**GUIA DE APRENDIZAGEM**

# RGPD em Portugal

*Regulamento Geral sobre a Proteção de Dados*

O que é, como funciona e como protege os seus dados pessoais

| Nível de aprendizagem | Edição |
|---|---|
| **Iniciante** | **Junho de 2026** |

Ver mais artigos em: **Ajuda à Informática**
(www.formacaoajuda.com)

# Introdução e Nota de Boas-Vindas

Bem-vindo ao Guia de Aprendizagem sobre o **Regulamento Geral sobre a Proteção de Dados** (RGPD) em Portugal, desenvolvido como parte dos guias de aprendizagem do site Ajuda à Informática (formacaoajuda.com).

Este guia foi criado para responder a uma necessidade real: muitas pessoas utilizam serviços digitais diariamente — redes sociais, serviços de saúde, plataformas de compras, bancos, aplicações de telemóvel — no entanto, a grande maioria não saber que têm direitos fundamentais sobre os seus dados pessoais que fornece sem qualquer reserva ou preocupação (erradamente). Todavia, o desconhecimento dessas regras pode ter consequências práticas para a nossa vida privada e a nossa segurança digital.

O presente guia não requer conhecimentos prévios de direito, nem de informática. A linguagem utilizada é clara e acessível, com exemplos do quotidiano que facilitam a compreensão. Cada capítulo está organizado de forma progressiva, permitindo ao leitor avançar ao seu ritmo.

**Como utilizar este guia**

Leia os capítulos pela ordem indicada, pois cada um prepara o seguinte. No final de cada módulo encontrará uma caixa de resumo com os pontos mais importantes. Os termos técnicos ou jurídicos encontram-se explicados na primeira vez que surgem no texto, e num glossário no final do documento.

# Índice

# Modulo 1 — O que é o RGPD e porque existe

## 1.1 Contexto histórico e surgimento do RGPD

Vivemos numa era em que a informação digital é um bem precioso. Cada vez que utilizamos um serviço online — ao criar uma conta de correio eletrónico (e-mail), ao fazer uma compra online num site, ao consultar o medico através de uma plataforma digital — estamos a partilhar dados sobre nós próprios. Durante muitos anos, as regras que regulavam a utilização desses dados foram insuficientes, fragmentadas e desatualizadas.

A União Europeia (EU) reconheceu que era necessário criar uma legislação moderna, uniforme e eficaz para proteger os cidadãos. Foi assim que surgiu o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, mais conhecido pela sigla RGPD — Regulamento Geral sobre a Proteção de Dados. Este regulamento entrou em vigor em maio de 2018 e aplica-se diretamente em todos os Estados-Membros da União Europeia, incluindo Portugal.

**Sabia que?**

Antes do RGPD, cada país da União Europeia tinha a sua própria lei de proteção de dados, baseada numa diretiva europeia de 1995. Com a revolução digital, essas leis tornaram-se obsoletas. O RGPD veio criar um quadro único, moderno e mais rigoroso para todos os países da UE.

## 1.2 O que é o RGPD em linguagem simples

O RGPD é um conjunto de regras que define como as empresas, organizações e entidades públicas devem recolher, guardar, utilizar e proteger os dados pessoais das pessoas. Ao mesmo tempo, confere aos cidadãos direitos concretos sobre os seus próprios dados.

Imagine que os seus dados pessoais são como os seus objetos pessoais numa mala. O RGPD define quem pode abrir essa mala, o que pode retirar dela, durante quanto tempo pode guardar o que retirou, e obriga a pedir a sua autorização antes de a abrir — salvo em situações previstas na lei.

## 1.3 Porque é importante para si

O RGPD é relevante para qualquer pessoa que:

- Utilize a internet, redes sociais ou aplicações no telemóvel
- Tenha cartões de fidelidade em supermercados ou lojas
- Utilize serviços de saúde, banca ou seguros
- Receba newsletters ou comunicações de marketing
- Trabalhe em qualquer organização, publica ou privada
- Seja proprietária de um negócio, mesmo que pequeno

## 1.4 Os princípios fundamentais do RGPD

O RGPD assenta em sete princípios fundamentais, previstos no artigo 5º do Regulamento, que regem qualquer tratamento de dados pessoais:

| Princípios (Parte 1) | Principios (Parte 2) |
|---|---|
| 1. Licitude, lealdade e transparência | 5. Limitação da conservação |
| 2. Limitação das finalidades | 6. Integridade e confidencialidade |
| 3. Minimização dos dados | 7. Responsabilidade (Accountability) |
| 4. Exatidão | |

Em termos práticos, estes princípios significam que as entidades só podem recolher os dados estritamente necessários, apenas para fins específicos, durante o tempo mínimo necessário, e são responsáveis por demonstrar que cumprem a lei.

> ⚠ **Atenção**
> O RGPD não se aplica apenas a grandes empresas tecnológicas. Aplica-se a qualquer entidade (alguns exemplos: uma clínica dentaria, uma associação de pais, uma pequena loja online, ou uma junta de freguesia) que trate dados pessoais de pessoas que se encontrem no espaço da União Europeia.

# Modulo 2 — O RGPD em Portugal: enquadramento jurídico

## 2.1 A Lei nº 58/2019 de 8 de agosto

Embora o RGPD seja diretamente aplicável em todos os países da União Europeia sem necessidade de transposição, ele reserva um conjunto de matérias para regulamentação nacional. Em Portugal, essa regulamentação foi assegurada pela Lei nº 58/2019, de 8 de agosto, que entrou em vigor no dia seguinte ao da sua publicação em Diário da República.

Esta lei complementa o RGPD e regula, em particular, os seguintes aspetos:

- A organização e o funcionamento da Comissão Nacional de Proteção de Dados (CNPD)
- As atribuições do Encarregado de Proteção de Dados – EPD (DPO — Data Protection Officer)
- O tratamento de dados de menores, pessoas falecidas, trabalhadores e dados de saúde
- Os prazos de conservação de dados pessoais
- O regime de coimas e sanções em Portugal

## 2.2 A Comissão Nacional de Proteção de Dados (CNPD)

A CNPD é a entidade pública responsável por supervisionar o cumprimento do RGPD e da legislação nacional de proteção de dados em Portugal. E uma entidade administrativa independente, dotada de autonomia financeira, que funciona junto da Assembleia da República.

As suas principais funções são:

- Fiscalizar e controlar o cumprimento do RGPD e da Lei nº 58/2019
- Receber e instruir queixas e participações de cidadãos
- Emitir pareceres e orientações técnicas
- Aplicar sanções administrativas e coimas
- Cooperar com outras autoridades de proteção de dados europeias

**Como contactar a CNPD**

O cidadão pode contactar a CNPD através do seu site oficial em www.cnpd.pt, por correio eletrónico para geral@cnpd.pt, por telefone: (+351) 213 928 400, ou por correspondência para Av. D. Carlos I, 134, 1º andar, 1200-651 Lisboa. A CNPD disponibiliza formulários próprios para apresentação de queixas e pedidos de informação.

## 2.3 A Lei nº 59/2019 de 8 de agosto

Publicada na mesma data que a Lei nº 58/2019, a Lei nº 59/2019 transpôs para a ordem jurídica portuguesa a Diretiva (UE) 2016/680. Esta lei estabelece regras especificas para o tratamento de dados pessoais pelas autoridades competentes no âmbito da prevenção, deteção, investigação ou repressão de infrações penais e execução de sanções penais.

Esta lei será analisada em detalhe no Modulo 7 do presente guia.

## 2.4 A Constituição da República Portuguesa e o artigo 35º

A proteção de dados pessoais tem raízes profundas no direito constitucional português. O artigo 35º da Constituição da República Portuguesa, sob a epigrafe "Utilização da informática", consagra um conjunto de direitos fundamentais dos cidadãos em relação ao tratamento automatizado de dados pessoais. Este artigo estabelece, desde a versão original da Constituição de 1976, o direito ao conhecimento, retificação e atualização dos dados pessoais, bem como a proibição de acesso a dados de terceiros sem autorização legal.

## 2.5 Sanções e coimas em Portugal

O incumprimento do RGPD e da legislação nacional pode resultar em coimas de valor muito elevado. Em Portugal, as coimas variam consoante a gravidade das infrações e o tipo de entidade infratora:

| Tipo de Infracoes | Valor das Coimas |
|---|---|
| Infrações muito graves (ex: tratamento ilícito de dados sensíveis) | Ate 20 milhões de euros ou 4% do volume de negócios mundial anual |
| Infrações graves (ex: falta de medidas de segurança adequadas) | Ate 10 milhões de euros ou 2% do volume de negócios mundial anual |
| Pequenas e Medias Empresas | Limites máximos proporcionalmente reduzidos |
| Grandes Empresas | Limites máximos conforme o RGPD |

> ⚠ **Importante**
> Em Portugal, a Lei nº 58/2019 estabelece que, excepto em casos de dolo, a abertura de processos contraordenacionais depende sempre de um aviso prévio da CNPD ao infrator, concedendo um prazo razoável para a regularização. Esta é uma proteção adicional oferecida pelo legislador português.

# Modulo 3 — O que são dados pessoais

## 3.1 Definição de dados pessoais

O conceito de “dado pessoal” é central em todo o RGPD. O artigo 4º, nº 1, do Regulamento define dados pessoais como qualquer informação relativa a uma pessoa singular identificada ou identificável.

Uma pessoa é considerada “identificável” quando pode ser identificada, direta ou indiretamente, nomeadamente por referência a um identificador como o nome, um número de identificação, dados de localização, identificadores por via eletrónica, ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa.

## 3.2 Exemplos práticos de dados pessoais

Para melhor compreensão, eis exemplos de dados que são considerados dados pessoais:

- Nome completo e apelidos
- Nº de Identificação Civil (BI ou Cartão de Cidadão)
- Nº de Identificação Fiscal (NIF), Nº de utente do cartão de Saúde, Nº de Segurança Social (NIIS)
- Morada de residência ou trabalho
- Número de telefone ou telemóvel
- Endereço de correio eletrónico (e-mail)
- Data de nascimento
- Fotografia ou imagem de vídeo
- Endereço IP do computador ou telemóvel
- IMEI do dispositivo
- Localização GPS
- Número de matrícula do automóvel ou veículo motorizado
- Cookies de navegação na internet

**Exemplos do quotidiano**

Quando preenche um formulário para receber uma newsletter, quando encomenda um produto online, quando vai ao médico, quando marca uma consulta por telefone, quando entra num edifício com videovigilância, ou quando utiliza um cartão de fidelidade num supermercado — em todos estes momentos, dados seus estão a ser recolhidos e tratados.

## 3.3 Categorias especiais de dados pessoais (dados sensíveis)

O artigo 9º do RGPD identifica categorias especiais de dados que merecem proteção reforçada, por serem particularmente sensíveis. O tratamento destes dados é, em princípio, proibido, salvo em situações expressamente previstas na lei:

- Origem racial ou étnica
- Opiniões políticas
- Convicções religiosas ou filosóficas
- Filiação sindical
- Dados genéticos
- Dados biométricos (impressão digital, reconhecimento facial)
- Dados relativos a saúde
- Dados relativos a vida sexual ou orientação sexual

> ⚠ **Dados de saúde — especial atenção**
> Os dados de saúde são dos mais sensíveis que existem. Quando uma clínica, hospital ou laboratório recolhe informação sobre o seu estado de saúde, diagnósticos ou medicação, esse tratamento é (ou deverá ser) regulado de forma muito rigorosa. Na maioria dos casos, estes tratamentos são legitimados pela lei (não pelo consentimento), pois servem para prestar cuidados de saúde, conforme previsto no artigo 9º, nº 2, alínea h) do RGPD.

## 3.4 Dados de menores

Os dados pessoais de crianças e jovens merecem atenção especial. Em Portugal, nos termos do artigo 8º do RGPD e do artigo 16º da Lei nº 58/2019, o tratamento de dados de menores baseado em consentimento exige que este seja prestado ou autorizado pelos representantes legais (pais ou tutores) sempre que a criança tenha menos de 13 anos. Entre os 13 e os 17 anos, é possível que a própria criança preste consentimento em determinadas situações, dependendo da sua maturidade.

## 3.5 Dados de pessoas falecidas

O RGPD não se aplica a dados de pessoas falecidas. Contudo, o artigo 17º da Lei nº 58/2019 estabelece que, quando estejam em causa dados sensíveis ou dados relativos a intimidade da vida privada, imagem ou comunicações, o exercício dos direitos pode ser feito por quem o titular tenha designado para o efeito, ou na sua falta, pelos herdeiros.

# Modulo 4 — Os seus direitos como titular de dados pessoais

## 4.1 Visão geral dos direitos

O RGPD conferiu mais direitos as pessoas e reforçou os já existentes. Ao mesmo tempo, impôs mais transparência nas comunicações entre as entidades responsáveis pelo tratamento dos dados e os titulares. A tabela seguinte resume os principais direitos:

| Direito | O que significa em linguagem simples |
|---|---|
| **Direito de Acesso (Art. 15.º)** | Saber quais os dados que uma entidade possui sobre si e como são utilizados. |
| **Direito de Retificação (Art. 16.º)** | Corrigir dados incorretos ou incompletos. |
| **Direito ao Apagamento (Art. 17.º)** | "Direito a ser esquecido" — pedir a eliminação dos seus dados. |
| **Direito à Limitação (Art. 18.º)** | Suspender temporariamente o tratamento dos seus dados. |
| **Direito à Portabilidade (Art. 20.º)** | Receber os seus dados num formato digital e transferi-los para outra entidade. |
| **Direito de Oposição (Art. 21.º)** | Opor-se ao tratamento dos seus dados, incluindo para fins de marketing. |
| **Direito de não ser sujeito a decisão automatizada (Art. 22.º)** | Não ser objeto de decisões tomadas exclusivamente por sistemas automáticos. |
| **Direito de Informação (Arts. 13.º e 14.º)** | Ser informado, de forma clara, sobre como os seus dados são tratados. |

## 4.2 Como exercer os seus direitos

O exercício dos seus direitos é gratuito e deve ser feito junto do responsável pelo tratamento dos seus dados — que é a entidade (empresa, organização, serviço público) que recolheu e trata os seus dados pessoais.

Regras praticas para exercer os seus direitos:

1. Identifique-se de forma clara no pedido, comprovando a sua identidade se necessário.
2. Utilize, sempre que possível, o canal indicado pela entidade na sua política de privacidade (geralmente um email especifico ou um formulário online).
3. Guarde copia do pedido que enviou e da data em que o enviou.
4. A entidade tem, em regra, um prazo de um mês para responder, podendo este prazo ser prorrogado por mais dois meses em casos complexos.
5. Se a entidade não responder ou recusar o seu pedido sem fundamento, pode apresentar queixa a CNPD.

**Exercício de direitos — o que escrever**

Não precisa de usar linguagem jurídica. Um e-mail simples é suficiente. Por exemplo: “Venho, ao abrigo do artigo 15º do RGPD, solicitar informação sobre todos os dados pessoais que a vossa organização possui sobre mim, bem como os fins para que são utilizados.” Indique sempre o seu nome completo e um contacto para resposta.

## 4.3 O direito ao apagamento (“direito a ser esquecido”)

Um dos direitos mais conhecidos e o direito ao apagamento, previsto no artigo 17º do RGPD. Este direito permite-lhe pedir a uma entidade que elimine os seus dados pessoais. No entanto, este direito não é absoluto e pode ter limites.

Pode pedir o apagamento dos seus dados quando:

- Os dados já não são necessários para a finalidade para que foram recolhidos
- Retirou o seu consentimento e não existe outra base legal para o tratamento dos dados
- Se opôs ao tratamento e não há interesses legítimos prevalecentes da entidade
- Os dados foram tratados de forma ilícita

A entidade pode recusar o apagamento quando:

- O tratamento seja necessário para cumprimento de uma obrigação legal
- Os dados sejam necessários para declaração, exercício ou defesa de um direito em processo judicial
- Existam outros fundamentos legais que justifiquem a manutenção dos dados

## 4.4 O direito a portabilidade

O direito a portabilidade, previsto no artigo 20º do RGPD, permite-lhe receber os seus dados pessoais num formato estruturado, de uso corrente e de leitura automática (como um ficheiro .csv ou .xml), e transferi-los para outra entidade. Este direito e particularmente útil, por exemplo, quando muda de fornecedor de serviços e quer levar o histórico das suas transações ou o seu perfil de utilizador.

## 4.5 O direito de oposição ao marketing direto

Qualquer pessoa tem o direito de se opor, em qualquer momento, ao tratamento dos seus dados pessoais para fins de marketing direto, incluindo a definição de perfis associada a esse marketing. A oposição é incondicional — a entidade deve cessar o tratamento imediatamente, sem necessidade de qualquer justificação por parte do titular.

# Modulo 5 — Política de privacidade: o que deve conter

## 5.1 O que é uma política de privacidade

A política de privacidade é o documento através do qual uma entidade cumpre a sua obrigação de transparência perante os titulares dos dados. O RGPD, nos artigos 13º e 14º, estabelece de forma detalhada quais as informações que devem ser comunicadas ao titular dos dados.

Na prática, quando visita um website, instala uma aplicação ou preenche um formulário, a entidade e obrigada a disponibilizar uma política de privacidade clara e acessível, antes ou no momento em que os dados são recolhidos.

## 5.2 Informações obrigatórias numa política de privacidade

Segundo os artigos 13º e 14º do RGPD, uma política de privacidade deve conter, no mínimo, as seguintes informações:

- Identidade e contactos do responsável pelo tratamento (a entidade que recolhe os dados)
- Contactos do Encarregado de Proteção de Dados (EPD), quando exista
- Finalidades do tratamento (para que são usados os dados)
- Base legal que justifica o tratamento (consentimento, contrato, obrigação legal, etc.)
- Destinatários dos dados (quem vai receber ou ter acesso aos dados)
- Transferências para países fora da União Europeia, se aplicável
- Prazo de conservação dos dados
- Direitos dos titulares e forma de os exercer
- Direito a apresentar reclamação a autoridade de controlo (CNPD em Portugal)

**Como ler uma política de privacidade**

As políticas de privacidade podem ser longas, mas foque-se nas secções: “Dados que recolhemos”, “Como usamos os seus dados”, “Partilha de dados com terceiros”, “Quanto tempo guardamos os seus dados” e “Os seus direitos”. Se não encontrar estas informações de forma clara, isso é um sinal de alerta.

## 5.3 A linguagem da política de privacidade

O RGPD exige que a informação seja prestada de forma concisa, transparente, de fácil e de compreensão fácil, assim como o seu acesso seja fácil, utilizando uma linguagem clara e simples, em especial quando a informação e destinada especificamente a crianças. A linguagem jurídica excessivamente técnica não é aceitável quando torna a política de privacidade incompreensível para o utilizador medio.

## 5.4 Consentimento versus outras bases legais

Um equívoco comum é pensar que o consentimento é sempre necessário para o tratamento de dados. Na realidade, o artigo 6º do RGPD prevê seis bases legais distintas que podem legitimar o tratamento de dados pessoais:

| Bases Legais (Grupo 1) | Bases Legais (Grupo 2) |
|---|---|
| a) Consentimento do titular | d) Defesa de interesses vitais |
| b) Execução de um contrato | e) Exercício de funções de interesse público |
| c) Cumprimento de obrigacao legal | f) Interesses legítimos do responsável |
| | |

Isto significa que, por exemplo, quando assina um contrato com um fornecedor de telecomunicações, a empresa pode tratar os seus dados sem pedir consentimento específico, porque esse tratamento é necessário para a execução do contrato — base legal prevista na alínea b). O consentimento só e a base legal adequada quando não existe outra que se aplique.

## 5.5 Requisitos do consentimento

Quando o consentimento e efetivamente a base legal adequada, este deve reunir os seguintes requisitos, conforme o artigo 7º do RGPD:

- Livre — não pode ser condicionado a prestação de um serviço se o tratamento não for necessário para esse serviço
- Específico — deve referir-se a uma finalidade concreta
- Informado — o titular deve saber exatamente o que esta a autorizar
- Inequívoco — deve resultar de um ato positivo claro (por exemplo, assinalar uma caixa; o silêncio ou as caixas pré-assinaladas não são válidos)
- Revogável — deve ser tão fácil de retirar como foi de dar

> ⚠ **Atenção as caixas pré-assinaladas**
> Se um formulário online já tem a caixa “Aceito receber comunicações de marketing” assinalada por defeito, isso não constitui consentimento valido nos termos do RGPD. O utilizador tem de assinalar ativamente a sua concordância.

# Modulo 6 — Partilha e transferência digital de dados e ficheiros

## 6.1 O que e a partilha de dados pessoais

A partilha de dados pessoais ocorre sempre que uma entidade comunica ou disponibiliza dados pessoais a outra entidade ou pessoa. Esta partilha pode ocorrer de várias formas: por e-mail, através de plataformas de colaboração, via API (interface de programação de aplicações), por transferência de ficheiros, ou através de bases de dados partilhadas.

O RGPD estabelece regras rigorosas sobre quando e como esta partilha pode ocorrer, quem pode ter acesso aos dados e que garantias devem estar em vigor.

## 6.2 Partilha dentro da União Europeia

A partilha de dados pessoais entre entidades localizadas em Estados-Membros da União Europeia é, em princípio, livre, desde que sejam respeitados as bases legais e os princípios do RGPD. Contudo, mesmo dentro da UE, a entidade que partilha os dados (responsável pelo tratamento) continua a ser responsável por garantir que a entidade que recebe os dados os trata em conformidade com o RGPD.

## 6.3 Transferência de dados para fora da União Europeia

A transferência de dados pessoais para países fora da União Europeia (países terceiros) ou para organizações internacionais esta sujeita a regras especificas, previstas nos artigos 44º a 49º do RGPD. O objetivo e garantir que os dados continuam a ser protegidos ao mesmo nível que na UE.

As transferências só são permitidas quando:

- O pais de destino foi reconhecido pela Comissão Europeia como tendo um nível de proteção adequado (decisão de adequação). Exemplos: Canada, Japão, Suíça, Nova Zelândia
- Existam garantias adequadas, como cláusulas contratuais-tipo aprovadas pela Comissão Europeia, regras vinculativas para empresas (Binding Corporate Rules), ou códigos de conduta
- Numa situação especifica, o titular tiver dado consentimento explicito para a transferência, apos ser informado dos riscos

**Exemplo pratico: serviços que utilizem a Nuvem (Cloud)**

Quando utiliza um serviço de armazenamento na nuvem (cloud) de uma empresa americana, como o Google Drive ou o Microsoft OneDrive, os seus dados podem ser transferidos para servidores localizados nos EUA. Estas transferências só são licitas se a empresa tiver implementado mecanismos legais adequados, como as cláusulas contratuais-tipo aprovadas pela UE.

## 6.4 Envio de ficheiros com dados pessoais — boas práticas

O envio de ficheiros que contenham dados pessoais por meios digitais (e-mail, plataformas de partilha, mensagens instantâneas) requer cuidados especiais. As seguintes boas praticas devem ser seguidas:

- Minimize os dados — envie apenas os dados estritamente necessários para a finalidade pretendida
- Utilize encriptação — ao enviar ficheiros com dados pessoais, utilize encriptação de ponta-a-ponta sempre que possível
- Proteja os ficheiros com palavra-passe — para ficheiros Excel, Word, PDF ou ZIP com dados pessoais, defina sempre uma palavra-passe de acesso
- Transmita as credenciais por canal diferente — envie a palavra-passe por SMS e o ficheiro por email
- Verifique o destinatário — antes de enviar, confirme que o endereço de email do destinatário esta correto
- Evite redes Wi-Fi públicas — nunca transmita dados pessoais em redes não seguras
- Documente as transferências — mantenha registo de quando, para quem e que dados foram partilhados

## 6.5 Cookies e rastreamento online

Os cookies são pequenos ficheiros de texto armazenados no seu navegador (browser) quando visita um website. Alguns cookies são essenciais para o funcionamento do site, mas outros destinam-se a rastrear o seu comportamento de navegação para fins de publicidade ou análise.

O RGPD, em articulação com a Diretiva ePrivacy (Lei das Comunicações Eletrónicas), exige que:

- Os websites informem o utilizador sobre os cookies utilizados antes de os instalarem
- Obtenham consentimento válido para os cookies não essenciais
- Permitam ao utilizador gerir as suas preferências de cookies
- Disponibilizem uma opção de rejeitar todos os cookies não essenciais tao facilmente quanto a opção de os aceitar

> ⚠ **Aviso sobre apps de telemóvel**
>
> As aplicações instaladas no seu telemóvel podem recolher dados de localização, contactos, histórico de chamadas, fotos e muito mais. Ao instalar uma app, leia com atenção as permissões que solicita. Pergunte-se: “Esta aplicação realmente precisa de aceder a minha localização ou aos meus contactos para funcionar?”. Em caso de dúvida, não autorize.

## 6.6 Violação de dados pessoais (data breach)

Uma violação de dados pessoais ocorre quando há um incidente de segurança que resulta na destruição, perda, alteração, divulgação ou acesso não autorizado a dados pessoais. Exemplos incluem: um ataque informático (hacking), o envio de dados para o destinatário errado, a perda

de um computador portátil ou telemóvel com dados, ou a publicação acidental de dados numa página web.

O artigo 33.º do RGPD obriga os responsáveis pelo tratamento a notificar a CNPD de qualquer violáceo de dados pessoais, sempre que possível, no prazo de 72 horas após tomar conhecimento da mesma. Quando a violação for suscetível de afetar gravemente os direitos dos titulares, é ainda obrigatório informar diretamente as pessoas afetadas.

# Modulo 7 — A Diretiva (UE) 2016/680 e o contexto penal

## 7.1 Enquadramento e objeto da Diretiva

A Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, constitui um instrumento jurídico distinto do RGPD, embora complementar. Enquanto o RGPD regula o tratamento de dados pessoais em geral, esta Diretiva tem um âmbito especifico: o tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e a livre circulação desses dados.

A Diretiva também revogou a Decisão-Quadro 2008/977/JAI do Conselho, que anteriormente regulava a matéria no espaço europeu.

## 7.2 Quem esta abrangido por esta Diretiva

A Diretiva aplica-se ás “autoridades competentes”, que são as entidades públicas dos Estados-Membros autorizadas a:

- Prevenir, investigar, detetar ou reprimir infrações penais
- Executar sanções penais, incluindo proteger e prevenir ameaças à segurança publica

Em Portugal, estas entidades incluem, por exemplo, a Polícia de Segurança Publica (PSP), a Guarda Nacional Republicana (GNR), a Polícia Judiciária (PJ), o Ministério Publico e os tribunais no exercício das suas funções penais.

## 7.3 Transposição para o direito português — Lei nº 59/2019

A Diretiva foi transposta para o direito português através da Lei nº 59/2019, de 8 de agosto. Esta lei define os princípios, as condições de licitude, os direitos dos titulares (com as restrições aplicáveis ao contexto penal), as obrigações das autoridades competentes e o regime de supervisão e controlo.

## 7.4 Princípios aplicáveis no contexto penal

A Lei nº 59/2019 adapta os princípios gerais do RGPD ao contexto específico da atividade policial e judicial. Em particular:

- Os dados devem ser recolhidos para fins determinados, explícitos e legítimos no âmbito penal, e não podem ser utilizados para fins incompatíveis
- É necessário distinguir, sempre que possível, entre diferentes categorias de titulares de dados: suspeitos, condenados, vítimas e testemunhas
- Devem ser distinguidas, na medida do possível, as categorias de dados com base no grau de exatidão e fiabilidade
- Os dados baseados em factos devem ser separados dos dados baseados em apreciações pessoais

## 7.5 Direitos dos cidadãos no contexto da Diretiva

No âmbito da Lei nº 59/2019, os direitos dos titulares de dados estão sujeitos a restrições especificas, justificadas pela natureza das atividades de prevenção e investigação criminal. No entanto, os seguintes direitos mantem-se em vigor:

- Direito de ser informado sobre o tratamento dos seus dados, salvo quando tal prejudique a investigação
- Direito de acesso aos dados que lhe digam respeito, sujeito a limitações operacionais
- Direito de retificação ou apagamento, quando os dados sejam incorretos ou tratados de forma ilícita
- Direito de apresentar queixa a CNPD

**Diferença essencial**

No contexto do RGPD (Lei nº 58/2019), os seus direitos são mais amplos e o acesso é relativamente direto. No contexto da Diretiva (Lei nº 59/2019), os direitos podem ser restringidos por razões operacionais de investigação criminal. Por isso, quando exercer direitos junto de autoridades policiais ou judiciais, a resposta pode ser mais limitada — e isso esta previsto e é legalmente admissível.

## 7.6 Supervisão e papel da CNPD

A CNPD é também a autoridade de supervisão para os efeitos da Diretiva (UE) 2016/680 em Portugal. A CNPD tem competência para verificar a licitude dos tratamentos de dados efetuados pelas autoridades competentes no âmbito penal, receber queixas de cidadãos e, se necessário, adotar as medidas corretivas adequadas.

# Modulo 8 — Consentimento, licitude e boas práticas

## 8.1 O consentimento como base legal — revisão aprofundada

Como referimos no Modulo 5, o consentimento e apenas uma das seis bases legais possíveis para o tratamento de dados. Contudo, e a base legal mais relevante para a relação entre cidadãos e serviços digitais (redes sociais, plataformas online, newsletters, etc.).

A CNPD alerta para três erros comuns em matéria de consentimento:

6. Considerar que o consentimento é sempre necessário (em muitas situações contratuais ou legais, existem outras bases legais mais adequadas).
7. Assumir que o consentimento dado numa situação se aplica a outra — o consentimento é especifico e não pode ser inferido de uma situação para outra.
8. Utilizar caixas de verificação pré-assinaladas ou silêncio como consentimento — isto não é valido nos termos do RGPD.

## 8.2 Responsabilidade (Accountability) — obrigacao de comprovar o cumprimento

Um dos princípios mais importantes do RGPD, frequentemente desconhecido do publico em geral, e o princípio da responsabilidade, consagrado no artigo 5º, nº 2. Segundo este princípio, o responsável pelo tratamento não só deve cumprir o RGPD, como deve ser capaz de demonstrar esse cumprimento.

Na prática, isto significa que as entidades devem:

- Manter um registo de atividades de tratamento
- Realizar avaliações de impacto sobre a privacidade (quando necessário)
- Documentar as bases legais de cada tratamento
- Implementar políticas internas de proteção de dados
- Formar os seus colaboradores sobre o RGPD

## 8.3 O Encarregado de proteção de Dados (EPD)

O artigo 37º do RGPD obriga determinadas entidades a designar um Encarregado de Proteção de Dados (EPD ou mundialmente conhecido como DPO — Data Protection Officer). A designação é obrigatória quando:

- A entidade e uma autoridade ou organismo publico
- As atividades principais implicam operações de tratamento em grande escala que exigem monitorização regular e sistemática dos titulares
- As atividades principais implicam tratamento em grande escala de categorias especiais de dados (dados sensíveis)

Em Portugal, a Lei nº 58/2019 alargou as atribuições do EPD (ou DPO), que passa a ser também responsável por assegurar a realização de auditorias periódicas e não programadas, entre outras funções.

## 8.4 Privacidade por concepção e por defeito

O artigo 25º do RGPD introduz dois conceitos inovadores que representam uma mudança de paradigma: a privacidade por concepção (privacy by design) e a privacidade por defeito (privacy by default).

Privacidade por concepção significa que a proteção dos dados deve ser considerada desde o inicio, no momento em que se concebe um produto, serviço ou sistema, e não apenas adicionada depois como um "complemento". Uma empresa que desenvolva uma nova aplicação deve integrar mecanismos de privacidade desde a fase de projeto.

Privacidade por defeito significa que, por defeito (ou seja, sem qualquer intervenção do utilizador), apenas devem ser tratados os dados pessoais necessários para cada finalidade especifica. As configurações mais protetoras da privacidade devem ser as predefinidas.

**Exemplo prático**

Uma rede social que, por defeito, tornasse públicos os dados dos utilizadores, estaria a violar o princípio da privacidade por defeito. As configurações de privacidade mais restritivas devem ser as que se aplicam automaticamente, sem que o utilizador precise de as configurar manualmente.

## 8.5 Boas práticas para o cidadão digital

Como utilizador de serviços digitais, pode adotar as seguintes praticas para proteger os seus dados pessoais:

- Leia as políticas de privacidade antes de se registar num serviço (pelo menos as secções principais)
- Não partilhe mais informação do que a estritamente necessária
- Utilize palavras-passe robustas e diferentes para cada serviço
- Ative a verificação em dois passos (ou autenticação de dois fatores) sempre que possível
- Reveja periodicamente as permissões das aplicações instaladas no seu telemóvel
- Seja cauteloso com e-mails que solicitem dados pessoais (phishing)
- Reveja regularmente as configurações de privacidade das suas redes sociais
- Exerça os seus direitos junto das entidades que tratam os seus dados

# Modulo 9 — O que fazer em caso de violação dos seus dados

## 9.1 O que fazer se suspeitar que os seus dados foram utilizados indevidamente

Se suspeitar que os seus dados pessoais foram utilizados sem a sua autorização, de forma incorreta, ou que foram divulgados indevidamente, pode e deve agir. O RGPD confere-lhe mecanismos concretos de tutela.

9. Contacte diretamente a entidade responsável pelo tratamento. Explique a situação e solicite esclarecimentos por escrito. Guarde sempre toda a correspondência trocada.
10. Se não obtiver resposta satisfatória, apresente uma reclamação á CNPD. Pode fazê-lo através do formulário disponível no site www.cnpd.pt ou por correspondência.
11. Pode também recorrer á via judicial, intentando uma ação contra o responsável pelo tratamento ou o subcontratante, para obtenção de indemnização por danos sofridos, conforme o artigo 82º do RGPD.
12. Em situações de carater penal (acesso não autorizado a sistemas informáticos, furto de identidade digital), deve apresentar queixa junto das autoridades competentes (PSP, GNR ou diretamente no Ministério Publico).

## 9.2 Como apresentar uma reclamação á CNPD

O processo de apresentação de reclamação é gratuito e pode ser feito por qualquer cidadão. A CNPD disponibiliza um formulário específico para o efeito no seu site. No formulário deve constar:

- A identificação do reclamante
- A identificação da entidade reclamada
- Descrição clara dos factos que motivam a reclamação
- Documentação de suporte disponível (e-mails, capturas de ecrã, contratos, etc.)

**Prazo de resposta da CNPD**

A CNPD tem o dever de informar o reclamante sobre o resultado da reclamação. Os prazos de instrução dos processos variam consoante a complexidade do caso. A CNPD pode tomar medidas corretivas, impor coimas, ou emitir ordens vinculativas a entidade reclamada.

## 9.3 Direito a indemnização

O artigo 82º do RGPD confere a qualquer titular de dados o direito de obter uma indemnização do responsável pelo tratamento ou do subcontratante pelos danos materiais ou imateriais que tenham sofrido em resultado de uma violação do RGPD. Os danos imateriais (como angustia, perda de controlo sobre os próprios dados, ou dano reputacional) são expressamente reconhecidos como indemnizáveis.

## 9.4 Associações de defesa dos direitos dos titulares

O artigo 80º do RGPD prevê a possibilidade de o titular dos dados conferir mandato a uma entidade sem fins lucrativos, cujos fins estatutários sejam de interesse público e cuja atividade abranja a defesa dos direitos em matéria de proteção de dados, para exercer os seus direitos em seu nome. Em Portugal, existem diversas associações de defesa do consumidor e dos direitos digitais que podem prestar este tipo de apoio.

**⚠ Phishing e roubo de identidade digital**

O phishing é uma das formas mais comuns de utilização indevida de dados pessoais. Consiste em comunicações fraudulentas (emails, SMS, chamadas telefónicas) que simulam ser de entidades legitimas (banco, finanças, CTT, etc.) para obter dados pessoais ou credenciais de acesso. Se receber uma comunicação suspeita, não clique em links, não forneça dados, e denuncie a entidade que esta a ser imitada e, se aplicável, as autoridades.

# Modulo 10 — Glossário e recursos de apoio

## 10.1 Glossário de termos essenciais

| Termo | Definicao |
|---|---|
| RGPD | Regulamento Geral sobre a Proteção de Dados — Regulamento (UE) 2016/679 |
| Dados pessoais | Qualquer informação relativa a uma pessoa singular identificada ou identificável |
| Titular dos dados | A pessoa singular a quem os dados dizem respeito |
| Responsável pelo tratamento | Entidade que define os fins e os meios do tratamento de dados |
| Subcontratante | Entidade que trata dados em nome do responsável pelo tratamento |
| Tratamento de dados | Operação sobre dados pessoais: recolha, registo, armazenamento, utilização, divulgação, etc. |
| Consentimento | Manifestação de vontade, livre, especifica, informada e inequívoca do titular para o tratamento dos seus dados |
| DPO / EPD | Data Protection Officer / Encarregado de Protecao de Dados: pessoa responsável pela conformidade com o RGPD na organização |
| CNPD | Comissão Nacional de Proteção de Dados — autoridade de controlo portuguesa |
| Finalidade do tratamento | O objetivo específico para o qual os dados são recolhidos e tratados |
| Minimização dos dados | Princípio que limita o tratamento aos dados estritamente necessários para a finalidade |
| Pseudonimização | Técnica que substitui os identificadores diretos por pseudónimos, mantendo a possibilidade de reidentificação com informação adicional |
| Anonimização | Processo que torna impossível a identificação do titular dos dados de forma irreversível |

| | |
|---|---|
| Data breach | Incidente de segurança que resulta em acesso, perda ou divulgação não autorizada de dados pessoais |
| Accountability | Princípio do RGPD que obriga o responsável a demonstrar o cumprimento do Regulamento |
| Cookies | Pequenos ficheiros de texto armazenados no navegador para diversos fins (sessão, preferências, rastreamento) |

## 10.2 Recursos de apoio e referencias legais

Para aprofundar os conhecimentos sobre o RGPD e a proteção de dados pessoais em Portugal, recomendamos os seguintes recursos:

### Entidades oficiais

- CNPD — Comissão Nacional de Proteção de Dados: www.cnpd.pt
- Autoridade Europeia para a Proteção de Dados (EDPS): www.edps.europa.eu
- Comité Europeu para a Proteção de Dados (EDPB): www.edpb.europa.eu
- Jornal Oficial da União Europeia (legislação): eur-lex.europa.eu

### Legislação de referência

- Regulamento (UE) 2016/679 (RGPD) — 27 de abril de 2016
- Diretiva (UE) 2016/680 — 27 de abril de 2016
- Lei nº 58/2019, de 8 de agosto — Lei de Execução do RGPD em Portugal
- Lei nº 59/2019, de 8 de agosto — Transposição da Diretiva 2016/680
- Artigo 35º da Constituição da Republica Portuguesa

### Plataforma: Ajuda á informática

- Site oficial: www.formacaoajuda.com
- Cursos e formações sobre literacia digital, segurança informática e privacidade online

## 10.3 Resumo final — Os 10 pontos que deve recordar

13. O RGPD aplica-se a qualquer entidade que trate dados de pessoas que se encontrem na União Europeia, independentemente da sua dimensão.
14. Os seus dados pessoais são seus. Tem o direito de saber como são usados, corrigi-los, apaga-los e transferi-los.

15. O consentimento não é sempre necessário — existem seis bases legais validas para o tratamento de dados.
16. Quando o consentimento é exigido, deve ser livre, especifico, informado, inequívoco e fácil de retirar.
17. Qualquer política de privacidade deve ser clara, acessível e conter informação sobre quem recolhe os dados, para que fins e durante quanto tempo.
18. A partilha de dados com terceiros, especialmente fora da UE, está sujeita a regras rigorosas.
19. Em caso de suspeita de utilização indevida dos seus dados, pode reclamar junto da CNPD ou recorrer a via judicial.
20. A CNPD é a autoridade portuguesa responsável por fiscalizar o cumprimento do RGPD e defender os seus direitos.
21. As autoridades policiais e judiciais estão sujeitas a regras próprias (Lei nº 59/2019), que equilibram a segurança pública com a proteção dos seus dados.
22. Proteger os seus dados pessoais é uma responsabilidade partilhada — entre as entidades que os tratam e os próprios cidadãos, através de comportamentos digitais responsáveis.

# Modulo 11 — Perguntas Frequentes dos Cidadaos (FAQ)

Este modulo responde, de forma direta e clara, as questões que os cidadãos colocam com mais frequência sobre o RGPD e a proteção dos seus dados pessoais no dia a dia. Cada resposta inclui a base legal aplicável.

## Pergunta 1. Sou obrigado a fornecer todos os dados do meu Cartao do Cidadao (incluindo NIF, NISS e Número do Cartão de Saúde)?

**Resposta: Nao.**

O princípio da minimização de dados (Artigo 5º, nº 1, alínea c) do RGPD) estabelece que os dados recolhidos devem ser adequados, pertinentes e limitados ao estritamente necessário em relação aos fins para os quais são tratados.

Se uma entidade — loja, banco ou empresa de telecomunicações — pedir o seu Cartão do Cidadão, não é obrigatório fornecer todos os dados visíveis (frente e verso). Deve fornecer apenas os dados estritamente necessários para a finalidade em questão.

| Finalidade | Dados Necessários | Dados que NAO deve fornecer |
|---|---|---|
| Identificação numa loja (ex.: devolução) | Nome + N.o do Cartao de Cidadao | NIF, NISS, Nº do Cartão de Saúde |
| Contrato de telemóvel | Nome, NIF (para faturar), morada | NISS, Nº do Cartão de Saúde |
| Serviço publico (ex.: marcação de consulta) | Nome, Nº do Cartão de Saúde | NIF, NISS |
| Emprego | Nome, NIF, NISS (Segurança Social) | Nº Cartão de Saúde (salvo função. relevante) |

O que fazer se pedirem mais dados do que o necessário:

- Pergunte: “Para que finalidade precisam destes dados?”
- Exija uma base legal — a entidade deve explicar porque precisa daqueles dados específicos.
- Recuse fornecer dados irrelevantes — se nao houver justificacao, nao e obrigatorio fornece-los.
- Denuncie a CNPD — se a entidade insistir sem fundamento legal.

**Base legal aplicável**

Artigo 5º, nº 1, alínea c) do RGPD (Minimização de dados). Artigo 6º do RGPD (Licitude do tratamento). Lei nº 58/2019 (Execução do RGPD em Portugal).

## Pergunta 2. Posso recusar-me a fornecer o meu NIF a uma empresa?

**Resposta: Depende do contexto.**

O NIF (Número de Identificação Fiscal) é exigido por lei em determinadas situações. Noutras, pode recusar-se a fornece-lo.

- Se o NIF for obrigatório por lei (ex.: para faturar serviços, contratos de telecomunicações, ou transações acima de 1.000 euros), não pode recusar, pois a empresa tem obrigação legal de o recolher, ao abrigo do Artigo 29.o do Código do IVA.
- Se o NIF não for necessário para a finalidade (ex.: comprar um produto numa loja física), pode recusar.
- Algumas empresas exigem o NIF por política interna, sem que seja um requisito legal. Nestes casos, pode pedir para faturar sem NIF (se for possível) ou fornecer um comprovativo de morada em alternativa.

**Base legal aplicavel**

Artigo 29º do Código do IVA (obrigação de emissão de fatura com NIF). Artigo 5º, nº 1, alínea c) do RGPD (minimização de dados). Artigo 6º, nº 1, alínea c) do RGPD (obrigação legal como base de licitude).

## Pergunta 3. Ao fazer o registo num hotel, sou obrigado a fornecer o meu Cartão do Cidadão para que o hotel faca fotocopia da frente e do verso?

**Resposta: Não.**

Os hotéis em Portugal tem obrigação legal de registar os seus hospedes (nome, número de identificação, nacionalidade, data de nascimento e morada) nos termos do Decreto-Lei nº 39/2008 (Regulamento dos Estabelecimentos de Alojamento Turístico). Contudo, essa obrigação não inclui fotocopiar o Cartão do Cidadão.

| O que o hotel PODE fazer | O que o hotel NAO pode fazer |
|---|---|
| Registar manualmente os dados necessários (nome, nº CC, data de nascimento, nacionalidade) | Exigir fotocopia da frente e do verso do Cartão de Cidadão para registo de hospedes |
| Verificar a identidade do hospede pedindo para mostrar o Cartão do Cidadão | Armazenar dados desnecessários como NIF, NISS ou Nº do Cartão de Saúde |

O verso do Cartão de Cidadão contem dados como NIF, NISS e Nº do Cartão de Saúde — informação que não é pertinente para o registo hoteleiro. A sua recolha viola o princípio da minimização de dados.

O que fazer se o hotel insistir em fotocopiar o documento:

- Recuse educadamente e explique que não é obrigatório por lei.
- Ofereça-se para mostrar o Cartão do Cidadão apenas para verificação visual.
- Peca a base legal que justifica a fotocopia completa — o hotel não terá uma resposta valida.
- Denuncie a CNPD se o hotel recusar o registo sem fotocopia ou insistir em armazenar dados desnecessários.

**⚠ Exceção admissível**

Se o hotel exigir garantia de pagamento e, por política interna, registar uma fotocopia da frente do Cartão do Cidadão para prevenir fraudes, tal pode ser tolerável — mas apenas a frente, nunca o verso. Se houver obrigação contratual (ex.: pacote turístico com documentação adicional), aplica-se o mesmo critério de proporcionalidade.

**Base legal aplicável**

Decreto-Lei nº 39/2008 (registo de hóspedes em estabelecimentos turísticos). Artigo 5º, nº 1, alínea c) do RGPD (minimização de dados). Artigo 6º, nº 1, alínea c) do RGPD (licitude com base em obrigação legal). Lei nº 58/2019 (Execução do RGPD em Portugal).

## Pergunta 4. Uma empresa pode partilhar os meus dados com terceiros sem o meu consentimento?

**Resposta: Só em casos específicos.**

A partilha de dados pessoais com terceiros só é permitida se existir uma base legal valida, nos termos do Artigo 6º do RGPD. O consentimento é apenas uma das seis bases possíveis. As situações admissíveis são as seguintes:

- Consentimento explicito do titular (Artigo 6.o, nº 1, alínea a)) — o titular autorizou expressamente a partilha.
- Necessidade para cumprimento de um contrato (Artigo 6º, nº 1, alínea b)) — por exemplo, uma loja online partilha a morada de entrega com o transportador.
- Obrigação legal (Artigo 6º, nº 1, alínea c)) — por exemplo, partilha de informação com a Autoridade Tributaria ou com a Segurança Social.
- Interesse legitimo (Artigo 6º, nº 1, alínea f)) — por exemplo, deteção de fraudes — desde que os direitos do titular não se sobreponham a esse interesse.

O que fazer se os seus dados foram partilhados sem base legal:

- Peca a empresa que apague os seus dados — direito ao apagamento (Artigo 17º do RGPD).
- Exija uma explicação sobre a base legal que justificou a partilha.
- Denuncie a CNPD se a empresa não conseguir apresentar uma justificação valida.

### Base legal aplicável

Artigo 6.o do RGPD (licitude do tratamento e bases legais possíveis). Artigo 17º do RGPD (direito ao apagamento). Lei nº 58/2019 (Execução do RGPD em Portugal).

**Tem mais questões sobre o RGPD?**

Peça apoio a um advogado especializado em **Proteção de Dados** para orientação jurídica personalizada.

Pode também contactar a CNPD em www.cnpd.pt para questões especificas sobre a sua situação.



*Este documento tem carater informativo e educativo. Para situações jurídicas especificas, consulte sempre um advogado*