GDPR

General Data Protection Regulation

Considerações iniciais

Prof. Ms. Edison Fontes, CISM, CISA, CRISC

Controles básicos de informação exigidos para a conformidade com o Regulamento (UL) 2016/679 do Parlamento Europeu e Conselho.

DOC ELGF.0100.01.0

São Paulo, abril, 2018 - Brasil

Licença para uso deste documento

Este documento

Este documento tem por objetivo descrever de maneira objetiva e simples os principais controles que uma organização precisa implementar e garantir o seu funcionamento para estar em conformidade com o Regulamento Europeu de Tratamento de Dados.

Este documento expõe a opinião pessoal do autor, considerando as informações disponíveis neste momento.

Este documento não é suficiente para a implementação dos controles do GDPR. Para a implementação destes controles o leitor deve ler por completo o Regulamento (UL) 2016/679 do Parlamento Europeu e Conselho.

Técnica e muito cuidado foram utilizados na elaboração deste documento. Porém erros podem acontecer, tipo digitação ou reprodução. Qualquer erro encontrado, qualquer dúvida de interpretação, solicitamos que seja enviada uma mensagem para edison@pobox.com para a devida verificação e resposta. O autor não assume qualquer responsabilidade por eventuais danos ou perdas a pessoas, organizações ou bens originados do uso deste documento. Este documento é conceitual e didático sobre os temas apresentados.

O Autor

Edison Fontes é Mestre em Tecnologia, certificado internacional CISA, CISM, CRISC e profissional de segurança da informação. É professor de MBAs, autor de livros e desenvolve atividades de Estrategista, Gestor, Consultor em Segurança Informação, Continuidade de Negócio, Risco Operacional, Conformidade *(Compliance)* da Informação e Combate à Fraude de Informação.

É sócio consultor da Núcleo Consultoria em Segurança

Contato: edison@pobox.com, ef@nucleoconsult.com.br

O Regulamento Geral de Proteção de Dados com validade a partir de 25 de maio de 2018 é um marco no tratamento da informação e impactará, de imediato ou em curto prazo, todas as organizações que utilizam a tecnologia da informação, inclusive as brasileiras.

INTRODUÇÃO

Apesar de ser uma legislação da União Europeia, este regulamento apresenta características que afetam um universo maior. Este assunto merece um tempo e um texto longo, além do que várias horas de debates. Para facilitar, apresento neste documento as principais diretrizes que você como executivo de uma organização (CEO, CFO, CIO, CISO) precisa conhecer e avaliar como a sua organização está tratando este tema.

O impacto do GDPR pode ser comparado com a Lei Sarbanes-Oxley dos USA, que afetou empresas de vários países. Muitas empresas querem negociar com os USA e para tanto devem estar adequadas á esta lei. Tem executivos brasileiros (e de outros países) que não podem passear nos USA sob pena de serem detidos.

As definições que descrevo neste documento estão baseadas no Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, que possui cerca de noventa páginas. Porém, apresento as mesmas de uma maneira mais simples baseado na minha experiência profissional e no estudo do assunto.

Direcionador dos controles

O primeiro entendimento que devemos ter do GDPR é que o principal direcionador desta legislação é o tratamento de dados pessoais de pessoas singulares. Isto é: o foco é a informação de dados pessoais.

Dado Pessoal
é uma informação ou um conjunto de informação que se refere a uma pessoa singular.

Foto: unsplash.com, sem reservas

Pessoa Singular
é uma pessoa que possa ser especificada, diretamente ou indiretamente, por um identificador (nome, CPF, localização, preferências).

Principais Características

Descrevo abaixo, neste primeiro texto, uma abordagem estruturada para as principais características deste regulamento: Também consolido alguns controles que entendo que facilita o entendimento. Por consequência, este meu artigo não deve substituir a leitura completa de todo o regulamento.

1. Aplicação: empresas de qualquer nacionalidade

O GDPR aplica-se a empresas de qualquer nacionalidade que satisfaçam qualquer uma das situações abaixo.

a. Empresas com matriz, filial ou representação física na União Europeia.

b. Empresas sem representação física na União Europeia, mas ofereça produtos ao mercado europeu.

c. Empresas que coletam dados de pessoas singulares localizadas na União Europeia.

d. Empresas que monitoram dados de pessoas singulares localizadas na União Europeia.

e. Empresas que terceirizam o processamento de dados para empresas localizadas na União Europeia.

Note que as empresas podem ser qualquer nacionalidade e os dados de pessoas singulares se referem a pessoas localizadas na União Europeia, não necessariamente cidadãos europeus.

Esta abrangência exige que muitas empresas brasileiras, dos mais variados portes e tipos de negócio devam, se adaptar a este regulamento para o caso de desejar fazer negócio com o mercado europeu. E quem não quer vender ou prestar serviço para os países da União Europeia.

Os dados pessoais de pessoas singulares que estão na União Europeia exigem um tratamento rigoroso em relação ao sigilo, uso, transferência ou qualquer outro tratamento, por qualquer empresa de qualquer país do mundo que queira realizar negócios com a União Europeia.

(Foto: unsplash.com, sem reservas)

2. Consentimento obrigatório

O regulamento declara explicitamente que qualquer dado pessoal para ser coletado e utilizado precisa ter formalmente o consentimento da pessoa singular. Simples assim. “Vai coletar meus dados? Tem que me pedir!”

Para aquelas empresas que possuem dados pessoais e não realizou este pedido de consentimento, deverão corrigir esta situação. A partir da data de validade do regulamento, estarão em não conformidade com a legislação da União Europeia.

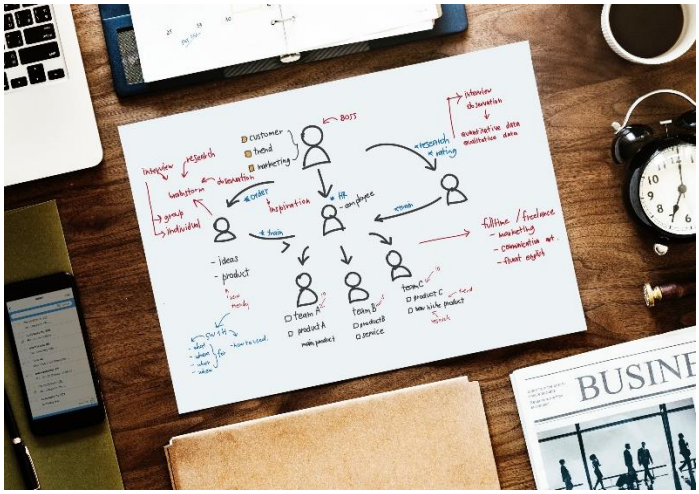
3. Uso com finalidade específica

A coleta de dado pessoal obrigatoriamente tem que indicar qual será o uso que a empresa fará com esta informação. Não se pode coletar dados pessoais para futuros usos. É obrigatório que o objetivo da coleta dos dados seja explicitado. Evidentemente o uso dos dados somente pode acontecer para o objetivo pré-definido. A informação coletada tem endereço certo.

(Foto: unsplash.com, sem reservas)

4. A Coleta deve ser mínima

A coleta dos dados pessoais deve conter exclusivamente os dados necessários para atender a finalidade específica. Sem enrolação. No Brasil muitas empresas coletam dados para lhe comunicar do resultado do sorteio, porém, você tem que responder um questionário financeiro social e de comportamento.



(Foto: unsplash.com, sem reservas)

5. Estruturação dos Dados Pessoais

Os dados pessoais devem ter uma estruturação técnica de maneira a facilitar a sua proteção e sua rastreabilidade. Quem trabalha com tecnologia da informação conhece muito bem como os sistemas aplicativos e como as bases de dados ao longo do tempo se transformam. Este controle facilita o controle seguinte.

6. Mapeamento dos dados pessoais

A empresa deve ter mapeado o fluxo de existência dos dados pessoais.

Foram coletados numa ficha de papel na entrada de um hotel (exemplo), ou foram coletadas pelo site de Internet? Depois foram armazenados? Existem cópias de segurança? Os dados pessoais são fornecidos ou vendidos para parceiros? Enfim, é necessário indicar onde e o que acontece com os dados pessoais. É necessário monitorar, gerenciar e controlar o fluxo dos dados pessoais.

(Foto: unsplash.com, sem reservas)

7. Responsabilização solidária

Ao interagir com parceiros, fornecendo ou recebendo, dados pessoais a empresa será solidária na responsabilização sobre a coleta e uso de dados pessoais. Isto é, não adianta terceirizar o trabalho sujo. Sua empresa será responsabilizada se não foi dado o tratamento adequado exigido pelo regulamento europeu.

8. Uso de técnicas de criptografia e similar

É aconselhável demostrar que a empresa trada de maneira adequada a privacidade dos dados pessoais, na medida em que arquivos ou transmissões de dados pessoais utilizam técnicas de criptografia ou similar para aumentar a segurança do sigilo e acesso aos dados pessoais.
Armazenar em um pen driver dados pessoais de clientes e funcionários sem criptografia demonstra uma falta de proteção adequada.

(Foto: unsplash.com, sem reservas)

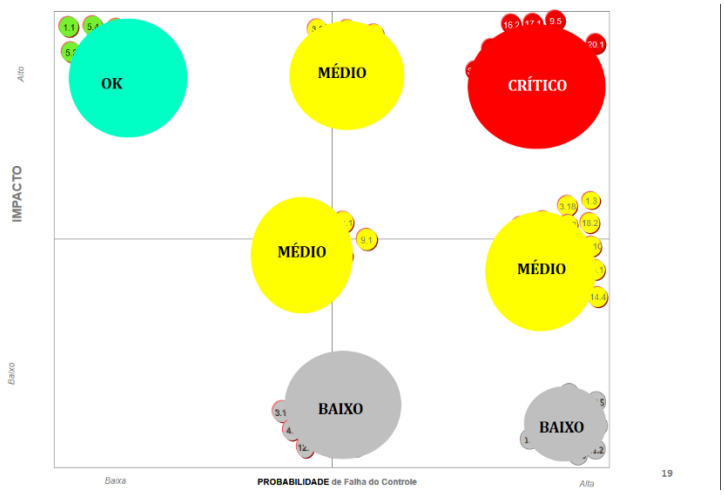
9. Data Protection Officer

A empresa deve ter um profissional para exercer as funções de Oficial de Proteção de Dados que tem a principal missão, garantir que a empresa segue ou estar a seguir as regras do regulamento. Ele fará a gestão de risco de dados pessoais e será o responsável pelo monitoramento e tratamento dos dados pessoais nestas empresas.

Este profissional responde pessoalmente e sua função, posição hierárquica não devem ter conflito de interesse. Para empresas maiores será um profissional dedicado. Empresas menores podem ter profissionais parciais. Todas devem ter uma solução adequada ao seu porte, tipo de negócio e que havendo uma auditoria, a solução seja razoavelmente aceita.

10. Data Protection Impact Assessment

A empresa deve ter no seu conjunto de Controles Corporativos, a Avaliação de Impacto na Proteção de Dados Pessoais. Este mapeamento deve ser apresentado para o corpo diretivo da organização para que os executivos tomem conhecimento dos possíveis impactos para a empresa, em função de vulnerabilidades e tratamento não adequado dos dados pessoais.



(Fonte: Autor, Avaliação de Impacto)

11. Comunicação de incidentes de dados

A empresa é obrigada a comunicar ao mercado e a autoridade europeia, a ocorrência de qualquer incidente que comprometa o sigilo e uso adequado dos dados pessoais. Entendo que começaremos a conhecer situações de perda, roubo ou vazamento de dados em empresas brasileiras.

(Foto: unsplash.com, sem reservas)

12. Penalidades

As multas deste regulamento são pesadas. Afinal o bolso é o órgão mais sensível dos gestores, conselhos de administração e acionistas. Podem chegar a vinte milhões de euros ou até 4% do faturamento bruto do ano anterior.

(Foto: unsplash.com, sem reservas)

13. Política de Dados Pessoais

Considerando a importância da proteção de dados pessoais, é recomendável que a empresa possua uma política específica para este tema. Este documento deve ser assinado pela presidência da empresa ou aprovado pelo conselho de administração.

(Foto: unsplash.com, sem reservas)

14. Direito ao esquecimento

É o direito que a pessoa singular tem para solicitar que seus dados sejam apagados, quando não forem relevantes para as motivações que coletaram estes dados inicialmente. Porém é definido que o interesse público na disponibilidade dos dados deverá ser considerado para o atendimento destas solicitações. Entendo que a praticabilidade desta questão irá depender muito de algumas leis específicas de cada país. Entendo que à princípio esta regra possui alguns controles que precisam ser melhores definidos e especificados.

Ao consultar buscadores estes dados não apareceriam.

(Foto: unsplash.com, sem reservas)

15. Circulação de dados europeus

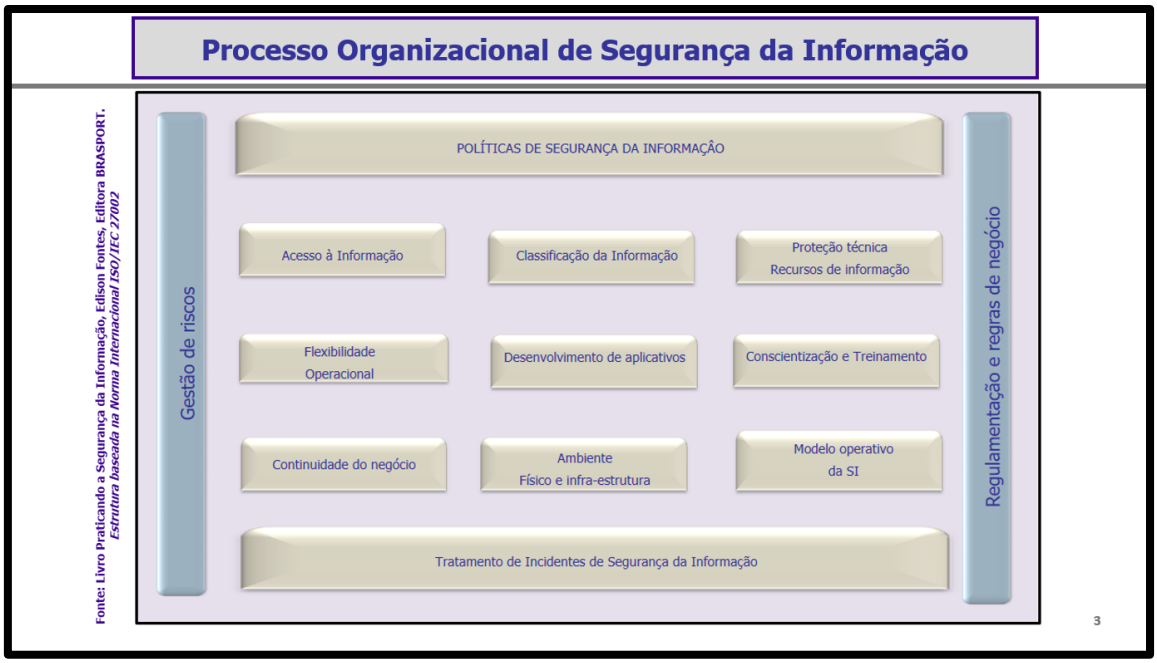
Qualquer transferência de dados pessoais para um outro país ou uma organização internacional deve seguir as regras do GDPR. Todos os controles definidos devem ser cumpridos de maneira a assegurar os dados das pessoas singulares.

Isto é, qualquer organização que queira transacionar dados que se refiram a pessoas singulares que estejam na União Europeia, deverá seguir todas as regras descritas no regulamento GDPR.

PROCESSO ORGANIZACIONAL DE SEGURANÇA DA INFORMAÇÃO

O Processo Organizacional de Segurança da Informação define em suas dimensões, macrocontroles que possibilitam que os requisitos exigidos pelo GDPR sejam considerados.

Segue abaixo a estrutura do Processo Organizacional de Segurança da Informação, baseado na Norma ISO/IEC 27002:2013, apresentando as suas dimensões.



Fonte: Livro Praticando a Segurança da Informação, Edison Fontes, Editora BRASPORT.
Estrutura baseada na Norma Internacional ISO/IEC 27002

Segue abaixo um quadro controle indicando os requisitos do GDPR e as Dimensões de Segurança da Informação que devem ter controles definidos para atendimento específicos destes requisitos.

	CONTROLES DE SEGURANÇA DA INFORMAÇÃO NECESSÁRIOS PARA ATENDER														
REQUISITOS GDPR ⬇	**Política de S.I.**	**Acesso Informação**	**Classificação Informação**	**Proteção Técnica**	**Flexibilidade Operacional**	**Desenvolv. Aplicativos**	**Continuidade Negócio**	**Cópias de Segurança**	**Gestão de Riscos S.I.**	**Email, Rede Social, Internet, computador, celular**	**Treinamento em S.I.**	**Ambiente Físico**	**Modelo Operativo S.I.**	**Criptografia**	**Prestadores serviço / Parceiros**
1. Aplicação: empresas de qualquer nacionalidade	X		X												
2. Consentimento obrigatório		X	X			X	X								
3. Uso com finalidade específica	X	X		X		X	X								
4. A Coleta deve ser mínima	X	X		X		X									
5. Estruturação dos dados pessoais		X		X		X									
6. Mapeamento dos dados pessoais		X		X		X									
7. Responsabilização solidária	X							X							X
8. Uso de técnicas de criptgrafia e similar														X	
9. Data Protection Officer	X			X									X		
10. Data Protection Impact Assessment							X		X						
11. Comunicação de incidentes de dados					X		X								
12. Penalidades									X						
13. Política de Dados Pessoais	X	X	X							X	X	X			
14. Direito ao esquecimento	X					X	X								
15. Cirdulação de Dados Europeus												X			X

Fonte: Autor.

O quadro acima demonstra que a existência de um efetivo Processo Organizacional de Segurança da Informação e a situação de negócio de que a empresa deve seguir o GDPR, possibilita de uma maneira estruturada a implementação dos controles necessários.

O Processo Organizacional de Segurança da Informação facilita o atendimento aos diversos controles exigidos pelo GDPR. Não só facilita como são obrigatórios para uma adequada proteção dos dados pessoais.

O Processo Organizacional de Segurança da Informação é a base para que a empresa tenha condições de cumprir os controles definidos pelo GDPR.

Sem Segurança da Informação não existe cumprimento do GDPR

O Processo Organizacional de Segurança da Informação é a base para que a empresa tenha condições de cumprir os controles definidos pelo GDPR.

Sem Segurança da Informação não existe o cumprimento do GDPR

CONCLUSÃO

O Brasil ainda não possui uma legislação do tipo GDPR, porém, está em andamento (será?) no Congresso Nacional um projeto de legislação de Proteção de Dados Pessoais, inspirado no GDPR. Será um grande avanço para o país e para a nossa ordem jurídica. Porém, pensando no mercado, no negócio das nossas organizações que vendem produtos e realizam serviços para todos os países, seguir o GDPR é uma decisão estratégica de negócio.

Se a sua organização, eventualmente, não tenha controles adequados para atender o GDPR, minha sugestão é que ela deve se programar e definir etapas. Porém, a primeira etapa é implementar ou aprimorar o Processo organizacional de Segurança da Informação.

Edison Fontes, CISM, CISA, CRISC

Sócio Núcleo Consultoria
Estrategista, Consultor e Gestor: Segurança da Informação, Riscos, Continuidade e Combate à Fraude, Compliance.
Coordenador do Comitê de Segurança da Informação da ABSEG.

edison@pobox.com
ef@nucleoconsult.com.br

www.nucleoconsult.com.br