DANIEL FRANCISCO • SANDRA FRANCISCO

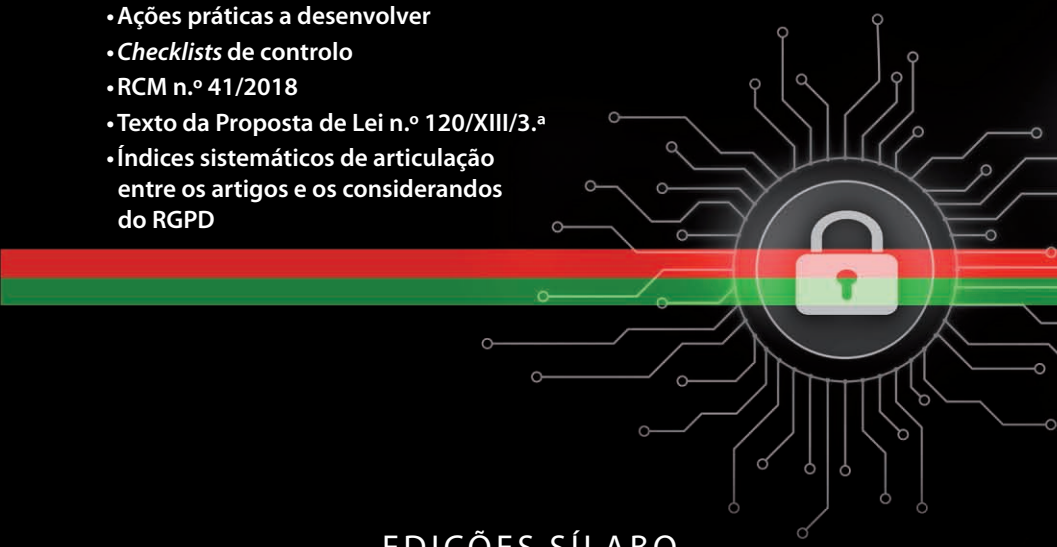
RGPD

Regulamento Geral de Proteção de Dados

7 passos para uma metodologia de implementação do RGPD na Administração Pública

Contém:

- Ações práticas a desenvolver
- *Checklists* de controlo
- RCM n.º 41/2018
- Texto da Proposta de Lei n.º 120/XIII/3.ª
- Índices sistemáticos de articulação entre os artigos e os considerandos do RGPD



EDIÇÕES SÍLABO

«Os dados são o novo petróleo. É valioso, mas se não refinado, não pode ser usado de forma direta (...) Assim, os dados devem ser divididos, analisados para ter valor»

Clive Humby, Matemático, 2006

«Ao reunir dados e poder de computação suficientes, empresas e governos poderão criar rapidamente algoritmos que me conhecem melhor do que eu próprio.»

Yuval Harari, entrevista publicada
no *Diário Noticias* em 27/05/2017

Regulamento Geral de Proteção de Dados

7 passos para uma metodologia de implementação do RGPD na Administração Pública

Contém a Resolução do Conselho de Ministros nº 41/2018
e o Texto da Proposta de Lei nº 120/XIII/3ª
aprovada na Assembleia da República em 14/06/2019

Daniel Francisco
Sandra Francisco

EDIÇÕES SÍLABO

Visite a Sílabo na rede
www.silabo.pt

FICHA TÉCNICA

Título: Regulamento Geral de Proteção de Dados – 7 passos para uma metodologia de implementação do RGPD na Administração Pública
Autores: Sandra Francisco, Daniel Francisco
© Edições Sílabo, Lda.
Capa: Pedro Mota
Imagem da capa: Alexandersikov | Dreamstime.com
1ª Edição – Lisboa, julho de 2019.

Impressão e acabamentos: ARTIPOL – Artes Tipográficas, Lda.
Depósito Legal: 458359/19
ISBN: 978-989-561-014-3

EDIÇÕES SÍLABO, Lda.
Publicamos conhecimento

Editor: Manuel Robalo

R. Cidade de Manchester, 2
1170-100 Lisboa
Tel.: 218130345
e-mail: silabo@silabo.pt
www.silabo.pt

Índice

Parte 2

Aspetos essenciais para a implementação do RGPD na Administração Pública

Parte 3

Da Implementação – Os 7 passos para Implementação do RGPD na Administração Pública

Parte 4

Considerações finais

Lista de abreviaturas e acrónimos

AIPD	Avaliação de Impacto de Proteção de Dados
AP	Administração Pública
BCR	*Binding Corporate Rules* criadas pelo GT 29
BPM	*Business Process Management*
BPMN	*Business Process Management Notation*
CE	Comunidade Europeia
CNPD	Comissão Nacional de Proteção de Dados
CRP	Constituição da República Portuguesa
EEE	Espaço Económico Europeu
EPD	Encarregado de Proteção de Dados
GAFAN	Google, Amazon, Facebook, Apple e Netflix
GT 29	Grupo trabalho do artº 29º da Diretiva 95/46/CE
IP	Protocolo Internet
ISO	*International Organization for Standardization*
NIF	Número de Identificação Fiscal
NISS	Número de Identificação da Segurança Social
PCM	Presidência do Conselho de Ministros
PIPEDA	Lei de Proteção de Informações Pessoais e Documentos Eletrónicos do Canadá
RCM	Resolução do Conselho de Ministros
RGPD	Regulamento Geral de Proteção de Dados
TI	Tecnologias de Informação

Nota prévia

Com a entrada em vigor com caráter obrigatório a 25 de maio de 2018 do Regulamento Geral de Proteção de Dados (RGPD) – Regulamento UE 2016/679, de 27 de abril de 2016, as Entidades Públicas e Privadas dos 28 Estados membros que compõem a União Europeia, tem necessariamente de se adaptar e reformular os seus procedimentos com vista a uma correta aplicação do RGPD.

O Regulamento Geral de Proteção de Dados, de aplicação obrigatória para todos os órgãos e serviços da Administração Pública, exige um elevado investimento na análise e revisão de todos os processos que tratam dados pessoais, com vista a garantir a sua conformidade.

Contudo, e no caso português, a realidade e especificidades da Administração Pública e das suas Entidades, não tem sido contemplada nas abordagens que se têm realizado.

Sendo que mesmo quando se procura essa abordagem a tendência é bipolarizar a análise, no sentido de ser eminentemente jurídica ou então eminentemente tecnológica.

Este livro é concebido para ser um manual breve que sistematiza o processo de implementação por passos, sequencia as ações a desenvolver e os resultados esperados, numa abordagem instrumental e procedimental que favorece a aplicação imediata do conhecimento.

Neste livro pretendemos sistematizar e identificar uma metodologia que permita operacionalizar e acompanhar as etapas necessárias à implementação do RGPD no universo concreto e específico da Administração Pública, tendo já por referência as especificidades técnicas das apontadas na RCM nº 41/2018 de 28 de março, que define as orientações técnicas para a Administração Pública em matéria de arquitetura de segurança das redes e sistemas de informação relativos a dados pessoais.

Igualmente já se tem por referência a proposta de Lei nº 120/XIII/3ª, aprovada no dia 14/06/2019 na Assembleia da República. Lei que assegura a execução do RGPD na ordem jurídica nacional (que disponibilizamos no Anexo II).

É destinado primeiramente a quem já tenha algum conhecimento do RGPD e a todos os que participam na sua implementação, mas também é destinado a todos os trabalhadores que tratam dados pessoais no seu exercício profissional. Muito em especial aos Dirigentes, aos Encarregados de Proteção de Dados, aos Trabalhadores que integram as equipas de implementação e aos que colaboram com essas equipas ao nível da análise dos processos das suas Unidades Orgânicas.

Ou simplesmente para quem relacionando-se com a Administração Pública (Cidadão ou Empresa) busca orientações, medidas técnicas, organizativas e de segurança necessárias, para uma correta aplicação do RGPD.

Apresentamos e sistematizamos algumas noções gerais e regras que se deve ter especialmente presentes antes de iniciar o estudo do processo de implementação.

Pretende-se que este manual e metodologia sirva para:

- Facilitar os processos de implementação do RGPD.
- Promover o conhecimento generalizado das exigências do processo de implementação do RGPD.

- O reconhecimento do impacto e investimento que se espera de cada organização quando implementa o RGPD.
- A perceção da necessidade de investir na constituição e formação das equipas de implementação.
- Contribuir para a integração, no funcionamento e cultura organizacional da Administração Pública, da conformidade com o RGPD.
- Implementar a RCM nº 41/2018 de 28 de março.
- Ou simplesmente apresentar orientações, medidas técnicas, organizativas e de segurança necessárias, para uma correta aplicação do RGPD e legislação de execução nacional nas Entidades Publicas.

Para a melhor compreensão estruturamos o livro em **cinco partes**:

- Uma **introdução** – Onde fazemos uma breve viagem pelo contexto da proteção de dados e a sua evolução até ao atual Regulamento.
- Uma **primeira parte** – com as definições base subjacentes e essenciais ao entendimento do RGPD e em que no final se colocam perguntas e um exercício para consolidação de conhecimentos.
- Uma **segunda parte** – com os aspetos essenciais para o planeamento e implementação do RGPD na Administração Pública. No final colocam-se perguntas para consolidação de conhecimentos e um espaço de documentação com uma ficha onde se resumem e autonomizam os principais tópicos a reter.

- Uma **terceira parte** – Onde se apresenta uma metodologia prática e orientada para a ação, que visa percorrer o processo de implementação do RGPD no contexto da Administração Pública, em 7 passos, etapa a etapa, através de:
  - — Explicação e contexto da etapa.
  - — Orientações práticas.
  - — Um espaço de documentação com:
    - – Fichas, com uma sistematização das entradas, das ações, dos entregáveis e uma lista de verificação de conclusão da etapa;
    - – Modelos, para adaptação aos processos de implementação dos órgãos e serviços.
- Uma **quarta parte** – com as considerações finais reforçando a constante necessidade de melhoria continua e de acompanhamento dos desenvolvimentos legislativos normativos e deliberativos nacionais e europeus, bem como alguns conselhos de boas práticas de privacidade e segurança para as Entidades Públicas.

Pretendendo-se assim que, com esta metodologia de implementação em 7 passos, que a Administração Pública possa em 1ª linha, salvaguardar os direitos dos titulares dos dados e por outro lado assegurar conformidade com o RGPD a que está obrigada.

Introdução

Breve enquadramento geral e legal do Regulamento UE 2016/679

O Regulamento Geral de Proteção de Dados (RGPD ou, em Inglês, GDPR) é um Regulamento Europeu (UE 2016/679), aprovado pelo Parlamento Europeu e Conselho, de 27 de abril de 2016, com aplicação direta em todos os 28 Estados Membros da União Europeia (UE).

Estabelece as regras referentes à proteção, tratamento e livre circulação de dados pessoais das pessoas singulares, que se encontrem na União Europeia, visando garantir uma aplicação uniforme de algumas dessas regras em toda a União Europeia.

Salienta-se que as regras referentes à proteção, tratamento e livre circulação de dados pessoais, das pessoas singulares, apenas se circunscrevem a pessoas vivas, uma vez que o considerando 27, refere explicitamente que «O presente regulamento não se aplica aos dados pessoais de pessoas falecidas. Os Estados-Membros poderão estabelecer regras para o tratamento dos dados pessoais de pessoas falecidas.»

Foi o que sucedeu com o Estado Português, que na lei nacional de execução do RGPD, aprovada em 14/06/2019 refere no nº 1 do Artigo 17º (Proteção de dados pessoais de pessoas falecidas), que os dados de pessoas falecidas que sejam da

categoria de dados «especiais» do nº 1 do artigo 9º do RGPD, se encontram «protegidos nos termos do RGPD».[1]

Contrariamente às Diretivas, designadamente a anterior Diretiva 95/46/CE, do Parlamento Europeu e do Conselho, datada de 23/11/1995, por ser um Regulamento, é um ato legislativo da UE que não carece de transposição, ou seja da publicação de legislação interna para poder ter imediata aplicação no Ordenamento Jurídico de cada Estado Membro.

Foi publicado no Jornal Oficial da União Europeia L 119/1, de 04/05/2016, mas em maio de 2018 sofreu uma alteração importante relacionada com especial incidência o âmbito de aplicação geográfico (artº 3º), cuja publicação ocorreu a 23 de maio de 2018.

O RGPD entrou em vigor no dia 24/05/2016, no entanto, e de acordo com o seu artº 99º, só se tornou de aplicação obrigatória em todos os Estados-Membros a partir do dia 25/05/2018, tendo assim, existido dois anos para a adaptação das organizações.

---

(1) Artigo 17º – Proteção de dados pessoais de pessoas falecidas

1. Os dados pessoais de pessoas falecidas são protegidos nos termos do RGPD e da presente lei quando se integrem nas categorias especiais de dados pessoais a que se refere o nº 1 do artigo 9º do RGPD, ou quando se reportem à intimidade da vida privada, à imagem ou aos dados relativos às comunicações, ressalvados os casos previstos no nº 2 do mesmo artigo.
2. Os direitos previstos no RGPD relativos a dados pessoais de pessoas falecidas, abrangidos pelo número anterior, nomeadamente os direitos de acesso, retificação e apagamento, são exercidos por quem a pessoa falecida haja designado para o efeito ou, na sua falta, pelos respetivos herdeiros.
3. Os titulares dos dados podem igualmente, nos termos legais aplicáveis, deixar determinada a impossibilidade de exercício dos direitos referidos no número anterior após a sua morte.

DANIEL FRANCISCO. Doutor em Comunicação Empresarial e Institucional (Universid Complutense de Madrid), mestre em Comunicação (Universidade Autónoma de Lisboa), licenciado em Estatística e Gestão de Informação (Universidade Nova/*Information Managment School* – ISEGI), bacharel em Gestão de Empresas (Escola Superior de Gestão de Santarém – Instituto Politécnico de Santarém). Mais de 20 anos como formador e consultor nas áreas de gestão, novas tecnologias e reengenharia de processos, a nível nacional e internacional (banca, petróleos, saúde e administração pública). Formador e especialista em RGPD para entidades privadas e para a Administração Pública central, local e regional em várias entidades como, entre outras, o INA, IGAP e o CEFAPA *(advisory*, *compliance* e implementação). Investigador, docente no Instituto Politécnico de Bragança. Autor e conferencista nacional e internacional.

SANDRA FRANCISCO. Inspetora-Jurista da carreira superior de inspeção, dirigente na Administração Pública Central e Local, docente universitária convidada, exerceu advocacia por cerca de oito anos, licenciada em Direito e com várias pós graduações pela Faculdade de Direito da Universidade de Lisboa e pós-graduada e mestranda na área de Administração e Politicas Públicas pelo ISCTE-IUL; Formadora certificada em várias áreas de Direito (Administrativo, Fiscal, Laboral e Legística), Recursos Humanos e Auditoria, ministrando ações de formação e diplomas de especialização para a Administração Pública, central, local e regional, há mais de 20 anos. Autora de diversas publicações, participou em inúmeras conferências, em particular nos congressos do INA, seminários e colóquios nacionais e internacionais.

As Entidades Públicas defrontam-se hoje com vários desafios, em especial o de implementarem e garantirem a conformidade com o Regulamento Geral de Proteção de Dados (RGPD), realidade que exige um elevado investimento na análise e revisão de todos os processos e tratamento de dados pessoais.

No mercado editorial português e outra documentação publicada, a implementação e manutenção de sistemas RGPD centrados nas especificidades da Administração Pública e suas Entidades tem sido ignorada.

Este livro, suprindo esta lacuna, foca-se nas necessidades e especificidades da Administração Pública central, local e regional em matéria de RGPD, tendo sido concebido para ser um guia de consulta rápida, breve e prático, e que sistematiza o processo de implementação do sistema RGDP em sete passos.

A metodologia apresentada contempla exercícios e ações práticas a desenvolver, como entradas, resultados a obter e listas de verificação e controlo, numa abordagem instrumental e procedimental que facilita a aplicação imediata do RGPD, das normas técnicas da RCM n.º 41/2018 e da legislação nacional de execução do RGPD, já aprovada na Assembleia da República.

ISBN 978-989-561-014-3
624
9 789895 610143