ROQUETTE
Offering the best of nature™

Privacy & Data Protection

COMO NOS ENGAJAMOS COM RELAÇÃO À PRIVACIDADE E À PROTEÇÃO DE DADOS TODOS OS DIAS

Privacidade e Proteção de Dados

Guia de Boa Conduta

GRUPO ROQUETTE

Departamento Jurídico e de Compliance

Principais desafios de Compliance da Roquette

Sob a liderança da Administração Geral, o escopo de compliance e seu gerenciamento na Roquette são uma parte fundamental do Departamento "Jurídico e de Compliance" do Grupo, conhecido como o Comitê de Compliance.

O Comitê de Compliance é responsável pelo Código de Conduta da Roquette, assim como pela sua atualização e implementação.

Também cobre as tres áreas seguintes:

- Segurança financeira,
- Ética profissional e
- Privacidade e Proteção de Dados.

Por isso, um Programa de Compliance foi desenvolvido e está em desenvolvimento para garantir que os nossos negócios são juridicamente e financeiramente irrepreensíveis.

Qual é o papel de Compliance?

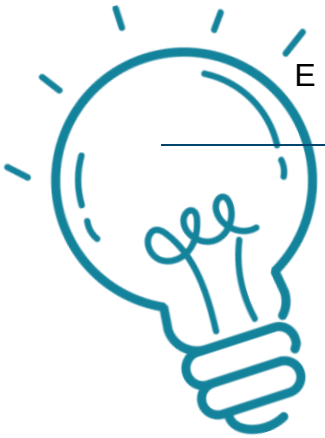
O papel de compliance é incutir **valores éticos** e implementar medidas de acordo com **exigências legais**, **normas** e **boas práticas.**

Nosso Programa facilita a implementação de procedimentos garantindo a conformidade com as regras aplicáveis à Roquette.

Nossos quatro valores – **autenticidade, excelência, orientação para o futuro, bem-estar** – constituem a base sólida nas quais trabalhamos **todos os dias**.

Tenha em mente que, atualmente, uma companhia sustentável é uma companhia ética.

E a companhia do futuro é a companhia que é transparente.



Pensar Globalmente

Agir Localmente

Editorial

Os princípios da Privacidade e Proteção de Dados fazem parte das normas definidas no nosso Código de Conduta.

Todos os funcionários, assim como terceiras partes com quem a Roquette se relaciona, têm o direito à privacidade. Por esse motivo, a Roquette está comprometida na proteção de seus dados pessoais.

Os dados pessoais são informações que permitem identificar direta ou indiretamente uma pessoa física (nome, data de nascimento, número de segurança social, foto, endereço de email, alterar para ID do computador, etc.).

A proteção dos dados pessoais é um direito fundamental que garante a privacidade

A proteção dos dados pessoais garante a cada pessoa o direito de controlar a coleta, o tratamento, a utilização e a distribuição desses dados.

Os dados pessoais devem ser utilizados de modo justo para um fim específico, explícito e legítimo e deve ser conservado apenas durante o tempo necessário para a realização do seu tratamento.

Na Europa, o tratamento dos dados pessoais foi definido no Regulamento Geral de Proteção de Dados (RGPD), que entrou em vigor no dia 25 de maio de 2018.

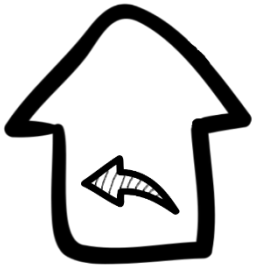
Uma vez que a legislação relacionada com a privacidade e os dados pessoais varia de país para país e porque a Roquette está presente a nível internacional, o Grupo adotou uma Política do Grupo com relação à proteção de dados pessoais. Esta Política se aplica a todos os funcionários do Grupo no mundo inteiro.

Este Guia explica a Boa Conduta a adotar em nossas atividades diárias, para estarmos em conformidade com os Princípios de Proteção de Dados Pessoais e com as exigências de nossa Política.

Jennifer GODIN, Responsável pela Proteção de Dados

Déléguée à la protection des données

Índice



Objetivo

O que é a Política de Privacidade e de Proteção de Dados?

O Grupo Roquette definiu uma Política de Privacidade e de Proteção de Dados (a “Política”) para resolver mais facilmente os problemas de Privacidade e Proteção de Dados em consonância com sua imagem, interesses e as leis e regulamentos aplicáveis com relação à proteção de dados.

Esta Política define os princípios e exigências para a proteção de dados pessoais e indica regras a serem respeitadas por todos os funcionários, gerentes, diretores e terceiras partes agindo em nome da Roquette em matéria de Privacidade e de Proteção de Dados.

Os princípios e regras desta Política de Proteção de Dados Pessoais estão detalhados em uma plataforma documental, com três níveis:

- Comprometimento da administração: Código de Conduta
- Regras internas: Manual e Diretivas de Proteção de Dados Pessoais em Q-Docs.
- Documentação do Sistema de Gerenciamento da Proteção de Dados (DPMS): Procedimentos, Diretrizes, Metodologias, Treinamento, etc.

Toda a documentação está em conformidade com as exigências legais e regulamentares para a proteção de dados.

O que é o Guia de Boa Conduta da Privacidade e da Proteção de Dados?

O Guia de Privacidade e Proteção de Dados (o “Guia”) pode nos ajudar a implementar e cumprir a nossa política de privacidade e proteção de dados.

Ele apresenta, de modo simplificado, regras e boas práticas que estão em conformidade com as diretivas do nosso Grupo e com as exigências das leis e regulamentos aplicáveis a nós em matéria de proteção de dados.

Ele está dividido em temas inspirados no Código de Conduta, sendo que a "Privacidade e a Proteção de Dados" é um dos tópicos de conformidade.

Descrição

A quem se aplica o Guia de Boa Conduta de Privacidade e de Proteção de Dados?

A Política e o Guia constituem as bases comuns para todas as entidades no mundo inteiro. Eles se aplicam a:

- Todos os funcionários, gerentes e diretores (“os Funcionários”)
- Quaisquer terceiras partes trabalhando para a Roquette, como:
  - Fornecedores e prestadores de serviços, incluindo consultores, trabalhadores autônomos e pessoal temporário
  - Estagiários e Aprendizes
  - Pessoal destacado de uma entidade não pertencente à Roquette
  - Trabalhadores temporários
  - Outros representantes
  - Qualquer terceira parte contratada ou remunerada pela Roquette.

Onde podemos encontrar o Guia de Boa Conduta de Privacidade e de Proteção de Dados?

Todos os Funcionários e terceiras partes trabalhando para a Roquette devem compreender e respeitar os princípios de Privacidade e Proteção de Dados incluídos em nossa Documentação e especialmente neste Guia.

O Guia pode ser acessado facilmente no Portal ONE:

Função Global > Proteção de Dados > Guia de Boa Conduta.

Este Guia é divulgado como parte de uma comunicação dedicada, acompanhada por um conjunto de cursos de "e-learning" sobre Princípios de Privacidade e de Proteção de Dados (definidos por normas internacionais e exigências específicas do RGPD).

Este curso de treinamento está incluído no Programa de Integração para a Proteção de Dados.

Responsabilidades

Quem é responsável pela implementação dos Princípios operacionais?

A privacidade dos dados é relevante para (e da responsabilidade de) todas as pessoas da nossa organização.

Todos temos uma responsabilidade de respeitar os Princípios operacionais descritos na Documentação DPMS fornecida pela Equipe do Comitê de Compliance e pela Rede de Proteção de Dados. Este Guia apoia esta implementação e aumenta o nosso nível de conformidade.

Como podemos nos certificar de que estamos tomando a decisão certa?

O Guia foi criado para nos ajudar a enfrentar a maior parte das situações de nossa vida profissional que podem representar dúvidas em matéria de privacidade. No entanto, ele não pode prever todas as situações que podemos enfrentar ao realizarmos nossas atividades profissionais. Se tivermos dúvidas a qualquer momento sobre a melhor atitude a tomar, devemos usar de bom senso e colocar a nós mesmos as seguintes perguntas:

- Isto está conforme com a lei em vigor?
- Isto se reflete de forma positiva em mim e na companhia?
- Eu contaria a um amigo, um familiar ou um colega sobre isso?
- Eu me sentiria confortável se esta situação fosse tornada pública?

Se a resposta a qualquer destas perguntas for negativa, não devemos dar continuidade. Em caso de dúvida, devemos falar com o Responsável pela Proteção de Dados do Grupo ou outra pessoa de contato relevante (veja os dados dos contatos na seção "Levantando questões ou preocupações").

O que acontece se não cumprirmos os Princípios de Privacidade e de Proteção de Dados?

O descumprimento dos Princípios pode ter um efeito negativo para a companhia. As consequências podem ser muito graves, tanto para a companhia quanto para as pessoas envolvidas (sanções disciplinares, multas, pena de prisão, reputação prejudicada, etc.).

Todas as violações reais ou suspeitas aos Princípios reportadas serão levadas a sério. Iremos investigar prontamente, com justiça e em conformidade com as exigências legais. Dependendo do tipo de Violação dos Dados, poderão ser impostas medidas disciplinares, em conformidade com as leis locais e os regulamentos da companhia.

Todos os funcionários deverão colaborar totalmente com qualquer investigação. A Roquette irá proteger a confidencialidade de todas as pessoas envolvidas.

Levantando questões ou preocupações

Os funcionários, terceiras partes agindo pela Roquette e outras partes interessadas são incentivadas a colocar dúvidas ou questões que ajudarão a Roquette a prevenir e reduzir quaisquer danos para a companhia.

Que tipo de questões podem ser abordadas?

Podem ser levantadas quaisquer questões, assim como qualquer violação potencial ou real dos Princípios de Privacidade e de Proteção de Dados, dos regulamentos da companhia ou das leis aplicáveis.

Quem devemos contatar?

Em caso de Violação dos Dados, favor contatar o Diretor de Proteção de Dados em dpo@Roquette.com e/ou relatar um incidente por meio de nosso formulário da web "Privacy Alert".

Se precisar relatar uma possível violação de conformidade, entre em contato com seu ponto de contato habitual ou relate um problema por meio do dispositivo Speakup©. Todos os alertas recebidos por meio desse dispositivo são tratados confidencialmente, respeitando as leis e os regulamentos relevantes.

SpeakUp®

A Roquette não irá tolerar qualquer forma de represália ou retaliação com relação a um funcionário ou uma terceira parte que reporte, de boa fé, uma violação potencial ou real dos Princípios de Privacidade e de Proteção de Dados ou das leis aplicáveis.

Por isso, se o autor de um alerta profissional tiver de se identificar, sua identidade deverá ser tratada de modo confidencial pela organização, para evitar o risco de represálias, discriminação ou medidas disciplinares contra ele/ela pela denúncia dos fatos.

Conformidade com leis e regulamentos

Cada um de nós, em cada entidade do Grupo, deverá cumprir as leis e regulamentos em vigor com relação à Proteção de Dados.

Nos casos em que os regulamentos locais são mais rigorosos do que nossa Política e o Guia, os primeiros deverão prevalecer.

Caso contrário (ausência de leis locais ou de leis menos restritivas), nossas boas práticas internas deverão prevalecer até ao limite permitido pela lei.

Consideramos que:

- Devemos implementar o mais rápido possível todos os novos regulamentos locais e aplicáveis.
- Cada um de nós deverá estar consciente de que qualquer violação das leis e regulamentos pode implicar a aplicação de sanções civis e penais, tanto para as pessoas envolvidas como para a companhia.
- A proteção de pessoas físicas com relação ao tratamento de dados pessoais é um direito fundamental.
- Os princípios e as regras sobre a proteção de pessoas físicas com relação ao tratamento de seus dados pessoais deverão, independentemente de sua nacionalidade ou residência, respeitar seus direitos e liberdades fundamentais, em particular o seu direito à proteção de dados pessoais.
- O direito à proteção de dados pessoais não é um direito absoluto; ele deve ser considerado com relação à sua função na sociedade e ser equilibrado com relação a outros direitos fundamentais, em conformidade com o princípio da proporcionalidade.

Que países adotaram uma legislação específica sobre a proteção de dados ou têm uma Autoridade de Proteção de Dados?

Para ter uma visão geral, consulte este mapa: https://www.cnil.fr/en/data-protection-around-the-world.

Nossas responsabilidades:

- Em todas as circunstâncias, devemos cumprir todas as leis e regulamentos aplicáveis no escopo da Proteção de Dados nos países dos Titulares dos Dados, assim como com todas as regras em vigor em cada uma das localizações da companhia.

- Como parte de nossas atividades profissionais, devemos reportar qualquer comportamento que entendemos estar contra as leis e regulamentos aplicáveis em matéria de Proteção de Dados (ex.: RGPD) ao nosso Responsável pela Proteção de Dados para o endereço dpo@Roquette.com e o dispositivo de alerta Roquette confidencial: Speakup©..

- Devemos implementar medidas de proteção de dados pessoais que sejam adequadas e proporcionais ao contexto, promovendo a conformidade com outras leis e regulamentos. Por outro lado, nossas ações para cumprir as leis e regulamentos aplicáveis ao Grupo deverão estar em conformidade com as regras e boas práticas para a proteção de dados pessoais (exemplo: no programa de compliance Anti-suborno e Anti-corrupção, devemos garantir a proteção do denunciante através de medidas de confidencialidade e de proteção de seus dados pessoais).

Você está sujeito(a) ao Regulamento Geral de Proteção de Dados (RGPD)?

Você entra no escopo do RGPD como **responsável pelo tratamento dos dados** (1) ou como **controlador** (2):

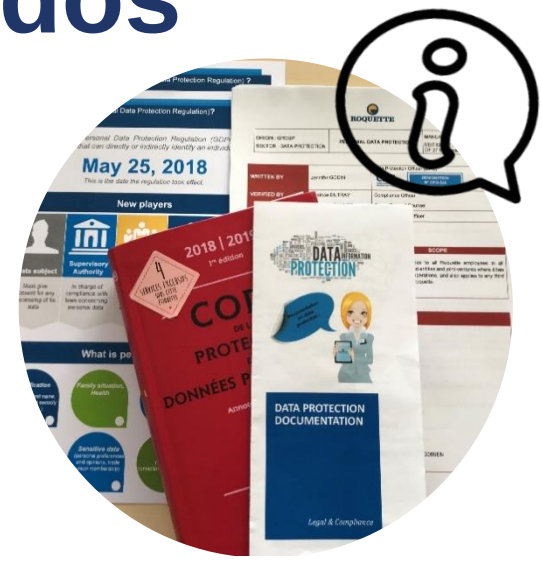
- se você estiver estabelecido(a) na União Europeia (UE) ou;
- caso você não esteja estabelecido(a) na UE, se: suas "atividades de tratamento estão relacionadas com
  - a oferta de bens ou serviços a titulares dos dados na UE;
  - ou o monitoramento de seus comportamentos, desde que seus comportamentos tenham lugar na UE" .

Texto oficial: Artigo 3 do RGPD sobre o Escopo Territorial

(1) e (2): Ver definições na página 38.

No Brasil: Lei Geral de Proteção de Dados Pessoais (LGPD).

Princípios de Proteção de Dados



Os dados pessoais devem ser/estar:

- seguros.
- exatos e atualizados.
- tratados de modo justo e legítimo.
- tratados para fins limitados.
- adequados, relevantes e não excessivos.
- conservados por um período de tempo limitado e determinado.
- tratados em conformidade com os direitos dos titulares dos dados.
- protegidos por medidas legais adequadas, se forem transferidos para outros países.

Seus Direitos:

Em conformidade com a legislação e regulamentos aplicáveis, você tem o direito de acessar, retificar e se opor ao tratamento de seus dados por motivos legítimos, assim como o direito de eliminação dos mesmos por motivos legítimos, o direito à portabilidade dos dados e o direito de limitação do tratamento de seus dados.

Para exercer esses direitos, favor preencher o formulário disponível em: Roquette.com/Data Protection.

Para quaisquer pedidos, favor contatar o **Responsável pela Proteção de Dados** (dpo@Roquette.com).

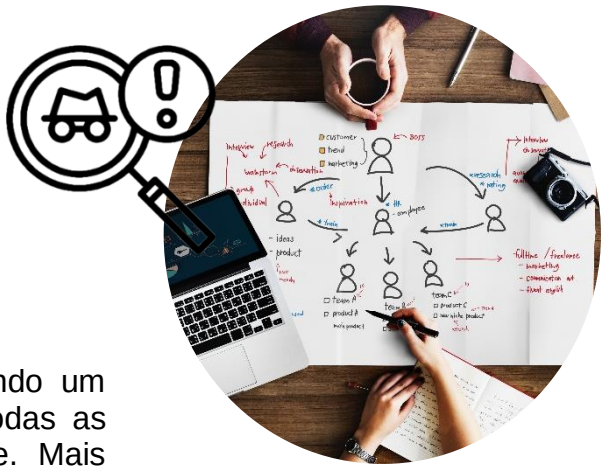
Nossas responsabilidades:

Devemos:

- Seguir a legislação local e as regras da Política do Grupo com relação à Proteção de Dados Pessoais.
- Notificar o Responsável pela Proteção de Dados sobre quaisquer novos tratamentos ou modificações.
- Não coletar, utilizar, divulgar ou armazenar dados de caráter pessoal exceto se for para fins específicos, legítimos e necessários.
- Garantir que as pessoas foram devidamente informadas de que seus dados estão sendo coletados.
- Proteger esses dados durante a coleta, o tratamento, a utilização, a comunicação, o armazenamento e a transferência.
- Garantir a segurança e a confidencialidade dos dados tratados.
- Manter os dados somente durante o tempo necessário para o tratamento e cumprir as leis aplicáveis.
- Contatar o Responsável pela Proteção dos Dados caso ocorra um incidente de segurança envolvendo dados pessoais.

Treinamos nossos funcionários e aprimoramos nossos processos internos.

Risco de privacidade



O que é um risco de privacidade?

Um risco é um cenário hipotético descrevendo um evento que possam ocasionar prejuízos e todas as ameaças que permitiriam que ele ocorresse. Mais especificamente, descreve:

- quais as origens do risco (ex.: um funcionário subornado por um concorrente)
- poderia explorar as vulnerabilidades dos bens de suporte (ex.: o sistema de gerenciamento dos que permite a manipulação dos dados)
- em um contexto de ameaças (ex.: má utilização ao enviar emails)
- e permitir a ocorrência de eventos que possam ocasionar prejuízos (ex.: acesso ilegítimo a dados pessoais)
- em dados pessoais (ex.: cliente)
- originando assim impacto na privacidade dos titulares dos dados (ex.: solicitações indesejadas, sentimentos de invasão da privacidade, problemas pessoais ou profissionais).

Efeito de incerteza na privacidade

A gravidade representa a magnitude de um risco. Ela é sobretudo calculada em termos de alcance dos potenciais impactos (**físicos**, **materiais**, **morais**) nos titulares dos dados, tendo em conta controles existentes, planejados ou adicionais.

Exemplo:

O risco mais importante apresentado pelo sistema de alerta profissional com relação ao denunciante é o risco de represálias, discriminação ou medidas disciplinares adotadas contra ele(ela) por ter denunciado os fatos.

Consideramos que:

Os direitos das pessoas se aplicam na totalidade, independentemente do nível de risco do tratamento.

No entanto, teremos de modular nossa conformidade em matéria de proteção de dados de acordo com o nível de risco que nossas operações de tratamento de dados pessoais colocam aos direitos e liberdades fundamentais das pessoas.

O RGPD dá um maior ímpeto a esta prática. Em consequência, as operações de tratamento que impliquem riscos menores para os direitos e liberdades fundamentais das pessoas podem em geral implicar menos obrigações de conformidade, ao passo que as operações de tratamento de "risco elevado" irão implicar obrigações de conformidade adicionais, como Avaliações do Impacto da Proteção de Dados (AIPD) [(1)]

Nossas responsabilidades:

A avaliação de risco é fundamental. Segundo o RGPD, a consideração do risco serve de base para a responsabilização organizacional e todo o tratamento dos dados.

Precisamos realizar avaliações de risco como parte da AIPD para o tratamento de risco elevado, assim como em conexão com muitas outras exigências do RGPD, incluindo a Segurança dos Dados, as notificações sobre Segurança e a Violação de Dados, a Privacidade por Design, o interesse legítimo, a limitação da finalidade e o tratamento justo.

(1): Ver definição na página 58.

Riscos no caso de não-conformidade

Pessoas físicas e jurídicas que não cumpram a lei e os regulamentos sobre a proteção de dados (ex.: RGPD), correm o risco de sofrer as seguintes sanções com os custos relacionados:

Sanções penais:

- Pena de prisão.
- Multas aplicadas por entidades jurídicas.

Sanções civis:

- Danos civis.

Sanções administrativas:

- Notificação formal.
- Advertência.
- Injunção.
- Limitação temporária ou definitiva do tratamento.
- Retirada de uma certificação ou liminar para retirar uma certificação.
- Suspensão de transferências de dados.
- Liminar para interromper o tratamento ou retirada da autorização.
- Publicidade das sanções impostas.
- Sanções sem notificação formal prévia (critério de urgência).
- Dependendo da violação, uma multa administrativa.

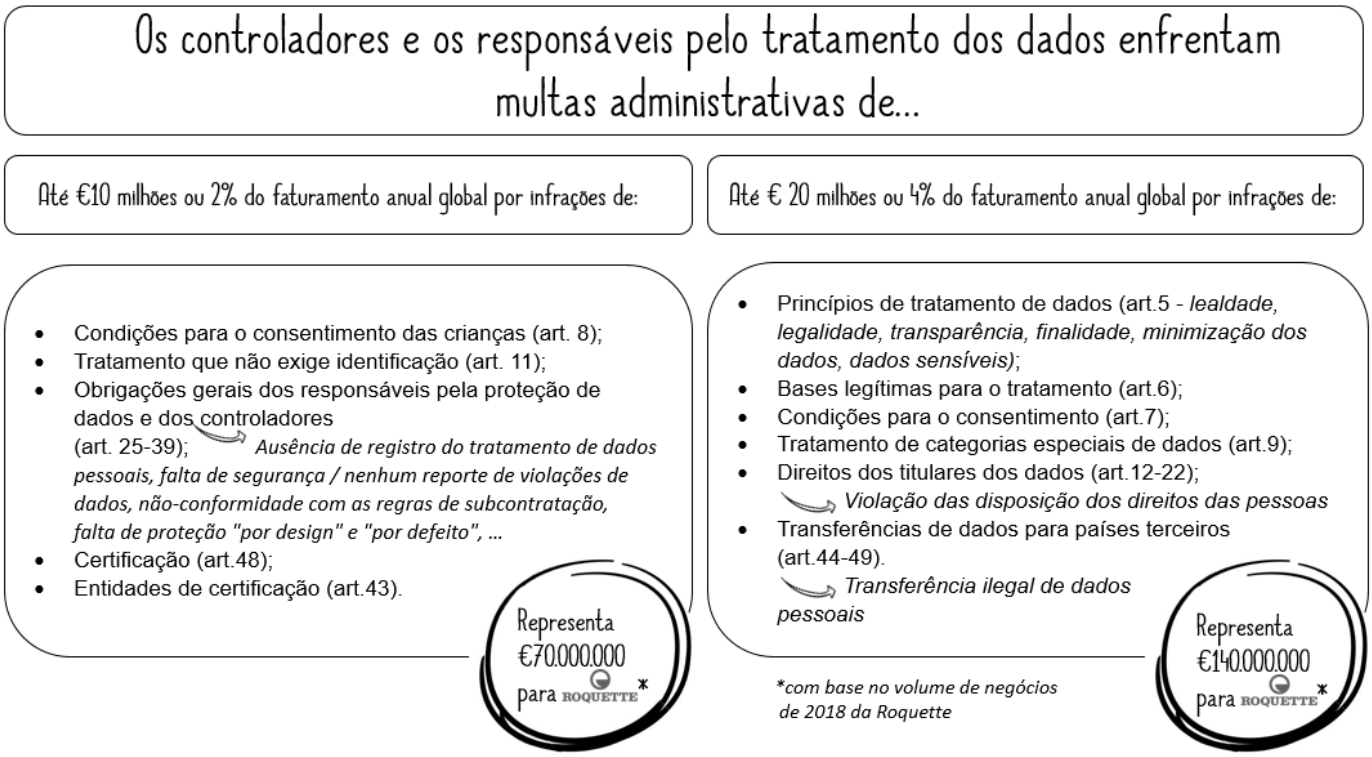
Custos significativos:

- Perda de rendimentos resultante de danos à sua reputação.

Qual é a multa administrativa máxima RGPD?

As multas são discricionárias e não obrigatórias. Elas devem ser impostas caso a caso e devem ser “eficientes, proporcionais e dissuasivas”.

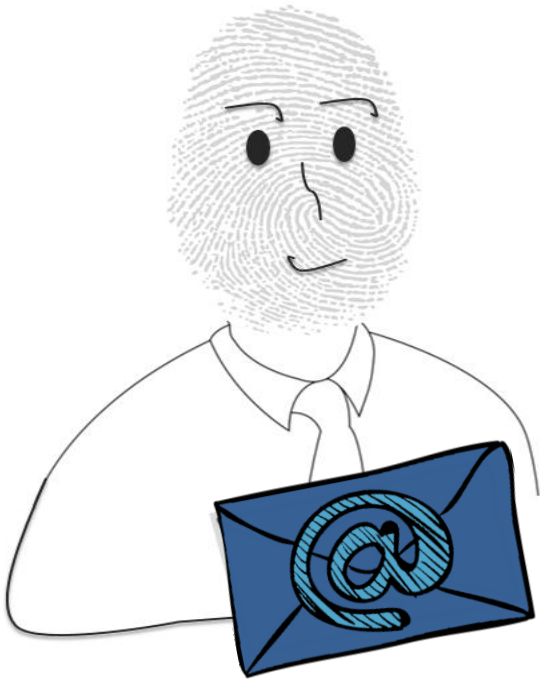
As multas se baseiam nos artigos específicos do Regulamento que a organização violou.



Quais podem ser as sanções penais?

Alguns exemplos das leis francesas:

- O ato de coletar dados pessoais por meios fraudulentos, injustos ou ilícitos deverá ser punível com uma pena de prisão de cinco anos e uma multa de €300.000 (Art. 226-18 do Código Penal).
- Para garantir um verdadeiro direito e proteção do denunciante, a lei anti-corrupção (Sapin II) pune gravemente qualquer obstáculo a um alerta. A confidencialidade ao redor do alerta é um elemento essencial da regulação. Assim, a divulgação de elementos confidenciais do alerta (identidade do denunciante, do demandado, informações prestadas como apoio ao alerta), exceto à autoridade judicial, é punível com uma pena de prisão de dois anos e uma multa de €30.000.



1 Nossas normas em RELAÇÕES COM OS TITULARES DOS DADOS

Cultura de Privacidade

A proteção de dados é um conjunto de leis, regulamentos e melhores práticas orientando a coleta e a utilização de dados pessoais dos indivíduos.

Os dados pessoais significam qualquer informação referente a uma pessoa física identificada ou identificável.

A privacidade dos dados se refere ao tratamento de dados pessoais.

Quem é abrangido?

A privacidade dos dados é relevante para (e de responsabilidade de) todas as pessoas da nossa organização.

Porque ela é importante?

Os dados mal utilizados podem ter repercussões muito negativas para as organizações, seus funcionários e clientes.

As violações de privacidade podem dar origem a sanções financeiras sem limites, artigos negativos na imprensa, reputação prejudicada, perda de confiança dos clientes, perda de negócios e perdas para os funcionários, reclamações e talvez queixas, em caso de violações de privacidade com relação a seus próprios dados pessoais, a possibilidade de ações disciplinares noutros casos. É do interesse de todos nós o tratamento adequado dos dados.

Consideramos que:

- Todos os funcionários da Roquette devem ser conscientizados para suas funções e responsabilidades com relação à proteção de dados pessoais. O aumento da conscientização tem como objetivo reforçar a cultura de respeito pela privacidade e proteção de dados pessoais na Roquette.

[DDPG001EN – Regra 1]

- O treinamento dos funcionários quanto à implementação da política de proteção de dados pessoais deve ser colocado em prática.

[DDPG001EN – Regra 2]

PENSAR NA PRIVACIDADE

É a nossa responsabilidade!

Precisamos dos dados pessoais dos clientes e dos funcionários para realizarmos nossos negócios com sucesso.

Eles confiam em nós para cuidarmos dessas informações essenciais.

Cada um de nossos funcionários tem a responsabilidade de cumprir com as leis de Proteção de Dados adequadas.

É a nossa reputação!

As reputações são conquistadas com dificuldade e perdidas com facilidade.

Tratar os dados de nossos clientes e funcionários com cuidado e respeito é essencial para protegermos nossa reputação.
VOCÊ é a nossa melhor defesa contra os danos na reputação.

É uma questão de respeito!

As escolhas que nossos clientes e funcionários fazem sobre o modo como seus dados pessoais são utilizados devem ser respeitadas, se quisermos manter a confiança que eles depositam em nós.

Está em suas mãos!

Todos somos responsáveis por garantir que os dados pessoais dos clientes e dos funcionários são mantidos em segurança e confidencialidade.
Deve ser tomado um cuidado particular com qualquer informação que precise ser enviada ou levada para o fora da companhia.

Treinamos nossos funcionários e aprimoramos nossos processos internos.

- Código de conduta – Privacidade e Proteção de Dados - p. 42 – 43.
- Para os recém-chegados: Várias informações e sessões de e-Learning sobre a Proteção de Dados serão disponibilizadas durante a Integração Global.
- Para os funcionários: O treinamento será colocado no Workday Learning.
- Para os Coordenadores de Proteção de Dados: A documentação é compartilhada em nossa Comunidade “Rede de Proteção de Dados”.
- Para todos: Estão disponíveis mais informações em ONE > Global Functions > Data Protection.

Dados Pessoais Tratamento

O Tratamento de Dados Pessoais significa qualquer operação ou conjunto de operações realizadas em matéria de dados pessoais ou de conjuntos de dados pessoais, seja ou não por meios automatizados, como a coleta, o registro, a organização, a estruturação, o armazenamento, a adaptação ou a modificação, a recuperação, a consulta, a utilização, a divulgação por transmissão, a disseminação ou por outra forma disponibilizar, o alinhamento ou a combinação, a limitação, a eliminação ou a destruição.

Uma exigência de Proteção de Dados (e RGPD) para a qual você deve estar ciente é que você precisa ter uma "base legítima" para coletar dados pessoais.

Dependendo da legislação local, podem existir várias bases jurídicas.

Qual é minha "base jurídica" para o tratamento de dados pessoais?

Você precisa ser capaz de responder claramente a esta pergunta:

"Como é que você obteve meus/minhas [dados/informações] e porque é que você tem permissão para acessá-los(las)?"

Mas especificamente, significa que você precisa cumprir pelo menos uma das seis bases jurídicas para o tratamento de dados. Ao abrigo do RGPD, você não pode tratar nenhum dado exceto em caso de:

1. Consentimento
2. Contrato
3. Obrigação
4. Interesses vitais
5. Função pública
6. Interesse legítimo

Legitimidade, justiça e transparência

Nossas responsabilidades:

Temos de aplicar regras para garantir o tratamento legítimo dos dados pessoais.

Regras	Referência de Q-Docs	Referência do RGPD
• Agir com legitimidade, justiça e transparência ao coletar os dados	DDPG002EN Regra 1	Art. 5 1. a)
• Demonstrar que o consentimento das pessoas envolvidas é respeitado (sempre que for necessário)	DDPG002EN Regra 2	Art. 7
• Respeitar os objetivos determinados durante a coleta dos dados	DDPG002EN Regra 3	Art. 5 1. b)
• Limitar as informações coletadas em formulários em papel ou digitais somente às utilizações rigorosamente necessárias	DDPG002EN Regra 4	Art. 5 1. c)
• Limitar a retenção de dados somente ao que for rigorosamente necessário	DDPG002EN Regra 5	Art. 5 1. e)
• Adotar medidas para transferir dados pessoais para países terceiros ou organizações internacionais	DDPG002EN Regra 6	Art. 44 to 50

Treinamos nossos funcionários e aprimoramos nossos processos internos.

Direitos dos Titulares dos Dados

Um titular dos dados significa uma pessoa física que pode ser identificada, direta ou indiretamente, em particular por referência a um identificador como o nome, um número de identificação, dados sobre a localização, um identificador online ou a um ou mais fatores específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa física.

O que é um "titular dos dados"?

Esse é o termo técnico para a pessoa a quem em particular pertencem os dados pessoais.

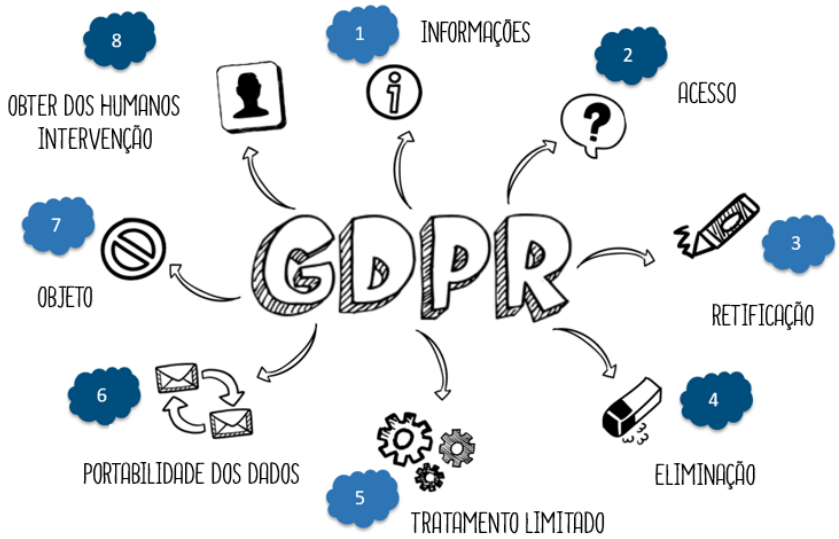
O que é um pedido de acesso de um titular?

Um dos principais direitos que as leis de Proteção de Dados em vigor conferem às pessoas é o direito de acessarem suas informações pessoais.

Uma pessoa pode enviar a você um "pedido pessoal de acesso" solicitando que você lhe fale das informações pessoais que tem a seu respeito, e que lhe envie uma cópia dessas informações. Na maior parte dos casos, você deve responder a um pedido válido de acesso de um titular no período de 30 (*) dias consecutivos após recebê-lo.

(*): Este período pode variar dependendo da lei aplicável ou do tipo de operação de tratamento de dados.

Quais são os outros direitos dos Titulares dos Dados?



Nossas responsabilidades:

Devemos aplicar regras para garantir os direitos dos titulares dos dados.

Regras	Referência de Q-Docs	Referência do RGPD
• Se certificar de que as notificações legais estão em conformidade com as obrigações	DDPG006EN Regra 1	Art. 12
• Permitir que os titulares dos dados exerçam seus direitos de acesso	DDPG006EN Regra 2	Art. 15
• Permitir que os titulares dos dados exerçam o seu direito de retificação	DDPG006EN Regra 3	Art. 16
• Permitir que os titulares dos dados exerçam o seu direito à portabilidade dos dados	DDPG006EN Regra 4	Art. 20
• Permitir que os titulares dos dados exerçam o seu direito à eliminação ("direito de ser esquecido")	DDPG006EN Regra 5	Art. 17
• Permitir que os titulares dos dados exerçam o seu direito à limitação de tratamento	DDPG006EN Regra 6	Art. 18
• Notificar a retificação ou eliminação de dados pessoais ou a limitação de tratamento	DDPG006EN Regra 7	Art. 19
• Controlar a tomada de decisões individual automatizada, incluindo a criação de perfis	DDPG006EN Regra 8	Art. 22

Treinamos nossos funcionários e aprimoramos nossos processos internos.

Declaração de Privacidade

O direito a ser informado se os dados pessoais estiverem sendo utilizados

Devemos informar vocês, enquanto funcionários, e todas as terceiras partes com quem a Roquette tem relação caso estejamos utilizando seus dados pessoais.

Devemos dar informações detalhadas sobre os seguintes tópicos:

- Porque a Roquette está utilizando seus dados.
- Que tipo de dados a Roquette está utilizando.
- Durante quanto tempo os seus dados serão conservados.
- Seus direitos de informação.
- Qual a origem dos dados.
- Informação sobre se a Roquette vai transferir seus dados às terceiras partes, incluindo seus nomes e os motivos da transferência.
- Informação sobre se a companhia vai transferir os dados para outra jurisdição, incluindo o país envolvido e o que será feito com esses dados.
- Se a Roquette está utilizando os dados para a criação de perfis (um tipo de tratamento automatizado em que seus dados pessoais sejam utilizados para analisar ou prever aspectos como o seu desempenho no trabalho, a situação econômica, a saúde).
- Como contatar o DPO (Responsável pela Proteção de Dados).
- Se for o caso, seu direito de apresentar uma reclamação junto à Autoridade de Supervisão.

A isso se dá o nome de **Informações sobre Privacidade** ou **Declaração de Privacidade**.

Devemos dar informações sobre privacidade no momento em que a Roquette coleta os dados. Se a Roquette obtiver os dados de outra fonte, a companhia deverá dar informações sobre a privacidade. Poderá fazê-lo através de uma notificação de privacidade.

A isso se dá o nome de **direito de ser informado**.

Regras	Referência de Q-Docs	Referência do RGPD
• Se certificar de que as notificações legais estão em conformidade com as obrigações	DDPG006EN Regra 1	Art. 12

Exemplos:

- Informação sobre privacidade no website da Roquette disponível em: https://www.Roquette.com/data-protection.
- Informação sobre privacidade no nos processos de RH no Workday@Roquette disponível no ONE: Employee Corner>Workday@Roquette.

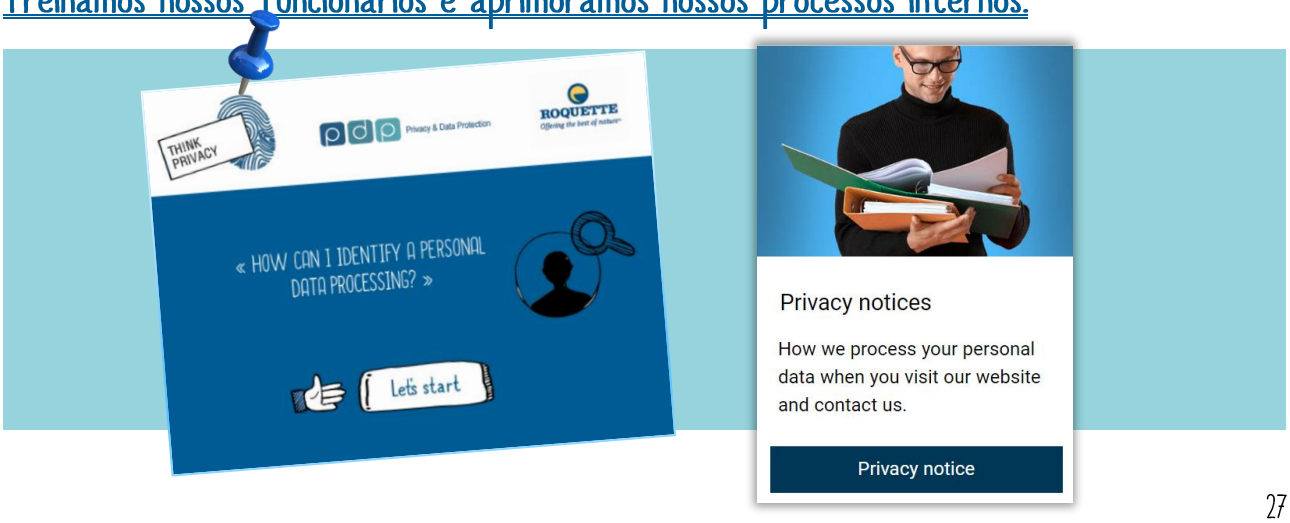
Quando é que a Roquette não tem de dar informações sobre suas atividades?

Em geral, devemos dar informações sobre privacidade, mas em algumas circunstâncias não precisamos fazê-lo. Estas circunstâncias incluem as seguintes situações:

- você já dispõe da informação sobre privacidade e nada mudou,
- dar informação sobre privacidade é algo impossível ou exigiria um "esforço desproporcionado", ou
- dar a informação sobre privacidade tornaria impossível a utilização de seus dados ou prejudicar fortemente os motivos para a utilização dos mesmos.

Nota: Sempre que forem necessárias medidas provisórias para evitar a ocultação ou destruição de provas, essas informações podem ser enviadas após a adoção das medidas provisórias.

Treinamos nossos funcionários e aprimoramos nossos processos internos.



Minimização dos Dados

Qual é o princípio da minimização de dados?

O artigo 5(1)(c)

> "1. Os dados pessoais deverão ser:
>
> (c) adequados, relevantes e limitados àquilo que for necessário com relação às finalidades para os quais eles são tratados (minimização de dados)"

Os formulários em papel ou digitais criados pelas Funções Globais para coletar dados pessoais deverão conter somente áreas de informação rigorosamente necessárias para a finalidade do tratamento, para evitar a coleta de dados não justificados pelo tratamento.

Nossas responsabilidades:

Devemos garantir que os dados pessoais que você está tratando são:

- adequados – suficientes para cumprir adequadamente a finalidade indicada;
- relevantes – tem um link racional para essa finalidade; e
- limitados ao que é necessário – você não dispõe de mais do que aquilo que precisa para a finalidade indicada.

Regras	Referência de Q-Docs	Referência do RGPD
• Limitar as informações coletadas em formulários em papel ou digitais somente às utilizações rigorosamente necessárias.	DDPG002EN Regra 4	Art. 5 1. c)

Lista de verificação:

- ☑ Apenas coletamos dados pessoais de que verdadeiramente precisamos para nossas finalidades específicas.
- ☑ Dispomos de dados pessoais suficientes para cumprimos adequadamente essas finalidades.
- ☑ Revisamos periodicamente os dados de que dispomos e eliminamos tudo o que não for necessário.
- ☑ Devemos identificar a quantidade mínima de dados pessoais que precisamos para cumprir o objetivo. Devemos somente conservar essas informações, não mais do que isso.

O princípio de responsabilização significa que você precisa ser capaz de demonstrar que possui os processos adequados para garantir que você só coleta e conserva os dados pessoais de que precisa.

Também é importante ter em mente que o RGPD estabelece que as pessoas têm o direito de completar quaisquer dados incompletos que não sejam pertinentes para a finalidade em questão, em conformidade com o direito à retificação. Elas também têm o direito de solicitar a eliminação de quaisquer dados que não sejam necessários para a finalidade em questão, em conformidade com o direito à eliminação (direito a ser esquecido).

Treinamos nossos funcionários e aprimoramos nossos processos internos.

Segurança dos Dados

A cibersegurança é uma atividade transversal cuja implementação garante que os dados podem ser compartilhados e utilizados com um nível adequado e garantido de proteção das informações e ativos relacionados:

- **Confidencialidade**: garante que as informações são mantidas em confidencialidade e que não são divulgadas a pessoas ou entidades inadequadas,
- **Integridade**: salvaguarda a exatidão e a integralidade das informações e dos métodos de tratamento,
- **Disponibilidade**: garante que os usuários autorizados sempre têm acesso às informações, às aplicações e aos serviços sempre que for necessário,
- **Rastreabilidade**: se refere à capacidade de manter rastros relevantes e, sempre que for necessário, provas do que foi feito em nossos sistemas. A rastreabilidade também cobre objetivos jurídicos, como o não-repúdio ou a responsabilização.

Os ativos dos Dados Pessoais incluem:

- Documentos em papel (textos, mapas, imagens…),
- Informação digital em ambiente de escritório,
- Informação digital em ambiente móvel,
- Conhecimentos e habilidades profissionais (detidas pelas pessoas ou transmitidas oralmente),
- Itens físicos (como amostras, estirpes, modelos…).

[DSUG006EN] Gerenciamento da Diretiva sobre Cibersegurança

A pseudonimização significa o tratamento de dados pessoais de tal modo que os dados pessoais não podem mais ser atribuídos a um titular de dados específicos sem a utilização de informações adicionais, desde que essas informações adicionais sejam conservadas separadamente e sejam sujeitas a medidas técnicas e organizacionais para garantir que os dados pessoais não sejam atribuídos a uma pessoa singular identificada ou identificável.

A anonimização é o processo pelo qual os Dados Pessoais são modificados de modo irreversível de tal modo que um Titular de Dados não possa mais ser identificado direta ou indiretamente, seja pelo **controlador** (1) dos dados sozinho ou em colaboração com outra parte.

A criptografia é o método pelo qual o purotexto ou qualquer outro tipo de dados é convertido de uma forma legível para uma versão codificada que apenas pode ser descodificada por outra entidade se ela tiver acesso a uma chave de descriptografia. A criptografia é um dos métodos mais importantes para garantir a segurança dos dados, em particular para uma proteção de ponta-a-ponta de dados transmitidos através de redes.

(1): Ver definição na página 38.

Consideramos que:

Para manter a segurança e para evitar o tratamento infringindo leis e regulamentos de proteção de dados, a Roquette e nossas companhias subcontratadas devem avaliar os riscos inerentes ao tratamento e implementar medidas para minimizar esses riscos, como a **criptografia** ou a **pseudonimização**.

Nossas responsabilidades:

Precisamos implementar medidas de segurança ao tratarmos qualquer tipo de dados pessoais, mas aquilo que implementamos depende de nossas circunstâncias particulares. Precisamos garantir a confidencialidade, a integridade e a disponibilidade dos sistemas e serviços que utilizamos para tratar os dados pessoais.

Entre outras coisas, isso poderá incluir políticas de segurança das informações, controles de acessos, monitoramento da segurança e planos de recuperação.

Devem ser adotadas medidas de segurança adequadas durante a vida útil dos dados pessoais e por todas as partes interessadas.

Regras	Referência de Q-Docs	Referência do RGPD
• Aplicar e revisar as medidas de segurança definidas na política e nas diretivas de segurança	DDPG007EN Regra 1	Art.32
• Integração da segurança da informação e da revisão da proteção de dados nos projetos.	DDPG007EN Regra 2	Art.32
• Segurança, Privacidade e Proteção de Dados por design e por padrão	DDPG007EN Regra 3	Art.25
• Integração da segurança da informação e das cláusulas de proteção de dados com as companhias subcontratadas	DDPG007EN Regra 4	Art.32

Treinamos nossos funcionários e aprimoramos nossos processos internos.

Dados Pessoais Classificação

O tratamento de dados pessoais sensíveis e de algumas categorias especiais de dados pessoais é proibido, exceto em casos específicos.

Esse tratamento requer medidas de proteção em termos de:

Identificação, Acesso, Transmissão, Transporte, Cópia e impressão, Estocagem e arquivamento, Destruição.

A classificação tem como objetivo a identificação de ativos de informação sensível, independentemente do seu caráter e do portador, e especificando, se necessário, medidas de proteção para reduzir os riscos na sequência de uma divulgação indesejada.

O nível de classificação da confidencialidade diz diretamente respeito ao impacto avaliado de uma divulgação indesejada de informações.

[DSUG001EN] Diretiva sobre a Proteção de Informações

Classificação da proteção das informações	Tipos de dados pessoais	Categorias de dados pessoais
Nível 1 =LIMITADO À ROQUETTE Definição: tipo de informação cuja divulgação aberta e ampla não é recomendada	Dados pessoais comuns	Estado civil, dados de identificação
		Vida pessoal (hábitos de vida, estado civil, excluindo dados sensíveis)
		Vida profissional (CV, educação e treinamento profissional, prêmios)
		Informações econômicas e financeiras (rendimento, situação financeira, situação fiscal)
		Dados de conexão (endereços IP, registros de eventos)
		Dados de localização (viagens, dados de GPS, dados GSM)
Nível 2 =CONFIDENCIAL DA ROQUETTE Definição: tipo de informação cuja divulgação pode prejudicar de modo significativo os interesses do Grupo	Dados pessoais considerados sensíveis	Número da segurança social
		Biometria
		Dados bancários
Nível 3 =SEGREDO DA ROQUETTE Definição: tipo de informação cuja divulgação prejudica gravemente os interesses do Grupo	Dados pessoais sensíveis dentro do significado da lei "Data Protection Act"	Preferências filosóficas, política, crenças religiosas e opiniões do sindicato, vida sexual, dados de saúde, origem racial ou ética
		Ofensas, condenações, medidas de segurança

Nossas responsabilidades:

Regras	Referência de Q-Docs	Referência do RGPD
• Respeitar o enquadramento legal para o tratamento de dados sensíveis	DDPG004EN Regra 1	Art.9
• Proibir o tratamento de dados sobre condenações e ofensas penais	DDPG004EN Regra 2	Art.10
• Limitar o acesso a dados de saúde somente a profissionais autorizados	DDPG004EN Regra 3	Art.9
• Proibir a utilização do número de identificação nacional como identificador único	DDPG004EN Regra 4	Art.87
• Limitar o acesso e a utilização de dados bancários	DDPG004EN Regra 5	Art.9
• Limitar o acesso a dados sensíveis somente para pessoas autorizadas	DDPG004EN Regra 6	Art.9
• Realizar avaliações de impacto sobre a privacidade de titulares de dados envolvidos no tratamento de dados sensíveis	DDPG004EN Regra 7	Art.35
• Limitar a utilização de áreas de comentários a informações gerais	DDPG004EN Regra 8	Melhor prática

Alguns conselhos práticos...

Exemplos de medidas de proteção a serem adotadas para cada categoria de ativos de informação classificada (papel, digital, conhecimentos, físicos).

Retenção de Dados

A crescente necessidade de desmaterializar as operações e a troca de informações entre o Grupo, nossos clientes e parceiros de negócios, assim como as exigências legais e regulamentares, sujeitaram a Roquette a um determinado número de obrigações em termos de comprimento do período de retenção dos dados e as políticas de gerenciamento dos registros.

Com base em nossas atividades, a Roquette adquire e trata uma grande quantidade de dados sensíveis relacionados com nossa estratégia, resultados financeiros, desenvolvimento comercial e ou comprometimentos, **assim como dados pessoais relacionados com nossos clientes, parceiros de negócios e membros das equipes**.

As informações enviadas ou recebidas pela Roquette com relação a nossas atividades devem ser mantidas por um período de retenção mínimo, embora nada impeça a companhia de mantê-los nos arquivos por mais tempo**, exceto caso eles incluam dados pessoais**.

Esse limite de tempo, durante o qual as autoridades administrativas e competentes podem realizar pós-inspeções, varia com base no caráter da informação a conservar e nas exigências legais relevantes.

Os tempos de armazenamento infinitos ou indeterminados são proibidos.

RGPD, Art. 5 1. E)

"limite de armazenamento"

Os dados pessoais devem ser conservados de modo que permitam a identificação de titulares dos dados não mais que o período necessário para os fins aos quais os dados pessoais são tratados.

Os dados pessoais podem ser armazenados para períodos mais longos desde que esses dados sejam tratados somente para fins de arquivamento do interesse público, fins de pesquisa científica ou histórica ou fins estatísticos sujeitos à implementação das medidas técnicas e organizacionais adequadas exigidas para salvaguardar os direitos e as liberdades do titular dos dados.

Nossas responsabilidades:

- A Roquette, enquanto controlador dos dados, deve definir tempos de armazenamento específicos e adequados para cada categoria de dados pessoais coletados e tratados.
- Antes da implementação do tratamento de dados pessoais, o proprietário do projeto, com a assistência de um coordenador de Proteção de Dados, deve especificar em nossos registros a duração da retenção de dados.
- Devemos conservar os dados pessoais somente durante o tempo necessário para o tratamento e cumprir às leis aplicáveis.

Regras	Referência de Q-Docs	Referência do RGPD
• Limitar a retenção de dados somente ao que for estritamente necessário	DDPG002EN Regra 5	Art. 5 1. E)

A este respeito, as Funções Globais, as GBUs e as áreas estão engajadas no cumprimento das regras de Retenção de Informações da Companhia e a manter os procedimentos associados em condições operacionais.

Exemplo:

No final de um processo de recrutamento, devemos eliminar informações sobre os candidatos preteridos, exceto se eles concordarem em ficar em nossa base por um período limitado (2 anos).

Treinamos nossos funcionários e aprimoramos nossos processos internos.

2 Nossas normas nas RELAÇÕES COM COMPANHIAS AFILIADAS e SUBCONTRATADAS

Qualificação de responsável pelo tratamento dos dados e de controlador

O controlador significa a pessoa física ou jurídica, autoridade pública, agência ou qualquer outra entidade que, sozinha ou em conjunto com outras, determina as finalidades e os meios de tratamento dos dados pessoais.

O Controlador Conjunto significa dois ou mais controladores que juntos determinam as finalidades e os meios de tratamento. No entanto, independentemente desse acordos, cada controlador é responsável pelo cumprimento de todas as obrigações dos controladores no escopo do RGPD.

O responsável pelo tratamento dos dados significa uma pessoa física ou jurídica, autoridade pública, agência ou outra entidade que trate os dados pessoais em nome do controlador.

Quem é um responsável pelo tratamento dos dados segundo o significado dado pelo Regulamento Geral de Proteção de Dados?

(Artigo 4 do RGPD – Definições).

Uma grande variedade de prestadores de serviços pode agir como responsável pelo tratamento dos dados no sentido jurídico do termo. As atividades dos responsáveis pelo tratamento dos dados podem se referir a tarefas muito específicas (subcontratação do serviço de entrega de correspondência) ou ser mais generalizado e abrangente (gerenciamento de todo um serviço em nome de outra organização, como o gerenciamento dos pagamentos aos funcionários, por exemplo).

Os tópicos que se seguem são abrangidos em particular pelo RGPD:

- prestadores de serviços de TI (alojamento, manutenção, etc.), integradores de software, companhias de cibersegurança ou companhias de consultoria em TI (anteriormente conhecidas como companhias de serviço de engenharia de TI) podendo acessar os dados,
- agências de marketing ou de comunicação que tratam dados pessoais em nome dos clientes, e
- de um modo mais genérico, qualquer organização prestando um serviço que implique o tratamento de dados pessoais em nome de outra organização,
- uma autoridade pública ou associação pode também ser considerada como tal.

Desde que não acessem ou tratem dados pessoais, os editores de software e os fabricantes de equipamentos (como terminais de contagem do tempo, equipamentos biométricos ou equipamentos médicos) não são abrangidos.

Exemplo de qualificação de responsável pelo tratamento dos dados e de controlador:

A companhia A presta um serviço de entrega de correspondência de marketing utilizando os arquivos de dados de cliente das companhias B e C.

A companhia A é um responsável pelo tratamento dos dados com relação às companhias B e C, desde que trate somente os dados de necessários dos clientes para enviar a correspondência em nome e consoante as instruções das companhias B e C.

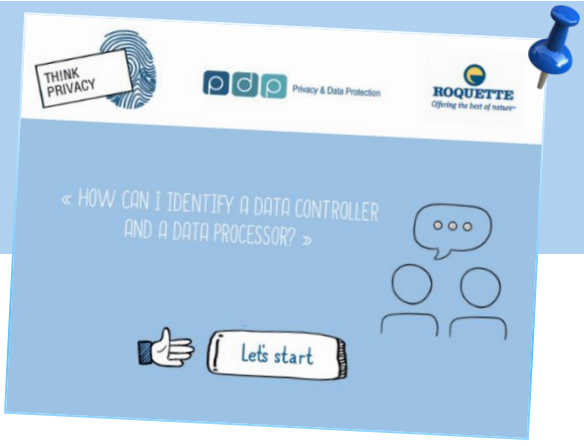
As companhias B e C são os controladores do gerenciamento de seus clientes, incluindo no que se refere à entrega da correspondência de marketing.

A companhia A também é o controlador no escopo do gerenciamento do pessoal que emprega, e do gerenciamento de seus clientes, nos quais se incluem as companhias B e C.

Texto oficial

- Artigo 4 do RGPD para as definições de controlador e responsável pelo tratamento dos dados
- Artigo 28.10 do RGPD sobre a noção de controlador

Treinamos nossos funcionários e aprimoramos nossos processos internos.



Cláusulas de proteção de dados

Quando é necessário um contrato e porque ele é importante?

Sempre que, enquanto controlador, recorremos a um responsável pelo tratamento dos dados para tratar os dados pessoais em nosso nome, deve ser assinado um contrato vinculando as partes.
O contrato é importante para que as duas partes compreendam nossas responsabilidades e obrigações.

Os contratos com cláusulas específicas de proteção de dados e/ou um acordo de proteção de dados entre a Roquette, como controlador, e seus responsáveis pelo tratamento dos dados garante que ambos compreendemos nossas obrigações, responsabilidades e obrigações. Os contratos também nos ajudam a cumprir com o RGPD e nos auxilia a demonstrar às pessoas e aos reguladores nossa conformidade, segundo a exigência do princípio da responsabilização.

Que responsabilidades e obrigações temos enquanto controlador ao recorrermos a um responsável pelo tratamento dos dados?

Devemos somente recorrer a responsáveis pelo tratamento dos dados que podem dar garantias suficientes de que irão implementar medidas técnicas e organizacionais adequadas para garantir que o seu tratamento cumpre as exigências do RGPD e proteger os direitos dos titulares dos dados.

Como Controlador, somos primeiramente responsáveis pela conformidade total com o RGPD e outras leis de proteção de dados em vigor, assim como pela demonstração dessa conformidade. Se isso não for conseguido, poderemos ter de pagar por danos em processos jurídicos ou ser sujeitos a multas ou outras sanções ou medidas corretivas.

O que há de novo no RGPD?

O RGPD torna os contratos escritos entre controladores e responsáveis pelo tratamento dos dados uma exigência, em vez de ser somente um modo de demonstrar a conformidade com o princípio da proteção dos dados (medidas de segurança adequadas) de acordo com as leis de Proteção de Dados em vigor.

Esses contratos devem agora incluir termos mínimos específicos. Esses termos são elaborados para garantir que o tratamento realizado por um responsável pelo tratamento dos dados cumpre as exigências do RGPD, não só as que estão mantendo os dados pessoais seguros.

Regras	Referência de Q-Docs	Referência do RGPD
• Integração de cláusulas de segurança da informação e de proteção de dados com companhias subcontratadas	DDPG007EN Regra 4	Art. 32
• Segurança dos fornecedores	DSUG016EN	

O que precisa ser incluído no contrato?

Os contratos devem definir:

- ☑ o escopo e a duração do tratamento;
- ☑ a natureza e a finalidade do tratamento;
- ☑ o tipo de dados pessoais e as categorias dos titulares dos dados; e
- ☑ as obrigações e direitos dos controladores.

Os contratos também devem incluir termos ou cláusulas específicas com relação:

- ☑ ao tratamento somente com base nas instruções documentadas do controlador;
- ☑ ao dever de confiança;
- ☑ às medidas de segurança adequadas;
- ☑ à utilização de sub-responsáveis pelo tratamento dos dados;
- ☑ aos direitos dos titulares dos dados;
- ☑ à assistência ao controlador;
- ☑ às disposições de término de contrato; e
- ☑ às auditorias e inspeções.

Treinamos nossos funcionários e aprimoramos nossos processos internos.

- Guia sobre a Proteção de Dados para subcontratos em conformidade com o RGPD.
- "Data Processing Agreement" modelo disponível em nosso "Privacy Management System": OneTrust@Roquette > "Vendor Risk Management" módulo.

Acordo de transferência de dados

Uma **Transferência de Dados** é qualquer comunicação, cópia ou transmissão de dados pessoais (como servidores de alojamento, envio de arquivos anexados por email, ferramentas de controle remoto, compartilhamento de telas, etc.) destinada ao tratamento em outros países que não têm as mesmas leis aplicáveis de proteção de dados pessoais.

Estamos mais conectados do que nunca. Para a Roquette operar a uma escala global, a transferência de dados a nível internacional é um elemento essencial das operações comerciais do cotidiano. A Roquette, por exemplo, armazena dados pessoais dos funcionários em um serviço de cloud (nuvem) alojado no estrangeiro e compartilha dados pessoais de funcionários e clientes entre suas subsidiárias estabelecidas no mundo inteiro.

Como é que o RGPD e outras leis de proteção de dados em vigor afetam essas transferências de dados internacionais?

Nossas responsabilidades:

Qualquer transferência de dados pessoais que estejam sendo tratados ou que venham a ser tratados após a transferência para um país terceiro ou uma organização internacional só deverá acontecer se:

- A lei local o permitir e/ou a autoridade de supervisão decidir que o país terceiro, um território ou um ou mais setores dentro desse país terceiro, ou a organização internacional em questão garante um nível adequado de proteção ou tiver dado sua autorização, e/ou
- Uma medida jurídica for adotada (ex.: Regras Corporativas Vinculativas ou cláusulas contratuais padronizadas para a transferência de dados pessoais para responsáveis pelo tratamento dos dados estabelecidos em países terceiros, em conformidade com a Diretiva 95/46/EC do Parlamento Europeu e do Conselho, etc.).

Regra	Referência de Q-Docs	Referência do RGPD
• Adotar medidas para transferir dados pessoais para países terceiros ou organizações internacionais	DDPG002EN Regra 6	Art. 44 a 50

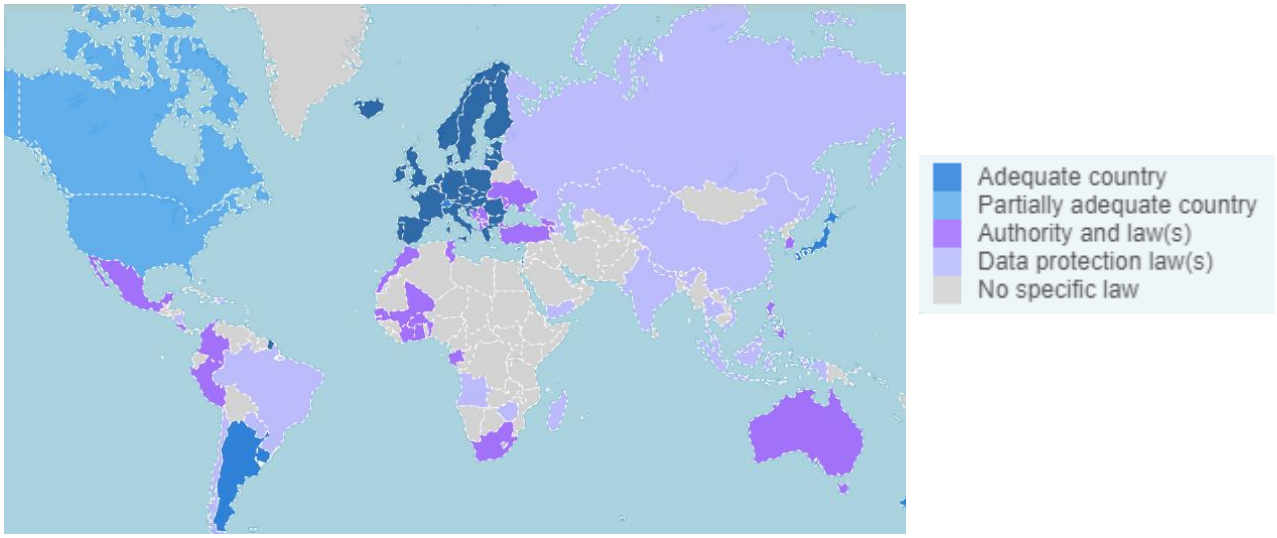
Em qualquer caso, por favor contatar o DPO em primeiro lugar.

Em que países posso transferir dados pessoais e quais as condições?

Para ter uma perspectiva geral, consulte este mapa:

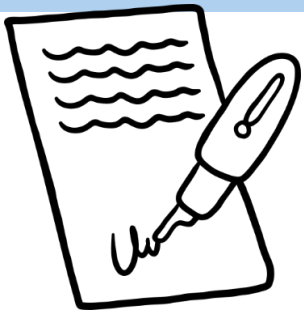
https://www.cnil.fr/en/data-protection-around-the-world.

Este mapa permite que você veja o nível de proteção de dados de cada país.



Treinamos nossos funcionários e aprimoramos nossos processos internos.

- " Data Transfer Agreement" incluindo em nosso modelo " Data Processing Agreement".
- Perguntas Frequentes para responder a algumas questões colocadas pela entrada em vigor da Decisão da Comissão da UE sobre as cláusulas contratuais padronizadas para a transferência de dados pessoais para responsáveis pelo tratamento de dados estabelecidos em países terceiros.



3 Nossas normas nas RELAÇÕES COM nossa REDE e AUTORIDADES DE SUPERVISÃO

Responsável pela Proteção de Dados

O Grupo nomeou um Responsável pela Proteção de Dados.

O Responsável pela Proteção de Dados ou DPO ("Data Protection Officer") nos auxilia no monitoramento da conformidade interna, informa e aconselha sobre nossas obrigações de proteção de dados, aconselha sobre Avaliações do Impacto da Proteção de Dados (AIPD) e intervém como ponto de contato para os titulares dos dados e autoridade de supervisão.

O DPO deve ser independente, um especialista em proteção de dados, possuir recursos adequados e reportar ao nível mais alto da administração.

O DPO pode nos ajudar a demonstrar conformidade e é parte de um maior enfoque na responsabilização.

Tarefas do DPO	Referência de Q-Docs	Referência do RGPD
• Nosso DPO tem como tarefas o monitoramento da conformidade com o RGPD e outras leis de proteção de dados, nossas políticas de proteção de dados, a conscientização, o treinamento e as auditorias.	MDPG001EN Manual de Proteção de Dados Pessoais	RGPD Artigo 39 Tarefas do responsável pela proteção de dados
• Teremos em consideração o aconselhamento do nosso DPO e as informações que der sobre nossas obrigações de proteção de dados.		
• Ao efetuarmos uma AIPD, procuramos o aconselhamento do nosso DPO, que também monitora o processo.		
• Nosso DPO intervém como ponto de contato para as Autoridades de Supervisão.		
• Ao realizar suas tarefas, nosso DPO tem em conta o risco associado às operações de tratamento, assim como o caráter, o escopo, o contexto e as finalidades do tratamento.		

O DPO do Grupo foi designado ao CNIL pelo CEO para iniciar funções no dia 25 de maio de 2018, a data de aplicação do RGPD.

Acessibilidade do DPO:

- Nossa Responsável pela Proteção de Dados, Jennifer Godin, pode ser acessada facilmente como ponto de contato para nossos funcionários, pessoas e a Autoridade de Supervisão.
- Publicamos os dados de contato do DPO e os transmitimos às Autoridades de Supervisão.

  ☑ https://www.Roquette.com/data-protection
  ☑ ONE > Global Functions > Data Protection
  ☑ ONE > Our Community > Data Protection Network

Contatar o DPO (Responsável pela Proteção de Dados) em caso de:

☑ Tratamento de Dados Pessoais

☑ Pedidos dos Titulares dos Dados

☑ Violação dos Dados Pessoais

☑ Necessidade de Aconselhamento ou Assistência

Um único ponto de contato: dpo@Roquette.com ou jennifer.godin@Roquette.com

Treinamos nossos funcionários e aprimoramos nossos processos internos.

Rede de Proteção de Dados

Os transmissores para os departamentos e os DPO ou Coordenadores Locais são uma rede que permite que o Responsável pela Proteção de Dados do Grupo, respectivamente, implemente regras de Proteção de Dados Pessoais em cada unidade de negócios e departamento de apoio, assim como permaneça em conformidade com as exigências das leis e regulamentos relevantes de proteção de dados nos países onde o Grupo está presente.

Os DPO/Coordenadores Locais deverão ter pelo menos as seguintes tarefas:

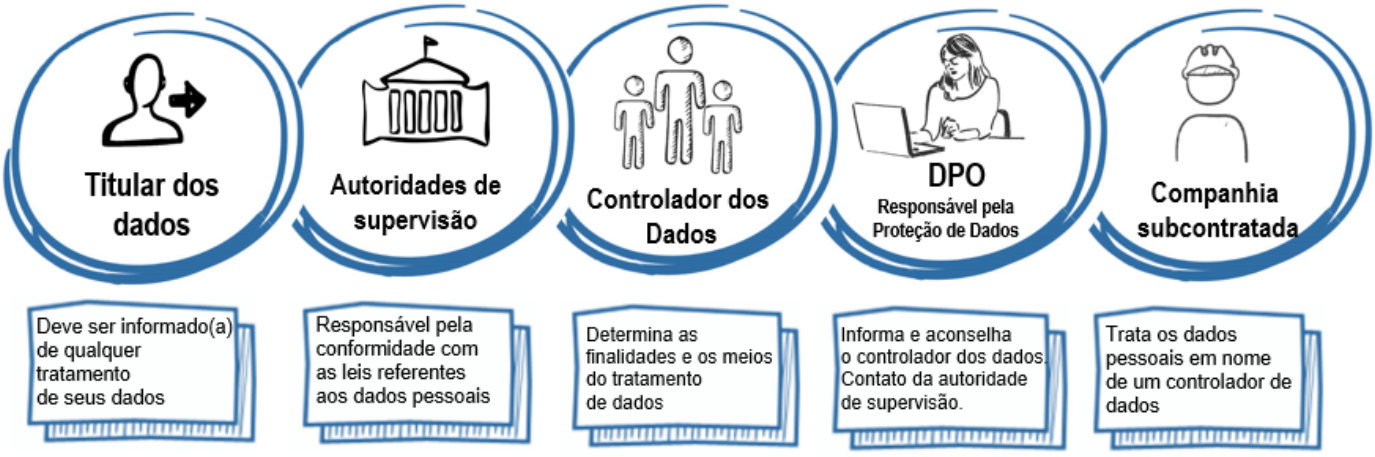
- Informar e aconselhar localmente sobre as obrigações no escopo da Política de Proteção de Dados Pessoais da Roquette definidas pelo DPO do Grupo Roquette e as exigências de suas leis locais aplicáveis com relação à proteção de dados;
- Monitorar a conformidade com a legislação local, com outras legislações e regulamentos aplicáveis com relação à proteção de dados, sempre que for necessário, com a assistência do DPO do Grupo Roquette, assim como com as políticas referentes à proteção de dados pessoais;
- Prestar aconselhamento localmente sempre que for necessário no escopo da avaliação do impacto da proteção de dados e monitorar o seu desempenho inerente;
- Cooperar com a autoridade de supervisão local;
- Intervir como ponto de contato para o DPO do Grupo Roquette sobre questões relacionadas com o tratamento, assim como consultar o DPO do Grupo Roquette, sempre que for necessário, com relação a qualquer outro assunto;
- Reportar suas atividades ao DPO do Grupo Roquette para contribuir para o Sistema de Gerenciamento da Proteção de Dados do Grupo.

Para saber mais...

Nosso Seminário PDP anual é o ponto de encontro de nossa rede de colaboradores de proteção de dados e privacidade.

e Partes Interessadas

Quem são os novos intervenientes?



Quais são as relações entre essas partes interessadas?

AS: Autoridade de Supervisão – Ver na página 50

Autoridades de supervisão

No mundo inteiro, muitos países têm uma lei de proteção de dados e uma independente

Autoridade de Proteção de Dados (APD).

Estas autoridades são o regulador nacional independente para a privacidade e a liberdade de informação. Elas promovem e defendem os direitos dos titulares dos dados de acessar informações que são mantidas nas organizações e terem suas próprias informações protegidas.

Qual é o papel de uma autoridade de supervisão no escopo do RGPD?

Cada Estado Membro deverá providenciar que uma ou mais autoridades públicas independentes sejam responsáveis pelo monitoramento da aplicação de leis de dados pessoais e de privacidade, para proteger os direitos e as liberdades fundamentais dos titulares dos dados, no escopo do tratamento de dados pessoais e para facilitar a livre circulação desses dados pessoais na UE.

No escopo do RGPD, todos os Estados Membros da UE têm uma autoridade de proteção de dados, em geral servindo como principal ponto de contato das partes interessadas dentro desse Estado Membro.

Para se certificar de que o RGPD é aplicado de modo consistente em toda a UE, cada autoridade de supervisão tem que trabalhar em conjunto com as outras e com a Comissão Europeia.

Cada autoridade de supervisão em seu território deverá promover a conscientização do público e a compreensão dos riscos, regras, salvaguardas e direitos com relação ao tratamento de dados pessoais.

Também é a ela que devemos nos dirigir em caso de violação da legislação sobre a proteção de dados e para aconselhamento e questões específicas e/ou assistência da perspectiva das organizações.

Em resumo, as responsabilidades das Autoridades de Supervisão (AS) são:

- Garantir a aplicação das regras, inclusive através de multas,
- Esclarecer a aplicação das regras, se for necessário, ex.: através das diretrizes,
- Promover uma cultura de diálogo com todas as partes interessadas, incluindo as companhias,
- Cooperar em conjunto.

CNIL: Commission Nationale de l'Informatique et des Libertés - APD francesa.

Autoridade Principal

- A autoridade de supervisão para o estabelecimento principal do controlador ou do responsável pelo tratamento dos dados deverá atuar como autoridade principal. Ela deve cooperar com as outras autoridades em questão.

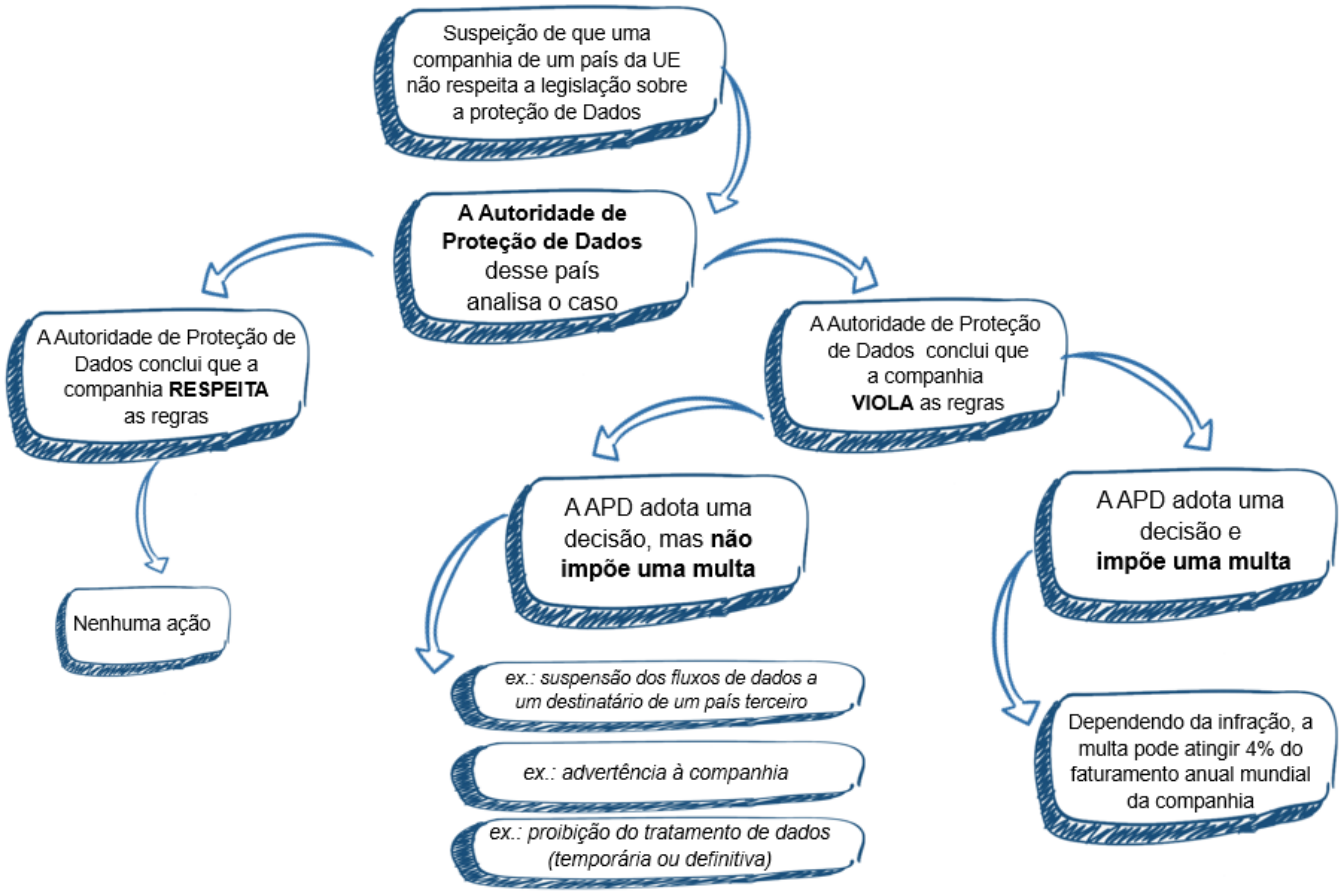
- Identificar uma autoridade de supervisão principal só é relevante quando o controlador ou o responsável pelo tratamento dos dados está efetuando o tratamento entre países de dados pessoais.

Como identificar a "autoridade de supervisão principal"?

Identificar a sede de administração central do controlador principal na UE.
A autoridade de supervisão do país onde a sede da administração central está localizada é a autoridade principal do controlador.

O **CNIL** *é a Autoridade de Supervisão Principal da Roquette*

Como funciona na prática o mecanismo de sanções da RGPD?



Governança

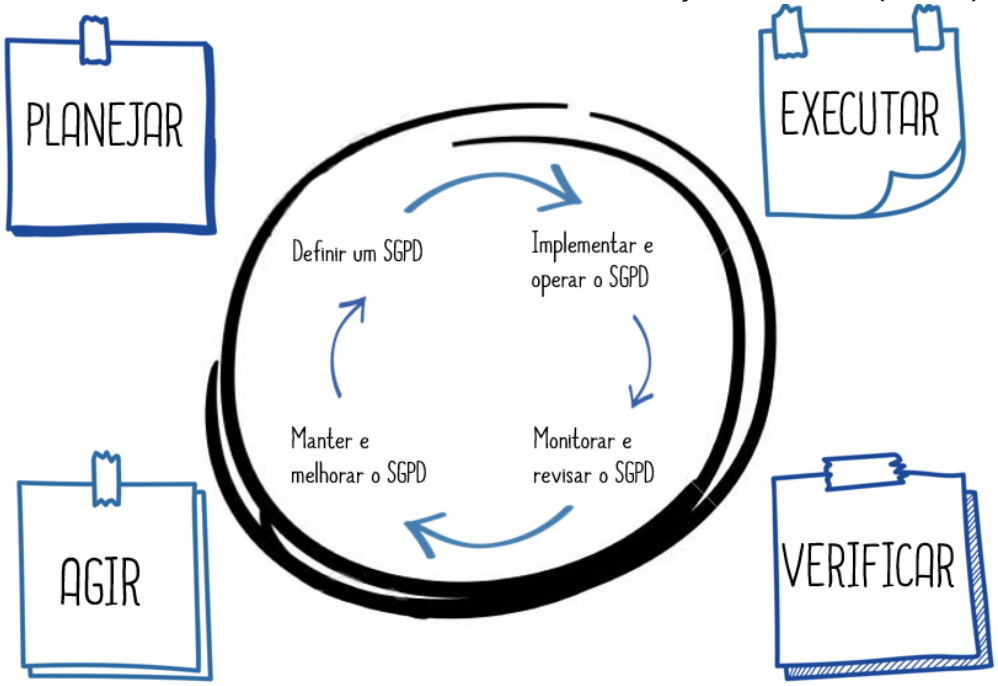
"A **organização da proteção de dados** está sobretudo estruturada ao redor do Responsável pela Proteção de Dados, seus coordenadores por site (planta) e por função, o Diretor Executivo como Controlador dos Dados, os Responsáveis pelas Funções Globais como responsáveis pela implementação do tratamento de dados pessoais e as companhias subcontratadas como Responsáveis pelo Tratamento dos Dados." [MDPG001EN]

Adotamos uma abordagem de tratamento para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar o **S**istema de **G**erenciamento de **P**roteção de **D**ados Pessoais (**SGPD**) da Roquette.

O processo e a abordagem para o gerenciamento da proteção de dados pessoais definida nesta governança incentiva seus usuários a enfatizar a importância:

1) de compreender as exigências de proteção de dados da Roquette e a necessidade de estabelecer diretivas e procedimentos para a proteção de dados;
2) de implementar e utilizar controles para gerenciar os riscos de proteção de dados da Roquette no escopo dos riscos globais de negócios da Roquette;
3) de monitorar e revisar o desempenho e a eficiência do SGPD; e
4) de um melhoramento continuado baseado na avaliação objetiva.

Adotamos o modelo "Planejar-Executar-Verificar-Agir" (PDCA), que é aplicado para estruturar todos os processos do Sistema de Gerenciamento da Proteção de Dados (SGPD).



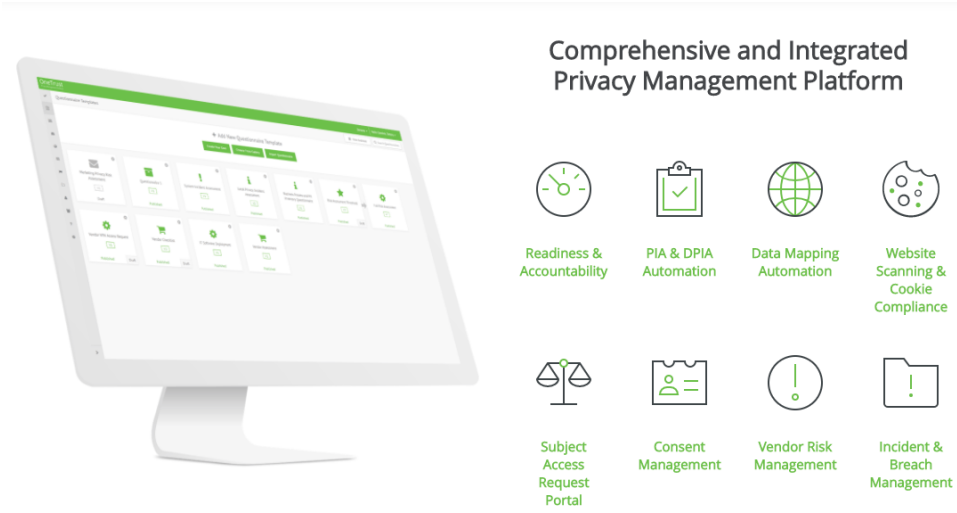
Nossa abordagem:

Nosso Programa de Compliance com o RGPD está focado em:

- Compreender como nossa organização coleta, armazena, utiliza e transfere dados para garantir a conformidade,
- Criar uma cultura de conformidade dentro de nossa organização,
- Realizar avaliações de impacto da privacidade,
- Preparar situações para casos de violação de dados,
- Alocar recursos para o Programa de Privacidade,
- Implementar um Sistema de Gerenciamento da Proteção de Dados (Planejar – Executar – Verificar – Agir).

Para atingir esses objetivos, como parte de nosso Programa nós:

- Definimos uma Política de Proteção de Dados e a Governança e a Documentação associadas,
- Gerenciamos um projeto de conformidade de RGPD para a revisão do tratamento, o gerenciamento das situações de violações de dados, a revisão de contratos, cláusulas sobre a proteção de dados, acordo de transferência de dados, etc.,
- Implementamos um software de gerenciamento da privacidade em conformidade com o RGPD.



As principais características desta plataforma de gerenciamento são:

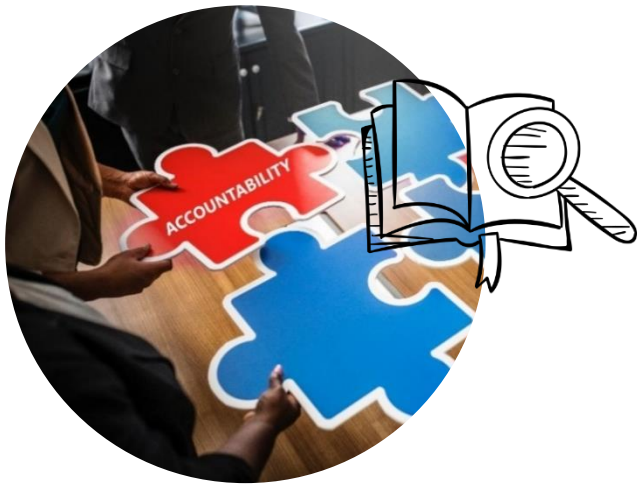
- Manutenção do registro de tratamento de dados (Mapeamento de Dados),
- Gerenciamento dos riscos associado ao tratamento (a partir da AIP, etc.),
- Gerenciamento de pedidos e de direitos (acesso, retificação, oposição, etc.),
- Gerenciamento de incidentes e de violações de dados,
- Gerenciamento da documentação sobre a conformidade.

Responsabilização

A responsabilização é um dos princípios de proteção de dados. Ela nos torna responsáveis pelo cumprimento do RGPD e estabelece que devemos ser capazes de demonstrar nossa conformidade.

Porque a responsabilização é importante?

Assumir a responsabilidade pelo que fazemos com os dados pessoais e demonstrar os passos que demos para proteger os direitos das pessoas não só promove uma maior conformidade jurídica, como também nos dá uma vantagem concorrencial. A responsabilização constitui uma verdadeira ocasião para mostrarmos e comprovarmos o quanto respeitamos a privacidade das pessoas. Este aspecto pode nos ajudar a desenvolver e aumentar a confiança das pessoas.



Além disso, se algo de errado acontece, ser capaz de mostrar que consideramos ativamente os riscos e implementamos medidas e salvaguardas pode nos ajudar a minimizar qualquer potencial ação repressiva. Por outro lado, se não formos capazes de demonstrar boas práticas de proteção de dados, poderemos ser alvo de multas e de danos em matéria de reputação.

O que significa concretamente aderir ao princípio da responsabilização?

O Tratamento de Dados Pessoais implica um dever de cuidar e a adoção de medidas concretas e práticas para a proteção do mesmo. Aderir ao princípio da responsabilização significa:

- documentar e comunicar adequadamente todas as diretivas, procedimentos e práticas relacionados com a privacidade (nossa “Política”);
- atribuir a uma pessoa específica da organização (que poderá por sua vez delegar a outras pessoas da organização, conforme seja adequado) a tarefa de implementar a Política;
- ao transferir Dados Pessoais para terceiras partes, garantir que o destinatário da terceira parte irá com toda a certeza providenciar um nível equivalente de Privacidade e Proteção de Dados através de meios contratuais e outros, como políticas internas obrigatórias (a lei aplicável pode conter exigências adicionais com relação a transferências de dados internacionais);
- disponibilizar treinamento adequado para o pessoal do Controlador de Dados que acessará os Dados Pessoais;

- implementar um tratamento interno eficiente das reclamações e corrigir procedimentos para utilização pelos Titulares dos Dados;
- informar os Titulares dos Dados sobre violações de privacidade que podem dar origem a danos significativos aos próprios (exceto em caso de proibição, por ex., durante o trabalho com o cumprimento da lei), assim como as medidas adotadas para encontrar uma solução;
- notificar todas as partes interessadas de privacidade relevantes sobre violações de privacidade, conforme exigido em algumas jurisdições (ex.: as autoridades de proteção de dados) e dependendo do nível de risco;
- permitir que um Titular de Dados prejudicado acesse as sanções e/ou as soluções adequadas e eficazes, como a retificação, a exclusão ou a restituição no caso de ocorrência de uma violação de privacidade; e
- considerar procedimentos para compensação de situações em que será difícil ou impossível devolver a situação de privacidade da pessoa física para uma posição como se nada tivesse acontecido.

Lista de verificação:

- ☑ Levamos a responsabilidade pelo cumprimento do RGPD até ao nível mais alto da administração e em toda a nossa organização.
- ☑ Mantemos um registro de todos os passos que damos para cumprir o RGPD.

Implementamos medidas técnicas e organizacionais adequadas, como:

- ☑ adotar e implementar regras de proteção de dados;
- ☑ adotar uma abordagem de "proteção de dados por design e por padrão" - implementar medidas de proteção de dados adequadas em todo o ciclo de vida de nossas operações de tratamento;
- ☑ elaborar contratos escritos com organizações que tratam dados pessoais em nosso nome;
- ☑ manter atualizada a documentação sobre nossas atividades de tratamento;
- ☑ implementar medidas de segurança adequadas;
- ☑ registrar e, sempre que for necessário, reportar violações de dados pessoais;
- ☑ efetuar avaliações do impacto da proteção de dados para utilizações de dados pessoais que possam dar origem a um risco elevado para os interesses das pessoas;
- ☑ nomear um responsável pela proteção de dados; e
- ☑ aderir aos códigos de conduta relevante e cumprindo planos de certificação (sempre que for possível).

- ☑ Revisamos e atualizamos nossas medidas de responsabilização com uma periodicidade adequada.

Documentação

O que é a documentação?

Devemos manter um registro de nossas atividades de tratamento, cobrindo áreas como finalidade do tratamento, o compartilhamento e a retenção de dados; a isso se dá o nome de **documentação**.

Documentar nossas atividades de tratamento é importante, não só porque isso é em si mesmo uma exigência legal, mas também porque pode apoiar a boa governança dos dados e nos ajudar a demonstrar nossa conformidade com outros aspectos do RGPD e das leis de proteção de dados em vigor.

Lista de verificação:

Documentação de atividades de tratamento – exigências

- ☑ Enquanto controlador dos dados pessoais que tratamos, documentamos todas as informações aplicáveis de acordo com o Artigo 30(1) do RGPD.
- ☑ Documentamos nossas atividades de tratamento por escrito.
- ☑ Documentamos nossas atividades de tratamento de modo granular com ligações relevantes entre os vários documentos informativos.
- ☑ Realizamos revisões frequentes dos dados pessoais que tratamos e atualizamos nossa documentação adequadamente.

Documentação de atividades de tratamento – melhores práticas

- ☑ Documentamos nossas atividades de tratamento em formato eletrônico para que possamos adicionar, remover e modificar as informações facilmente.

Ao nos prepararmos para documentar nossas atividades de tratamento, nós:

- ☑ procedemos a auditorias de informações para saber quais os dados pessoais que nossa organização possui;
- ☑ recorremos a questionários através de nossas ferramentas Digitais, de Segurança e Privacidade e falamos com pessoal de toda a organização para obtermos uma perspectiva mais completa de nossas atividades de tratamento; e
- ☑ revisamos nossas políticas, diretivas, procedimentos, contratos e acordos para abordar áreas como a retenção, a segurança e o compartilhamento de dados.

Como parte de nosso registro de atividades de tratamento, documentamos, ou vinculamos nossa documentação, sobre:

- ☑ informações exigidas por notificações de privacidade;
- ☑ registros de consentimento sempre que for necessário;
- ☑ contratos entre controlador e responsáveis pelo tratamento dos dados;
- ☑ a localização dos dados pessoais;
- ☑ relatórios de Avaliação do Impacto da Proteção de Dados; e ainda
- ☑ registros de violações de dados pessoais;
- ☑ registros de pedidos de titulares dos dados.

Onde está a nossa documentação sobre a Proteção de Dados?

ONE
Função Global
Proteção de Dados

Privacy & Data Protection

"A Proteção de Dados é relevante e da responsabilidade de todos em nossa organização"

Conteúdo

- Leis e regulamentos
- Informação e conscientização
- Melhores práticas e políticas

ONE
Comunidade
Rede de Proteção de Dados

Data Protection Network

"Todos somos intervenientes para a proteção de dados pessoais"

Conteúdo

- Política de Proteção de Dados Pessoais
- Sistema de Gerenciamento de Proteção de Dados
- Legislação Local
- Recursos Humanos
- Global Digital
- Departamento Jurídico e Compliance
- Auditoria e Controle Interno
- GBU e Área Comercial
- Inovação, P&D
- Segurança Global
- Seguros e Gerenciamento dos Riscos

OneTrust
Software de Gerenciamento da Privacidade

OneTrust
Privacy Management Software
@ ROQUETTE

"Nossa ferramenta de Gerenciamento da Privacidade dedicada à Segurança da Privacidade e ao Risco de Terceiras Partes"

Módulos

CULTURA → CONFORMIDADE → RESPONSABILIZAÇÃO

Avaliação do Impacto da Privacidade

A Avaliação do Impacto da Privacidade ou **AIP** é um processo criado para descrever o tratamento, avaliar sua necessidade e proporcionalidade e ajudar a gerenciar os riscos para os direitos e liberdades das pessoas físicas resultando do tratamento de dados pessoais avaliando-os e determinando medidas para abordá-los.

A abreviatura "**AIP**" é utilizado de modo intermutável para se referir tanto à **Avaliação do Impacto da Privacidade** quanto à **Avaliação do Impacto de Proteção dos Dados** (**AIPD**).

Como é a AIP efetuada?

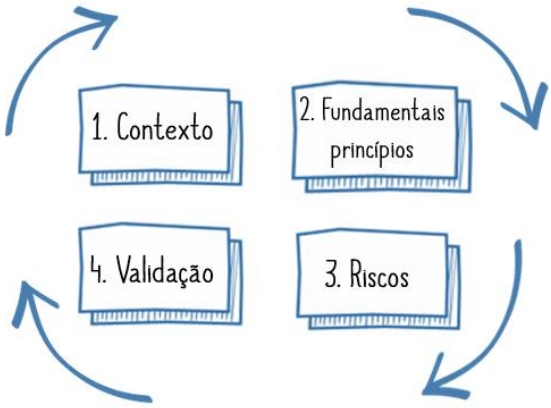
A abordagem de conformidade implementada pela realização de uma AIP se baseia em dois pilares:

1) **princípios e direitos fundamentais**, que "não são negociáveis", são definidos pela lei e devem ser respeitados, independentemente da natureza, da gravidade e da probabilidade de ocorrência dos riscos;
2) **gerenciamento dos riscos de privacidade dos titulares dos dados**, que determina os controles técnicos e organizacionais adequados para proteger dados pessoais.

Abordagem de conformidade utilizando a AIP

Em resumo, para efetuar uma AIP, é necessário:

1) definir e descrever o contexto do tratamento de dados pessoais em consideração;
2) analisar os controles que garantem a conformidade com os princípios fundamentais: a proporcionalidade e a necessidades de proceder ao tratamento, assim como a proteção dos direitos dos titulares dos dados;
3) avaliar riscos de privacidade associados à segurança dos dados e garantir que eles são tratados corretamente;
4) documentar formalmente a validação da AIP à luz dos fatos anteriores para entregar ou decidir revisar as etapas anteriores.



Abordagem geral para a realização de uma AIP

Este é um processo de melhoria contínua. Por isso, por vezes são necessárias várias repetições para conseguirmos obter um sistema aceitável de proteção da privacidade. Também é necessário um monitoramento das modificações ao longo do tempo (em contexto, controles, riscos, etc.), por exemplo, todos os anos, e atualizações sempre que se verificar uma modificação significativa.

A abordagem deverá ser implementada assim que um novo tratamento de dados pessoais for criado. A implementação desta abordagem logo no início torna possível determinar os controles necessários e suficientes e assim otimizar os custos. Por outro lado, a sua implementação após à criação do sistema e a implementação de controles poderá colocar em dúvida as escolhas efetuadas.

Nossas responsabilidades:

- Sempre que um tipo de tratamento em particular utilizando novas tecnologias, e tendo em conta a natureza, o escopo, o contexto e as finalidades do tratamento, puder representar um risco elevado para os direitos e liberdades de pessoas físicas, a Roquette, como controlador, deverá, antes do tratamento, proceder a uma avaliação do impacto das operações de tratamento previstas no escopo da proteção de dados pessoais.
- O proprietário do projeto deverá procurar aconselhamento junto ao Responsável pela Proteção de dos Dados designado ao realizar uma avaliação do impacto da proteção dos dados.

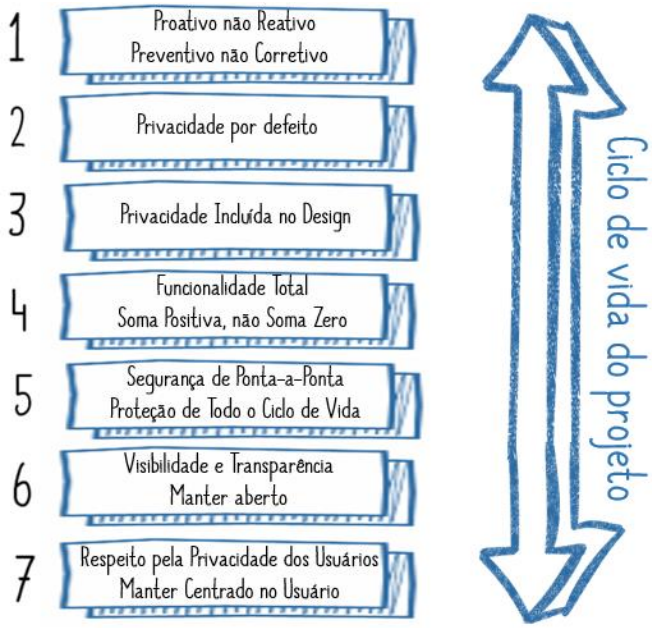
Regras	Referência de Q-Docs	Referência do RGPD
• Realização de uma AIP em caso de risco elevado	DDPG003EN Regra 1	Art. 35
• Conteúdo de uma AIP	DDPG003EN Regra 2	
• Tarefas do DPO com relação à AIP	DDPG003EN Regra 3	
• Revisão da AIP	DDPG003EN Regra 4	

Treinamos nossos funcionários e aprimoramos nossos processos internos.

- Aprendendo sobre “ Security & Privacy Review” em “ Projects & Contracts”.
- O modelo “Privacy Impact Assessment” é iniciado automaticamente em nosso software de gerenciamento de privacidade OneTrust@Roquette quando necessário.
- **Para saber mais**: CNIL Metodologia da AIP, edição de fevereiro de 2018 - https://www.cnil.fr/en/home.

Privacidade por Design e por Padrão

A Privacidade por Design significa a construção da privacidade na criação, operação e gerenciamento de um determinado sistema, processo de negócios ou especificação de design.



O que é a Proteção de Dados por Design?

A legislação sobre a proteção de dados inclui princípios básicos para salvaguardar a privacidade dos titulares dos dados.

A proteção de dados por design e por padrão ajuda a garantir que os sistemas de informação que utilizamos cumprem esses princípios de proteção de dados e que os sistemas salvaguardam os direitos dos titulares dos dados.

Consideramos que:

A Roquette confia em sistemas de informação e bases de dados para realizar uma variedade de tarefas operacionais e administrativas. Uma grande parte desses sistemas de informação trata dados pessoais, por isso a sua total conformidade com os regulamentos é da maior importância.

Os negócios que levam a proteção de dados muito a sério criam confiança.
Por isso, as medidas robustas de proteção de dados podem constituir uma vantagem concorrencial.

O comprometimento da direção é fundamental para tomar a decisão de aplicar os princípios de utilização da proteção de dados por design nos suprimentos da organização e no desenvolvimento de software.
A direção também deve garantir que disponibiliza recursos suficientes para a realização dessa tarefa.

Ter em consideração a proteção de dados ao longo do processo de desenvolvimento é simultaneamente econômico e mais eficiente do que fazer modificações em um software já existente.

Nossas responsabilidades:

No escopo do RGPD, a proteção de dados por design se tornou, pela primeira vez, uma obrigação jurídica. Isto significa que a proteção de dados e a privacidade deverão ser incorporadas nas especificações e na arquitetura de base dos sistemas e tecnologias de informação e comunicação.

A Roquette, enquanto controlador de dados, deve cumprir as exigências governando a proteção de dados por design durante o desenvolvimento de software, e ao encomendar sistemas, soluções e serviços.

As exigências devem, conforme o disposto acima, também ser incluídas ao assinar contratos com fornecedores e ao recorrer a consultores (consultar nossas normas com companhias subcontratadas).

Regra	Referência de Q-Docs	Referência do RGPD
• Segurança, Privacidade e Proteção de Dados por design e por padrão	DDPG007EN Regra 3	Art. 25

Lista de verificação:

- ☑ Revisar a Avaliação do Impacto da Proteção de Dados (AIPD)
- ☑ Evitar, limitar ou minimizar a necessidade de coletar e tratar dados pessoais sensíveis
- ☑ Limitar e minimizar a exposição de funcionalidades e dados pessoais desnecessários na interface do usuário
- ☑ Anonimizar ou pseudonimizar os dados pessoais sempre que for possível
- ☑ Todas as configurações protegendo a privacidade precisam estar ativadas por padrão
- ☑ O rastreamento de um website para outro deve ser desativada por padrão
- ☑ Retirar o consentimento através de um menu do software. Ter em mente que a coleta de dados pessoais deve terminar se o consentimento for retirado
- ☑ As definições devem ser apresentadas em um menu no qual o titular dos dados deve fazer uma escolha consciente de “modificar” ativamente para definições menos protetoras da privacidade
- ☑ O rastreamento dos dispositivos deve ser desativado por padrão

Treinamos nossos funcionários e aprimoramos nossos processos internos.

- Diretriz na nossa Comunidade de Rede de Proteção de Dados.
- Metodologias: Revisão da Segurança e Conformidade com relação a projetos e contratos.
- Aprendizado na plataforma de RH.

Notificação de Violação de Dados

O que é uma violação de dados pessoais?

Uma violação de dados pessoais significa uma violação de segurança dando origem à destruição, perda, modificação, divulgação não-autorizada ou acesso acidental ou ilícito de dados pessoais transmitidos, armazenados ou tratados de qualquer outro modo.

Isso significa que uma violação é mais do que somente ***perder*** *dados pessoais.*

Exemplos:

- Perda de uma base de dados de clientes
- Divulgação da avaliação do desempenho dos funcionários

Nossas responsabilidades:

Precisamos aplicar regras para tratar qualquer violação de dados pessoais de modo a limitar o seu impacto nos titulares dos dados e a evitar que tal violação aconteça de novo.

Regras	Referência de Q-Docs	Referência do RGPD
• Notificação de uma violação de dados pessoais ao Responsável pela Proteção de Dados.	DDPG008EN Regra 1	Art. 33
• Notificação de uma violação de dados pessoais à autoridade de supervisão.	DDPG008EN Regra 2	
• Comunicação de uma violação de dados pessoais ao titular dos dados.	DDPG008EN Regra 3	Art. 34

Quem devemos contatar em caso de Violação de Dados?

Por favor contatar o Responsável pela Proteção de Dados no endereço dpo@Roquette.com e também a linha de alerta confidencial da Roquette alert@Roquette.com

Quanto tempo temos para reportar uma violação?

Devemos reportar uma violação passível de notificação à Autoridade de Supervisão sem demora injustificada, mas nunca mais de 72 horas após ter tomado conhecimento da mesma.

Que violações precisamos notificar à autoridade de supervisão relevante?

Somente precisamos notificar a autoridade de supervisão relevante de uma violação se provavelmente ela resultar um risco para os direitos e liberdades das pessoas. Se não for tida em conta, essa violação pode ter um efeito prejudicial significativo nas pessoas. Por exemplo:

- resultar em discriminação;
- prejudicar a reputação;
- perdas financeiras; ou
- perda de confidencialidade ou qualquer outra desvantagem econômica ou social significativa.

Precisamos avaliar este aspecto caso a caso e precisamos ser capazes de justificar a sua decisão de reportar uma violação à autoridade de supervisão.

Quando devemos notificar as pessoas?

Se provavelmente uma violação venha a dar origem a um **risco elevado** para os direitos e liberdades das pessoas, devemos notificar as pessoas afetadas diretamente sem demora injustificada.

A obrigação de notificar uma pessoa sobre uma violação não se aplica se:

- tivermos implementado medidas técnicas e organizacionais adequadas que foram aplicadas aos dados pessoais afetados pela violação;
- tivermos adotado medidas subsequentes para garantir que não haverá uma possibilidade de risco elevado para os direitos e liberdades das pessoas; ou
- no implicar um esforço desproporcionado.

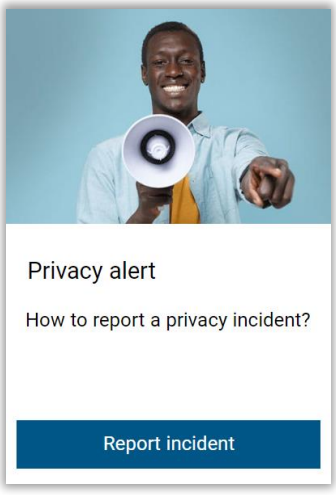
Sempre que a comunicação de uma violação implicar um esforço desproporcionado, devemos disponibilizar as informações de outro modo igualmente eficaz, como a comunicação pública.

Com quem devemos entrar em contato em caso de violação de dados?

Entre em contato com o **Diretor de Proteção de Dados** em dpo@Roquette.com e/ou informe o incidente por meio do nosso formulário da Web "Privacy Alert".

Se precisar denunciar uma possível violação de conformidade, entre em contato com seu ponto de contato habitual ou denuncie um problema por meio do dispositivo de alerta confidencial da Roquette: Speakup©.

SpeakUp



Monitoramento e Revisão

Consideramos que:

A Roquette está comprometida em:

- ☑ garantir um **monitoramento** jurídico e tecnológico sobre as exigências em matéria de proteção de dados,
- ☑ **revisar** e **melhorar** nosso Sistema de Gerenciamento de Proteção de Dados (SGPD)

para ter em conta evoluções regulamentares e tecnológicas, assim como as limitações internas dos serviços. [DDPG009EN]

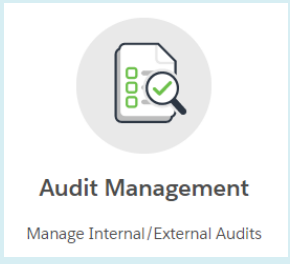
Nossas responsabilidades:

Regras	Referência de Q-Docs	Referência do RGPD
• Garantir um monitoramento e revisão jurídica e tecnológica com relação à proteção de dados pessoais	DDPG009EN Regra 1	
• Monitorar frequentemente a implementação do SGPD e das diretivas de proteção de dados	DDPG009EN Regra 2	Melhores Práticas
• Revisar frequentemente a política de proteção de dados pessoais e a documentação do SGPD	DDPG009EN Regra 3	

Treinamos nossos funcionários e aprimoramos nossos processos internos.

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

pdp Privacy & Data Protection News



Criar e apoiar nosso Programa de Privacidade

Software de Pesquisa Regulamentar:

Utilizamos uma plataforma que disponibiliza um conjunto de soluções de privacidade criadas para nos ajudar a monitorar os desenvolvimentos regulamentares, minimizar os riscos e atingir a conformidade global:

- ☑ Rastreamento regulamentar
- ☑ Gráficos comparativos entre países
- ☑ Notas de orientação
- ☑ Portal do RGPD
- ☑ Modelos e listas de verificação
- ☑ Solicitar um serviço de análise
- ☑ Pesquisa jurídica

Auditoria e Revisão do Sistema de Gerenciamento da Proteção de Dados:

Realizamos auditorias internas para determinar se os aportes do SGPD:

- ☑ estão em conformidade com as exigências deste Guia, da Política e da legislação e regulamentos aplicáveis;
- ☑ são implementados e mantidos eficientemente; e
- ☑ são executados como se espera.

Realizamos uma revisão do gerenciamento do SGPD para garantir que o escopo permanece adequado e que os melhoramentos do processo do SGPD são identificados.

Para isso, os aportes são:

- ☑ Objetivos, controles, processos e procedimentos do SGPD;
- ☑ Resultados de auditorias e controles de conformidade anteriores;
- ☑ Feedback proveniente de partes interessadas;
- ☑ Técnicas, produtos ou procedimentos, que podem ser utilizados na organização para melhorar o desempenho e a eficiência do SGPD;
- ☑ Estado de ações preventivas e corretivas;
- ☑ Vulnerabilidades e ameaças não resolvidas adequadamente na avaliação de riscos anterior;
- ☑ Resultados de avaliações de eficiência;
- ☑ Ações de atualizações a partir de revisões de gerenciamento anteriores;
- ☑ Quaisquer modificações que possam afetar o SGPD; e
- ☑ Recomendações de melhorias.

Documentos de referência

- [Código de Conduta] Código de Conduta do Grupo Roquette
- [GDPG001EN] Glossário de definições referentes à Proteção de Dados
- [MDPG001EN] Manual de Proteção de Dados Pessoais
- [DDPG001EN] Diretiva sobre a cultura de respeito da privacidade e da proteção de dados
- [DDPG002EN] Diretiva sobre a legitimidade do tratamento de dados pessoais
- [DDPG003EN] Diretiva sobre a avaliação do impacto da privacidade
- [DDPG004EN] Diretiva sobre o tratamento de dados sensíveis
- [DDPG005EN] Diretiva sobre registros de atividades de tratamento
- [DDPG006EN] Diretiva sobre a conformidade com os direitos das pessoas
- [DDPG007EN] Diretiva sobre a segurança dos dados pessoais
- [DDPG008EN] Diretiva sobre a notificação de uma violação de dados pessoais
- [DDPG009EN] Diretiva sobre a revisão do sistema de gerenciamento da proteção de dados pessoais
- [DSUG001EN] Diretiva sobre a Proteção da Informação
- [DSUG006EN] Gerenciamento da Diretiva sobre a Cibersegurança
- [DSUG016EN] Diretiva sobre a Segurança dos Fornecedores

Bibliografia

[Carta da UE] Carta dos Direitos Fundamentais da União Europeia, 2010/C 83/02.

[RGPD] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 sobre a proteção de pessoas singulares com relação ao tratamento de dados físicas e sobre a livre circulação desses dados, e revogando a Diretiva 95/46/EC (Regulamento Geral de Proteção de Dados).

[DP-Act] Lei francesa de Proteção de Dados no. 78-17 de 6 de janeiro de 1978, modificada 25.

[WP29 – Diretrizes] Diretrizes para a identificação da autoridade de supervisão principal de um controlador ou de um responsável pelo tratamento dos dados | WP 244 rev.01 (5 de abril de 2017).

[WP29- Diretrizes] Diretrizes sobre a Avaliação do Impacto da Proteção de Dados (AIPD) e determinação se o tratamento "pode dar origem a um risco elevado" para os fins do Regulamento 2016/679 | WP 248 rev.01 (13 de outubro de 2017).

[WP29- Diretrizes] Diretrizes sobre a aplicação e implementação de multas administrativas para os fins do Regulamento 2016/679 | WP 253 (21 de outubro de 2017).

[WP29 - Diretrizes] Diretrizes sobre a Tomada de decisões individuais automatizadas e Definição de perfis para os fins do Regulamento 2016/679 | WP 251 rev.01 (13 de fevereiro de 2018).

[WP29 – Diretrizes] Diretrizes sobre os Responsáveis pela Proteção de Dados ("DPOs") | WP 243 rev.01 (5 de abril de 2017).

[WP29 - Diretrizes] Diretrizes sobre a Transparência conforme o Regulamento 2016/679 | WP260 rev.01 (11 de abril de 2018).

[WP29 - Diretrizes] Diretrizes sobre o Consentimento conforme o Regulamento 2016/679 | WP259 rev.01 (11 de abril de 2018).

[EDPB – Opinião] Opinião 23/2018 sobre Propostas da Comissão sobre Ordens Europeias de Produção e Conservação para Evidência Eletrônica em Assuntos Criminais (Art. 70.1.b) (26 de setembro de 2018).

[EDPB – Opinião] Opinião 28/2018 relativa ao Esboço da Decisão de Implementação da Comissão Europeia sobre a Proteção Adequada de Dados Pessoais no Japão (5 de dezembro de 2018).

[EDPB – Opinião] Opinião 14/2019 sobre o esboço das Cláusulas Contratuais Padronizadas apresentado pela DK SA (Artigo 28(8) do RGPD) (12 de julho de 2019).

[EDPB - Recomendação] Recomendação 01/2019 sobre o Esboço da Lista de Supervisores Europeus de Proteção de Dados com Relação às Operações de Tratamento Sujeitas ao Pedido de uma Avaliação do Impacto da Proteção de Dados (Artigo 39(4) do Regulamento (UE) 2018/1725) (10 de julho de 2019).

[EDPB – EDPS Resposta Conjunta] EPDB-EDPS Resposta Conjunta ao Comitê LIBE sobre o Impacto da lei "US Cloud Act" sobre o Enquadramento Legal Europeu para a Proteção de Dados Pessoais (Anexo) (10 de julho de 2019).

[EDPB Opinião] Opinião 13/2019 sobre o esboço da lista da autoridade de supervisão competente da França com relação às operações de tratamento isentas do pedido de uma avaliação do impacto da proteção de dados (Artigo 35(5) do RGPD) (10 de julho de 2019).

Fontes

- Commission Nationale de l'Informatique et des Libertés
    - https://www.cnil.fr/en/home
    - Setembro de 2019
    - Licença: CC-BY-ND 3.0 FR
- Gabinete do Comissário para a Informação
    - https://ico.org.uk/
    - Setembro de 2019
    - Licenciado nos termos da Open Government Licence
- União Europeia
    - https://eur-lex.europa.eu
    - 1998-2019
- https://www.iso.org/home.html
- https://www.dataguidance.com/
- https://www.onetrust.com/
- https://www.corporatefiction.fr/
- https://pixabay.com/fr/service/license/

Estas fontes são somente e rigorosamente utilizadas para fins educativos, de treinamento e conscientização.

O intervenientes mencionados não apoiam nem dão quaisquer garantias sobre o conteúdo deste trabalho.

Os direitos de propriedade intelectual, incluindo os direitos autorais sobre seus materiais, continuam pertencendo a eles.

A versão inglesa deste Guia serve como referência.
As traduções deste documento poderão ser sujeitas a interpretação.
Primeira edição: Setembro de 2019
Publicado por ROQUETTE FRERES
Design editorial e gráficos: Comitê de Compliance
Fotografia: utilização livre

ROQUETTE

Offering the best of nature™