

QPMC PT, Lda
Aldeamento Turistico Pedras da Rainha
Casa da Recepção
8800-591 Cabanas de Tavira
fred.delien@qpmc.com
+351 932 566 211

LISTA DE CONTRÔLE RGPD

A abordagem certa para a conformidade ao PRIVACIDADE da sua empresa!

Siga os 10 passos deste guia, respondendo a todas as perguntas, e descubra o que você precisa resolver para tornar-se compatível com o regulamento de privacidade da UE.

Passo 1 – Mapear os seus dados

Fazer algum tipo de inventário de dados é a primeira e mais importante etapa na preparação do roteiro de conformidade.

Tente recapitular e documentar todos os dados que você usa para administrar o negócio ¹.

Pode fazer este exercício usando um arquivo Excel, por exemplo. Isso permitirá provar que você passou por essa importante primeira etapa de análise, além do que adicionar maturidade à compreensão das funções do negócio.

Responda as perguntas abaixo. Elas vêm ajudar a obter informações sobre os seus fluxos de dados.

De quem você guarda informações pessoais?

- Clientes
- Fornecedores
- Pessoal
- Clientes potenciais
- Outros:

Quais categorias de informações pessoais você mantém?

- Dados de identidade (nome, endereço, número de telefone,...)
- Dados de facturação
- Dados sensíveis (saúde, biometria, genética...)
- Outros:

De onde vem esta informação pessoal?

.....
.....

Atenção: De acordo com a RGPD, você deve cooperar apenas com empresas "seguras". É importante incluir cláusulas de garantia nos contratos que você tem com os seus parceiros.

Onde você armazena esta informação? Em qual banco(s) de dados, e onde é / são este / estes base(s) de dados localizado(s)?

.....
.....

¹ usa para administrar o negócio => sentido muito amplo como reunir, gravar, classificar, armazenar, atualizar, alterar, solicitar, consultar, usar, fornecer por meio de encaminhamento, distribuição ou disponibilização de qualquer tipo de forma, combinando, relacionando, inclusive protegendo, excluindo ou destruindo em dados pessoais.

- Quem tem acesso a este / estes banco(s) de dados? Quais são as suas funções?

.....
.....

É absolutamente necessário que todas essas pessoas tenham acesso ao banco de dados? O acesso ao banco de dados é seguro? Tome as medidas necessárias para garantir o acesso seguro às informações. Essas medidas podem ser digitais, mas também um simples bloqueio no armário onde alguns dos documentos são armazenados.

- As informações pessoais são compartilhadas ou encaminhadas para outra empresa? Em caso afirmativo, dentro da UE ou fora da UE (armazenamento em nuvem)

.....
.....

Cuidado: Se, por exemplo, você corrigir informações pessoais, você deverá informar à empresa a quem encaminhais as informações pessoais da correção que você aplicou.

O encaminhamento para empresas fora da UE só é possível se todas as condições e obrigações de encaminhamento forem atendidas (art. 13.1 e); art. 14.1 f); art. 15,2; art. 30.1 e); art. 44-50; ...).

- Por que você precisa manter esses dados pessoais?

.....
.....

Atenção: Você só pode coletar e manter dados pessoais para propósitos específicos, explicitamente definidos e legítimos. Os dados pessoais coletados devem ser relevantes e limitados aos objetivos do tratamento. (veja mais no texto)

- Por quanto tempo você mantém os dados?

.....
.....

Cuidado: Você não pode manter informações pessoais por mais tempo do que o necessário para as finalidades pretendidas do tratamento.

O resultado do exercício deste etapa ajudará nas próximas etapas necessárias para tornar a privacidade da sua empresa compatível. Isso será especialmente útil na etapa 9, que trata da configuração do registo com a descrição do tratamento de dados para cada transação comercial individual.

Passo 2 – Refletir sobre o fundamento jurídico para tratar dados pessoais

Você só pode recolher e tratar dados pessoais quando existe uma base jurídica (art. 6).

Portanto, você precisa definir o tipo de tratamento de dados que deseja fazer e em qual base jurídica isso pode ser feito. Marque-os abaixo:

Você trata dados pessoais porque:

- a pessoa em questão deu o seu **consentimento**;
- o tratamento é necessário para a execução de um contrato;
 - *Se, por exemplo, um cliente fez um pedido que você precisa entregar, você poderá tratar os dados de endereço dessa pessoa.*
 - *Se, por exemplo, um cliente paga on-line, você poderá tratar os dados do cartão de crédito para receber o pagamento.*
- o tratamento é necessário para cumprir uma **obrigação legal**;
 - *Se, por exemplo, você administra uma empresa, então você tem que fornecer informações sobre os seus funcionários para a segurança social.*
- o tratamento é necessário para proteger **os interesses vitais** da pessoa em questão ou de outra pessoa;
- o tratamento é necessário para cumprir uma **tarefa de interesse comum**;
- o tratamento é necessário para satisfazer um **interesse legítimo**.
 - *por exemplo fins de saúde como saúde pública, proteção social, prevenção de fraude, marketing direto,...*
 - *Em qualquer caso, um equilíbrio de interesses sempre terá ser feito (consideração 47).*

Por que é tão importante saber tudo isso?

Dependendo do fundamento jurídico, os direitos da pessoa em questão podem variar.

Uma pessoa cujos dados pessoais tenham sido tratados com base em seu consentimento prévio tem um direito mais poderoso de solicitar a remoção de seus dados pessoais (Etapa 4).

A base legal também precisa ser esclarecida na Política de Privacidade e cada vez que você responder a uma solicitação de acesso a informações pessoais.

Passo 3 – Cuidado com os informações pessoais sensíveis

É **proibido** tratar informações pessoais que revelem raça ou origem étnica, opiniões políticas, convicção religiosa ou filosófica ou associação a sindicatos, além de tratar dados genéticos ou biométricos para fins de identificação única de uma pessoa, ou dados de saúde ou dados relacionados com a orientação ou comportamento sexual de uma pessoa (art. 9).

Várias exceções são definidas abaixo:

- Caso a pessoa tenha dado o seu consentimento explícito;
- Para satisfazer uma obrigação legal;
- Na proteção de interesses vitais;
- Informações pessoais que obviamente foram tornadas públicas pela pessoa em questão;
- Em caso de necessidade de levantar uma reivindicação legal ou quando um tribunal atua dentro de sua jurisdição;
- Quando necessário para satisfazer razões de interesse geral muito importante (a proporcionalidade em relação ao objetivo perseguido deve ser garantida);
- Quando necessário para o propósito de medicina preventiva ou ocupacional, o julgamento médico da capacidade de trabalho de um empregado, diagnósticos médicos, provisão de cuidado médico ou serviços sociais;
- Quando requerido por razões de interesse comum para a saúde pública;
- Quando necessário, por razões de arquivamento de interesse comum, pesquisa científica ou histórica ou fins estatísticos.

Valide isso aqui para sua empresa, marque e complete:

Trato dados confidenciais:

.....

Tenho as seguintes exceções:

.....

.....

O tratamento de dados pessoais relacionados a condenações criminais e atos ilegais também só pode ocorrer sob condições particulares (art. 10).

Trato dados pessoais relacionados a condenações criminais:

.....

.....

Se tratar o tipo de dados acima, você deve consultar o site da Comissão de Privacidade, onde ides encontrar mais informações sobre dados pessoais sensíveis e condenação criminal. Você provavelmente também pode consultar um profissional de Segurança da Informação.

Passo 4 – Pedir o consentimento de maneira correta?

Um ato muito importante no RGDP está solicitar o consentimento de uma pessoa. De acordo com as regras, este consentimento deve ser voluntário, específico, bem informado e não ambíguo. O consentimento também precisa sempre ser um ato de confirmação (art. 4, 11 e art. 7).

Valide isso aqui para sua empresa, marque e complete:

- Prevejo uma escolha voluntária para o consentimento, em que a pessoa pode concordar expressamente (um "opt-in").
- Informo claramente a pessoa sobre o que é o consentimento e para que propósitos (cf. direito de informação).
- Não deduzo o consentimento do silêncio, de uma caixa pré-marcada ou de nenhuma reação a um pedido de consentimento oculto em termos e termos legais e longos.
- Prevejo a possibilidade de que a pessoa possa retirar o seu consentimento em todos os momentos. A retirada do consentimento é tão fácil quanto fornecer consentimento, por ex. indicar claramente as formas pelas quais a retirada pode ser feita ou solicitada.

Observe também que é importante que o ato de dar consentimento seja controlável. Ou seja você deve ser capaz de demonstrar quem, quando e como o consentimento foi fornecido. Você deve registrar essas informações em um documento.

- Fornecer consentimento é controlável (rastreado).

Cuidado: Crianças -13!

Se você, como empresa, coletar e tratar informações pessoais de crianças com idade inferior a 13 anos, os pais ou responsáveis precisarão fornecer consentimento (art. 8). Esta obrigação só se aplica quando o tratamento é baseado em consentimento e quando se trata de serviços oferecidos pela empresa de informação.

Você também precisa ser capaz de demonstrar que exerceu um esforço razoável para validar o consentimento.

Valide isso aqui para a sua empresa

- Eu salvo dados de crianças -13 com base no consentimento.
- Tenho um sistema que permite-me controlar se o consentimento foi dado por um pai / responsável

E quanto ao consentimento passado?

Não precisa solicitar consentimento novamente quando o consentimento, que foi dado no passado, está em conformidade com os novos requisitos. Se esse não for o caso, você precisa solicitar o consentimento de maneira correta novamente.

Passo 5 – Você garante os direitos das pessoas envolvidas?

Como empresa, você precisará prender em conta um número substancial de direitos que o RGPD oferece às pessoas envolvidas. Faça uma avaliação rigorosa para descobrir onde as alterações devem estar em conformidade. É importante entender como você vai reagir a solicitações de pessoas que desejam exercer os seus direitos. Quem será o responsável? Essa pessoa sabe o que fazer? É tecnicamente viável?

Verifique abaixo se você pode (corretamente) lidar com esses direitos; marque as caixas ou indique se os itens não são aplicáveis:

Verifique: Comunicação e procedimentos claros para reagir a pedidos de exercício de direitos pessoais (art. 12 RGPD)

Toda a informação e comunicação devem ser fornecidas de forma concisa, transparente, compreensível e de fácil acesso, por um lado, e, numa linguagem clara e simples, por outro lado. Se uma pessoa invoca um dos seus direitos, então você precisa reagir dentro de um mês após o recebimento da solicitação. Em função da complexidade do pedido, o prazo de resposta pode ser alongado com mais de 2 meses.

Verifique: O direito de informação é aplicado corretamente (art. 13 e 14 RGPD)

- ⇒ Eu não trato dados pessoais quando o cliente em questão não está ciente.
- ⇒ O regulamento define que os seguintes dados precisam ser fornecidos ao seu cliente:
 - nome e endereço da sua empresa,
 - o objetivo do seu tratamento (por exemplo, “marketing direto”),
 - existência de direito de resistência sem custo,
 - existência de direito de consultar e corrigir os dados,
 - os receptores ou as categorias de receptores dos dados;
- ⇒ Esta obrigação se aplica independentemente de os dados terem sido obtidos diretamente ou indiretamente do cliente.

Verifique: O direito de consultar os dados (art. 15 RGPD)

- ⇒ A pessoa de quem você mantém informações tem o direito de consultar certas informações e obter informações adicionais sobre várias coisas;
- ⇒ Eu organizo uma cópia gratuita dos dados pessoais tratados dentro de um mês (prorrogável por 2 meses);
- ⇒ Tenho um modelo para responder a pessoas solicitando acesso as suas informações.

Verifique: O direito de corrigir os dados (art. 16 RGPD)

- ⇒ A pessoa de quem você guarda informações tem o direito de corrigir informações pessoais erradas ou incompletas;
- ⇒ Eu reajo dentro de um mês (prorrogável com 2 meses);
- ⇒ Informa também todos os terceiros a quem os dados foram fornecidos e informa a pessoa em questão a quem a informação foi enviada.

Verifique: O direito de remover os dados (art. 17 RGPD)

- ⇒ Em vários casos específicos, a pessoa de quem você mantém informações tem o direito de ser “esquecida” e removida do banco de dados.
- ⇒ Pode recusar um pedido de remoção em um número de casos, como direito de liberdade de expressão, obrigação legal de tratar, tarefa de interesse público ou saúde pública, arquivamento de interesse público ou fins de pesquisa científica ou histórica, ou iniciação ou exercício de ação legal.
- ⇒ Informe todos os destinatários terceiros para quem os dados foram fornecidos sobre a remoção, a menos que não seja possível ou exigiria esforço desproporcional (art. 19 RGPD).

Verifique: O direito de restringir os dados (art. 18 RGPD)

Em vários casos, a pessoa em questão pode solicitar a restrição do escopo das informações pessoais tratadas:

- A pessoa em questão contesta a exatidão dos dados;
- A pessoa em questão se opõe ao tratamento;
- No caso de tratar os dados ilegais (solicitação de remoção alterada para restrição);
- Não precisa mais os dados, mas a pessoa em questão precisa os dados.

Informe todos os destinatários terceiros para quem os dados foram fornecidos sobre a restrição, a menos que não seja possível ou exigiria um esforço desproporcional (art. 19 RGPD).

Verifique: O direito de transferir os dados (art. 20 RGPD)

A pessoa cujos dados você mantém, tem o direito de solicitar a transferência das informações pessoais que ele forneceu para outra empresa. Essa transferência precisa ser gratuita, precisa acontecer dentro de um mês (prorrogável em 2 meses), em um formato eletrônico estruturado e comumente usado.

Isso só é possível para os dados que você trata como empresa de maneira automatizada e é baseado no consentimento ou em um contrato.

- Não aplicável

Verifique: O direito de opor-se ao tratamento (art. 21 RGPD)

A pessoa de quem você guarda dados tem, em todos os momentos e por causa de sua situação específica, o direito de opor-se ao tratamento de suas informações (a menos que seja legalmente determinado ou quando necessário para executar um contrato). Quando as informações são coletadas para fins de marketing direto (incluindo o perfil relacionado ao marketing direto), a pessoa em questão pode, sem custo e sem justificativa, objetar ao tratamento de seus dados.

- Informe a pessoa em questão, em qualquer caso, sobre o seu direito de oposição e mencione isso explicitamente na política de privacidade.

Verifique: Tomada de decisão automatizada, dentre as quais a profiling (art. 22 RGPD)

Toda pessoa de quem você mantém informações tem o direito de não estar sujeita a uma tomada de decisão completamente automatizada. Este direito não é aplicável quando o processo de tomada de decisão 1) é necessário para construir ou executar um acordo; 2) é legalmente permitido; 3) baseia-se no consentimento explícito.

Passo 6 – Preparado para vazamentos?

Se você for confrontado com um vazamento de dados (por exemplo, o seu sistema de computador foi invadido e todas as suas informações podem ter sido roubadas), você tem uma obrigação de informar (imediatamente ou dentro de 72 horas) quando identifica uma violação.

a) Obrigação de informar a Comissão de Privacidade (art. 33 RGPD)

Você deve informar a Comissão de Privacidade dentro de 72 horas de qualquer infração quando essa infração for susceptível de constituir um risco para os direitos e / ou a liberdade dos indivíduos. Só precisa denunciar as infrações que possam causar danos à pessoa em questão. Por exemplo. roubo de identidade, violação de confidencialidade,...

b) Obrigação de relatório com as pessoas preocupadas (art. 34 RGPD)

Se a infração for susceptível de representar um risco elevado para os direitos e a liberdade das pessoas em questão, devem ser notificadas sem demora. Por exemplo se detalhes bancários não criptografados foram roubados.

A obrigação de comunicar aos interessados não se aplica nos seguintes casos:

- ⇒ Você já tomou medidas de proteção técnica e organizacional apropriadas com relação a esses dados (por exemplo, criptografia).
- ⇒ Você tomou medidas posteriormente para garantir que o risco não ocorrerá mais.
- ⇒ Se a obrigação de relatar exigiria esforços desproporcionais. Nesse caso, você deve fazer um anúncio público ou tomar uma medida equivalente igualmente eficaz.

c) Dados necessários para denunciar infrações

A notificação à Comissão de Privacidade e as pessoas envolvidas devem conter um número mínimo de dados; veja o site da Comissão de Privacidade. Também é obrigado a registrar com precisão todas as violações que ocorreram em um documento.

Certifique-se de aplicar a seguinte prática:

- Indique uma pessoa responsável por verificar e denunciar infrações:
.....
- Prepare um modelo para denunciar infrações

Faça uma estimativa do risco e da exposição aos direitos e à liberdade das pessoas se você perder os dados pessoais - de qualquer maneira - com antecedência. Dependendo dessa avaliação, você pode ou não estar se preparando para uma possível violação em maior grau. Aconselhamos que você consulte seu parceiro de TI para validar a avaliação.

Passo 7 – Preciso um Encarregado da Proteção de Dados (EPD)?

A nomeação de um EPD é completamente nova. Algumas empresas terão de nomear um EPD, uma espécie de conselheiro de prevenção de privacidade. É uma pessoa com conhecimento especializado e prático de questões de privacidade, que deve auxiliar a empresa na supervisão do cumprimento interno do RGDP (Artigos 37-39).

Quando precisa de nomear um EPD?

Existem duas situações em que o RGDP obriga as empresas a nomear um EPD:

- Você é principalmente responsável pelo tratamento de informações confidenciais, conforme definido na Etapa 2?
- Você é principalmente responsável pelo tratamento de dados pessoais que exigem observação regular e sistemática em larga escala?

O último caso é bastante vago como tal. Você deve interpretar essa situação no sentido de tratar informações pessoais como seu core business. Por exemplo, se você faz marketing direto com base em dados pessoais ou quando a criação de perfis em grande escala faz parte do seu negócio. Além disso, deve ser uma quantidade considerável de dados pessoais que você trata.

Se você não se encontrar nos casos anteriores:

- Não aplicável

O que exatamente esse especialista faz?

- ⇒ O EPD fornece informações e conselhos sobre as obrigações de RGPD para sua empresa.
- ⇒ Um EPD monitora a conformidade com o RGPD.
- ⇒ Um EPD é o ponto central de contato para proteção de dados (para a empresa, para a comissão de privacidade, bem como para pessoas cujos dados foram tratados).
- ⇒ O EPD aconselha a empresa sobre a análise de risco obrigatória e os resultados relacionados.

Para quem você pode atribuir esse papel?

- ⇒ Um **funcionário existente** com conhecimento suficiente sobre a privacidade e a segurança. As tarefas profissionais do empregado devem ser compatíveis com as tarefas de um EPD. Sob nenhuma circunstância isso pode levar a um conflito de interesses.
- ⇒ Um **EPD externo**, por exemplo um consultor, que execute essa tarefa pelo número necessário de horas por semana / mês.

Mais informações estão disponíveis no site da Comissão de Privacidade e nas diretrizes do Grupo de Trabalho 29 (um órgão europeu). Se você precisar um EPD, é recomendável solicitar suporte especializado para colocá-lo em ordem com o Regulamento.

Passo 8 – A necessidade de Avaliação de Impacto da Proteção de Dados (AIPD)?

Algumas empresas terão de realizar um AIPD, um tipo de auditoria de segurança, para certas operações de tratamento.

Quando um AIPD é necessário?

Existem 3 situações em que o RGPD impõe o AIPD:

- Quando você sistematicamente avaliar as características pessoais dos indivíduos (por exemplo, por perfis) de forma automatizada e tomar medidas com base nesta análise que tenham consequências legais ou um impacto semelhante sobre esses indivíduos (por exemplo, marketing direto);
- No caso de tratamento em grande escala de categorias especiais de dados pessoais ou dados relacionados a condenações e delitos penais;
- No caso de monitoramento sistemático e em grande escala de áreas de acesso público.

Essa avaliação não será necessária para muitas empresas micro, pequenas e médias.

Se você não estiver em um dos casos acima, marque a caixa abaixo:

- Não se aplica

Se o AIPD indica que o tratamento dos dados pessoais representa um alto risco e se você não puder limitar esse alto risco por medidas razoáveis em termos de tecnologia disponível e os custos de implementação associados, você deve procurar orientação da Comissão de Privacidade e medidas necessárias para controlar o risco.

Esta obrigação aplica-se apenas a **situações de alto risco**. A avaliação de um "alto risco" deve sempre ser executada em função dos tipos de dados pessoais, do escopo e da frequência do tratamento (artigos 35 a 36). Por exemplo, quando uma nova tecnologia é implementada ou quando uma operação de criação de perfis pode ter um efeito significativo sobre o titular dos dados / pessoa em questão.

Mais informações sobre o AIPD pode encontrar no site da Comissão de Privacidade ou nas diretrizes do Grupo de Trabalho 29. Ver também Diário da República, 2.a série — N.º 231 — 30 de novembro de 2018. Caso você precise de realizar um AIPD, recomenda-se consultar um profissional.

Passo 9 – Mantém um registo das atividades da tratamento dos dados?

Toda empresa que trata informações pessoais deve manter um registo das suas atividades de tratamento dos dados (art. 30).

Marque as caixas abaixo para verificar se você atende aos requisitos.

O registo de tratamento de dados contém as seguintes informações:

- O **nome e as informações de contato** da pessoa responsável pelo tratamento de dados, ou do representante da pessoa responsável pelo tratamento de dados e / ou do Encarregado da Proteção de Dados
- Os **objetivos do tratamento**
- Uma descrição das **categorias das pessoas em questão**, por um lado, e das **categorias de dados pessoais**, por outro
- As **categorias de receptores** para quem as informações pessoais são ou serão fornecidas (entre outros, receptores em países terceiros ou organizações internacionais)
- Se possível, o **termo pretendido** no qual as diferentes categorias de dados precisam ser apagadas
- Se possível, uma descrição geral das **medidas de segurança técnica e organizacional**
- Se aplicável, **encaminhamento** de informações pessoais a um país terceiro ou a uma organização internacional, incluindo a identificação do país terceiro ou organização internacional, e, se necessário, uma referência à documentação com as devidas salvaguardas.

Vários modelos estão disponíveis em diferentes fontes para gerenciar o registo das atividades da tratamento de dados pessoais da empresa.

Não há documento oficial que precise ser usado e você pode escolher livremente compor o seu próprio modelo em função de, por exemplo, software que você gostaria de usar. O essencial do objetivo básico do registo precisa ser respeitado: registo de uma visão global e completa de todas as atividades de tratamento dos dados.

Passo 10 - Revise a sua Política de Privacidade e adapte os seus contratos

Política de Privacidade (art. 24.2)

Este exercício também é uma boa oportunidade para avaliar a sua política de privacidade.

Para ser em conformidade com o RGPD, deve adicionar ou modificar vários elementos:

- A identidade legal completa do subcontratante, ou processador de dados, e o modo da usada das informações;
- A base legal que é necessária para o tratamento da informação;
- O período de tempo em que manterá as informações;
- Se você trocareis ou não informações com países fora da União Europeia;
- A possibilidade de a pessoa envolvida a apresentar uma queixa ao Comitê de Privacidade quando ela considera que as suas informações pessoais são tratadas incorretamente;
- Os direitos das pessoas envolvidas;
- As medidas de segurança técnica e organizacional tomadas para estar em conformidade;
- O(s) propósito(s) para o qual a informação será tratada;
- ...

É muito importante permanecer a **transparência tão completo que possível** (veja também direito à informação, art. 13-14). Enquanto você elabora / altera a sua política de privacidade, deve considerar todos os elementos de informações individuais que você pode precisar para fornecer à pessoa titular no momento que solicita o consentimento para tratar as suas informações pessoais.

Em qualquer caso, você precisará de garantir que a política de privacidade seja o mais condensada possível e escrita em uma linguagem clara e compreensível.

Contratos (art. 28)

Todos os seus contratos (com fornecedores, funcionários, subcontratantes²...) precisarão de ser em conformidade com o RGPD.

Sob o novo regulamento, também precisa de garantir que trabalha com empresas "seguras". O RGPD impõe que você proteja os seus próprios bancos de dados adequadamente em primeiro lugar. Além disso, quando você terceiriza determinadas atividades, é crucial avaliar se as precauções de segurança definidas nos contratos existentes são adequadas, além de estar em conformidade com o RGPD. Os contratos existentes podem ser estendidos usando por exemplo anexos.

Avaliais os contratos existentes com fornecedores, subcontratantes, etc. e alterais se necessário

- Asseguro sempre ter um contrato por escrito com as devidas precauções de segurança.

² Como empresa, você pode decidir delegar o trabalho e o tratamento relacionado de informações pessoais a um subcontratado externo. Esses subcontratantes são denominados "processadores"

Depois de passar por essa lista de verificação e aplicar todos os itens de ação necessários, você está normalmente em conformidade com o RGPD. Nós encorajamos você a documentar e armazenar adequadamente todos os seus passos e ações.

Nome: **Data:**.....

Empresa:..... **Assinatura:**