RGPD

Owned by Miguel Branco •••
Mar 29, 2022

Este documento resume o curso obrigatório sobre RGPD que os colaboradores têm de fazer.

Dá ainda exemplos de perguntas que podem ser feitas e as suas respostas.

RGPD (Regulamento Geral sobre a Proteção de Dados)

- Entrou em vigor 25 Maio 2018
- Cidadãos passam a ser donos dos seus dados
- Aplica-se ao tratamento de dados efetuado por Pessoas Singulares, Coletivas, Públicas ou Privadas, bem como organismos públicos.

Curso enquadra a compliance como uma oportunidade de transformação para as empresas, para que fiquem mais confiáveis e transparentes, potenciando uma maior quota de mercado.

Enquadramento Geral

História

- 1948 Declaração Universal dos Direitos do Homem (vida privada, liberdade de expressão)
- 1950 Convenção para a proteção dos Direitos do Homem
- 1995 Legislação Europeia
- 2012 Início do processo de uniformização
- 2016 Publicação
- 2018 Entrada em vigor
    - União Europeia e Espaço Económico Europeu (Islândia, Liechtenstein e Noruega)

Em Portugal

- 1976 Constituição
- 1991 Primeira lei de proteção de dados + Comissão Nacional de Proteção de Dados Pessoais Informatizados
- 1998 Nova lei, renomeia para Comissão Nacional de Proteção de Dados (CNPD)

Porquê mudar?

- Digital Single Market (uniformização)
- Cyber ataques
- Big Data (cloud)
- Go Digital (mais canais, mobile)
- User Experience (prevenir desconfiança)

Objetivos

- Permitir o desenvolvimento da economia digital
- Permitir que as pessoas controlem os seus dados
- Reforçar a segurança jurídica e prática dos operadores económicos e entidades públicas

O incuprimento é punido com coimas até 4% da faturação global anual ou € 20.000.000,00.

Definições

Dados pessoais

Informação relativa a uma pessoa singular (titular) identificada ou identificável (ex: nome, morada, telefone, etc).

Outros exemplos: IP, impressão digital, dados biométricos, GPS, imagens, matrículas.

Tratamento

Operações efetuadas sobre os dados pessoais.

O tratamento deve:

- Ser lícito, leal e transparente;
- Ter uma finalidade determinada, explícita e legítima;
- Recolher os dados adequados, pertinentes e limitados à finalidade;
- Conservar os dados apenas pelo período necessário;
- Garantir a segurança dos dados.

Tratamento é **lícito** se (uma das seguintes):

- O titular dos dados deu consentimento;
- For necessário para execução de um contrato;
- For necessário para o cumprimento de uma obrigação jurídica;
- For necessário para defesa dos interesses do titular ou outra pessoa singular;
- For necessário para exercício de funções de interesse público;
- For necessário para interesses legítimos do responsável pelo tratamento, exceto se estiverem em causa direitos fundamentais do titular ou crianças.

Ex: um banco tem licitude para pedir alguns dados pessoais sem consentimento explícito (são dados obrigatórios juridicamente / para um contrato). Mas para realizar campanhs de marketing já tem de obter consentimento para utilizar os dados dessa forma.

Responsável pelo tratamento

Pessoa singular, coletiva ou organismo que defina o tratamento (finalidades e meios).

Subcontratante

Pessoa singular, coletiva ou organismo que trate os dados em nome do responsável pelo tratamento.

Consentimento

Manifestação de vontade do titular dos dados a que estes sejam tratados. Tem de ser claro, específico, inequívoco e revogável com a mesma facilidade.

Os Estados-Membros podem legislar que uma criança com idade inferior a 16 anos possa dar consentimento, mas uma inferior a 13 não (terão de ser os pais).

Tipos/Categorias de dados

Grupos distintos de dados. O tratamento de algumas categorias é proibido:

- Origem racial ou étnica
- Opiniões políticas, religiosas ou filosóficas

- Filiação sindical
- Dados genéticos
- Dados biométricos para identificação inequívoca
- Dados relativos à saúde
- Dados relativos à vida e orientação sexual

Exceções:

- Consentimento expresso do cidadão no tratamento desses dados ou que este os tenha tornado públicos
- Garantia dos interesses vitais do titular quando este está incapacitado
- Associação ou fundação sem fins lucrativos e para fins políticos, religiosos, filosóficos ou sindicais do interesse do titular que seja membro ou antigo membro
- Processos judiciais
- Interesse público
- Medicina preventiva, avaliação de capacidade profissional, diagnóstico, cuidados de saúde, contrato profissional de saúde

Mesmo nas exceções, o tratamento destes dados carece de medidas de segurança adicionais.

Autoridade de Controlo

Autoridade criada por cada um dos Estados-Membros para supervisionar. Em Portugal: CNPD.

Âmbito:

- **Material**: dados pessoais tratados por meios (semi/) automatizados ou em ficheiros.
  - Exceções:
    - Segurança Nacional / Política Externa da União / Âmbito Penal / Segurança Pública
    - Atividades pessoais/domésticas de pessoas singulares (ex: lista telefónica pessoal, correspondência)
    - Poder Judicial (cada Estado-Membro decide como aplicar nos tribunais e etc)
- **Territorial**: Responsáveis ou subcontratantes sedeados na União Europeia (independentemente de onde ocorre o tratamento) + Entidades que, estando fora da União, tratem dados de clientes da União.
  - Exemplos:
    - Empresa com sede na Holanda que trata dados de residentes na Austrália.
    - Empresa com sede em Marrocos que contrata outra em Espanha para tratar dados de residentes na África do Sul.
    - Empresa com sede em Israel que trata dados de clientes Europeus para oferta de bens e serviços, mesmo que gratuitos.

FAQ

- Facebook não precisa de cumprir porque eu partilho de livre vontade?
  - Falso, o Facebook precisa de cumprir porque trata os dados.
- Senhor A é empresário e fornece os dados para contrato de eletricidade. Quais os dados abrangidos pelo RGPD?
  - Apenas os que coincidirem com os de pessoa singular. RGPD não abrange dados de pessoa coletiva.
- Empresa com sede na Bélgica mas filiais em todo o lado precisa de cumprir onde?
  - Em todo o lado porque tem sede dentro da UE.
- Outsourcing de Arquivo e Destruição, tem de cumprir?
  - Sim porque recolha, transporte, armazenamento e destruição são considerados tratamento de dados.
- Cliente africano abre conta num bano português, que recolhe etnia no campo observações. É lícito?
  - Não, está proibido recolher dados de origem racial ou étnica.
- Instituição fornece no registo consentimento através de checkboxes previamente preenchidas. É válido?

- Não, porque o consentimento não foi explícito, positivo e inequívoco.

Direitos dos Titulares

Direito de informação

Direito de ser informado acerca dos seus dados e dos tratamentos que lhes são efetuados.

- Contactos do responsável pelo tratamento (ou representante)
- Contactos do encarregado de proteção de dados
- Finalidades do tratamento
- Destinatários ou categorias de dados
- Possíveis transferências para outras entidades
- Prazos de conservação
- Direitos restantes
- Como fazer valer os direitos, ex: apresentar uma reclamação à autoridade de controlo

Mesmo nos dados obrigatórios (que não carecem de consentimento), é sempre necessário informar para que finalidade os dados estão a ser recolhidos.

Direito de acesso

Direito de aceder a qualquer altura aos dados e finalidades, prazos, terceiros, etc., que uma determinada entidade tem sobre ele.

É possível pedir uma cópia dos dados. As informações devem ser prestadas gratuitamente, mas pode ser cobrada uma taxa caso o número de pedidos do titular dos dados seja excessivo (ex: todos os meses). A entidade pode recusar-se a entregar a informação se já o tiver feito diversas vezes num espaço de tempo razoável.

A informação deverá ser dada no práximo máximo de um mês (extensível até 2) e em formato eletrónico sempre que pedida por essa via.

Direito de retificação

Direito de corrigir os dados. Deverá ser sem demora.

Direito de apagamento / esquecimento

Titular pode pedir para ser os dados serem apagados quando:

- Os dados deixam de ser necessários para as finalidades para que foram recolhidos
- O titular retira o consentimento e não há fundamento jurídico para o mesmo
- Os dados foram tratados ilicitamente
- Há uma decisão judicial para tal

Ex: quando encerramos uma conta bancária, ou quando percebemos que uma entidade nos faz campanhas de marketing sem termos um contrato/consentimento

Não é um direito absoluto (ex: no encerramento da conta pode ser necessário guardar os dados durante X tempo por natureza fiscal, contratual, jurídica, etc).

Mas mesmo que tenha esses dados pelas obrigações legais, a empresa não pode utilizá-los para outros fins (ex: marketing).

Direito à limitação

Titular pode pedir limitação do tratamento caso os dados estejam incorrectos.

Pode também pedir limitação do direito de apagamento (antes da data efetiva de apagamento) caso necessite dos dados para um processo judicial.

Estados-Membros podem ainda introduzir limitações excecionais em casos de segurança nacional, prevenção ou investigação de crimes, etc. Ex: cimeira do G8 ou Jogos Olímpicos podem necessitar alterações temporárias a algumas regras de vigilância sobre os cidadãos.

Direito à portabilidade

O titular pode pedir os seus dados em formato estruturado e leitura automática, de modo a poder transmiti-los a outra entidade.

Estes dados são os recolhidos pela entidade, e não os construídos posteriormente sem terem sido fornecidos (ex: scoring de crédito, dados de tráfego de internet).

Direito de oposição

- Direito a opor-se ao tratamento dos dados, mesmo que previamente tenha consentido.
- Direito a opor-se a perfilagem (criação de perfis de consumo e comercialização direta).
- Direito a opor-se a decisões individuais automatizadas, como atribuição de crédito, recrutamento ou avaliação de desempenho. Nesse caso pode sempre pedir avaliação de uma pessoa.

Direito de reclamação

Direito a fazer uma reclamação. A reclamação pode ser feita em qualquer autoridade de controlo no espaço europeu (não precisa de ser a portuguesa). Isto é denominado Balcão Único, ou "One-Stop-Shop".

Direito de indemnização

Sempre que os direitos forem violados e o titular tenha sofrido danos, pode pedir uma indemnização por parte do responsável pelo tratamento ou do subcontratante.

FAQ

- Que informação posso pedir à operadora de telecomunicações onde tenho contrato?
  - Toda a informação referida acima no "Direito de informação".
- Na abertura de conta o Banco informa-me de todos os dados que precisa, dos contactos e direitos. Isso chega?
  - Não, é necessário informar sobre a finalidade dos dados e diferenciar os obrigatórios dos facultativos.
- É verdade que o titular de uma conta bancária pode pedir uma cópia dos seus dados gratuitamente sempre que necessitar?
  - Sim, mas a seguir à primeira vez poderá ser cobrada uma taxa mediante a complexidade e periodicidade dos pedidos.
- Se invocar o direito ao apagamento ou esquecimento, o que deve a empresa fazer?
  - Apagar definitivamente os contactos e nunca mais contactar.
- Posso pedir à minha operadora atual para enviar os meus dados pessoais à minha operadora futura?
  - Sim, desde que ela só envie os dados fornecidos pelo titular (e não todos os construídos desde então, como o tráfego gasto no tarifário).
- Posso invocar o direito de oposição para retirar consentimento aos e-mails de marketing mas manter os e-mails de extrato de pontos do cartão cliente do hipermercado?
  - Sim, posso opor-me ao tratamento dos dados para essa finalidade.

Responsáveis pelo Tratamento

Os responsáveis pelo tratamento têm de:

- Implementar as medidas necessárias para assegurar os direitos e liberdades dos titulares dos dados
- Demonstrar o cumprimento das suas obrigações
  - Observação de códigos de conduta ou procedimentos de certificação aprovados
  - Demonstrar a execução das medidas adequadas face à finalidade e riscos do tratamento dos dados e suas categorias

Violação / data breach

Quebra de segurança que provoca destruição, perda, alteração ou divulgação não autorizada de dados pessoais.

Existe obrigação de reportar certos tipos de violação dos dados à Autoridade de Controlo e aos titulares, quando resultam num risco para os direitos e liberdades das pessoas singulares. A violação deverá ser reportada até 72h depois da descoberta (sob pena de coima). Caso não seja possível identificar os titulares afetados, a comunicação deverá ser pública.

Se os dados perdidos forem ilegíveis por terceiros e recuperáveis para o Responsável, não é necessário comunicar a violação.

Proteção de dados pessoais

- Pseudonimização: desligar dados do titular reversivelmente
- Anonimização: tornar dados anónimos irreversivelmente
- Encriptação: tornar ilegível via cifra com chave

Importante também:

- Capacidade para assegurar a confidencialidade, integridade, disponibilidade e resiliência dos sistemas
- Capacidade para testar de forma regular as medidas implementadas

Tratamento dos dados

- Responsáveis conjuntos: mais do que um responsável.
- Representante: entidade sedeada na União que representa outra fora.
- Encarregado de proteção de dados: responsável interno pela proteção de dados. Elo de ligação com a autoridade de controlo e com os titulares dos dados.

Responsáveis / subcontratantes fora da União têm de ter um representante legal estabelecido no Estado-Membro onde é feito o tratamento.

Minimização dos dados

Os dados deverão ser adequados, pertinentes e limitados às funcionalidades para as quais foram recolhidos. Volume inferior de dados representará um custo inferior pelo seu tratamento e segurança.

Subcontratantes

Os Responsáveis pelo tratamento podem subcontratar entidades para fornecer serviços que não conseguem internamente. Nesse caso têm de informar os titulares de quaisquer dados que sejam cedidos aos subcontratantes no âmbito desses serviços.

Os Subcontratantes têm a responsabilidade de garantir as medidas adequadas à segurança dos dados pessoais, e os Responsáveis têm de garantir que os Subcontratantes têm condições para isso, devendo isso estar no contrato entre ambos.

Registo de atividades

O Responsável pelo tratamento (e todas as restantes entidades como subcontratantes e representantes) tem de demonstrar perante a Autoridade de Controlo e os titulares que mantém um registo de todas as atividades de tratamento.

- Nome e contacto do responsável, responsáveis conjuntos, subcontratantes, encarregados de proteção de dados
- Finalidades do tratamento de dados
- Categorias de dados pessoais
- Categorias de destinatários a quem os dados são divulgados
- Transferência para países terceiros
- Prazos previstos de apagamento das diferentes categorias
- Descrição geral das medidas de segurança aplicadas

Avaliações de impacto

Responsável pelo tratamento deve avaliar novos processos quanto ao impacto no tratamento de dados.

Autoridade de Controlo pode tornar pública uma lista de atividades de tratamento que dispensam avaliação de impacto.

Avaliações de impacto que resultem em elevado risco que não se consiga mitigar, o Responsável pelo tratamento deverá contactar a Autoridade de Controlo.

Certificações

Existem Códigos de Conduta e Certificações. Certificações são válidas por 3 anos.

FAQ

- Tem de existir um contrato entre o Responsável pelo tratamento e o Subcontratante?
  - Sim.
- Quem tem de manter o Registo de Atividade?
  - O Reponsável pelo Tratamento, Subcontratantes e Representantes.
- Que cuidados de segurança deverá ter o Responsável pelo tratamento?
  - Deverá garantir níveis apropriados de pseudonimização, cifragem e procedimentos de contigência de dados pessoais em toda a organização.
- O roubo do portátil pessoal de um Gestor de Conta é uma violação de dados dos clientes?
  - Não, porque o portátil pessoal não tem os dados dele.
- Uma empresa sofre um ataque de ransomware e demora 4h a repôr os dados. Deve comunicar à Autoridade de Controlo?
  - Não, uma vez que não houve roubo nem destruição irreversível dos dados.
- Devido ao aparecimento de novos métodos de tratamento de dados e inerente Avaliação de Impacto, é expectável que a Autoridade de Controlo publique uma lista de atividades que não requer avaliação de impacto?
  - Sim.

Encarregado de Proteção de Dados e Autoridades de Controlo

Responsável pelo tratamento e subcontratante (entidades) podem nomear uma pessoa como Encarregado de Proteção de Dados (EPD / Data Protection Officer).

O EPD é responsável por:

- Garantir que o RGPD é aplicado.
- Fazer a ponte entre o Responsável pelo tratamento, a Autoridade de Controlo e os titulares dos dados.

É obrigatório nomear um EPD quando:

- O tratamento é realizado por um organismo público.
- As atividades principais da entidade consistem num tratamento que exige controlo regular e sistemático dos dados em larga escala.

- As atividades principais da entidade consistam em tratamento de larga escala de categorias especiais de dados.

Nomeação

- Um grupo empresarial pode designar apenas um EPD.
- Um grupo de organismos públicos pode designar apenas um EPD.
- O EPD pode pertencer à organização ou ser através de um contrato de prestação de serviços.
- A entidade deverá publicar o contacto do EPD e comunicá-lo à Autoridade de Controlo.
- O EPD responde ao mais alto nível da direção da entidade
- O EPD Está sujeito ao dever de sigilo

Transferência de dados para países terceiros

Efetuadas:

- Com base numa decisão de adequação (a Comissão decide se a transferência cumpre os níveis de proteção adequados)
- Com base em garantias adequadas (apresentadas pelas entidades)
- Com base em regras vinculativas aplicáveis às empresas (salvaguarda dos direitos, designadamente o de oposição)

Caso não se verifique nenhuma das anteriores, só se efetua se:

- O titular der o seu consentimento expresso
- For necessária para a execução de um contrato ou por interesse público
- For necessária para a defesa de um direito num processo judicial
- For necessária para a defesa dos interesses vitais do titular que esteja impossibilitado de consentir

Autoridades de Controlo

- Pode haver mais do que uma Autoridade por Estado-Membro.
- Têm de ter total independência.
- Têm regras quanto à:
  - Sua constituição
  - Nomeação dos seus membros
  - Duração dos mandatos
  - Garantia de não existência de conflitos de interesse
- Têm poderes:
  - De investigação
  - De correção
  - Consultivos
  - De autorização
- Elaboram um relatório anual de atividades que é apresentado ao Parlamento, governo, etc, e fica público.

FAQ

- De quem depende o EPD?
  - Da gestão do responsável pelo tratamento ao mais alto nível.
- Que Autoridades de Controlo pode um Estado-Membro ter?
  - Várias sectoriais que respondem à Autoridade Principal, que representa o país perante o Comité Europeu para a Proteção de Dados.

- Uma empresa de GPS dos EUA que recolha dados por todo o mundo está abringida pelo RGPD?
  - Sim, porque são tratamentos de dados efetuados dentro do espaço comunitário.
- O tratamento dos dados é lícito se for para execução de um contrato do titular?
  - Sim.
- O tratamento de categorias especiais de dados está sempre proibido?
  - Podem fazer-se a título excecional, nas condições do Regulamento.
- É correcto não pedir consentimento para dados obrigatórios?
  - Sim, para dados regulatórios não é necessário consentimento.
- É correcto ter de esperar 2 meses pela informação que pedi sobre os meus dados pessoais?
  - Sim, o prazo é um mês, extensível até 2.
- Um subcontratante deteta uma violação de dados dos clientes fora da União Europeia. Deve notificar?
  - Sim, o tratamento foi feito por um subcontratante europeu.

Avaliação Final

16 Questões, Requisito de 70% (12 questões certas)

Poderá realizar esta Avaliação as vezes que entender, ficando registada a melhor nota.