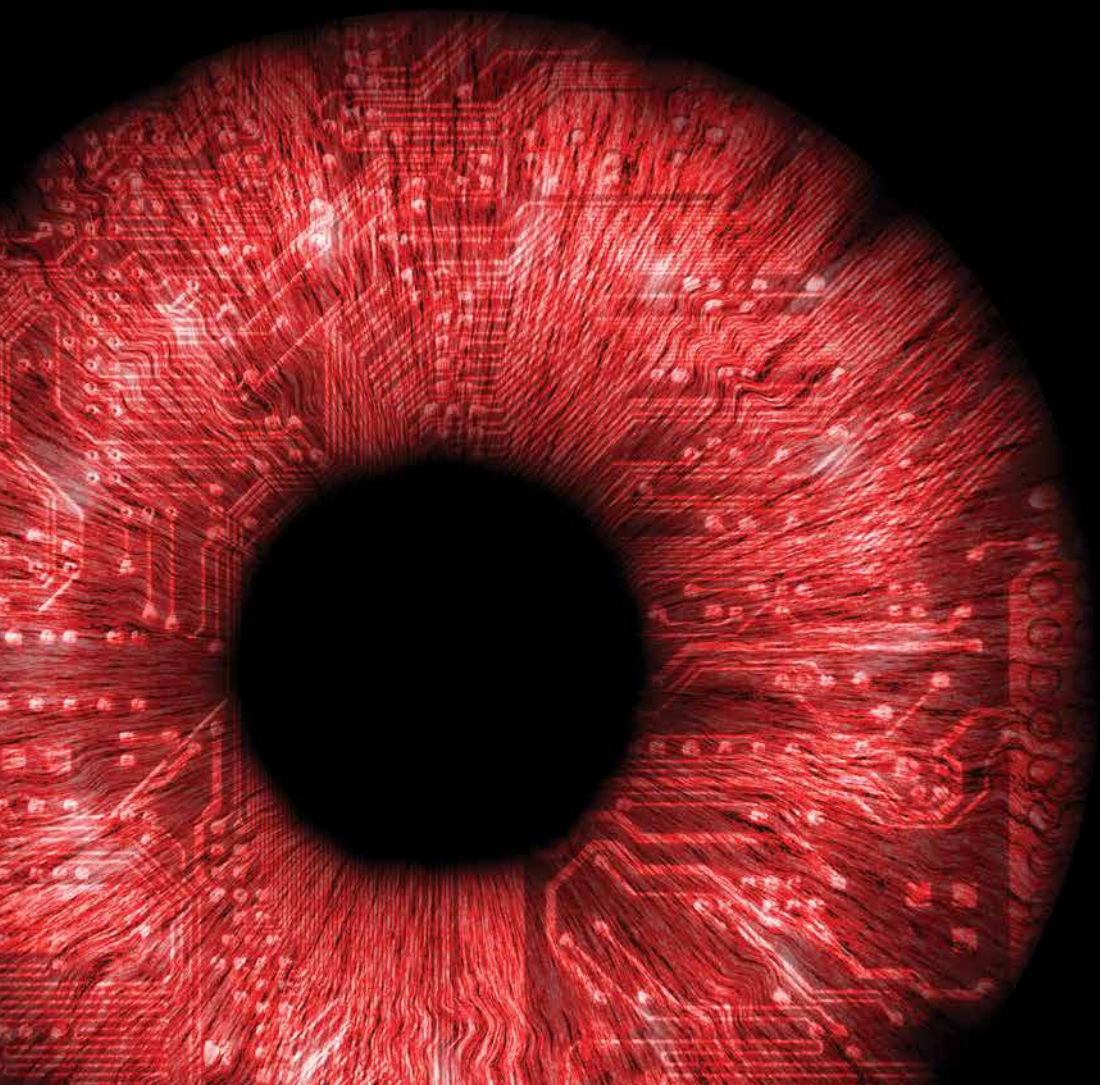
HISCOX

O SEU NEGÓCIO ESTÁ PREPARADO PARA O NOVO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS?



Innovarisk
UNDERWRITING

Introdução

Com a introdução do novo Regulamento Geral de Proteção de Dados (RGPD), as empresas devem adaptar sua política de gestão de informações pessoais dos seus clientes a esta nova realidade regulamentar.

O primeiro passo é entender quem será afetado por este novo regulamento. O RGPD é aplicado a qualquer empresa que ofereça bens ou serviços que façam gestão de dados de pessoas que habitem num dos estados membros da União Europeia. Ou seja, não falamos somente de empresas sediadas nesses países, mas sim de qualquer empresa que possua dados de clientes que habitem na União Europeia.

Assim, milhares de empresas em todo o mundo têm feito por adaptar-se a esta nova realidade. O nosso compromisso com o setor empresarial, por segurarmos mais de 300.000 profissionais e empresas em todo o mundo, leva-nos além da mera colaboração. Preparámos este guia onde respondemos às seguintes questões:

1. O que é o novo Regulamento Geral de Proteção de Dados?
2. O que devo fazer para cumprir o RGPD?
3. O que acontece se violar a proteção de dados dos meus clientes já com o novo regulamento em funcionamento?
4. Quais serão as consequências de não adaptar o meu negócio?
5. Onde posso obter mais informações ou suporte adicional?

1. O que é o novo Regulamento Geral de Proteção de Dados?

O Regulamento Geral de Proteção de Dados (RGPD - Regulamento da UE 2016/679) é um quadro regulamentar pelo qual o Parlamento Europeu, o Conselho da União Europeia e a Comissão Europeia pretendem reforçar e unificar a proteção de dados e a sua livre circulação para todas as pessoas da União Europeia. Esta nova legislação concedeu um período de adaptação de dois anos, terminando em maio de 2018.

A resposta da União Europeia ao novo paradigma da ciber-segurança

O objetivo do regulamento é salvaguardar os dados pessoais dos cidadãos da União Europeia que sejam geridos e controlados por instituições públicas, empresas e organizações em todo o mundo. Assim, perante o novo paradigma de segurança cibernética, milhões de dados - nomes, endereços, dados pessoais e até mesmo identificadores online (por exemplo, um endereço IP) - terão maior proteção.

Sou uma pequena empresa tenho que cumprir com o regulamento?

Sim. Seja qual for a dimensão da sua empresa, independentemente do setor em que opera, qualquer empresa ou instituição que trate informações sobre os cidadãos da UE está sob o escopo deste novo regulamento. Existem algumas singularidades que têm em conta os recursos menores das PMEs como, por exemplo, não as obrigando a nomear um responsável pela proteção de dados (Data Protection Officer - DPO) da empresa. Mesmo assim, o novo regulamento é tão rigoroso que mesmo que uma PME esteja dentro destas exceções mas seja fornecedora de uma empresa que é obrigada a ter um elevado nível de segurança, esta pode ser obrigada a cumprir com todas as normas.

Mais uma vez, as grandes empresas são chamadas a liderar as mudanças e abrir caminho para a adaptação do tecido empresarial. Nesse sentido, muitas delas já estão preparadas para o RGPD: protegendo os dados dos seus clientes e exigindo aos seus fornecedores e colaboradores, por contrato, que cumpram com determinados requisitos de segurança.

Oportunidade de negócio

O novo quadro regulamentar pode tornar-se uma vantagem competitiva para muitas empresas quando se trata de optar por um novo negócio. As empresas devem aproveitar o RGPD como um catalisador para transformar as suas empresas em negócios centrados no cliente e usar o novo regulamento como base para um relacionamento autêntico e transparente com os seus clientes.

2. O que devo fazer para cumprir o RGPD?

Há uma série de etapas simples a serem consideradas para garantir o cumprimento de todos os requisitos.

Que dados tenho, de onde vêm e por onde circulam?

Em primeiro lugar é importante entender e controlar quais os dados pessoais geridos pelo seu negócio, como os obteve, como são armazenados, como são usados e por onde podem circular. A UE define "dados pessoais" como "qualquer informação de um indivíduo, relacionada com a sua vida privada, profissional ou pública". Pode ser qualquer coisa, desde um nome, uma fotografia, um endereço de email, dados bancários, publicação nas redes sociais, informação médica ou o endereço IP do computador. Isto amplia o conceito de dados pessoais em relação à estrutura regulatória anterior, incluindo conceitos como IDs de dispositivos, dados de localização e dados genéticos e biométricos.

A figura do responsável e subcontratante: responsabilidades

Existem dois tipos de entidades que podem tratar dados pessoais. Por um lado, existe o chamado responsável pelos dados, que possui os dados e determina o seu propósito, utilização e circulação. Por outro lado o subcontratante, que pode processar dados pessoais em nome do responsável. A obrigação de proteger os dados é agora partilhada entre responsável e subcontratante e ambos são regidos pelo RGPD. Além disso, os subcontratantes estarão sujeitos a sanções quando não cumprirem as obrigações contratuais ou agirem fora das instruções do Responsável.

6 Princípios para as empresas sobre como deverão ser os dados pessoais que gerem:

1. Transparentes, exatos e legalmente processados.
2. Processados para um propósito específico.
3. Adequados e relevantes para o propósito para o qual estão a ser processados.
4. Precisos (eliminando e corrigindo-os com maior regularidade).
5. Não devem ser mantidos por mais tempo do que o estritamente necessário e para o propósito para o qual foram processados.
6. Seguros.

Temos o consentimento para recolher e operar com esses dados?

O RGPD torna muito mais complicado obter o consentimento para processar os dados pessoais de um individuo (por exemplo, para fins comerciais). A definição de consentimento foi ajustada para que seja "inequívoca" quando ocorre, isto é, que o indivíduo tenha assinalado ativamente uma caixa ou selecionado a opção de consentimento. Também é aplicado retroativamente, portanto devemos obter a permissão inequívoca também dos dados pessoais que já armazenamos.

As solicitações de consentimento devem ser enviadas individualmente, com espaço próprio, para que não possam ser incluídas ou ocultas em outras políticas ou letras pequenas. Assim, além de obter esse consentimento, devemos ser capazes de demonstrar, se necessário, qual foi o processo pelo qual os obtivemos. As caixas marcadas previamente ou a não-resposta como resposta positiva vão deixar de ser válidas. O processo de obtenção só será considerado válido se o consentimento for adquirido de forma ativa por parte do sujeito.

Perante esta nova exigência deve perguntar-se: "Como obtenho o consentimento agora? Que mudanças terei que fazer nos processos para garantir poder demonstrar onde, quando e como as pessoas deram o seu consentimento para que pudesse processar os seus dados?"

Proteção de dados desde a sua conceção

Agora a proteção de dados deve ser considerada e integrada em qualquer sistema ou processo desde a sua conceção. Este conceito aplica-se tanto na forma como são projetados como nas políticas e procedimentos estabelecidos que determinem como devem ser usados.

Uma solução neste campo é o uso de criptografia pois oferece um perfil de segurança elevado e pode também reduzir a multa a que estamos expostos, bem como a probabilidade de sermos sancionados no caso de uma violação de dados.

Direito de acesso aos dados

Com a entrada em vigor do Regulamento, os indivíduos aumentam os seus direitos em relação à forma como os seus dados pessoais são protegidos. As empresas devem garantir que existem processos e modelos adequados para qualquer pessoa que queira exercer o seu direito. Qualquer pedido neste âmbito deve ser atendido no prazo máximo de um mês.

De que direitos falamos?

- Ter acesso fácil a todos os seus dados pessoais armazenados.
- Direito de retificação de dados imprecisos. Negar o processamento dos seus dados em determinadas circunstâncias como, por exemplo, ações comerciais.
- O direito de transferir os seus dados de um serviço para outro.
- Exportar os dados num formato que possa ser usado noutros ambientes de TI.
- Eliminar completamente, em determinadas circunstâncias, todos os seus dados.
- O consentimento deve ser claro, livre, específico, informado e não ambíguo. Além disso, esse consentimento deve ser especificado, detalhado, definido, documentado e facilmente rescindido.
- Informação clara sobre o processamento.
- Direito à notificação se os dados estiverem comprometidos.
- Requisitos de segurança mais rigorosos a serem transferidos para fora da UE.

O que constitui uma violação de dados pessoais?

Devemos certificar-nos de que todas as pessoas que fazem parte da nossa empresa entendam o que constitui uma violação de dados, bem como estabelecer um processo para localizar links ou processos internos mais fracos. Este trabalho de consciencialização e formação será vital para estar preparado antes da entrada iminente do RGPD.

Mas para além de formar e fornecer as ferramentas necessárias para toda a equipa, também é preciso desenvolver e fomentar uma cultura na qual os funcionários se sintam à vontade e avisem quando cometem um erro inocente, a principal causa da grande maioria das violações de dados.

Rever os termos e condições, bem como os contratos com fornecedores

Ao adaptar o nosso negócio ao RGPD, devemos incluir também os fornecedores que processam os dados pessoais em nosso nome ou coordenados connosco, para assegurar que há uma proteção adequada e em conformidade com o regulamento. Assim, podemos solicitar-lhes que preencham um formulário para avaliar quais medidas e estratégia de segurança cibernética têm implementadas, avaliar se são suficientes ou executando uma auditoria física no local.

Além disso, quando os nossos fornecedores processam dados pessoais em nosso nome, é obrigatória a atualização dos contratos com estes mesmos fornecedores para incluir uma série de cláusulas obrigatórias que podem ser encontradas no Artigo 28 do RGPD. Assim, garantimos que o fornecedor está obrigado a fornecer padrões de proteção de dados compatíveis com o RGPD.

Obviamente que pode dar-se o caso inverso, que somos nós os fornecedores que processam os dados pessoais para outras empresas, portanto, somos a entidade a quem estes critérios se aplicam. Estar preparado ajudar-nos-á perante possíveis negociações de novos contratos e dar-nos-á uma vantagem competitiva.

Rever o nosso aviso de privacidade

Tendo em vista os novos requisitos provavelmente a nossa política de privacidade deverá tornar-se mais extensa. Deve ser detalhada, compreensível e acessível. O conteúdo irá variar conforme se os dados pessoais recolhidos forem para nossa utilização ou se forem armazenados por terceiros.
A informação fornecida deve incluir:

- O propósito para o qual os dados pessoais estão a ser processados, bem como a base legal para o processamento (por exemplo consentimento, interesses legítimos, requisitos contratuais, entre outros).
- O destinatário ou tipos de destinatários entre os quais esses dados pessoais podem circular.
- O nome e os detalhes da entidade que controlará os seus dados pessoais e outras entidades que poderão usar os seus dados pessoais.
- O período de retenção desses dados ou os critérios usados para determinar o período de retenção.
- Informação detalhada sobre cada um dos direitos da pessoa autorizada (exclusão, portabilidade, retificação, entre outros).
- Qualquer outra informação sobre o perfil da entidade responsável que seja de utilidade.

Além disso, o aviso de privacidade deve ser conciso, transparente, inteligível e de fácil acesso, escrito numa linguagem clara e simples.

Caso real: o Facebook foi multado em 1,2 milhões de euros em Espanha por violar leis de privacidade.
O regulador descobriu que o Facebook não informou os utilizadores como é que os seus dados seriam usados nas campanhas publicitárias. O Facebook foi acusado de usar termos “genéricos” e “pouco claros” e uma política de privacidade de difícil acesso.

Dados de risco elevado

Antes de iniciar o processamento de dados considerados de risco elevado, é necessária uma avaliação documentada que identifique esses riscos para demonstrar a conformidade com o RGPD. Embora este requisito não especifique quais dados que podem ser de risco elevado, pode incluir informações como cadastro criminal ou processamento de dados confidenciais, tais como dados de contas bancárias ou informações de saúde, que poderiam ter um impacto prejudicial no indivíduo caso esses dados fossem expostos.

É necessário nomear um responsável pela proteção de dados (DPO)?

Sim, embora a maioria das empresas com menos de 250 funcionários esteja isenta, no caso das suas atividades principais envolverem a monitorização ou processamento de dados confidenciais em "grande escala" (que incluam dados reveladores de origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas, afiliações sindicais, ou dados relacionados com a saúde ou a vida sexual), deverão nomear um responsável de proteção de dados independente da administração da empresa e da equipa que trabalha no processamento de dados. Ou seja, as responsabilidades do responsável não podem ser entregues a nenhum membro da equipa de gestão de sistemas da empresa.

Embora até agora não tenha sido totalmente definido o que constitui "grande escala", alguns exemplos seriam:

- Dados de pacientes de um hospital.
- Dados de pessoas que utilizam o serviço de transporte de passageiros numa cidade.
- Dados de cliente numa companhia de seguros ou de um banco.

Resumo: cinco pontos que demonstram que adaptámos o nosso negócio:

- Implementar medidas técnicas e organizacionais que garantam e demonstrem que o nosso negócio se encontra adaptado: novas políticas, programas de formação e capacitação, auditorias e avaliações.
- Oferecer documentação atualizada sobre os processos que estamos a adotar.
- Se aplicável, nomear um DPO.
- Implementar medidas que cumpram os princípios de design de proteção de dados e proteção de dados por defeito: minimização de dados e transparência.
- Desenvolver avaliações dos nossos processos de proteção de dados.

3. O que acontece se violar a proteção de dados dos meus clientes perante o novo regulamento?

O RGPD define como “violação de dados pessoais” uma violação de segurança que permita a destruição, perda, alteração, divulgação não autorizada ou acesso a dados pessoais. Isso significa que uma “violação de dados pessoais” é mais do que simples invasão ou perda de dados pessoais. Isto também se aplica a todos os dados armazenados, independentemente do processo, para que os dados em papel sejam tratados com o mesmo nível de cuidado.

Quando reportar uma infração

As infrações terão de ser comunicadas à Comissão Nacional de Proteção de Dados, caso “os direitos e liberdades das pessoas forem suscetíveis de estar em risco”. Os exemplos fornecidos cingem-se a informações que possam “levar à discriminação, danos à reputação, perda financeira, perda de confidencialidade ou qualquer outra desvantagem económica ou social significativa”.

As pessoas afetadas só terão que ser notificadas sobre as infrações quando houver um risco elevado de partilha de informação pessoal.

Qual é o prazo para informar sobre uma infração?

O aviso de uma infração deve ser feito dentro das primeiras 72 horas da sua ocorrência e o relatório deve conter, no mínimo:

- A natureza da violação dos dados pessoais incluindo, sempre que possível, as categorias e o número aproximado de pessoas e dados pessoais, o nome e as informações de contacto do DPO (se a organização tiver um) ou um contato que for capaz de confirmar as informações.
- Uma descrição das prováveis consequências causadas por esta infração.
- Uma descrição das medidas propostas ou adotadas para gerir a “violação de dados pessoais” e, quando apropriado, as medidas tomadas para minimizar possíveis efeitos adversos.

Como preparar-se para infrações

Dada a definição ampla de “violação de dados pessoais” e “dados pessoais”, é quase inevitável que qualquer empresa caia numa infração menor (apenas enviando um email para a pessoa errada), pelo que devemos pensar sobre o que vamos fazer quando isso ocorre, especialmente tendo em conta o prazo estrito necessário para a notificação da infração.

Definir um plano de resposta simples para estes incidentes pode fazer uma grande diferença e minimizar o possível impacto negativo sobre nós. Considere então:

- Quem deve ser informado internamente se ocorrer uma infração?
- Quem participa na avaliação das consequências da infração?
- Quais são os nossos sistemas e dados mais sensíveis e aos quais devemos dar prioridade nos nossos processos de proteção e restauro?

4. Quais poderiam ser as consequências de não adaptar o meu negócio?

Em primeiro lugar vamos dar um tom mais positivo à pergunta: o que vou ganhar se cumprir o RGPD?
Irei garantir uma melhor proteção dos dados pessoais dos meus clientes, enquanto me protejo de quaisquer sanções ou danos à minha reputação. Portanto, o cumprimento do novo regulamento irá beneficiar o meu negócio.
Agora, o que acontece se não me adaptar?

Multas por incumprimento

O incumprimento do RGPD não só ocorre quando acontece um incidente mas também se for cometido um erro administrativo ou se um dos seus requisitos não for cumprido, podendo dar lugar a uma investigação regulamentar, o que por si só requer tempo e esforço da empresa e em extremo poderá originar uma multa.

Nos seus valores máximos, a multa pode chegar a 4% da faturação do exercício do ano transato ou 20 milhões de euros para infrações mais graves. Poderá ainda ser aplicada uma multa até 2% ou 10 milhões de euros para infrações administrativas. Embora seja pouco provável que uma PME venha a ser multada nestes valores, a Comissão Nacional de Proteção de Dados (CNPD) mostrou-se disposta a impor sanções financeiras contra as PME, sendo que estará sempre atenta à sua capacidade de continuar a operar após a sanção.

5. Onde posso obter mais informações ou suporte adicional?

Existem entidades públicas e privadas que estão a disponibilizar recursos para as empresas de forma a garantir que cumpram os requisitos do RGPD. Aqui estão algumas delas:

A CNPD criou um espaço dedicado a este tema onde disponibiliza informações sobre o trabalho que está a ser desenvolvido pelas autoridades de proteção de dados a nível europeu e pela CNPD.

A Hiscox oferece uma solução de seguro de dados e segurança cibernética desenvolvida para fornecer uma resposta rápida e especializada no caso de violação de dados pessoais, o que pode, entre outras coisas, ajudar uma empresa a cumprir os requisitos rígidos do RGPD.

Innovarisk
UNDERWRITING

Representação do Grupo Hiscox em Portugal:

Innovarisk Lda – Av. Duque de Loulé, 123 - 7º, 1069-152 Lisboa

T +351 215 918 370 **F** +351 215 918 379 **E** geral@innovarisk.pt **http://innovarisk.pt**