idwall

GENERAL DATA PROTECTION REGULATION

Guia prático de recomendações e aplicações às organizações brasileiras

O QUE É A GDPR

O General Data Protection Regulation ("GDPR")[1] é um novo diploma normativo da União Europeia ("UE")[2] que regula privacidade e tratamento de dados pessoais que passará a vigorar no dia 25 de Maio de 2018. O objetivo é otimizar a proteção de dados pessoais de cidadãos da União Europeia, bem como regulamentar as obrigações de organizações que coletam e processam dados pessoais. A nova diretriz se baseia em diversos requerimentos ligados à privacidade de dados e segurança da antiga DPD, porém também traz à mesa novas provisões visando consumar os direitos dos usuários e estipular duras sanções para eventuais violações.

A íntegra do texto sobre o GDPR pode ser encontrada **aqui** e um glossário de todos os termos legais que você precisa saber pode ser acessado **aqui**.

CENÁRIO ANTERIOR AO GDPR

GDPR tem sido pauta de diversas discussões nos últimos tempos, porém a regulação de privacidade e dados pessoais não é novidade. O novo diploma substitui a antiga Data Protection Directive ("DPD"), promulgada em 1995, que já determinava diretrizes a serem seguidas por empresas que lidam com tipos específicos de dados pessoais. Mesmo com a DPD sendo substituída pelo GDPR, foi a primeira regulação que definiu os oito princípios de proteção de dados que tem governado o tratamento de dados feito por empresas por mais de 20 anos. Uma vez que o GDPR aperfeiçoa e potencializa esses princípios, é importante obter uma compreensão sobre o novo diploma antes de implementá-lo, evitando erros e equívocos.

OBRIGAÇÕES SOB O GDPR

Enquanto a atual legislação da UE (DPD de 1995) governa entidades dentro da UE, o escopo territorial do GDPR é bem mais abrangente e será aplicável a organizações fora da UE nas seguintes condições:

a) qualquer organização que vende seus produtos para pessoa dentro da UE;

b) qualquer organização que monitora o comportamento de pessoas que vivem na UE. Em outras palavras, mesmo que você opere fora da UE, se você controla ou processa dados de cidadãos da UE o GDPR será aplicável a sua organização.

PASSOS PARA IMPLEMENTAÇÃO

Para que uma organização esteja operando de acordo com os princípios e diretrizes do GDPR, a implementação das regras do novo diploma europeu pode começar através de 8 passos:

1. A empresa que estará sujeita ao GDPR deve notificar e deixar claro para todos de sua organização que as regras do GDPR passarão a vigorar a partir do dia 25 de maio de 2018 e que devem ser integralmente observadas e respeitadas;

2. Todos os dados armazenados pela empresa devem ser documentados, bem como sua procedência e com quem tais dados são disponibilizados. Uma auditoria periódica de dados e processos é uma boa prática recomendável sob a tutela do GDPR;

3. As políticas de privacidade e de dados de uma empresa devem ser revistas, alterando-as de acordo com as diretrizes estipuladas pelo GDPR, não esquecendo de incluir as bases legais para o armazenamento e processamento dos dados utilizados;

4. Recomenda-se que a empresa revise todos seus processos e procedimentos internos, de modo que os direitos dos usuários, conforme estipulados pelo GDPR e elencados acima, possam ser exigidos e atendidos a qualquer momento, e no prazo estipulado, especialmente no que diz respeito ao Direito de Portabilidade e à investigação de eventuais vazamentos de dados;

5. Formalizar com sua base de usuários/clientes o consenso de que determinadas informações serão armazenadas, utilizadas ou até compartilhadas, de acordo com as diretrizes do GDPR e da legislação vigente;

6. Verificar a idade e data de nascimento de cada usuário, a fim de determinar se será necessário exigir autorização dos pais em relação ao uso de dados em geral, se o usuário for menor de idade;

7. Designar alguém para ocupar o cargo de Data Protection Officer, para que a implementação de diretrizes se faça de maneira organizada e independente das demais áreas da empresa;

8. Atualizar políticas, processos e procedimentos de acordo com demaisdiplomas normativos, visando o maior nível de segurança, controle e privacidade de dados possível.

PRINCIPAIS PONTOS DE ATENÇÃO

Dentre as várias diretrizes estipuladas pelo GDPR, existem algumas que valem ser discutidas mais a fundo. A regulação tem como objetivo proteger as informações dos usuários, porém tem como premissa que os usuários sempre agirão de boa-fé. Entendemos que seja importante reconhecer o atual efeito que fraudes e pessoas de má-fé tem na indústria de tecnologia, pagamentos e varejo, entre outras.

Um dos pontos trazidos pela regulamentação europeia é o "Right to Erasure"[3] ou "Right to be Forgotten"; Direito de Esquecimento, em Português. Em suma, o Direito

de Esquecimento garante ao usuário o direito de ser apagado de qualquer base de dados, mediante pedido encaminhado à empresa responsável e detentora dos dados. Partindo de uma premissa de que todos agirão de boa-fé, esse direito faz sentido e está de acordo com as expectativas razoáveis e desejáveis de privacidade de dados de usuários. Porém, atualmente diversas empresas, e pessoas, são prejudicadas através do uso ilegal de dados pessoais por pessoas agindo de má-fé, com o objetivo de realizarem fraudes e outros atos ilícitos.

Em uma pesquisa realizada em 2016 pela Consumer Card Fraud[4], com o apoio do Aite Group, foi verificado que o Brasil ocupa o 2º lugar do ranking mundial de fraudes envolvendo cartões de crédito, perdendo apenas para o México. De acordo com a pesquisa, aproximadamente 49% dos cidadãos brasileiros alegam terem sofrido com fraudes de cartão de crédito. Ou seja, quase metade da sociedade brasileira já foi prejudicada por fraudadores.

Se o Direito de Esquecimento fosse estendido e mantido em caráter absoluto, é possível, e provável, que o número de fraudes aumentem, pois mesmo que fosse possível identificar fraudadores e/ou ex-fraudadores, não seria permitido às empresas manter essa informação para proteger a si mesmo e seus clientes/usuários.

Deste modo, é interessante que o debate acerca da privacidade de dados e dos níveis de autonomia que o usuário pode ter sobre o armazenamento e utilização de seus dados seja feito de maneira abrangente, de modo que todos os principais atores contribuam com experiências reais e tangíveis de como dados podem ser utilizados e como remediar que pessoas de má-fé, tanto físicas quanto jurídicas, prejudiquem terceiros.

Benefícios e Implicações
No fim do dia, o GDPR serve para regular a privacidade e o tratamento de dados pessoais de cidadãos europeus. Assim, o beneficiário direto do GDPR são todos os cidadãos europeus, sejam naturais ou com dupla cidadania. Existem, porém outros beneficiários da regulação, e, ainda, aqueles que terão que lidar com as severas penas instituídas mediante descumprimento da regulação.

De acordo com o diploma europeu, multas serão majoradas pela autoridade supervisora, na medida do descumprimento, considerando as maneiras e vias pelas quais tal descumprimento se deu. Em determinados casos, a pena pode ser estipulada discricionariamente pela autoridade supervisora, em outros casos, o valor da multa é estipulado expressamente. Considerando as multas que já estão provisionadas na regulação, organizações podem sofrer sanções de 10.000.000,00 (dez milhões de euros) até 4% (quatro por cento)[5], aplicando-se o maior entre os dois valores.

A possibilidade de majoração de multas desta magnitude acaba por abalar a indústria de tecnologia e aquelas organizações que lidam com dados, estes valores podem acabar com um projeto, da noite para o dia. Por isso a importância de empresas que são sujeitas ao GDPR estarem de olhos bem abertos à regulação e suas disposições, bem como conscientes de suas obrigações perante as autoridades supervisoras competentes.

de privacidade de dados de usuários. Porém, atualmente diversas empresas, e pessoas, são prejudicadas através do uso ilegal de dados pessoais por pessoas agindo de má-fé, com o objetivo de realizarem fraudes e outros atos ilícitos.

Nota Legal: Esse conteúdo não é uma referência sobre privacidade de dados na EU, tampouco uma recomendação jurídica acerca de como observare cumprir normas legais, como o GDPR. Esta peça disponibiliza informações contextualizadas para auxiliar a compreensão do GDPR e como a IDwall aborda e entende os principais pontos legais dessa nova regulação. A informação legal apresentada não é, sob qualquer hipótese, aconselhamento ou recomendação legal. Nós insistimos que uma recomendação legal apropriada seja procurada, a fim de compreender com maior profundidade os aspectos e obrigações do GDPR e quais ações devemser tomadas para que uma empresa seja em observância às disposições do GDPR. Este artigo não deve, sob qualquer hipótese e de qualquer forma, ser considerado como recomendação e/ou opinião jurídica, tampouco como recomendação legal de qualquer natureza.

---

[1] https://gdpr-info.eu/
[2] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML
[3] https://gdpr-info.eu/art-17-gdpr/
[4] https://www.aciworldwide.com/-/media/files/collateral/trends/2016-global-consumer--card-fraud-where-card-fraud-is-coming-from.pdf
[5] https://gdpr-info.eu/art-83-gdpr/

Escrito por

João Mendes
Jurídico, IDwall

Design por

Lucas Torres
Marketing, IDwall

PARA CONHECER TODOS OS SERVIÇOS
DA IDWALL, ACESSE IDWALL.CO

Sobre a IDwall
A IDwall é uma empresa de segurança digital fundada em 2016 por Lincoln Ando e Raphael Melo. A ideia do negócio surgiu após os fundadores notarem a dificuldade de encontrar uma solução de segurança para o cadastro de funcionários, usuários e fornecedores.

A empresa foi uma das primeiras selecionadas no programa de residência do Google Campus e recebeu investimento de fundos como a 500 startups (venture capital internacional), da Canary (maior investidora semente do Brasil) e da Monashees+ (um dos principais fundos de investimentos em série A e B da américa latina).

No decorrer de sua trajetória, a IDwall já conseguiu grandes feitos, como ser selecionada para o programa Cybersecurity Tel Aviv do Google Exchange, o prêmio de maior inovação do evento Pagamento.me, estar entre as Top 100 RegTech do mundo de acordo com a Global RegTech e foi selecionada entre as Top 10 RegTech mais inovadoras do mundo pela Banking CIO Outlook. Hoje, a IDwall conta com clientes como bancos, fintechs, fundos de investimento, traders de bitcoins, transportadoras e outras empresas.