Grant Thornton

An instinct for growth™

Risco

Regulamento

Segurança da Informação

Proteção de Dados Pessoais

Preparando seu negócio para o GDPR

Índice

O que é GDPR e como isso afeta o seu negócio?

A regulamentação de proteção de dados europeia (GDPR) entrou em vigor no dia 25 de maio de 2018.

Implementado para a União Europeia, o GDPR rege todos os negócios em operação e insere uma proteção de dados mais consistente aos países membros. Adicionalmente, empresas que realizam negócios com empresas europeias também são sujeitas a atender ao GDPR, além de conhecer as mudanças e estar em *compliance* com a norma.

Multas pelo não cumprimento da legislação podem chegar a €20 milhões ou 4% da receita global anual.

Por que a legislação de proteção de dados foi renovada?

Desde 1995, a Diretiva de Proteção de Dados Europeia (Directive 95/46/EC) determina a maneira como os dados pessoais dos indivíduos europeus estão protegidos na União Europeia. Porém, houve diversos desdobramentos no que tange a sofisticação e escala de criação e coleta de dados como nas mídias sociais, computação na nuvem e serviços de geolocalização, por exemplo. Como a Diretiva é anterior a esses desdobramentos, a norma supracitada não era mais suficiente diante do panorama de proteção de dados que vivemos atualmente. Sendo assim, a Diretiva precisava ser atualizada para endereçar as preocupações relacionadas à privacidade moderna e facilitar esta consistência de transmissão de dados pela União Europeia. É isso que o GDPR propõe.

Nesse contexto, a União Europeia preparou sua agenda para desenvolver formas de proteger seus cidadãos e suas informações privadas. O GDPR define novos direitos aos indivíduos e fortalece as proteções já existentes, aplicando medidas mais rígidas para adequar os negócios para o uso dos dados pessoais. Se houver alguma falha no cumprimento das normas, as sanções serão bastante severas.

O que isso significa para o seu negócio?

O GDPR é uma oportunidade valiosa para entender os dados que estão sob seu negócio e usá-los de forma mais efetiva. Contudo, isso pede uma aderência rígida à legislação e um entendimento claro das mudanças a fim de evitar punições severas.

Primeiramente, é importante estar atento que o GDPR substitui todas as legislações já existentes sobre proteção de dados, e isso aumenta as obrigações às empresas sobre a proteção de dados e probabilidade de falha na prestação de contas. Isso também se aplica a uma gama completa de engajamento de dados – desde a coleta de dados pessoais até seu uso e descarte. Sua companhia precisa inserir políticas e procedimentos para assegurar que seu monitoramento de GDPR (controles e documentos) estão em *compliance*.

As novas regras se aplicam às empresas de todos os portes que tratam dados pessoais. Qualquer que seja a natureza do seu negócio, o GDPR causa um impacto substancial. Com a implementação desde o dia 25 de maio de 2018, a sua empresa deve cumprir o que a norma exige.

Todas as empresas, seja europeia ou que faça negócios com companhias europeias, devem estar em *compliance* com o GDPR.

Compreenda as principais mudanças

O GDPR introduz mudanças abrangentes que requer entendimentos rigorosos, aceitação dos investidores, preparação apropriada e implementação em toda a companhia. Para promover uma visão geral, relacionamos abaixo as principais mudanças:

Aperfeiçoamento de direitos para proteção de dados
A maior mudança com o GDPR é voltada para o indivíduo dono do dado pessoal, que vai se beneficiar com os direitos aprimorados, como o de contestar determinado tipo de caracterização de dados e automatização para tomada de decisões, por exemplo. O pedido de consentimento também está mais rigoroso: deve estar explícito e assertivo, além de ser dado para casos específicos e fáceis de serem rejeitados. Os indivíduos também podem pedir que seus dados pessoais sejam excluídos ou removidos se não tiver uma razão específica para continuar sendo processado.

Aumento de prestação de contas
As empresas têm mais obrigações e responsabilidades. Elas devem publicar de forma detalhada e justa os avisos de processamento – informando aos indivíduos sobre os direitos de proteção de dados que eles possuem, adicionalmente, explicando como, por que e por quanto tempo seus dados serão utilizados. O novo regulamento abrange, ainda, o conceito de privacidade customizável, significando que as organizações devem customizar a proteção de dados em novos negócios de processamento e sistemas.

Processos formais de gerenciamento de riscos
Empresas devem identificar formalmente os riscos em ascensão relacionados à privacidade, particularmente os que estiverem associados à novos projetos, ou onde houver atividades de processamento de dados sensíveis. Elas também devem manter os registros das atividades de processamento criando inventários/relatórios internos. Para a atividade de processamento de dados de alto risco, a Avaliação de Impacto de Proteção de Dados (AIPA ou DPIAs *Data Protection Impact Assessments*) será obrigatória. Também será obrigatório indicar um responsável pela proteção de dados, isto é, um *Data Protection Officer* (DPO).

Relatório de violação de dados
Buscando maior responsabilidade, os relatórios de violação de dados estão se tornando mais rigorosos. Em caso de uma violação de dados significativa, deverá ser comunicada aos reguladores (europeus) em até 72 horas e, em alguns casos, ao indivíduo afetado sem atrasos indevidos.

Sanções significativas
As multas pelo não cumprimento do GDPR aumentarão consideravelmente até 10 milhões de euros ou 2% da receita global anual (o que for maior) para infrações menores ou técnicas, e 20 milhões de euros ou 4% da receita global anual da empresa, por falhas operacionais mais graves.

Requisitos de processamento de dados
O regulamento do GDPR impõe novas regras para os responsáveis pelo processamento dos dados, o que inclui elementos que devem ser abordados contratualmente entre quem processa os dados e quem controla os dados.

Características fundamentais do GDPR

Aperfeiçoamento de direitos para proteção de dados – o direito de contestar determinados tipos de uso e automatização de tomada de decisões e pedidos para a exclusão de dados pessoais quando desnecessários.

Aprimoramento de obrigações para empresas – por exemplo, a publicação detalhada no aviso de processamento a fim de informar os indivíduos sobre seus direitos de proteção de dados e como suas informações pessoais são usadas e por quanto tempo.

Pedido de consentimento rigoroso ao indivíduo – o consentimento deve ser explícito, informando o objetivo específico e de fácil retirada da base de dados.

Reporte rígido de violação de dados – as violações significativas de dados devem ser reportadas aos reguladores (europeus) em até 72 horas e, dependendo do caso, ao indivíduo também.

Avaliação de impacto de privacidade rígida – as empresas devem identificar e formalizar os riscos de privacidade, particularmente, para novos projetos.

Privacidade customizável – empresas devem customizar a proteção de dados em procedimentos e sistemas de negócios novos e existentes.

Aumento da proteção de registros de dados – empresas devem manter os registros das atividades de processamento quando executadas, com a Avaliação de Impacto de Proteção de Dados para o alto risco de processamento de dados.

Sanções significativas – o tamanho potencial das multas para o não cumprimento são consideráveis, alcançando até 20 milhões de euros ou 4% da receita global anual da empresa, qual for maior.

Nomear um DPO – nomear um Data Protection Officer é mandatório para diversas empresas.

Escopo regulamentar amplo – o GDPR aplica-se tanto para o controlador quanto para o responsável pelo processamento do dado.

Como podemos ajudar a preparar seu negócio para o GDPR?

O panorama jurídico para proteção de dados está em constante evolução e apresenta desafios para os negócios, governos e autoridades públicas. Se a sua empresa lida com consumidores, opera online, atua no setor financeiro ou na posse de dados sensíveis, ela pode ser atingida.

Já que estamos sob a vigência do GDPR, as empresas devem examinar e fiscalizar as mudanças regulatórias e entender como elas afetam as operações dentro de seus negócios. Tenha em mente que o impacto do GDPR não está restrito a uma área específica – isso exige que amplie seus negócios a fim de adotar uma aproximação orientada para a execução destes processos.

É provável que sua empresa precise alterar suas práticas de negócio para o cumprimento do GDPR e a implementação de novos controles. Então, como iniciar? Criamos um fluxograma simples para lhe ajudar a atingir o cumprimento da norma:

GDPR

- Entenda os principais pontos que esta legislação impõe.

***"Check list"* de proteção de dados**

- Avalie a arquitetura de dados da sua empresa, procedimentos e riscos de controle e de *compliance.*

Análise e resultados da auditoria

- Identifique os riscos de proteção de dados na sua empresa;
- Rever quão preparado seu negócio está para o GDPR.

Roteiro de implementação

- Desenvolva um roteiro de implementação que englobe a arquitetura adequada de *compliance* e regulatória;
- Garanta que o plano é realista e alcançável para sua empresa.

Implementação

- Defina um consultor de confiança para:
  - Identificar e documentar as atividades de processamento de dados;
  - Executar as avaliações de impacto de proteção de dados;
  - Desenvolver um plano de ação para os casos de violação de dados;
  - Implementar os procedimentos de dados em andamento.
- Escrever uma política de proteção de dados e definir um padrão que garanta que seu negócio está em conformidade com o GDPR;
- Oportunamente, determine o *Data Protection Officer* e um sistema de gerenciamento de proteção de dados para os controles em andamento.

Medição de efetividade da proteção de dados

- Realize uma análise de FIT/GAP para GDPR ou ISO 27001 FIT/GAP · essa é uma avaliação de aderência do seu ambiente para o GDPR.

Melhoria contínua

- Mantenha regularmente auditorias de GDPR e Avaliação de Impacto de Dados Pessoais;
- Garanta que o gerenciamento de risco de dados está integrado à estrutura de gerenciamento de riscos geral;
- Revise regularmente os dados da sua empresa tempestivamente.

Contate-nos

Fabiano Castello
Sócio-líder de Advisory
E fabiano.castello@br.gt.com
T +55 11 3886-5100

Adriana Moura
Sócia de Advisory
E adriana.moura@br.gt.com
T +55 11 3886-5100

Vitor Pedrozo
Diretor de Advisory – FIDS
E vitor.pedrozo@br.gt.com
T +55 11 3886-5100

grantthorntonbrasil@br.gt.com

/company/grant-thornton-brasil

/GrantThorntonBrasil

Grant Thornton
An instinct for growth™

grantthornton.com.br