo, no exercício das suas funções e no exercício das suas competências em conformidade com o presente regulamento, permanecem isentos de influência externa, direta ou indireta, e não solicitam nem aceitam instruções de qualquer pessoa.
3. Os membros ou membros de cada Autoridade Supervisora devem abster-se de qualquer ação incompatível com as suas obrigações e não devem, durante o seu mandato, exercer qualquer ocupação incompatível, lucrativa ou não.
4. Cada Estado-Membro deve assegurar que cada autoridade de controle disponha dos recursos humanos, técnicos e financeiros, das instalações e infraestruturas necessárias ao desempenho eficaz das suas funções e do exercício das suas competências, incluindo as que são realizadas no contexto de mútua assistência, cooperação e participação no Conselho.
5. Cada Estado-Membro deve assegurar que cada autoridade de controlo escolha e possua o seu próprio pessoal, o qual ficará sujeito à direção exclusiva do membro ou dos membros da Autoridade Supervisora em causa.
6. Cada Estado-Membro deve assegurar que cada Autoridade Supervisora seja sujeita a um controlo financeiro que não afete a sua independência e que tenha orçamentos anuais públicos separados, que possam fazer parte do orçamento geral ou do Estado.

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Artigo 52).

7.1 Responsabilidades Gerais de uma Autoridade Supervisora

A principal responsabilidade de uma Autoridade Supervisora é **monitorar e fazer cumprir a aplicação** do GDPR com o objetivo de **proteger** os direitos e liberdades fundamentais das pessoas singulares em relação ao processamento e facilitar o livre fluxo de dados pessoais na União (Artigo 51).

Outra importante responsabilidade é promover a conscientização pública e a compreensão dos riscos, regras, salvaguardas e direitos em relação ao processamento de dados pessoais. As atividades dirigidas especificamente às crianças devem receber atenção extra.

A lista de 'tarefas' detalhadas no Artigo 57(1) do GDPR é longa e aberta, pois a última da lista é ' cumprir qualquer outra tarefa relacionada à proteção de dados pessoais '.

Abaixo as várias tarefas são resumidas e categorizadas em grupos.

7.1.1 Acompanhar e fazer cumprir a aplicação do regulamento

A Autoridade Supervisora monitora a aplicação do GDPR.

Isso pode ser **preventivo**, monitorando desenvolvimentos relevantes ou conduzindo investigações, sempre que tenham impacto na proteção de dados pessoais.

Pode também ser **remediadora**, investigando operações de processamento, incluindo investigações baseadas em reclamações de titulares de dados, organizações ou associações e em informações recebidas de outra Autoridade Supervisora ou outra autoridade pública.

A Autoridade Supervisora também pode realizar uma revisão periódica das certificações emitidas aos controladores de acordo com o Artigo 42 (7).

7.1.2 Aconselhar e promover a conscientização

Em conformidade com a legislação do membro da AEE, a Autoridade Supervisora aconselha o parlamento nacional, o governo e outras instituições e organismos relacionados com a proteção dos direitos e liberdades das pessoas singulares em relação ao processamento.

A Autoridade Supervisora também dá conselhos sobre as operações de processamento, seja para promover a conscientização dos controladores e processadores de suas obrigações sob o GDPR ou mais específico em resposta a uma solicitação de consulta de um controlador ou no curso de uma investigação após uma notificação de violação de dados.

Por outro lado, a pedido, a Autoridade Supervisora fornecerá também informações a qualquer titular de dados sobre o exercício dos seus direitos ao abrigo do GDPR e, se for caso disso, cooperará com as Autoridades Supervisoras de outros Estados-Membros para esse efeito.

7.1.3 Administrar violações de dados e outras violações

A Autoridade Supervisora manterá registros internos de infrações do GDPR e de medidas tomadas de acordo com os poderes da Autoridade Supervisora, conforme definido no Artigo 58 do GDPR. (ver tópico 7.3).

7.1.4 Estabelecer Padrões

A Autoridade Supervisora tem a responsabilidade de estabelecer normas e diretrizes e atuar como um órgão certificador.

7.1.4.1 Processamento que requer DPIA

A Autoridade Supervisora publica a lista das operações de processamento que estão sujeitas ao requisito de uma avaliação do impacto da proteção de dados (ver tópico 8.3).

7.1.4.2 Código de conduta e certificação

A Autoridade Supervisora encorajará a elaboração de códigos de conduta destinados a contribuir para a correta aplicação do GDPR. A Autoridade Supervisora deve emitir um parecer sobre

propostas de associações e organismos para preparar ou alterar um código de conduta e aprovar códigos de conduta que forneçam garantias suficientes. A Autoridade Supervisora também conduzirá o credenciamento de um órgão para monitorar os códigos de conduta, conforme descrito.

A Autoridade Supervisora encorajará o estabelecimento de mecanismos de certificação de proteção de dados e de selos e marcas de proteção de dados com a finalidade de demonstrar a conformidade com o GDPR das operações de processamento pelos controladores e processadores e aprovar os critérios de certificação.

A Autoridade Supervisora também elaborará e publicará os critérios de credenciamento de um organismo de certificação para monitorar esse mecanismo de certificação.

7.1.4.3 Cláusulas contratuais padrão e regras corporativas vinculativas e – contratos

Uma Autoridade Supervisora pode adotar cláusulas contratuais-padrão para o contrato vinculante entre o controlador e o processador e, se apropriado (por exemplo, com autorização prévia por escrito do controlador), entre o processador e o subprocessador.

Uma Autoridade Supervisora pode também adotar cláusulas contratuais-padrão para contratos entre controladores no AEE e processadores em países fora do AEE para os quais não foi implementada nenhuma decisão de adequação (ver tópico 7.4).

Particularmente para empresas e organizações multinacionais, a Autoridade Supervisora pode aprovar Regras Corporativas Vinculantes (ver tópico 7.6.3).

7.1.5 Cooperação com outras autoridades supervisoras e a AEPD[1] (EDPS).

A fim de contribuir para a aplicação coerente do presente regulamento em toda a União, as Autoridades Supervisoras cooperam entre si e, se for caso disso, com a Comissão, através do mecanismo de coerência estabelecido na presente secção.

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Artigo 63.

Nos parágrafos anteriores, pode-se ter a ideia de que as mais de cinquenta Autoridades Supervisoras nos cerca de trinta países do AEE estão inventando independentemente os mesmos padrões ao mesmo tempo. O oposto é verdadeiro, no entanto. Por meio do mecanismo de consistência, as Autoridades Supervisoras compartilham informações e fornecem assistência mútua a outras Autoridades Supervisoras 'com o objetivo de garantir a consistência da aplicação e aplicação do GDPR'.

Eles também compartilham todas as informações relevantes com o Conselho Europeu de Proteção de Dados (também conhecido como 'Conselho'), que é composto pelo chefe de uma Autoridade Supervisora de cada Estado-Membro e pela Autoridade Europeia para a Proteção de Dados, ou seus respectivos representantes.

Quando uma Autoridade Supervisora toma uma decisão que afeta apenas o processamento de dados pessoais em seu próprio território, o mecanismo de consistência não se aplica. Portanto, quando uma Autoridade Supervisora toma uma decisão, por exemplo, planejar adotar normas, diretrizes ou cláusulas contratuais, ela compartilhará essas informações com o Conselho. Na maior parte dos casos, o Conselho, em estreita comunicação com a Comissão Europeia, providenciará para que, após a discussão necessária e as alterações necessárias, a proposta se transforme numa norma europeia adoptada por todas as Autoridades.

[1] AEPD – Autoridade Europeia para a Proteção de Dados: EDPS – European Data Protection Supervisor.

Em princípio, o mecanismo de consistência se destina a garantir que as organizações que operam internacionalmente enfrentam requisitos de conformidade consistentes nos países da AEE em que atuam.

7.2 Papeis e Responsabilidades Relacionadas a Violações de Dados Pessoais

Quando uma Autoridade Supervisora recebe uma notificação de uma violação de dados pessoais, deve poder avaliar vários critérios importantes para avaliar a importância da violação de dados pessoais e avaliar como a proteção de dados foi implementada pelo controlador e pelo processador ou processadores.

A avaliação dos riscos para os titulares dos dados e as medidas mitigadoras que já foram ou ainda devem ser tomadas são claramente as mais imediatas. A responsabilidade da Autoridade Supervisora de fazer cumprir as regras do GDPR segue diretamente depois disso.

Em princípio, o controlador é responsável por:

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

No entanto, uma Autoridade Supervisora pode receber amplos poderes para monitorar essa investigação e ordenar que os controladores e processadores envolvidos tomem outras medidas ou medidas extras para alinhar as operações de processamento com o GDPR e até para restringir ou bloquear o processamento.

7.3 Poderes da Autoridade Supervisora na aplicação do GDPR

Uma das principais responsabilidades de uma Autoridade Supervisora é fazer **cumprir** a aplicação do GDPR. Além dos poderes consultivos, uma Autoridade Supervisora possui amplos poderes de investigação e correção para impor a implementação do GDPR. Isso inclui, quando necessário, a aplicação de multas paralisantes.

A fim de assegurar um controlo e aplicação coerentes do presente regulamento em toda a União, as Autoridades Supervisoras devem ter em cada Estado-Membro as mesmas funções e poderes efetivos, incluindo poderes de investigação, poderes de correção e sanções, e poderes de autorização e aconselhamento, nomeadamente em casos de queixas de pessoas singulares, (…).

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Considerando (129).

7.3.1 Poderes de investigação da Autoridade Supervisora

O Artigo 58(1) do GDPR concede às Autoridades Supervisoras alguns de poderes de investigação. Elas têm o poder:

(a) ordenar ao controlador e ao processador (...) que forneçam qualquer informação necessária para o desempenho de suas tarefas.
(b) realizar investigações sob a forma de auditorias de proteção de dados
(c) proceder a uma revisão das certificações emitidas (…)

(d) notificar o controlador ou o processador de uma alegada infracção ao presente regulamento.
(e) obter, do controlador e do processador, acesso a todos os dados pessoais e a todas as informações necessárias para o desempenho de suas tarefas
(f) obter acesso a quaisquer instalações do controlador e do processador, incluindo equipamentos e meios de processamento de dados, em conformidade com o direito processual da União ou do Estado-Membro

7.3.2 Poderes corretivos da Autoridade Supervisora

O Artigo 58(2), do GDPR concede às Autoridades Supervisoras que também alcançam poderes de correção:

(a) emitir advertências a um controlador ou processador que pretenda que as operações de processamento possam infringir as provisões do GDPR
(b) emitir repreensões a um controlador ou processador em que as operações de processamento tenham infringido as provisões do GDPR
(c) ordenar ao controlador ou ao processador que cumpra com as solicitações do titular dos dados para exercer seus direitos de acordo com o GDPR
(d) ordenar ao controlador ou ao processador que as operações de processamento entrem em conformidade com as disposições do GDPR (...)
(e) ordenar ao controlador que comunique uma violação de dados pessoais à pessoa em causa
(f) impor uma limitação temporária ou definitiva, incluindo a proibição de processamento
(g) ordenar a retificação ou o apagamento de dados pessoais ou a restrição de processamento (...) e a notificação de tais ações aos destinatários a quem os dados pessoais tenham sido divulgados (...)
(h) retirar uma certificação ou ordenar ao organismo de certificação que retire uma certificação emitida (...), ou ordenar ao organismo de certificação que não emita a certificação (...)
(i) impor uma multa administrativa (...), em complemento ou em vez das medidas referidas no presente número, consoante as circunstâncias de cada caso individual
(j) ordenar a suspensão dos fluxos de dados para um destinatário num país terceiro ou para uma organização internacional

7.3.3 Condições gerais para a imposição de multas administrativas

Cada autoridade de controlo assegurará que a aplicação de multas administrativas ao abrigo do presente Artigo no que se refere às infrações ao presente regulamento referidas nos parágrafos 4, 5 e 6 sejam, em cada caso, eficazes, proporcionadas e dissuasivas.

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Artigo 83(1).

As multas administrativas devem ser proporcionadas e dissuasivas.

7.3.3.1 Proporcional

Quando uma Autoridade Supervisora decidir impor uma multa administrativa, além de outras medidas, ela deve dar a devida atenção às circunstâncias.

Os critérios para essa decisão são:

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

A cooperação com a Autoridade Supervisora para remediar uma infração e mitigar os possíveis efeitos adversos da infração será favorável aos controladores e processadores.

7.3.3.2 Dissuasivo

Uma multa também deve ser dissuasiva. Qualquer que seja o custo da implementação de medidas para cumprir o GDPR em uma organização, nenhuma empresa deve arriscar ignorar as regras, porque as multas vão muito além do que custará a conformidade.

Ainda assim, a intenção é incentivar as empresas a cumprir o GDPR, e não destruí-las financeiramente.

Existem duas categorias de multas:

- multas de € 10.000.000 ou 2% do volume de negócios mundial da empresa no ano financeiro anterior, o que for maior.
- multas de € 20.000.000 ou 4% do faturamento mundial da empresa no exercício financeiro anterior, o que for maior.

Por violações das **obrigações do controlador e do processador**, a multa máxima será da primeira categoria, portanto, 10.000.000 € ou 2% do faturamento mundial da empresa no exercício financeiro anterior, o que for maior.

Algumas categorias de infrações serão penalizadas com mais rigor:

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

Para estas categorias, a multa administrativa máxima será de € 20.000.000 ou até 4% do volume de negócios mundial da empresa no ano financeiro anterior, o que for maior.

Se um controlador ou processador, intencional ou negligentemente, infringir várias disposições do presente regulamento para as **mesmas** operações de processamento ou **ligadas**, o montante total da multa administrativa não deve exceder o montante especificado para a infração mais grave. As multas não se acumulam com cada infração relacionada.

7.4 Transferência de Dados Transfronteiriça

7.4.1 'One-stop-shop'

A regra geral é que a supervisão da atividade de processamento transfronteiriço, ou processamento envolvendo cidadãos de mais de um país da UE, é liderada por apenas uma Autoridade Supervisora, denominada "Autoridade Supervisora principal". Isso é conhecido como o princípio One Stop Shop ("Balcão Único").

A autoridade principal coordenará as operações que envolvam as Autoridades Supervisoras interessadas, em conformidade com os Artigos 60-62 do regulamento (por exemplo, balcão único, assistência mútua e operações conjuntas). Submete qualquer projeto de decisão às Autoridades Supervisoras interessadas neste assunto.

Fonte: WP244 ANEXO II - Perguntas Frequentes

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

7.4.2 Processamento transfronteiriço

O GDPR distingue dois tipos de processamento transfronteiriço:

Processamento transfronteiriço significa:

(a) a) Processamento de dados pessoais que ocorra no contexto das atividades de estabelecimentos em mais do que um Estado-Membro de um controlador ou de um processador na União em que o controlador ou o processador esteja estabelecido em mais de um Estado-Membro; ou

(b) b) Processamento de dados pessoais que ocorre no contexto das atividades de um único estabelecimento de um controlador ou de um processador na União, mas que afeta substancialmente ou é suscetível de afetar substancialmente os titulares de dados em mais de um Estado-Membro.

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Artigo 4(23).

7.4.3 Empresa multinacional

A primeira situação é a de uma empresa multinacional que tenha estabelecimentos em mais do que um Estado-Membro. Por exemplo, ABNAMRO, um grande banco com escritórios na Holanda, Bélgica, França, Alemanha, etc.

7.4.4 Empresa que opera internacionalmente

A segunda situação é a de um único estabelecimento de um controlador ou processador na união, onde o processamento de dados pessoais afeta substancialmente (...) os titulares de dados em mais de um Estado-Membro. Por exemplo, esse seria o tipo de processamento que ocorre em um hospital no leste da Holanda com pacientes na Holanda e na Alemanha: O processamento é 'transfronteiriço', afeta a saúde dos indivíduos e uma análise de dados médicos e, portanto, dados especiais.

7.4.5 Afetar substancialmente

O GDPR não define estritamente o que 'afetar substancialmente' significa. No entanto, em dezembro de 2016, o Grupo de Trabalho do artigo 29 publicou diretrizes[2] nas quais eles escrevem que as autoridades de supervisão interpretarão isso caso a caso, considerando:

- o contexto do processamento
- o tipo de dados
- a finalidade do processamento

[2] 16/EN/WP 244 http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp244_en_40857.pdf. Acessado pela última vez em 25 de julho de 2019.

- outros fatores, como se o processamento
  - causa, ou é provável que cause, dano, perda ou angústia aos indivíduos
  - tem, ou é provável que tenha, um efeito real em termos de limitação de direitos ou de negação de uma oportunidade
  - afeta, ou é provável que afete a saúde, o bem-estar ou a tranquilidade dos indivíduos
  - afeta ou é susceptível de afetar o estado financeiro ou econômico ou as circunstâncias
  - deixa as pessoas abertas à discriminação ou processamento injusto
  - envolve a análise das categorias especiais de dados pessoais ou outros intrusivos, particularmente os dados pessoais de crianças
  - causa, ou é suscetível de causar, indivíduos a mudar seu comportamento de forma significativa
  - tem consequências improváveis, imprevistas ou indesejadas para os indivíduos
  - cria constrangimento ou outros resultados negativos, incluindo danos à reputação ou
  - envolve o processamento de uma ampla gama de dados pessoais

Por exemplo, um clube de remo tem membros nos dois lados de uma fronteira com o país. O processamento dos endereços dos membros não seria "afetado" substancialmente os membros. Como consequência, esse processamento não seria considerado "processamento transfronteiriço".

7.5 Regulamentos Aplicáveis à Transferência de Dados dentro da AEE

7.5.1 Identificar a Autoridade Supervisora principal

(...) A Autoridade Supervisora do estabelecimento principal ou do estabelecimento único do controlador ou processador deve ter competência para agir como autoridade de controlo principal para o processamento transfronteiriço realizado pelo referido controlador ou processador, em conformidade com o procedimento [de cooperação] previsto no Artigo 60.

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Artigo 56.

Para uma multinacional, como um banco, o "estabelecimento principal" é o local da administração central dessa organização. No entanto, se outro estabelecimento toma as decisões sobre as finalidades e meios do processamento e tem o poder de implementá-las, esse estabelecimento se torna o estabelecimento principal. Consequentemente, a autoridade supervisora principal seria a autoridade do Estado membro onde o estabelecimento principal é identificado.

No caso de um único estabelecimento de um controlador ou processador na união, onde ocorre o processamento de dados pessoais que afeta substancialmente (...) titulares de dados em mais do que um único Estado-Membro, a Autoridade Supervisora principal é a do país onde o estabelecimento do controlador é.

Se o processamento não for susceptível de afetar substancialmente os titulares de dados "através da fronteira", a mesma Autoridade Supervisora estaria supervisionando, mas o processamento não seria considerado "processamento transfronteiriço" e, consequentemente, o mecanismo de consistência não precisa ser ativado.

7.6 Regulamentos aplicáveis à transferência de dados fora do AEE

Em geral, as transferências de dados entre fronteiras para um destinatário em um terceiro país só podem ocorrer se a transferência for feita para uma 'jurisdição adequada' ou se a parte ou partes que exportam os dados tiverem implementado um mecanismo legal de transferência de dados.

7.6.1 Transferências com base em uma decisão de adequação

A transferência de dados pessoais para um país terceiro ou uma organização internacional pode ter lugar quando a Comissão tiver decidido que o país terceiro, um território ou um ou mais sectores especificados nesse país terceiro ou a organização internacional em questão garantem um nível adequado de proteção de segurança. Tal transferência não exigirá nenhuma autorização específica.

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Artigo 45(1).

Uma “decisão de adequação” é uma decisão adotada pela Comissão Europeia, estabelecendo que um país terceiro garante um nível adequado de proteção de dados pessoais em razão de sua legislação interna ou dos compromissos internacionais assumidos. O efeito dessa decisão é que os dados pessoais podem ser transmitidos dos Estados-Membros da UE e dos países membros do Espaço Econômico Europeu (AEE) ou Área Econômica Europeia (AEE), quais sejam países da UE juntamente com Noruega, Liechtenstein e Islândia, para esse país terceiro, sem quaisquer salvaguardas adicionais.

A Comissão Europeia emitiu (julho de 2019) decisões de adequação, reconhecendo que Andorra, Argentina, Canadá (organizações comerciais), Ilhas Faroé, Guernsey, Israel, Ilha de Man, Jersey, Nova Zelândia, Suíça EUA[3] e Uruguai proporcionam proteção adequada.

A maioria dessas decisões já estava em vigor quando o GDPR entrou em vigor. O Artigo 45(4), exige que a Comissão acompanhe os desenvolvimentos em países terceiros e organizações internacionais que possam afetar o funcionamento dessas decisões. Se a Comissão considerar que um país terceiro, um território (etc.) ou uma organização internacional já não garante um nível adequado de proteção (…), pode revogar, alterar ou suspender a decisão.

7.6.2 Transferências sujeitas a salvaguardas apropriadas

Na ausência de uma decisão de adequação, o controlador ou o processador deve tomar medidas para compensar a falta de proteção de dados em um terceiro país por meio de salvaguardas apropriadas para o titular dos dados.

Essas salvaguardas adequadas podem consistir na utilização de regras vinculantes para as empresas, cláusulas-padrão de proteção de dados adotadas pela Comissão, cláusulas-tipo de proteção de dados adotadas por uma Autoridade Supervisora ou cláusulas contratuais autorizadas por uma Autoridade Supervisora.

Essas salvaguardas devem garantir a conformidade com os requisitos de proteção de dados e os direitos dos titulares de dados adequados ao processamento dentro da União, incluindo a disponibilidade de direitos dos titulares de direitos aplicáveis e de recursos legais efetivos, inclusive para obter reparação administrativa ou judicial efetiva e reivindicar compensação, na União ou num país terceiro.

(…) as transferências podem igualmente ser realizadas por autoridades ou organismos públicos com autoridades ou organismos públicos de países terceiros ou com organizações internacionais com funções ou deveres correspondentes, incluindo com base em disposições a

[3] The adequacy decision on the USA is limited to the Privacy Shield Network (see § 7.5.4).

inserir em disposições administrativas, como um memorando de entendimento, prevendo direitos aplicáveis e efetivos para os titulares dos dados.

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; item 108.

Ao transferir dados entre autoridades públicas, as autoridades públicas devem garantir a conformidade com os requisitos do RGPD. Os outros casos exigem a adoção de uma norma aprovada ou a adoção de cláusulas de proteção pela Autoridade Supervisora.

7.6.3 Regras Corporativas Vinculantes (BCR)

Um grupo de empresas, ou um grupo de empresas envolvidas numa atividade econômica conjunta, deve poder utilizar as regras empresariais vinculantes aprovadas para as suas transferências internacionais da União para organizações pertencentes ao mesmo grupo de empresas ou grupo de empresas uma atividade econômica conjunta, desde que tais regras corporativas incluam todos os princípios essenciais e direitos aplicáveis para garantir as salvaguardas apropriadas para transferências ou categorias de transferências de dados pessoais.

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; item 110.

Requisitos essenciais para a Autoridade Supervisora Competente aprovar um conjunto de Regras Corporativas Vinculantes:

- são juridicamente vinculantes
- aplicam-se e são reforçadas por todos os membros envolvidos do grupo, incluindo seus empregados
- conferem expressamente direitos aplicáveis aos titulares dos dados no que diz respeito ao tratamento dos seus dados pessoais;
- cumprir os requisitos estabelecidos no Artigo 47 (2) do GDPR.

Esta lista bastante longa especifica, entre outras, que as Regras Corporativas Vinculantes (BCR) devem especificar pelo menos:

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

7.6.4 Transferências ou divulgações não autorizadas pela lei da UE

O GDPR limita a transferência de dados pessoais para países terceiros (países fora do AEE).

Qualquer sentença de um tribunal ou qualquer decisão de uma autoridade administrativa de um país terceiro que exija que um controlador ou processador transfira ou divulgue dados pessoais só pode ser reconhecida ou exequível de qualquer maneira se baseada em um acordo internacional (...) em vigor entre o país terceiro requerente e a União ou um Estado-Membro, sem prejuízo de outros motivos de transferência nos termos do presente capítulo.

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Artigo 45(1).

7.6.5 Regulamentos aplicáveis à transferência de dados entre o AEE e os EUA

Conforme detalhado no ponto 7.6.1, a Comissão Europeia pode tomar uma '**decisão de adequação**', reconhecendo um país ou parte de um país como tendo uma proteção de dados adequada (GDPR, Capítulo V). Entretanto, como a lei de proteção de dados dos EUA difere consideravelmente daquilo que o GDPR (e a diretiva anterior) exige, não há uma decisão de adequação em relação aos EUA ou às partes geográficas dos mesmos.

Em vez disso, em julho de 2016, a Comissão aplicou a decisão (UE) 2016/1250 sobre a adequação da proteção fornecida pelo "EU-US Privacy Shield", conforme emitido pelo Departamento de Comércio dos EUA.

Em um comunicado de imprensa (IP-16-2461 de 12 de julho de 2016), a Comissão Europeia descreveu os princípios em que o EU-US Privacy Shield se baseia:

Obrigações das empresas que lidam com dados:

(…) O Departamento de Comércio dos EUA realizará atualizações e análises regulares das empresas participantes, para garantir que as empresas sigam as regras a que se submeteram. Se as empresas não cumprirem na prática, elas enfrentam sanções e são removidas da lista. O reforço das condições para as transferências subsequentes de dados para terceiros garantirá o mesmo nível de proteção quando da transferência de uma empresa da Privacy Shield.

Salvaguardas claras e obrigações de transparência no acesso do governo dos EUA:

Os EUA deram à UE garantias de que o acesso das autoridades públicas à aplicação da lei e à segurança nacional está sujeito a limitações, mecanismos de salvaguardas e mecanismos de supervisão claros. Todos na UE beneficiarão também, pela primeira vez, de mecanismos de reparação neste domínio. Os EUA descartaram a vigilância indiscriminada em massa de dados pessoais transferidos para os EUA sob o acordo Privacy Shield UE-EUA. O Gabinete do Diretor da Inteligência Nacional esclareceu ainda que a recolha de dados a granel só podia ser utilizada em pré-condições específicas e deveria ser a mais direcionada e focada possível. Ele detalha as salvaguardas em vigor para o uso de dados em tais circunstâncias excepcionais. O Secretário de Estado dos EUA estabeleceu uma possibilidade de reparação na área de inteligência nacional para os europeus através de um mecanismo de Provedor de Justiça (Ombudsperson) dentro do Departamento de Estado.

Proteção efetiva dos direitos individuais:

Qualquer cidadão que considere que os seus dados foram utilizados indevidamente sob o esquema Privacy Shield irá beneficiar de vários mecanismos acessíveis e acessíveis de resolução de litígios. Idealmente, a reclamação será resolvida pela própria empresa; ou soluções gratuitas de resolução alternativa de litígios (ADR - Alternative Dispute Resolution) serão oferecidas. Os indivíduos também podem dirigir-se às suas autoridades nacionais de proteção de dados (DPA-Autoridade de Proteção de Dados), que trabalharão com a Comissão Federal do Comércio (Federal Trade Commission) para garantir que as queixas de cidadãos da UE sejam investigadas e resolvidas. Se um caso não for resolvido por qualquer outro meio, como último recurso, haverá um mecanismo de arbitragem. A possibilidade de reparação no domínio da segurança nacional para os cidadãos da UE será tratada por um Provedor de Justiça independente dos serviços de inteligência dos EUA.

Mecanismo Anual de Revisão Conjunta:

O mecanismo monitorará o funcionamento do Privacy Shield, incluindo os compromissos e a garantia no que diz respeito ao acesso aos dados para fins de aplicação da lei e segurança nacional. A Comissão Europeia e o Departamento de Comércio dos EUA conduzirão a revisão e associarão especialistas nacionais em inteligência das autoridades de proteção de dados dos EUA e da Europa. A Comissão recorrerá a todas as outras fontes de informação disponíveis e publicará um relatório público ao Parlamento Europeu e ao Conselho.

8 Aspectos de qualidade

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

O controlador deve, tanto no momento da determinação dos meios de processamento como no momento do próprio processamento, implementar medidas técnicas e organizacionais adequadas, tais como a pseudomização, que são projetadas para implementar os princípios de proteção de dados, como minimização de dados, de forma eficaz e integrar as salvaguardas necessárias no processamento, a fim de cumprir os requisitos do presente regulamento e proteger os direitos dos titulares dos dados

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Artigo 25(1).

Com este artigo, o GDPR faz do princípio de proteção de dados **desde a concepção** (by design) um **requisito legal**, e não apenas uma maneira eficaz de cumprir as obrigações relacionadas à segurança dos dados. O controlador é responsável pela implementação de um conjunto completo de medidas técnicas e organizacionais **apropriadas**.

Além disso, o GDPR declara no artigo 25(1) que o conjunto de medidas técnicas e organizacionais apropriadas é necessário para integrar as salvaguardas necessárias ao processamento para (...) proteger os direitos dos titulares dos dados. Dessa maneira, um relacionamento legal é definido entre os princípios de segurança de dados e a privacidade, como os direitos e liberdades dos indivíduos.

O segundo parágrafo do artigo 25 exige que o controlador implemente medidas técnicas e organizacionais apropriadas para garantir que, **por padrão** (by default), apenas sejam processados dados pessoais necessários para cada finalidade específica do processamento. Isso se aplica à quantidade de dados pessoais coletados, à extensão de seu processamento, ao período de armazenamento e à acessibilidade.

8.1.1 Os sete princípios de proteção de dados desde a concepção (by design)

A ideia de proteção de dados desde a concepção (by design) foi desenvolvida por Ann Cavoukian, PhD., ex-Comissária de Privacidade e Informações de Ontário, Canadá. Em uma publicação sobre os princípios, ela escreveu:

Privacidade desde a concepção (by design) é um conceito que desenvolvi nos anos 90, para abordar os efeitos sempre crescentes e sistêmicos das Tecnologias de Informação e Comunicação e dos sistemas de dados em rede em larga escala. A Privacidade desde a concepção (by design) promove a visão de que o futuro da privacidade não pode ser assegurado apenas pelo cumprimento de estruturas regulatórias; em vez disso, a garantia da privacidade deve idealmente se tornar o modo de operação padrão de uma organização.

Fonte: Ann Cavoukian. 2011. Privacy by Design, the 7 foundational principles

O GDPR usa o Proteção de Dados desde a concepção (by design) e por padrão (by default), como será feito nos próximos parágrafos.

8.1.1.1 Proativo não reativo; preventiva não remediadora

A abordagem de Proteção de Dados desde a Concepção (by design) é caracterizada por medidas proativas em vez de reativas. Ele antecipa e evita eventos invasivos de privacidade antes que eles aconteçam. A Proteção de Dados desde a Concepção (by design) não espera que os riscos de privacidade se concretizem, nem oferece remédios para resolver infrações de privacidade depois de terem ocorrido - ele visa **impedir** que ocorram. Em resumo, a Proteção de Dados desde a Concepção (by design) vem antes do fato, não depois.

8.1.1.2 Proteção de dados como configuração padrão

Todos podem ter certeza de uma coisa: as regras padrão. A Proteção de Dados desde a Concepção (by design) busca oferecer o máximo grau de privacidade, garantindo que os dados pessoais sejam protegidos automaticamente em qualquer sistema de TI ou prática comercial. Se um indivíduo não faz nada, sua privacidade permanece intacta. Nenhuma ação é necessária por parte de um titular de dados para proteger sua privacidade. Privacidade e proteção de dados são incorporadas ao sistema, por padrão.

8.1.1.3 Privacidade Incorporada ao Design

A Proteção de Dados desde a Concepção (by design) está incorporado ao design e à arquitetura de sistemas de TI e práticas de negócios. Não é acoplada como um complemento após o fato. O resultado é que a privacidade se torna um componente essencial da funcionalidade principal que está sendo entregue. A proteção de dados é parte integrante do sistema, sem diminuir suas funcionalidades.

8.1.1.4 Funcionalidade Total - Soma Positiva, Não Soma Zero

A Proteção de Dados desde a Concepção (by design) busca acomodar todos os interesses e objetivos legítimos de uma maneira positiva para todos, não por meio de uma abordagem de soma zero, em que compensações desnecessárias são feitas. A Proteção de Dados desde a Concepção (by design) evita a pretensão de falsas dicotomias, como privacidade versus segurança, demonstrando que é possível ter ambas.

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

A Proteção de Dados desde a Concepção (by design) tendo sido incorporada ao sistema antes do primeiro elemento da informação que está sendo coletada, se estende com segurança durante todo o ciclo de vida dos dados envolvidos - medidas de segurança fortes são essenciais à privacidade, do início ao fim. Isso garante que todos os dados sejam retidos com segurança e, em seguida, destruídos com segurança no final do processo, em tempo hábil. Assim, a Proteção de Dados desde a Concepção (by design) garante o gerenciamento do ciclo de vida de informações de ponta a ponta, seguro e de ponta a ponta.

8.1.1.6 Visibilidade e transparência - Abertura

A Proteção de Dados desde a Concepção (by design) procura assegurar a todos os stakeholders 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. Seus componentes e operações permanecem visíveis e transparentes para usuários e provedores. Lembre-se, confie, mas verifique.

8.1.1.7 Respeito à privacidade do usuário – Centrada no Usuário

Acima de tudo, a Proteção de Dados desde a Concepção (by design), exige que os arquitetos e operadores mantenham os interesses do indivíduo (usuário) em primeiro lugar, oferecendo medidas como padrões de privacidade fortes, notificação apropriada e capacitando opções fáceis de usar. Manter foco no usuário.

8.1.2 Benefícios da aplicação dos princípios de Privacidade desde a Concepção (by design) e Privacidade por Padrão (by default)

Em seu site, o Gabinete do Comissário de Informação do Reino Unido[4] escreveu:

Adotar uma abordagem de Proteção de Dados desde a Concepção (by design) é uma ferramenta essencial para minimizar os riscos de privacidade e criar confiança. Projetar projetos, processos, produtos ou sistemas com a privacidade em mente desde o início pode levar a benefícios que incluem:

- problemas potenciais são identificados em um estágio inicial, quando resolvê-los será sempre mais simples e menos dispendioso
- maior conscientização sobre privacidade e proteção de dados em toda a organização
- as organizações são mais propensas a cumprir suas obrigações legais e menos propensas a violar a Lei de Proteção de Dados.
- é menos provável que as ações sejam invasivas à privacidade e tenham um impacto negativo nos indivíduos

8.2 Contratos Escritos entre Controlador e Processador

O Artigo 25 do GDPR exige que o controlador implemente medidas técnicas e organizacionais apropriadas e garanta que essas precauções permaneçam em vigor durante o processamento, na verdade, implementando um dos princípios da Proteção de Dados desde a Concepção (by design): segurança de ponta a ponta.

Quando um processador é contratado para executar o processamento ou parte do processamento, a consequência lógica é um contrato por escrito e é exatamente isso que o GDPR requer.

O processamento por um transformador será regido por um contrato ou outro ato jurídico ao abrigo da legislação da União ou de um Estado-Membro, vinculante para o transformador em relação ao controlador e que define o objeto e a duração do processamento, a natureza e o objetivo do processamento, o tipo de dados pessoais e categorias de titulares dos dados e as obrigações e direitos do controlador. (...)

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Artigo 28(3).

8.2.1 Cláusulas do contrato escrito

O Artigo 28(3), prossegue: esse contrato (ou outro ato jurídico) estipula, em especial, que o processador:

(a) processa os dados pessoais apenas em instruções documentadas do controlador, incluindo no que diz respeito a transferências de dados pessoais para um país terceiro ou uma organização internacional (...)
(b) assegura que as pessoas autorizadas a tratar os dados pessoais se comprometeram com a confidencialidade ou estão sujeitas a uma obrigação legal adequada de confidencialidade.
(c) adota todas as medidas exigidas nos termos do Artigo 32 (segurança do processamento)
(d) respeita as condições (...) para contratar outro processador
(e) (...) auxilia o controlador, por meio de medidas técnicas e organizacionais apropriadas, na medida do possível, pelo cumprimento da obrigação do controlador de responder aos pedidos de exercício dos direitos do titular dos dados (...)

[4] https://ico.org.uk/, viewed on 25-04-2017

(f) auxilia o controlador a garantir o cumprimento das obrigações previstas nos Artigos 32 a 36, considerando a natureza do processamento e as informações de que dispõe o transformador;
(g) à escolha do controlador, suprime ou devolve todos os dados pessoais ao controlador após o termo da prestação de serviços relacionados com o processamento e elimina cópias existentes, a menos que a legislação da União ou do Estado-Membro exija a conservação dos dados pessoais.
(h) disponibiliza ao controlador todas as informações necessárias para demonstrar o cumprimento das obrigações estabelecidas no presente Artigo, permitindo e contribuindo para as auditorias, incluindo as inspeções realizadas pelo controlador ou por outro auditor mandatado pelo controlador.

8.2.1.1 Exemplo

A tabela a seguir mostra um exemplo do conteúdo de tal contrato de processamento de dados entre o controlador e o processador:

Conteúdo	Referência GDPR
Escopo e finalidade do contrato	Artigo 4(2) definições: processamento
Dados cobertos pelo acordo	Artigo 4(1) dados pessoais; Artigo 9 / item 10 categorias especiais de dados pessoais (dados sensíveis);
Segurança geral e salvaguardas no processamento de dados	Artigo 32 segurança do processamento
Medidas técnicas e organizacionais	Artigo 28(3 a até h)
Monitoramento da segurança da informação e proteção de dados	Artigo 35 avaliação de impacto sobre proteção de dados
Violação de segurança da informação e violação de dados pessoais	Artigo 33(2) notificação de uma violação de dados pessoais à Autoridade Supervisora
Correção, exclusão e bloqueio / obrigações específicas para auxiliar o controlador	Artigo 32.36
Acordo com outro processador de dados	Artigo 28(2) e (4) subprocessador
Transferência de dados	Rec. (112), (113); Artigo 47 Regras Corporativas Vinculantes; Artigo 49 derrogações para situações específicas; o capítulo V transfere (..) para países terceiros ou organizações internacionais.
Outras obrigações do processador	Artigo 39 tarefas do DPO; (1b) ... sensibilização e formação do pessoal envolvido nas operações de processamento
Os direitos de controle dos controladores	Artigo 4(7) controlador Artigo 28(3f) suporte ao controlador …
Retorno e exclusão dos dados pessoais	Artigo 28(3g) eliminar ou devolver
Dever de confidencialidade	Artigo 28(3b) confidencialidade
Duração	Artigo 28(3) duração do processamento Artigo 5 princípios relativos ao processamento de dados pessoais (1) (e) limitação de armazenamento
Precedência	No caso de cláusulas conflitantes, o GDPR tem precedência
Assinaturas	

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

O primeiro princípio de Proteção de Dados desde a Concepção (by design) requer que o controlador (e, na verdade, qualquer pessoa que processe dados pessoais) antecipe e evite eventos invasivos de privacidade antes que eles ocorram.

O GDPR inclui este princípio no Artigo 35:

> Sempre que um tipo de processamento, em especial utilizando novas tecnologias, e tendo em conta a natureza, âmbito, contexto e finalidades do processamento, possa resultar num risco elevado para os direitos e liberdades das pessoas singulares, o controlador do processamento, proceder a uma avaliação do impacto das operações de processamento previstas na proteção de dados pessoais. Uma única avaliação pode abordar um conjunto de operações de processamento semelhantes que apresentam riscos elevados semelhantes.
>
> Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Artigo 35(1).

O GDPR não exige que uma DPIA seja executada para cada operação de processamento. Nas Diretrizes sobre a Avaliação do Impacto na Proteção de Dados, caso um processamento for suscetível de resultar em alto risco (17/EN WP248), o Grupo de Trabalho do Artigo 29 (WP29) detalha o que é uma DPIA e quando conduzir uma DPIA é obrigatório ou desejável:

- DPIA é um processo concebido para descrever o processamento, avaliar a necessidade e a proporcionalidade de um processamento e ajudar a gerir os riscos para os direitos e liberdades das pessoas singulares resultantes do processamento de dados pessoais
- DPIA só é exigida quando o processamento é "susceptível de resultar em um alto risco aos direitos e liberdades das pessoas físicas" (Artigo 35(1))

O GDPR não define exatamente quais são os critérios, mas fornece alguns exemplos:

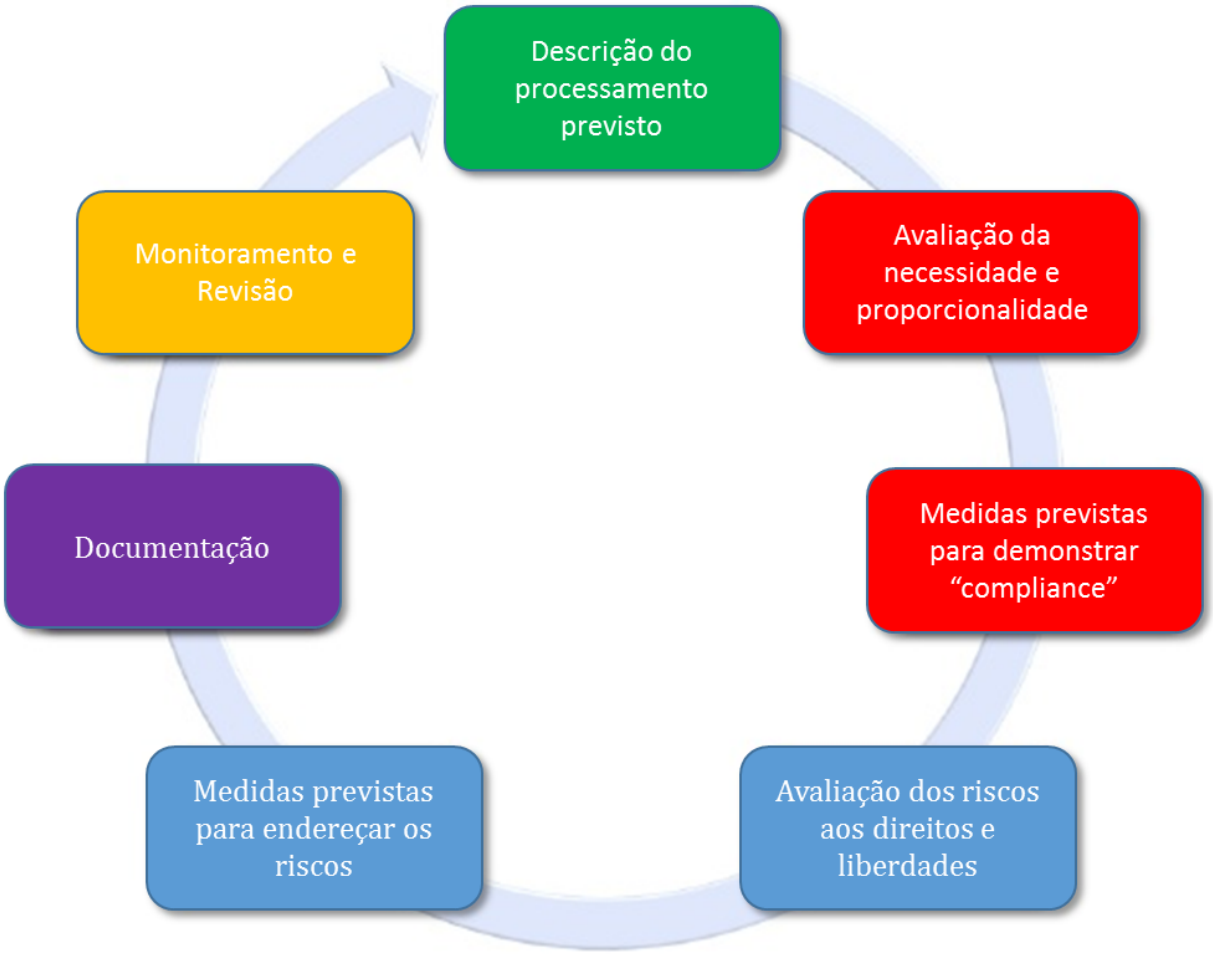
> (a) uma avaliação sistemática e exaustiva dos aspectos pessoais relativos às pessoas físicas, baseada no processamento automatizado, incluindo a definição de perfis e em que se baseiam as decisões que produzem efeitos jurídicos em relação à pessoa natural ou afetam igualmente de forma significativa a pessoa natural;
> (b) Processamento em larga escala de categorias especiais de dados referidas no Artigo 9 (1) ou de dados pessoais relativos a condenações penais e crimes referidos no Artigo 10; ou
> (c) um acompanhamento sistemático de uma área de acesso público em grande escala.
>
> Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Artigo 35 35(3)

Uma DPIA pode endereçar uma única operação de processamento ou um conjunto de operações de processamento semelhantes. Isso significa que **uma única DPIA poderia ser usado para avaliar várias operações de processamento que são semelhantes em termos dos riscos apresentados**, desde que seja dada consideração adequada à natureza específica, ao escopo, ao contexto e às finalidades do processamento. Isso pode significar onde uma tecnologia semelhante é usada para coletar o mesmo tipo de dados para os mesmos fins.

A DPIA deve ser realizada **antes do processamento** (Artigos 35(1) e 35(10); explicações 90 e 93). Isto é consistente com a Proteção de Dados desde a Concepção (by design), e por padrão (by default) (Artigo 25 e item 78).

A DPIA deve ser iniciado **o mais cedo possível** no projeto da operação de processamento, mesmo que algumas das operações de processamento ainda sejam desconhecidas. À medida que a DPIA for atualizada durante todo o projeto de ciclo de vida, ela garantirá que a proteção de dados e a privacidade sejam consideradas e promova a criação de soluções que promovam a conformidade.

Também é necessário repetir etapas individuais da avaliação à medida que o processo de desenvolvimento avança porque a seleção de certas medidas técnicas ou organizacionais pode afetar a gravidade ou a probabilidade dos riscos representados pelo processamento.



O fato de que a DPIA pode precisar ser atualizado uma vez que o processamento tenha realmente iniciado **não** é uma razão válida para adiar ou não executar uma DPIA. Em alguns casos, a DPIA será um processo contínuo, por exemplo, quando uma operação de processamento é dinâmica e está sujeita a alterações contínuas. Executar uma DPIA é um processo contínuo, não um exercício único[5].

8.3.1 Objetivos de uma DPIA

Existem vários motivos para realizar uma DPIA, como a ideia de prevenção, conforme vista em um dos princípios de Proteção de Dados desde a Concepção (by design) a obrigação de documentar a conformidade e outros. Em detalhes, um DPIA ajudará:

- evitar mudanças dispendiosas nos processos, redesenho de sistemas ou encerramento de projetos
- reduzir as consequências da supervisão e fiscalização
- melhorar a qualidade dos dados
- melhorar a prestação de serviços
- melhorar a tomada de decisão
- aumentar a conscientização sobre privacidade em uma organização

[5] Figura adaptada de Guidelines on Data Protection Impact Assessment (DPIA), WP29 document 17/EN/248.

- melhorar a viabilidade do projeto
- melhorar a comunicação em relação à privacidade e proteção de dados pessoais
- reforçar a confiança dos titulares de dados na forma como os dados pessoais são processados e a privacidade é respeitada

8.3.2 Tópicos de um relatório DPIA

O GDPR estabelece as características mínimas de uma DPIA (Artigo 35(7) e itens 84 e 90):

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

8.4 Gestão do Ciclo de Vida de Dados (GCVD)

Independentemente de os dados serem gerados por e dentro da organização ou coletados pela organização por meio de terceiros (cliente, fornecedor, parceiro), a única maneira de protegê-los é entendê-los. Eles contêm dados pessoais de qualquer tipo, como informações sobre clientes, informações sobre funcionários, comunicações confidenciais, informações de identificação pessoal, informações sobre saúde ou dados financeiros? Em cada um desses casos, provavelmente, o GDPR se aplica, exigindo proteção apropriada a partir do momento em que os dados são coletados. Exige uma estrutura de privacidade e segurança nos fundamentos de qualquer projeto. Mas, na verdade, os dados mudam ao longo de toda a sua vida útil e muitas vezes são armazenados por anos - seja para registro ou apenas o momento. Com o GDPR, no entanto, este último está se tornando um hábito caro.

8.4.1 Finalidade do GCVD

A Gestão do Ciclo de Vida do Dado (GCVD) é um processo que ajuda as organizações a gerenciar o fluxo de dados em todo o seu ciclo de vida: da criação, uso, compartilhamento, arquivamento e exclusão.

Rastrear dados com precisão em todo o ciclo de vida da informação é a base de uma estratégia de proteção de dados confidencial e ajuda a determinar onde aplicar os controles de segurança.

8.4.2 Compreendendo os Fluxos de Dados

Os vários requisitos do GDPR exigem que uma empresa saiba:

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

8.4.2.1 Coleta de dados

Desde o início, é importante ter em mente quais dados pessoais são necessários para os fins do processamento pretendido. O GDPR requer um motivo para manter os dados pessoais armazenados, portanto, a qualquer momento, deve ser claro e fácil demonstrar ao menos:

- com que finalidade ou finalidades as informações foram coletadas
- em que data os titulares dos dados foram informados da coleta e da sua finalidade

- se o consentimento foi adquirido para o processamento pretendido
- se esse consentimento ainda é válido (e não retirado)
- outro fundamento legal para processamento existe

Na prática, cada “pedaço” de informação precisa de numerosas etiquetas indicando porque existe e por quanto tempo continuará existindo.

8.4.2.2 Estrutura das permissões

Qualquer coleta de dados, mas uma coleta de dados pessoais em particular, precisa de uma estrutura de permissões, definindo claramente quais funcionários precisam, por conta de sua função na organização, acessar quais dados pessoais.

No entanto, as coisas mudam. Um bom programa deve avaliar e revisar continuamente quem precisa acessar que tipo ou tipos de informação. Controladores e processadores devem trabalhar com seus colegas de TI para automatizar controles em todos os sistemas corporativos. Eles devem facilitar para que os funcionários façam a coisa certa contra a coisa errada. Eles devem evitar que os funcionários tenham consequências negativas através de suas ações, desde a simples negligência em fazer alguma coisa.

Depois que a estrutura de permissões estiver em vigor, ela deve ser mantida por meio de avaliações regulares e contínuas.

8.4.2.3 Construir regras de retenção e exclusão

Um dos princípios fundamentais do GDPR é a minimização de dados: a obrigação de os controladores e processadores garantirem que os dados pessoais são adequados, relevantes e limitados ao necessário em relação aos fins para os quais são processados (Artigo 5(1c)). Na prática, isso leva a um equilíbrio contínuo entre quais dados manter e por que e quais dados descartar de maneira segura.

Armazenar dados pessoais é um fardo para qualquer organização. É preciso muito esforço para manter os dados seguros, completos e atualizados, e ainda mais esforços para responder às solicitações dos titulares de dados, solicitando informações sobre o processamento de seus dados e para lidar com reclamações referentes a seus direitos. Adicionalmente, há sempre a ameaça de uma violação de dados pessoais, com os procedimentos resultantes, o risco para os titulares de dados e o risco de dados para a empresa, como perda de reputação, custo de reparações e possíveis multas.

Há muitas obrigações legais em relação à retenção de dados pessoais por um determinado período. Por exemplo, considere-se registros de clientes, como vendas e transações financeiras, garantias ou informações de recursos humanos, como currículo, histórico de pagamento ou informações tributárias.

A boa Gestão do Ciclo de Vida do Dado (GCVD):

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

8.5 Auditoria de Proteção de Dados

Vários artigos do GDPR mencionam as auditorias como um dos métodos para monitorar a conformidade com o GDPR. Por exemplo, nas tarefas de um DPO:

O DPO deve desempenhar, pelo menos, as seguintes funções: controlar o cumprimento do presente regulamento, outras disposições de proteção de dados da União ou dos Estados-Membros e as políticas do controlador ou do subprocessador relacionadas com a proteção de dados pessoais, incluindo a atribuição de responsabilidades, conscientização e treinamento do pessoal envolvido nas operações de processamento, e as auditorias relacionadas;

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Artigo 39(1) (b).

Ao lado do Artigo 39, o Artigo 47 (2j) exige que Regras Corporativas Vinculantes (BCR) devem especificar, entre outras, auditorias para avaliar os mecanismos contratados para assegurar a verificação do cumprimento dessas BCR.

O Artigo 58(1b), confere às Autoridades Supervisoras o direito de realizar investigações sob a forma de auditorias de proteção de dados.

8.5.1 Finalidade de uma auditoria

A finalidade de um processo de auditoria de proteção de dados é testar, avaliar e avaliar regularmente a eficácia de medidas técnicas e organizacionais para garantir a conformidade com o GDPR, incluindo a segurança do processamento.

Normalmente, uma auditoria revelará **lacunas** nas políticas de privacidade que precisam ser abordadas para aprimorar a governança de privacidade de dados.

No mínimo, uma auditoria tornará a proteção de dados pessoais o "tópico da semana", aumentando a conscientização em toda a organização.

De um modo geral, dois tipos de auditorias de privacidade podem ser distinguidos: uma auditoria de adequação e uma auditoria de conformidade.

8.5.1.1 Auditoria de adequação

Uma auditoria de adequação visa:

- assegurar que as políticas de proteção de dados da organização sejam aplicadas a todas as instâncias de processamento de dados pessoais realmente acontecendo
    - incluindo conjuntos de dados históricos, backups, equipamentos obsoletos
- avaliar se estas políticas são adequadas para atender aos requisitos do GDPR e outras leis e regulamentos de proteção de dados possivelmente aplicáveis
    - tanto dentro como fora do AEE.

Isso requer um entendimento e um mapeamento completos dos fluxos de dados em toda a empresa, e é mais do que apenas revisar todas as políticas, procedimentos, códigos de prática e diretrizes da empresa que afetam o manuseio de dados pessoais durante seu ciclo de vida. A auditoria de adequação deve ser feita dentro da empresa e com todos os terceiros envolvidos, como processadores.

8.5.1.2 Auditoria de Conformidade

Após a conclusão da auditoria de adequação, a próxima etapa poderá ser, e talvez até deva ser, uma auditoria de conformidade, para determinar se a organização está de fato cumprindo as políticas e procedimentos identificados durante e, talvez, aprimorada como resultado da auditoria de adequação.

Uma auditoria de conformidade requer uma investigação de como os dados pessoais são tratados **na prática** dentro das várias unidades de negócios, entre departamentos e ao lidar com terceiros.

Uma auditoria abrangente de conformidade também deve examinar fatores como:

- se a organização oferece treinamento de conformidade de privacidade de dados
- como as políticas de privacidade de dados são disseminadas para os funcionários
- como as reclamações de violações de políticas são tratadas

A profundidade da auditoria de conformidade dependerá dos riscos percebidos para a empresa de violações legais e violações de dados.

8.5.2 Conteúdo de um plano de auditoria

- Desenvolvimento de programas de auditoria (planejamento)
  - Contatos, finalidades, prazo ...
- Descrição da abordagem e o escopo da auditoria:
  - Será uma adequação - ou uma auditoria de conformidade?
  - Auditoria vertical (funcional), visando um departamento específico (como Recursos Humanos) ou
  - Auditoria horizontal (processo); rastreamento de um determinado processo de uma ponta à outra
  - Escopo da auditoria (governança de proteção de dados, gerenciamento de registros, gerenciamento de acesso e segurança de dados, proteção de dados, treinamento e conscientização etc.)
- Preparativos, reunindo evidências das áreas incluídas:
  - Acordos de parcerias
  - Contratos, como contrato de processador-controlador, BCR, acordos de divulgação, etc.
  - Descrições de processos; ordens de serviço, avisos, …
  - Material de treinamento, panfletos etc.
- Realizando a auditoria
- Relatório:
  - Conclusão geral
  - Áreas de boa prática
  - Áreas para melhoria
- Acompanhamento

8.6 Práticas Relacionadas a Aplicações do Uso de Dados, Marketing e Mídias Sociais

8.6.1 O uso de informações de mídia social em atividades de marketing

Não há muito tempo, havia três métodos de informar ao público sobre o produto ou serviço que um vendedor estava tentando vender:

- comprar publicidade cara
- pedir à mídia para contar sua história
- contratar uma enorme força de vendas para incomodar as pessoas diretamente sobre o produto

Nenhum desses métodos foi realmente muito eficaz. Todos os três métodos foram baseados em interromper as pessoas no que estavam fazendo, esperando que elas pudessem ver o produto e pensar: “é isso o que tenho procurado” e, se assim fosse, então elas se lembrariam de quem anunciava e onde deveriam ir para encontrar esse produto.

Usando a internet, existem melhores opções para que seu produto seja notado. Dos produtores e consumidores, as pessoas se tornaram “prosumidores”[6]„ realizando o design de produtos, criticando e consumindo gastando dinheiro. Tornou-se fácil criar um site, escrever um blog, publicar conteúdo e mídia (fotos, som, vídeo) nas mídias sociais. Não apenas os fornecedores, mas praticamente todos podem publicar seu próprio conteúdo, que seus consumidores desejam comprar.

Com as mídias sociais, todos podem entrar em contato com outras pessoas conectadas a essas mídias sociais, em qualquer lugar do mundo. Com apenas o Facebook com mais de 1,5 bilhão de usuários, um vasto mercado global está aberto.

Com essas mudanças soando na era digital, o negócio está se tornando "multicanal" e interativo. Os fornecedores escrevem sobre seus produtos como jornalistas, e as pessoas reagem a isso indicando que gostam do que veem, gostam do que está sendo produzido, do que está sendo oferecido. Claro, se elas não gostarem, elas não hesitarão em dizer ao mundo sobre isso também, muitas vezes em termos bastante contundentes.

Finalmente, um novo conceito de vendas está surgindo. Muitas pessoas acham importante o que as outras pessoas e, em particular, seus amigos, acham do produto que estão procurando. A mensagem de que "76% dos seus amigos gostam deste produto "prova ser um incentivo para comprar. Mesmo que não haja como verificar essa afirmação, todos parecemos acreditar.

Os consumidores podem ser divididos em grupos com gostos semelhantes, interesses semelhantes e outros grupos relevantes. Ao ler uma loja on-line, todos vimos comentários como "compradores do <produto que você acabou de ver> também compraram: <esses outros produtos>". Mensagens como essa provam ser um facilitador de vendas muito forte, desde que o consumidor-alvo tenha gostos e interesses semelhantes aos dos "outros compradores".

8.6.2 Uso da internet no campo do marketing

Para que essa nova e mais economia digital funcione, as empresas precisam de informações sobre potenciais compradores. Na prática, isso significa que eles precisam de informações sobre o maior número possível de consumidores. Que tipo de consumidor é esse? O tipo "radical", precisando de equipamentos e roupas de boa qualidade para o ar livre? O tipo "eu quero a mais nova tecnologia"? Ou talvez o tipo de melhor relação preço / desempenho, ou melhor, o tipo de comprador com preço mais baixo garantido.

Perfis como esse pedem muitos dados sobre pessoas e seu comportamento. Como essas empresas obtêm essa informação?

8.6.3 Cookies

Um cookie é apenas um arquivo de texto (geralmente pequeno), armazenado no computador do usuário. Os cookies mais comuns são:

- cookies de sessão
- cookies persistentes
- cookies de rastreamento

8.6.3.1 Cookies de sessão

Os cookies de sessão permitem que os usuários sejam reconhecidos dentro de um site, de modo que qualquer alteração de página ou seleção de item ou de dados que o usuário faça, seja lembrada de uma página para outra. O exemplo mais comum é o recurso de carrinho de compras de qualquer loja virtual. Sempre que os itens são selecionados, a seleção é armazenada no cookie da sessão, por isso é lembrada até que o usuário esteja pronto para fazer check-out.

[6] para mais informações verifique: https://pt.wikipedia.org/wiki/Prosumer

Ao fazer logon em um site, um cookie de sessão na memória do computador do usuário retém as informações de que o logon foi bem-sucedido, pois o site não tem como lembrar que você fez logon. Ao sair do site, o que usualmente significa fechar o navegador, o cookie da sessão é apagado da memória do computador do usuário e, como resultado, ele é desconectado.

8.6.3.2 Cookies persistentes

Os cookies persistentes permanecem no disco rígido do usuário até serem apagados pelo usuário ou até expirarem. Os cookies persistentes podem oferecer serviços simples ao usuário como visitante recorrente. Por exemplo, para manter a seleção de idioma do usuário. Quando o usuário revisitar esse site, ele oferecerá, com base nas informações do cookie, o conteúdo no idioma escolhido durante a visita anterior.

Esse tipo de cookie pode tornar a experiência do visitante do site mais pessoal. Por exemplo, um usuário usa um site de reservas para reservar um voo barato para o distrito de British Lake. Para que as transações (financeiras e com a companhia aérea) sejam bem-sucedidas, o usuário deve preencher informações pessoais (nome, endereço, número do passaporte, detalhes do cartão de crédito). Na próxima vez que o usuário visitar o site, a combinação dessas informações poderá levar a uma saudação mais pessoal, como "Bom dia, <nome>", mas também a ofertas de outras viagens, seguro de viagem, ofertas de bons equipamentos para caminhadas, malas de viagem, e mais. Tudo com base nas informações coletadas da viagem reservada e, se aplicável, nas viagens reservadas anteriormente.

Não há necessidade de salvar informações no cookie. De fato, um identificador único é suficiente para reconhecer o usuário (ou pelo menos seu dispositivo ou browser) e vincular esse identificador a um banco de dados.

8.6.3.3 Cookies de rastreamento

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

Assim como acontece com os cookies padrão, os cookies de terceiros colocados no computador do usuário possibilitam salvar algumas informações sobre o usuário para uso posterior. Entretanto, os cookies de terceiros, no entanto, são geralmente definidos por redes de publicidade nas quais um site pode se inscrever.

O objetivo dos cookies é acompanhar quais páginas uma pessoa está visitando, construindo um perfil da pessoa com base em interesses. O perfil pode ser adicionado usando informações de outros sites em sua rede. Ele não está vinculado a detalhes pessoais conhecidos do site, mas apenas exibe anúncios ao perfil do usuário para que eles sejam os mais relevantes possível.

8.6.4 Outras informações de perfil: o preço dos serviços "gratuitos"

O Facebook e o Google sabem quase tudo o que há para saber sobre os usuários de seus produtos gratuitos.

> Coletamos o conteúdo e outras informações que você fornece ao usar nossos serviços, inclusive quando você se inscreve em uma conta, cria ou compartilha e envia mensagens ou se comunica com outras pessoas. Isso pode incluir informações no ou sobre o conteúdo que você fornece, como a localização de uma foto ou a data em que um arquivo foi criado. Também coletamos informações sobre como você usa nossos serviços, como os tipos de conteúdo visualizados ou envolvidos, ou a frequência e duração de suas atividades.
>
> Fonte: Política de Privacidade do Facebook

O mesmo vale para o Google. Com seu mecanismo de pesquisa usado por bilhões de pessoas, combinado com informações do LinkedIn, mapas do Google e postagens de blog, o Google sabe

quais pessoas estão pesquisando ou comprando ativamente e quais palavras ou frases elas usam para encontrá-las. Eles sabem para cada um de seus usuários o que provavelmente comprarão em breve, o que precisarão comprar agora, mais tarde hoje, amanhã e muito mais.

O Google sabe, por causa das informações que eles têm sobre onde estamos, quem somos, onde estaremos e o que faremos. Eles sabem quem somos, quanto gastamos, o que fazemos para viver, nossos dados demográficos (idade, sexo, religião, renda, educação), onde moramos, quem são nossos amigos, o que fazemos fora do trabalho, em quem votamos, em que televisão, podcasts, música ou outro entretenimento que consumimos e muito mais.

O Google também sabe como todas essas coisas mudaram ao longo do tempo. Isso lhes permite encontrar tendências e prever o comportamento, tanto no nível individual quanto no agregado. Em resumo, eles têm exatamente as informações que as empresas precisam para maximizar seu marketing. Essas também são as informações necessárias para fornecer o produto ou serviço que você precisa, exatamente no momento em que você precisa.

8.6.5 Perspectiva de proteção de dados

A proposta de Regulamento sobre Privacidade e Comunicações Eletrônicas (Regulation on Privacy and Electronic Communications[7]), publicada em janeiro de 2017 e destinado a revogar a atual Diretiva (2002/58 / CE), detalha as regras relativas à proteção dos dados pessoais nas comunicações eletrônicas.

As alterações propostas farão com que a Diretiva e-Privacidade esteja alinhada com o GDPR. Nos termos do artigo 27.o da proposta, a intenção original era que o regulamento entre em vigor em 25 de maio de 2018, paralelamente ao GDPR. No entanto, discussões no Conselho da União Europeia sobre detalhes do texto jurídico ainda ocorrem quase todos os meses. Como resultado, não se espera uma implementação definitiva do regulamento antes de 2020.

O Regulamento sobre Privacidade e Comunicações Eletrônicas, em particular, visa o processamento de dados sobre a comunicação e o processamento de metadados. O Artigo 8 trata da "proteção das informações armazenadas e relacionadas ao equipamento terminal do usuário final", ou seja, com cookies, mas também com spywares, identificadores ocultos, bugs da web e " dispositivos de impressões digitais ", etc.

8.6.5.1 Cookies

É proibida a utilização das capacidades de processamento e armazenamento dos equipamentos terminais e a recolha de informações dos equipamentos terminais dos utilizadores finais, incluindo sobre o seu software e hardware, para além do utilizador final em causa, exceto nos seguintes motivos: (...)

Fonte: (draft) Regulamento sobre Privacidade e Comunicações Electrónicas (2017/0003) Artigo 8(1) (acessado em 6 de maio de 2017).

[7] Proposal for REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

As exceções são:

(a) é necessário exclusivamente com o objetivo de efetuar a transmissão de uma comunicação eletrônica através de uma rede de comunicações electrónicas ou,
(b) o usuário final deu o seu consentimento ou,
(c) é necessário fornecer um serviço da sociedade da informação requerido pelo utilizador final ou,
(d) se for necessário para a medição do público na web, desde que essa medição seja efetuada pelo fornecedor do serviço da sociedade da informação solicitado pelo utilizador final.

Os cookies de sessão normalmente cabem em (a), (c) ou (d) e, como tal, podem ser armazenados sem o consentimento, como no carrinho de compras on-line discutido anteriormente.

Para outros cookies, é necessário o consentimento conforme definido no GDPR. Esse consentimento deve ser dado livremente, específico, informado, ativo e não ambíguo. Novo na proposta é que os usuários finais podem expressar o consentimento (ou a falta dele) pelas configurações do navegador. Isso ajudará a minimizar a sobrecarga de banners e pop-ups.

8.6.5.2 Criação de Perfil

Não há dúvida de que o GDPR se aplica à criação de perfil, conforme descrito no item (72). Por conseguinte, o titular dos dados tem o direito de se opor ao processamento:

> Quando dados pessoais são processados para fins de marketing direto, o titular dos dados deve ter o direito de se opor a tal processamento, incluindo o perfil na medida em que está relacionado a tal marketing direto, seja em relação ao processamento inicial ou posterior, em qualquer tempo e gratuitamente. Esse direito deve ser explicitamente levado ao conhecimento dos dados e apresentado de forma clara e separada de qualquer outra informação.
>
> Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; item 70.

Uma nova consequência do GDPR, em particular o direito de inspeção e correção, irá capacitar o titular dos dados um pouco mais do que antes:

> Um titular de dados deve ter o direito de acesso aos dados pessoais que foram coletados a respeito dele e de exercer esse direito facilmente e em intervalos razoáveis, a fim de estar ciente e verificar a legalidade do processamento.
>
> Isto inclui o direito de os titulares de dados terem acesso a dados relativos à sua saúde, por exemplo, os dados dos seus registos médicos que contêm informações como diagnósticos, resultados de exames, avaliações por processamento de médicos e qualquer processamento ou intervenções fornecidas.
>
> Todos os titulares de dados devem, portanto, ter o direito de conhecer e obter comunicação, especialmente no que diz respeito aos fins para os quais os dados pessoais são processados, quando possível, o período pelo qual os dados pessoais são processados, os destinatários dos dados pessoais, a lógica envolvida em qualquer processamento automático de dados pessoais e, pelo menos quando baseado em perfis, as consequências de tal processamento.
>
> Sempre que possível, o controlador deve ser capaz de fornecer acesso remoto a um sistema seguro que forneceria ao sujeito dos dados acesso direto aos seus dados pessoais. Esse direito não deve afetar adversamente os direitos ou liberdades de terceiros, incluindo segredos comerciais ou propriedade intelectual e, em particular, os direitos autorais que protegem o software. Contudo, o resultado dessas considerações não deve ser uma recusa em fornecer todas as informações à pessoa em causa.
>
> Quando o controlador processa uma grande quantidade de informações relativas ao titular dos dados, o controlador deve poder solicitar que, antes da entrega da informação, o titular dos dados especifique as informações ou atividades de processamento a que o pedido se refere.

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; item 63

Mas ainda há muitos serviços "gratuitos", oferecendo conteúdo ou outros produtos ou serviços gratuitos, desde que o usuário consinta em coletar informações sobre eles, seus interesses e gostos para "selecionar propaganda apropriada". O GDPR não mudará isso, mas pelo menos nos dará a chance de corrigir essa informação.

Cabe ao titular dos dados ter cuidado com as informações reveladas às empresas que oferecem boletins ou outros serviços gratuitos. Como citado acima, assim que um titular dos dados se conscientizar de uma empresa rastreando seu comportamento, a objeção a esse processamento deve ser bem-sucedida.

O ponto é que a maioria das pessoas está acostumada a concordar com declarações longas sem realmente lê-las. O GDPR proíbe a declaração longa e ilegível e requer uma linguagem simples e clara, explicando para que os dados pessoais coletados devem ser usados.

8.7 Big data

O processamento atual de grandes quantidades de informações dos clientes (ou melhor, de todos que usam a Internet) para criar os perfis descritos nos parágrafos anteriores, ilustra a observação no primeiro parágrafo deste documento.

O desafio era e ainda é, encontrar um equilíbrio entre as preocupações com a proteção das liberdades pessoais e a possibilidade de apoiar o livre comércio em toda a Europa.

Há razão para duvidar se a "privacidade" realmente tem um futuro. Embora o GDPR indique claramente que a Comissão Europeia assume a sua obrigação, tal como referido nos itens 1 e 2, seriamente:

Os princípios e as regras relativas à proteção das pessoas físicas em relação ao processamento dos seus dados pessoais devem, independentemente da sua nacionalidade ou residência, respeitar os seus direitos e liberdades fundamentais, em especial o seu direito à proteção de dados pessoais. O presente regulamento destina-se a contribuir para a realização de um espaço de liberdade, segurança e justiça e de uma união econômica, para o progresso econômico e social, para o reforço e convergência das economias no mercado interno e para o bem-estar das pessoas físicas.

Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; item 2

Contato EXIN

www.exin.com