CNPD
Comissão Nacional
de Proteção de Dados

ORDEM DOS ADVOGADOS
CONSELHO REGIONAL DE LISBOA

Q&A

ciclo de conferências

REGULAMENTO GERAL de PROTEÇÃO DE DADOS

ciclo de conferências

REGULAMENTO GERAL DE PROTEÇÃO DE DADOS

VEJA NO **YOUTUBE**

YouTube

DIPLOMAS*

LEGISLAÇÃO EUROPEIA

DIRETIVAS

JOUE, L 201/37, DE 31 DE JULHO DE 2002

Directiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas)

https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:02002L0058-20091219&from=EN

COMUNICAÇÕES E INFORMAÇÕES

JOUE, C 326/391, DE 26 DE OUTUBRO DE 2012

Carta dos Direitos Fundamentais da União Europeia

https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=uriserv%3AOJ.C_.2012.326.01.0391.01.POR&toc=OJ%3AC%3A2012%3A326%3ATOC

REGULAMENTOS

JOUE, L 119/1, DE 4 DE MAIO DE 2016

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (Texto relevante para efeitos do EEE)

https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN

* A presente compilação resulta de uma seleção concebida pelo CRL, a qual não pretende ser exaustiva e não prescinde a consulta destes e de outros textos legais publicados em Diário da República, disponíveis em https://dre.pt/.

DIRETIVAS

JOUE, L 119/89, DE 4 DE MAIO DE 2016

Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho

https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:02016L0680-20160504&from=EN

DIRETIVAS

JOUE, L 119/132, DE 4 DE MAIO DE 2016

Diretiva (UE) 2016/681 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à utilização dos dados dos registos de identificação dos passageiros (PNR) para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave

https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0132.01.POR

DIRETIVAS

JOUE, L 194/1, DE 19 DE JULHO DE 2016

Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União

https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L1148

REGULAMENTOS

JOUE, L 295/39, DE 21 DE NOVEMBRO DE 2018

Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE (Texto relevante para efeitos do EEE.)

https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32018R1725

COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU E AO CONSELHO

COM(2020) 264 final, 24 de junho de 2020

A proteção de dados enquanto pilar da capacitação dos cidadãos e a abordagem da UE para a transição digital – dois anos de aplicação do Regulamento Geral sobre a Proteção de Dados

https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52020DC0264

DECISÕES

JOUE, L 199/18, DE 7 DE JUNHO DE 2021

Decisão de Execução (UE) 2021/915 da Comissão de 4 de junho de 2021 relativa às cláusulas contratuais-tipo entre os responsáveis pelo tratamento de dados pessoais e os subcontratantes nos termos do artigo 28.º, n.º 7, do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho e do artigo 29.º, n.º 7, do Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho (Texto relevante para efeitos do EEE)

https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32021D0915

LEGISLAÇÃO NACIONAL

DECRETO-LEI N.º 122/2000

Diário da República n.º 152/2000, Série I-A de 2000-07-04

Ministério da Cultura

Transpõe para a ordem jurídica interna a Directiva n.º 96/9/CE, do Parlamento Europeu e do Conselho, de 11 de Março, relativa à protecção jurídica das bases de dados

https://dre.pt/web/guest/legislacao-consolidada/-/lc/124444219/view?p_p_state=maximized

LEI N.º 41/2004

Diário da República n.º 194/2004, Série I-A de 2004-08-18

Assembleia da República

Transpõe para a ordem jurídica nacional a Directiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de Julho, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas

https://dre.pt/web/guest/pesquisa/-/search/480710/details/normal?p_p_auth=nBCSqsA0

Leitura aconselhada:

Lei n.º 46/2012, publicada em Diário da República n.º 167/2012, Série I de 2012-08-29, disponível em:

https://dre.pt/web/guest/pesquisa/-/search/174793/details/normal?p_p_auth=6G3CfkyO

LEI N.º 43/2004

Diário da República n.º 194/2004, Série I-A de 2004-08-18

Assembleia da República

Lei de organização e funcionamento da Comissão Nacional de Protecção de Dados

https://dre.pt/web/guest/legislacao-consolidada/-/lc/122101697/view?q=Lei+43%2F2004?q=Lei+43%2F2004

Leitura aconselhada:

Regulamento n.º 310/2020, publicado em Diário da República n.º 64/2020, Série II de 2020-03-31, disponível em:

https://dre.pt/home/-/dre/130887195/details/maximized

LEI N.º 26/2016

Diário da República n.º 160/2016, Série I de 2016-08-22

Assembleia da República

Aprova o regime de acesso à informação administrativa e ambiental e de reutilização dos documentos administrativos

https://dre.pt/web/guest/legislacao-consolidada/-/lc/106603618/view?p_p_state=maximized

LEI N.º 46/2018

Diário da República n.º 155/2018, Série I de 2018-08-13

Assembleia da República

Estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União

https://dre.pt/web/guest/pesquisa/-/search/116029384/details/normal?p_p_auth=WGrssS4h

LEI N.º 58/2019

Diário da República n.º 151/2019, Série I de 2019-08-08

Assembleia da República

Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados

https://dre.pt/web/guest/pesquisa/-/search/123815982/details/normal?p_p_auth=nBCSqsA0

LEI N.º 59/2019

Diário da República n.º 151/2019, Série I de 2019-08-08

Assembleia da República

Aprova as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, transpondo a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016

https://dre.pt/home/-/dre/123815983/details/maximized

DECRETO-LEI N.º 93/2020

Diário da República n.º 214/2020, Série I de 2020-11-03

Presidência do Conselho de Ministros

Estabelece regras de segurança aplicáveis a navios de passageiros e regras de tratamento de dados das pessoas que neles viajam e cria um sistema de inspeções relativo a outras embarcações, transpondo a Diretiva (UE) 2017/2108, a Diretiva (UE) 2017/2109 e a Diretiva (UE) 2017/2110

https://dre.pt/web/guest/pesquisa/-/search/147432950/details/normal?p_p_auth=D7YOmJmB

LEI N.º 27/2021

Diário da República n.º 95/2021, Série I de 2021-05-17

Assembleia da República

Carta Portuguesa de Direitos Humanos na Era Digital

https://dre.pt/web/guest/legislacao-consolidada/-/lc/164870244/view?p_p_state=maximized

PORTARIA N.º 121/2021

Diário da República n.º 111/2021, Série I de 2021-06-09

Justiça

Regulamenta o arquivo eletrónico de documentos lavrados por notário e de outros documentos arquivados nos cartórios, a certidão notarial permanente e a participação de atos por via eletrónica à Conservatória dos Registos Centrais

https://dre.pt/web/guest/home/-/dre/164870237/details/maximized

CNPD: PARECERES, DELIBERAÇÕES E OUTROS DOCUMENTOS

PARECER N.º 20/2018
Data: 2 de maio de 2018

Parecer sobre proposta de lei que executa o RGPD em Portugal
https://www.uc.pt/protecao-de-dados/suporte/20180502_parecer_20_cnpd

DELIBERAÇÃO/2019/494
Data: 3 de setembro de 2019

CNPD delibera desaplicar algumas normas por violação do Direito da União
https://crlisboa.org/wp/wp-content/uploads/2021/06/DELIBERACAO_2019_494.pdf

ORIENTAÇÕES
Data: 17 de abril de 2020

Orientações sobre o controlo à distância em regime de teletrabalho
https://www.cnpd.pt/media/zkhkxlpx/orientacoes_controlo_a_distancia_em_regime_de_teletrabalho.pdf

ORIENTAÇÕES
Data: 22 de abril de 2020

Orientações sobre divulgação de informação relativa a infetados por Covid-19
https://www.cnpd.pt/media/juelxzcj/orientacoes_divulgacao_informacao_infetados_covid-19.pdf

DELIBERAÇÃO/2020/262
Data: 17 de junho de 2020

Deliberação relativa à averiguação efetuada pela CNPD sobre o funcionamento da plataforma Trace Covid-19
https://crlisboa.org/wp/wp-content/uploads/2021/06/DELIBERACAO_2020_262.pdf

PARECER/2020/82
Data: 21 de julho de 2020

Parecer sobre o projeto de decreto-lei que estabelece o responsável pelo tratamento dos dados e regula a intervenção do profissional de saúde no sistema STAYAWAY COVID

https://crlisboa.org/wp/wp-content/uploads/2021/06/PARECER_2020_82.pdf

PARECER/2020/129
Data: 27 de outubro de 2020

Parecer sobre a obrigatoriedade do uso de máscara para acesso ou permanência nos espaços e vias públicas e a obrigatoriedade de utilização da aplicação STAYAWAY COVID

https://crlisboa.org/wp/wp-content/uploads/2021/06/PARECER_2020_129.pdf

ORIENTAÇÕES
Data: 13 de novembro de 2020

Orientações sobre os tratamentos de dados de saúde previstos no Decreto n.º 8/2020, de 8 de novembro

https://www.cnpd.pt/media/1bbppegs/orienta%C3%A7%C3%B5es_decreto_8_2020.pdf

INFORMAÇÃO
Data: 4 de fevereiro de 2021

Informação da CNPD relativa à suspensão dos prazos nos procedimentos de natureza contraordenacional, conforme previsto na Lei n.º 4-B/2021

https://www.cnpd.pt/media/glxnoibz/info_lei-1-a-2020.pdf

PARECER/2021/34
Data: 24 de março de 2021

Parecer sobre o projeto de decreto-lei que visa agilizar o processo de obtenção e comunicação do código de legitimação no âmbito do sistema STAYAWAY COVID

https://crlisboa.org/wp/wp-content/uploads/2021/06/PARECER_2021_34.pdf

Ciclo de Conferências sobre o Regulamento Geral sobre a Proteção de Dados

Incidentes de Segurança no Contexto do RGPD

Maio de 2021

PROGRAMA

01 O RGPD E A SEGURANÇA DA INFORMAÇÃO E RISCO

02 VIOLAÇÃO DE DADOS PESSOAIS

03 PROCEDIMENTO EM CASO DE INCIDENTE

04 EXEMPLOS

05 Q&A

O RGPD E A SEGURANÇA DA INFORMAÇÃO E RISCO

Overview

Aumento significativo do valor das coimas

Punidas com coimas até €20.000 000 ou 4% do volume anual mundial de negócios (empresas)

Poder Sancionatório

Sanções e fiscalização das autoridades nacionais de proteção de dados

Segurança

Notificações de ***data breaches*** e **reforço das medidas de segurança dos dados**

Autorresponsabilização

Privacy by design e by default, privacy impact assessment , registos de tratamento de dados

Consentimento

Validade do consentimento do titular dos dados

Novos direitos dos titulares

Direito de informação e de acesso , de apagamento, limitação do tratamento e portabilidade

Principais requisitos e obrigações de segurança da informação

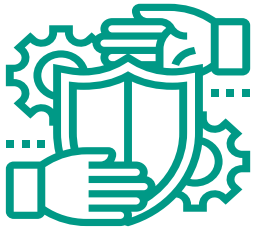
*Tendo em conta as **técnicas mais avançadas**, os **custos de aplicação** e a **natureza, o âmbito, o contexto e as finalidades do tratamento**, bem como **os riscos, de probabilidade e gravidade variável**, para os direitos e liberdades das **pessoas singulares**, o responsável pelo tratamento e o subcontratante aplicam as **medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado** ao risco*

*Ao avaliar o nível de segurança adequado, devem ser tidos em conta, designadamente, os **riscos apresentados pelo tratamento**, em particular devido **à destruição, perda e alteração acidentais ou ilícitas**, e à **divulgação ou ao acesso não autorizados**, de dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.*

Artigo 32.º do RGPD

Principais requisitos e obrigações de segurança da informação

Principais requisitos e obrigações de segurança da informação



A fim de preservar a segurança e evitar o tratamento em violação do presente regulamento, **o responsável pelo tratamento, ou o subcontratante**, deverá **avaliar os riscos** que o tratamento implica e **aplicar medidas que os atenuem**, como a cifragem. Essas medidas deverão assegurar um **nível de segurança adequado**, nomeadamente a confidencialidade, tendo em conta as técnicas mais avançadas e os custos da sua aplicação em função dos riscos e da natureza dos dados pessoais a proteger.
Ao avaliar os riscos para a segurança dos dados, deverão ser tidos em conta os riscos apresentados pelo tratamento dos dados pessoais, tais como a **destruição, perda e alteração acidentais ou ilícitas, e a divulgação ou o acesso não autorizados a dados pessoais** transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento, riscos esses que podem dar azo, em particular, a **danos físicos, materiais ou imateriais**.

Considerando 83 do RGPD

O RGPD e o Risco

*Os **riscos** deverão ser aferidos com base numa avaliação objetiva, que determine se as operações de tratamento de dados implicam risco ou risco elevado.*

*As crianças merecem proteção especial quanto aos seus dados pessoais, uma vez que podem estar menos cientes dos **riscos***

QUANTAS VEZES É REFERIDA A PALAVRA RISCO NO REGULAMENTO GERAL SOBRE A PROTEÇÃO DE DADOS?

74!

*A fim de preservar a segurança e evitar o tratamento em violação do presente regulamento, o responsável pelo tratamento, ou o subcontratante, deverá **avaliar os riscos** que o tratamento implica e aplicar medidas que os atenuem*

*As pessoas singulares a quem os dados dizem respeito deverão ser alertadas para os **riscos**, regras, garantias e direitos associados ao tratamento dos dados pessoais*

*Merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar **riscos significativos***

VIOLAÇÃO DE DADOS PESSOAIS

Violação de Dados Pessoais

VIOLAÇÃO DE SEGURANÇA

PROVOCA A DESTRUIÇÃO, PERDA, ALTERAÇÃO OU ACESSO NÃO AUTORIZADOS

ACIDENTAL OU ILÍCITA

VIOLAÇÕES DE DADOS PESSOAIS

Critérios de avaliação

Violações de dados pessoais

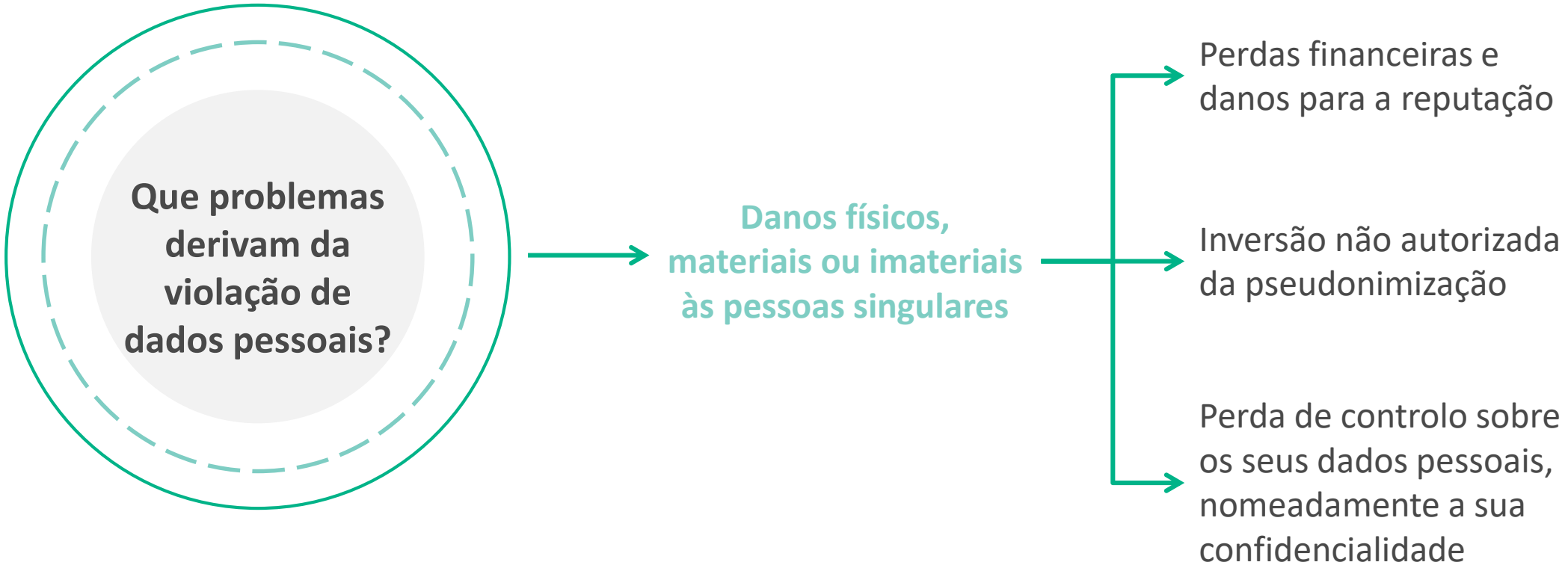
Podem ser avaliadas através dos seguintes critérios de segurança:

(i) **Violação da disponibilidade** – corresponde à destruição (situação na qual a informação já não existe, ou não existe num formato que possa, de algum modo, ser utilizado pelo responsável pelo tratamento, acidental ou ilícita, ou à perda situação na qual a informação poderá existir, mas em relação à qual o responsável pelo tratamento perdeu o controlo ou acesso, ou a posse) de dados pessoais;

(ii) **Violação da integridade** – corresponde à alteração dos dados pessoais; e

(iii) **Violação da confidencialidade** – corresponde à divulgação ou acesso não autorizado a dados pessoais

Consequências



Exemplos

exemplos de
VIOLAÇÕES
de dados pessoais

Deixar acessível um dossier (físico ou informático) com dados pessoais
(Ex: PC desbloqueado)

Fornecer/deixar visível a password de acesso ao PC

Informação confidencial comunicada a pessoas sem legitimidade

Fazer “bases de dados próprias” e arquivar informação em suportes não estruturados
(Ex: Excel)

Furto ou perda de PC com informação que contenha dados pessoais
(encriptada ou não)

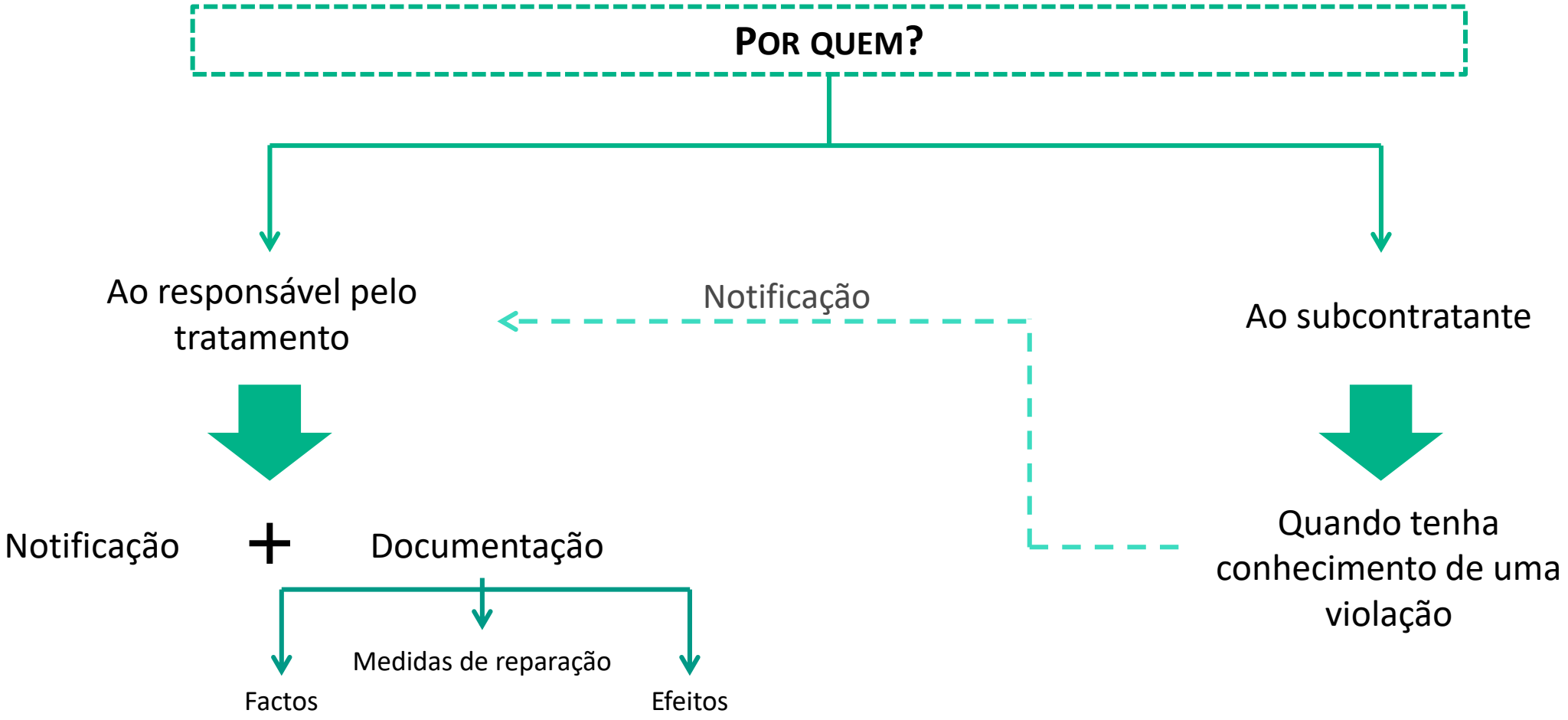
Pirataria informática a uma base de dados com informação pessoal

Transmitir informação através de email pessoal
(incluindo anexos)

Comunicar a um terceiro informação pessoal de outro titular
(incluindo dos respetivos colaboradores)

PROCEDIMENTO EM CASO DE INCIDENTE

Notificação à CNPD e aos Titulares



Procedimento

VIOLAÇÃO DE DADOS PESSOAIS

RESPONSÁVEL PELO TRATAMENTO

72h

AUTORIDADE DE CONTROLO

elevado risco para os direitos e liberdades das pessoais singulares

TITULARES DOS DADOS

SUBCONTRATANTE

Notificação à CNPD

Às Autoridades de Controlo

QUANDO?

A regra	Sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma
A justificação	Se a notificação à autoridade de controlo não for transmitida no prazo de 72 horas, é acompanhada dos motivos do atraso
O envio parcial	Caso, e na medida em que não seja possível fornecer todas as informações ao mesmo tempo, estas podem ser fornecidas por fases, sem demora injustificada

Notificação à CNPD

Às Autoridades de Controlo

FUNÇÕES E CONTEÚDO

1. Descrever a natureza da violação dos dados pessoais incluindo, se possível, as categorias e o número aproximado de titulares de dados afetados, bem como as categorias e o número aproximado de registos de dados pessoais em causa
2. Comunicar o nome e os contactos do encarregado da proteção de dados ou de outro ponto de contacto onde possam ser obtidas mais informações
3. Descrever as consequências prováveis da violação de dados pessoais
4. Descrever as medidas adotadas ou propostas pelo responsável pelo tratamento para preparar a violação de dados pessoais, inclusive, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos

Notificação à CNPD

EXCEÇÕES?

Às Autoridades de Controlo

A obrigatoriedade de proceder à notificação é obrigatória *a menos que a violação dos dados pessoais não seja suscetível de resultar num* ***risco*** *para os direitos e liberdades das pessoas singulares*

Notificação aos titulares dos dados

Aos titulares

QUANDO?

Sempre que a violação de dados pessoais seja suscetível de implicar um **elevado risco** para os direitos e liberdades das pessoas singulares

+

Comunicação **sem demora injustificada** (sem concretização temporal)

A autoridade de controlo pode exigir ao responsável pelo tratamento que proceda à notificação quando esta não tenha sido feita tempestivamente

Notificação aos titulares dos dados

Aos titulares

FUNÇÕES E CONTEÚDO

1. Deve descrever em linguagem clara e simples a natureza da violação dos dados pessoais

2. Deve fornecer, pelo menos, as seguintes informações:

- Comunicação do nome e dos contactos do encarregado da proteção de dados ou de outro ponto de contacto onde possam ser obtidas mais informações
- Descrição das consequências prováveis da violação de dados pessoais
- Descrição das medidas adotadas ou propostas pelo responsável pelo tratamento para preparar a violação de dados pessoais, inclusive, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos

Notificação aos titulares dos dados

EXCEÇÕES?

Quando é que a comunicação **deixa de ser exigida**?

1

Aos titulares

Quando tenham sido aplicadas **medidas de proteção adequadas**

- **Técnicas**
- **Organizativas**

+

Tais medidas **tenham sido aplicadas aos dados pessoais afetados** pela violação

↓

Com especial relevância para as medidas que tornem os **dados pessoais em causa incompreensíveis**

Notificação aos titulares dos dados

Aos titulares

EXCEÇÕES?

Quando é que a comunicação **deixa de ser exigida**?

2

Quando o responsável pelo tratamento tenha tomado **medidas subsequentes que eliminem o risco** para os direitos e liberdades dos titulares dos dados

3

Quando tal comunicação exija um **esforço desproporcionado**

É feita uma **comunicação pública**

É tomada uma qualquer medida que permita que os **titulares tenham acesso à informação**

Sanções do RGPD

Sanções previstas

Qualquer pessoa que tenha sofrido um dano devido à violação de normas do RGPD, pode **obter uma indemnização por esse dano**

As contraordenações graves podem ter valores de:

- **Grandes empresas** – **2500 a 10 000 000 de euros** ou **2% do volume de negócios** anual, mundial, conforme o que for mais elevado
- **PMEs** – **1000 a 1 000 000 de euros** ou **2% do volume de negócios** anual, mundial, conforme o que for mais elevado

As contraordenações muito graves podem ter valores de:

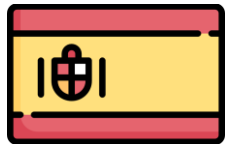
- **Grandes empresas** – **5000 a 20 000 000 de euros** ou **4% do volume de negócios** anual, mundial, conforme o que for mais elevado
- **PMEs** – **2000 a 2 000 000 de euros** ou **2% do volume de negócios** anual, mundial, conforme o que for mais elevado

EXEMPLOS

Algumas coimas relevantes

Quem? TIM (operador de telecomunicações)
Quando? 15 de janeiro de 2020
Quanto? 27,8M
Porquê? Por várias violações, mas também por falhas nas **medidas de segurança**

Quem? British Airways
Quando? 16 de outubro de 2020
Quanto? 22M
Porquê? Neste caso, a principal violação foi relativa a **medidas de segurança**, que expôs dados de 400 000 titulares



Quem? Vodafone ES
Quando? 2019
Quanto? 48 000
Porquê?
Apenas por violação das regras aplicáveis a medidas de segurança

Quem? Marriot International
Quando? 30 de outubro de 2020
Quanto? 20,5M
Porquê?
Apenas por violação das regras aplicáveis a medidas de segurança

O incidente da British Airways

Dear Customer,

From 22:58 BST 21 August 2018 until 21:45 BST 5 September 2018 inclusive, the personal and financial details of customers making or changing bookings at ba.com, and on our app were compromised. The stolen data did not include travel or passport information.

The breach has been resolved and our website is working normally.

We're deeply sorry, but you may have been affected. We recommend that you contact your bank or credit card provider and follow their recommended advice.

We take the protection of your personal information very seriously. Please accept our deepest apologies for the worry and inconvenience that this criminal activity has caused.

Further information can be found at ba.com.

Yours sincerely,

Alex Cruz
Chief Executive Officer

A imagem reflete o email enviado pela British Airways, contactando os potenciais titulares afetados

O incidente da British Airways

beth globo @bethglobo · Sep 13, 2018

@British_Airways @TulipSiddiq my personal ID was stolen from BA due to BA sloppy data protection which is in breach GDPR as BA is the controller of personal data. What can the gov do to introduce regulations to the wild west which is the internet? I am constituent of Tulip Siddi

2

British Airways ✓
@British_Airways

Replying to @bethglobo and @TulipSiddiq

Hi Beth. Sorry for the late reply. We have sent our email communication to those customers affected by the data breach and there is an offer of a year's free subscription to Experian. There will be a voucher code attached ^Neil

2:44 AM · Sep 14, 2018 · Conversocial

Andre McGregor
@AndreOnCyber

Mark this day. Corporations no longer fear data breaches taking down their company. The consumer is left with platitudes like "Deeply sorry" and "contact your bank...and follow their advice". Not even offering credit monitoring anymore. Thanks @British_Airways and @alex_cruz

Sumaya
@1sumaya

Your response is unacceptable. If you were "deeply sorry" @British_Airways and @alex_cruz you'd take responsibility and measures to protect impacted customers. #Unbelievable #fail

Alexandros K. Antoniou @alexkantoniou · Sep 7, 2018

I'm confused by the @British_Airways data breach. They claim they "take the protection of [my] personal information very seriously" but some of my personal and financial details were compromised. Now, what do I do with their apology? Can I trust this won't happen again?

Dan Lazard @dan_lazard · Sep 8, 2018

Spending half my Saturday sorting out @British_Airways data breach mistakes! Thank you very much!!!

1

Q&A

Contactos

Magda Cocco

Sócia

mpc@vda.pt

T. 21 311 3400

Inês Antas de Barros

Associada Coordenadora

iab@vda.pt

T. 21 311 3400

CNPD
Comissão Nacional de Proteção de Dados

Conselho Regional Lisboa

THE LAWYER
European Awards 2019
WINNER
Law firm of the year: Iberia

Luís Neto Galvão

DPIA - AVALIAÇÃO DE IMPACTO SOBRE A PROTEÇÃO DE DADOS

Maio de 2021

DPIA - Introdução

As DPIA são uma consequência do princípio da responsabilidade (arts. 5.º, n.º2, 24.º), que perpassa todo o RGPD

(substituem regime da Lei 67/98 / Diretiva 95/46/CE de notificação / pedido de autorização prévios ao tratamento pouco eficiente)

Processos com objetivo de estabelecer e demonstrar conformidade

Ajudam ao cumprimento de requisitos do RGPD + a demonstrar que foram tomadas medidas adequadas

- Concebidas para descrever o tratamento, avaliar a sua necessidade de proporcionalidade e ajudar a gerir os riscos para os direitos, liberdades das pessoas decorrentes do tratamento
- Processo contínuo, não um exercício a ocorrer uma só vez.
- Realização pode ser delegada em prestador externo, mas a responsabilidade é do responsável pelo tratamento.

Base Jurídica

Artigos 35.º e 36.º do RGPD

Considerandos (89) a (96) do RGPD

Artigo 7.º da Lei 58/2019, de 8 de agosto (“Lei 58/2019”)

Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679 (4/10/2017)

Regulamento 1/2018 da CNPD

Recomendado: Metodologias das DPIA da CNIL e da AEPD – ICO brit
com tendência a divergir da UE

Requisitos dos Tratamentos Sujeitos a DPIA – Requisitos desafiantes

Não são obrigatórias para todos os tratamentos, mas apenas para aqueles:

- Suscetíveis de implicar um elevado risco para os direitos e liberdades das pessoas singulares – em virtude da natureza, âmbito, contexto e finalidades, e, em particular;
- Tratamentos que utilizem novas tecnologias.

→ Devem ser efetuadas previamente ao início do tratamento e responsáveis podem, por sua iniciativa, realizar DPIA, quando facultativa (Art. 7.º, n.º2, Lei 58/2019)

→ Conjunto de operações que apresente riscos elevados e semelhante natureza, âmbito, contexto finalidade e riscos semelhantes pode ser analisado numa única avaliação (e.g. CCTV de um grupo de freguesias).

→ Sujeitas ao Parecer do Encarregado da Proteção de Dados/DPO, quando designado.

Realização obrigatória de DPIA

Na dúvida, realizar

Nomeadamente em caso de:

- Avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões com efeitos jurídicos ou que afetem significativamente pessoa em causa (e.g. segmentação de clientes por instituição bancária);

- Operações de tratamento em grande escala de categorias especiais de dados ou de dados pessoais relacionados com condenações penais e infrações (e.g. app de fitness);

- Controlo sistemático de zonas acessíveis ao público em grande escala.

(Art. 35.º RGPD)

Realização obrigatória de DPIA – Grande Escala

Conceito de grande escala não definido no RGPD

Como Interpretar Grande Escala

- número de titulares de dados envolvidos, quer através de um número específico quer através de uma percentagem da população pertinente;
- volume de dados e/ou a diversidade de dados diferentes a tratar;
- duração da atividade de tratamento de dados ou a sua pertinência;
- dimensão geográfica da atividade de tratamento.

GT29: Orientações sobre DPO, WP243

Realização obrigatória de DPIA – Grande Escala

Considerandos fundamentais, mas por vezes a tratar *cum grano salis*

Considerando (91) RGPD: O tratamento de dados pessoais não deverá ser considerado de grande escala se disser respeito aos dados pessoais de pacientes ou clientes de um determinado médico, profissional de cuidados de saúde, **hospital** ou advogado. **Nesses casos, a realização de uma avaliação de impacto sobre a proteção de dados não deverá ser obrigatória**.

Exemplos de tratamento	Critérios pertinentes possíveis	Exige-se a realização de uma AIPD?
Um hospital que faz o tratamento dos dados genéticos e de saúde dos seus doentes (sistema de informação do hospital).	- Dados sensíveis ou dados de natureza altamente pessoal. - Dados relativos a titulares de dados vulneráveis. - Dados tratados em grande escala.	
Utilização de um sistema de câmaras para controlar o comportamento dos condutores nas autoestradas. O responsável pelo tratamento pretende utilizar um sistema inteligente de análise através de vídeo para selecionar carros específicos e reconhecer automaticamente as matrículas.	- Controlo sistemático. - Utilização de soluções inovadoras ou aplicação de novas soluções tecnológicas ou organizacionais.	
Uma empresa que controle sistematicamente as atividades dos seus empregados, incluindo o controlo dos computadores, da atividade internet, etc. dos seus empregados.	- Controlo sistemático. - Dados relativos a titulares de dados vulneráveis.	
Recolha de dados públicos das redes sociais para elaborar perfis.	- Avaliação ou classificação. - Dados tratados em grande escala. - Estabelecer correspondências ou combinar conjuntos de dados. - Dados sensíveis ou dados de natureza	Sim

Realização obrigatória de DPIA

RGPD estabelece obrigatoriedade de Autoridade de Controlo elaborar e tornar pública lista dos tipos de operações de tratamento sujeitas a DPIA

- Em Portugal, a CNPD publicou o Regulamento n.º 1/2018, relativo à lista de tratamentos de dados pessoais sujeitos a Avaliação de Impacto sobre a Proteção de Dados.
- Lista não exaustiva, podendo ainda surgir outras situações em que se justifique realizar obrigatoriamente a DPIA, designadamente em função do desenvolvimento tecnológico.
- Tem por referência as Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) - WP248 rev.01, do Grupo de Trabalho do Artigo 29 e assumidas pelo Comité Europeu de Proteção de Dados
- Sujeita a procedimento de controlo da coerência por parte do CEPD
- Podem ser elaboradas listas de atividades não sujeitas a DPIAs, que devem ser também comunicadas ao CEPD.

Tratamentos de dados pessoais sujeitos a DPIA (Regulamento n.º 1/2018, CNPD)

- Utilização de dispositivos eletrónicos que transmitam, por redes de comunicação, dados pessoais relativos à saúde;

- Interconexão de dados pessoais ou tratamento que relacione categorias especiais de dados pessoais ou dados de condenações penais e infrações ou dados de natureza altamente pessoal

- Tratamento de categorias especiais de dados pessoais ou dados de condenações penais e infrações ou dados de natureza altamente pessoal com base em recolha indireta dos mesmos, quando não seja possível ou exequível assegurar o direito de informação;

- Profiling em grande escala;

- Rastreamento da localização ou comportamento dos titulares (por exemplo, trabalhadores, clientes ou apenas transeuntes), que tenha como efeito a avaliação ou classificação destes, exceto quando tratamento seja indispensável para a prestação de serviços requeridos especificamente pelos mesmos;

Tratamentos de dados pessoais sujeitos a DPIA (Regulamento n.º 1/2018, CNPD)

- Tratamento de categorias especiais, condenações penais e infrações ou dados de natureza altamente pessoal para arquivo de interesse público, investigação científicae histórica ou fins estatísticos, exceto se previstos na lei, com garantias adequadas dos direitos dos titulares;

- Tratamento de dados biométricos para identificação inequívoca dos seus titulares, quando estes sejam pessoas vulneráveis, com exceção de tratamentos previstos e regulados por lei que tenha sido precedida de uma avaliação de impacto sobre a proteção de dados;

- Tratamento de dados genéticos de pessoas vulneráveis, com exceção de tratamentos previstos e regulados por lei que tenha sido precedida de uma avaliação de impacto sobre a proteção de dados.

- Tratamento de categorias especiais de dados pessoais ou dados de condenações penais e infrações ou dados de natureza altamente pessoal com utilização de novas tecnologias ou nova utilização de tecnologias já existentes.

Realização obrigatória de DPIA – Grande Escala

Conceito de dados altamente pessoais

- Categorias especiais, dados sobre condenações penais e infrações;
- Dados sensíveis, porque associados a atividades privadas e familiares:
  - Emails;
  - Dados de localização;
  - Dados financeiros;
  - Documentos pessoais;
  - Diários;
  - Notas em dispositivos eletrónicos de leitura;
  - Calendários virtuais, etc.

GT29: Orientações sobre DPIA, WP248

Tratamentos de dados pessoais não sujeitos a DPIA

Se não registaram alterações nas características essenciais

Tratamentos realizados com base em autorizações emitidas nos termos da Lei n.º 67/98, de 26 de outubro dispensados de DPIA.

Características essenciais: âmbito, finalidade, categorias, responsáveis, destinatários dos dados, período de conservação, medidas técnicas e organizativas. Alteração de riscos, como adoção de nova tecnologia.

- Por uma questão de boa prática, uma DPIA deve ser continuamente revista e regularmente reavaliada.

Intervenção do EPD/DPO

O GT 29 (hoje CEPD) recomenda que o responsável pelo tratamento solicite o parecer do EPD/DPO sobre as seguintes questões, entre outras:

- se deve ou não efetuar uma DPIA;
- qual a metodologia a seguir na realização de uma DPIA;
- se deve realizar a DPIA internamente ou externalizá-la;
- que salvaguardas (incluindo medidas técnicas e organizativas) aplicar no sentido de atenuar os eventuais riscos para os direitos e interesses dos titulares de dados;
- se a DPIA foi ou não corretamente efetuada e se as suas conclusões (se o tratamento deve ou não ser realizado e quais as salvaguardas a aplicar) estão em conformidade com o RGPD.

(Orientações Sobre DPOs - wp243rev.01)

Requisitos de uma DPIA

Avaliação/DPIA inclui, pelo menos:

- Descrição sistemática das operações de tratamento previstas e a finalidade do tratamento, inclusive, se for caso disso, os interesses legítimos do responsável pelo tratamento;
- Avaliação da necessidade e proporcionalidade das operações de tratamento em relação aos objetivos;
- Avaliação dos riscos para os direitos e liberdades dos titulares dos dados
- Medidas de mitigação, para fazer face aos riscos, incluindo garantias, medidas de segurança e procedimentos destinados a assegurar a proteção dos dados pessoais e demonstrar a conformidade com o RGPD.

Requisitos de uma DPIA

Realizadas com regularidade

A realidade dos tratamentos é, em regra, dinâmica, pelo que deve existir um rotina de repetição das DPIAs adaptada à organização

Se necessário, deve ser feito um controlo para avaliar se o tratamento é realizado em conformidade com a DPIA, pelo menos quando haja uma alteração dos riscos que as operações de tratamento representam.

Consulta prévia à Autoridade de Controlo - CNPD

Obrigatória se resultado de avaliação/DPIA indicar elevado risco residual, porque o responsável não conseguiu reduzi-lo para nível aceitável com medidas para atenuar/mitigar o risco.

A ter lugar antes de iniciado o tratamento

Regulamento 310/2020 - Taxas da CNPD – Sujeita a taxa de 12 UCs

Consulta prévia à Autoridade de Controlo - CNPD

O que deve constar da consulta à autoridade de controlo:

- Repartição de responsabilidades entre:
  - responsável pelo tratamento
  - responsáveis conjuntos pelo tratamento;
  - subcontratantes envolvidos no tratamento, nomeadamente no caso de um tratamento dentro de um grupo empresarial, quando aplicável;
- Finalidades e os meios do tratamento previsto;
- Medidas e garantias previstas para defesa dos direitos e liberdades dos titulares dos dados;
- Se aplicável, os contactos do DPO;
- A avaliação de impacto sobre a proteção de dados;
- Outras informações solicitadas pela autoridade de controlo.

O que pode fazer a Autoridade de Controlo (CNPD)

Até 8 semanas + 6 semanas (em função da complexidade do tratamento) após pedido de consulta

Emite orientações por escrito

Se houver prorrogação, a CNPD informa num mês o responsável e subcontratante (se existir) e fundamenta atraso.

Suspensão de prazos enquanto não forem obtidas informações solicitadas ao responsável ou subcontratante.

A CNPD é **obrigada** a emitir orientações: se tratamento violar o RGPD, nomeadamente por o responsável não identificar ou atenuar suficientemente os riscos.

Orientações emitidas ao(s) responsável(eis) pelo tratamento e, caso exista, ao subcontratante.

O que pode fazer a Autoridade de Controlo (CNPD)

CNPD pode ainda usar os vastos poderes de investigação e correção conferidos pelo RGPD (art. 58.º), incluindo, entre outros:

(i) Ordenar fornecimento de informações necessárias a responsável/subcontratante/representante;

(ii) Realizar investigações sob a forma de auditorias sobre a proteção de dados;

(iii) Notificar ao responsável ou subcontratante alegadas violações do regulamento;

(iv) Obter acesso a instalações e a equipamentos e meios de tratamento de dados;

O que pode fazer a Autoridade de Controlo (CNPD)

(v) Fazer advertências, repreensões ou impor coimas;

(vi) Dar ordens, nomeadamente para que responsável satisfaça pedidos de exercício de direitos ou para que operações de tratamento passem a cumprir o RGPD;

(vii) Ordenar retificação, apagamento ou limitação de tratamento.

O que pode fazer a Autoridade de Controlo (CNPD)

Não conformidade com requisitos de um DPIA pode conduzir à imposição de coimas pela CNPD – É contraordenação grave

Se o responsável pelo tratamento, nomeadamente:

(i) não realizar uma DPIA quando tratamento está sujeito à mesma;

(ii) realizar uma AIPD de forma incorreta

(iii) não consultar a autoridade de controlo competente quando necessário

pode resultar numa coima, no caso de grande empresa, de **2.500 euros a 10 milhões de euros ou até 2 % do seu volume de negócios anual** a nível mundial correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado.

(Arts. 35.º, 36.º, 83.º, n.º4, al. a), RGPD, Art. 38.º, n.º1, als. l) e m) da Lei 58/2019)

reconheço a situação muito grave que vivemos todos
e lamento profundamente quem muito sofreu, directa
ou indirectamente, com a mesma

Pedro Simões Dias

os dados ao limite

a presente apresentação parte de duas premissas e pretende ser um exercício meramente jurídico de cariz prospectivo com base num “se”

“não nos podemos permitir ser apanhados novamente desprevenidos. a ameaça da próxima pandemia pairará sempre por cima das nossas cabeças”
“a preparação para a próxima pandemia deve ser levada tão a sério como a ameaça de uma guerra”

Bill Gates
Público, 28 Janeiro 2021

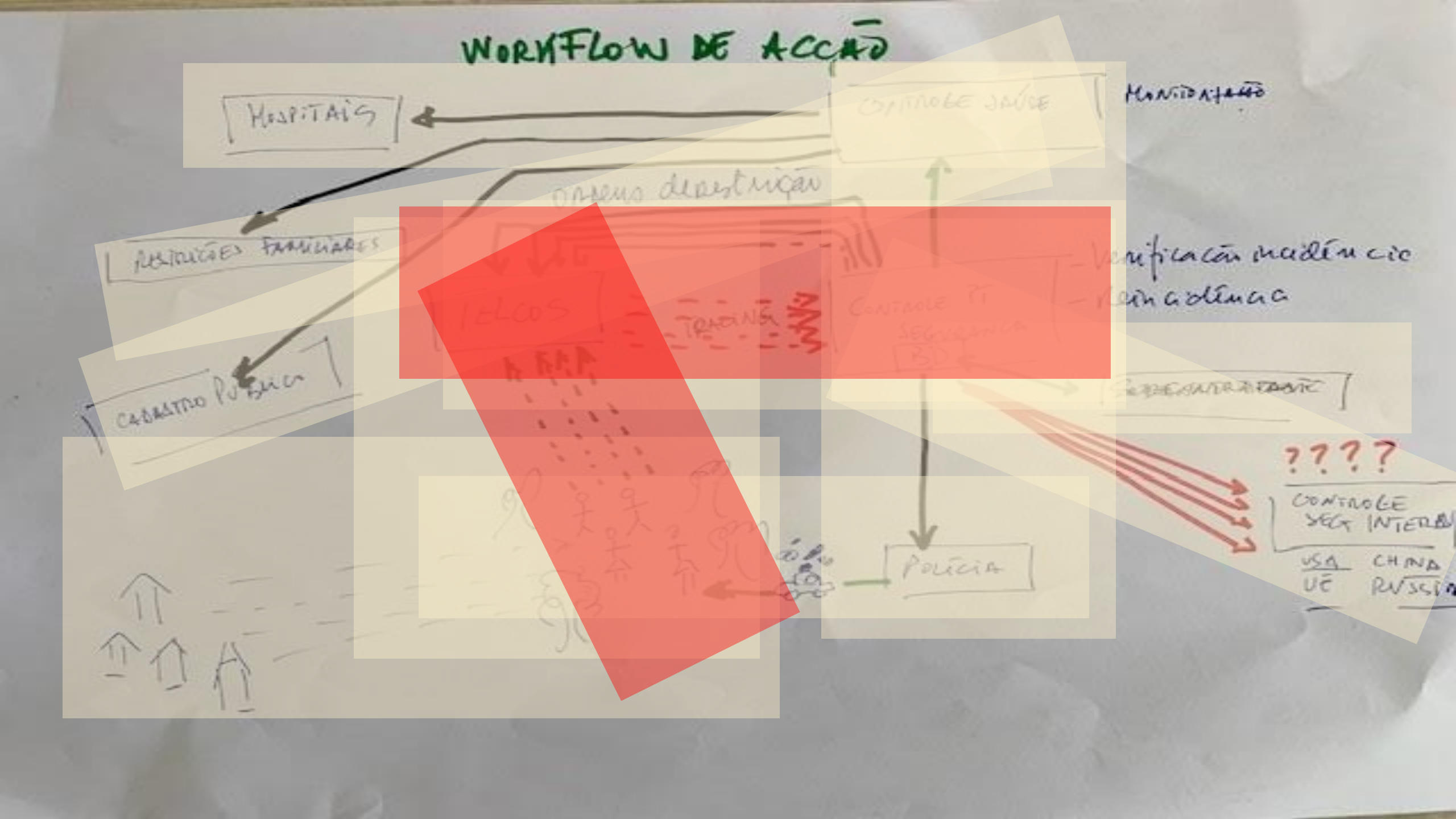
“O vírus é mortífero apenas o suficiente (mata entre 1 e 1,6% das pessoas com sintomas) ... É mortífero o suficiente para nos prejudicar, mas não o suficiente para o levarmos tão a sério quanto devíamos.”

Nicholas A. Christakis
Público, 19 de Abril de 2021

assumption #1: uma nova pandemia grave virá ao mundo

assumption #2: o Sars Cov-2 não acaba com a espécie humana

projecção: e se a pandemia que vier tiver potencial para acabar com a espécie humana?


WORKFLOW DE ACÇÃO
HOSPITAIS
CONTROLE SAÚDE
MONITORAMENTO
INSTITUIÇÕES FINANCEIRAS
CADASTRO PÚBLICO
TELCOS
TRIAGEM
CONTROLE TI SEGURANÇA
POLÍCIA
????
CONTROLE SEG INTERN
USA
UE
CHINA
RUSSIA

#1 comunicação blootooth telco - tracing
#2 comunicação telco/controle de segurança – flagging incidência/ reincidências
3.1 comunicação controle de segurança/policia - deslocação
3.2 comunicação controle de segurança/ controlo de saúde
3.3 comunicação controle de segurança/EU-USA-China-Russia- flagging incidência (?)
4 subcontratação BD/gestão
5.1 comunicação controle de saúde/hospitais locais- prevenção
5.2. comunicação controlo de saúde / publicitação de cadastrados
5.3. comunicação controlo de saúde a familiares: confinamento
6 comunicação controlo de segurança/telcos: repressão tecnológica

#1 Telcos :tracing
#2 Centro de Segurança:
- comunicações a terceiros
- flagging incidência/ reincidências
3 Controle de Saúde:
- comunicações a terceiros
- registos familiares
- registo de incidências
4 Polícia: registo de incidências
5 Entidades Internacionais: o mundo cabe lá

RAT:

finalidade: gestão de dados de localização para efeitos de reacção a disseminação de doença

licitude: 6/1(d) para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular

ou

9/2(i) por motivos de interesse público no domínio da saúde pública

categoria de dados: dados de localização

comunicação de dados: telcos, diversas entidades (Centros Nacionais diversos, incluindo "exposição pública" do cadastrado)

fluxo transfronteiriço: sim, EU, USA, China, Rússia, [lista]

interconexões: "total"

conservação: durante duração da doença

direito de acesso: sim, centro de segurança

direito de oposição: não (apenas mediante decisão judicial)

subcontratação: sim [listar]

avaliação de impacto: sim

formas modernas de repressão (#1, #2, #3):

- strike #1 – bloqueio 3 apps favoritas 3 h


Filipe Silveira
Jornalista

formas modernas de repressão:

- strike #2 - bloqueio Internet 3 dias
- strike #3 - mobile off 30 dias

ok + coimas

Returning to our APP
key topics:
- tracing tool
- monitor tool
- communication to third entities tool

Como as instituiçoes têm tratado estes temas:

- UE
- PT

EU / EPDB (Comité Europeu para a Protecçao de Dados

- Guidelines 04/2020 (April 2020)
- WP251rev.01 decisões automatizadas/profiling (2016)

Tracing tool e fundamento de licitude

EPDB Guidelines 04/2020 (April 2020)
purposes of the tracing tools:
- using location data to support the response to the pandemic
- contact tracing (to notify individuals)

EPDB **generally** considers that data and technology used to help fight COVID-19 should be used to empower, rather than to control, stigmatise, or repress individuals

EPDB Guidelines 04/2020 (April 2020)

but location data collected may only be processed within articles 6 and 9 of the ePrivacy Directive

lei 41/2004
art 6 - dados de tráfego :consentimento prévio e expresso;
-pode ser retirado a qualquer momento...

Artigo 7.º dados de localização: - consentimento prévio e expresso: - retirar a qualquer momento o consentimento; - recusar temporariamente o tratamento desses dados (!!!!!)

ePrivacy Directive permite a derrogação destes direitos
mas para a segurança nacional. não a saúde

E PT não adoptou derrogações!!

EPDB WP251rev.01 decisões automatizadas/profiling (2016)

Artigo 6/1(d) – necessário para a defesa de interesses vitais : - à vida do titular dos dados
- ou de qualquer outra pessoa singular.

.. incluem a definição de perfis necessária para desenvolver modelos que prevejam a propagação de doenças potencialmente fatais ou situações de emergência humanitária.

Nota: a diretiva 95 não tinha a “salvífica” al. i) art.9 RGPD

Se o tratamento for necessário por motivos de interesse **público no domínio da saúde pública, tais como a proteção contra ameaças transfronteiriças graves para a saúde** …,

Salvaguardando em particular o sigilo profissional.

[quem é que se importa com o sigilo profissional???]

anotação #1: o RGPD é mais lato do que diretiva 95

PT = CNPD

- Parecer app Staway Covid

parecer da CNPD stayway covid:
"o rastreamento de localização e movimentação .. **não devem ter um carácter obrigatório**, … porque claramente violadoras do princípio da proporcionalidade num Estado de Direito democrático.

Mesmo em causa uma situação excepcional de emergência de saúde pública, a imposição de tal tipo de controlo – como se de uma panaceia se tratasse – não cumpriria os princípios de adequação, necessidade e proporcionalidade"

parecer da CNPD stayway covid:

- condição de licitude: consentimento do titular

- vertente voluntária e autodeterminação
desligar blootooth

Desligar o blootooth - really?
Resposta: privacy by default: o máximo no máximo

anotação #2: a posição do EPDB é menos “core” e “radical” do que CNPD (“generally” vs “mesmo em causa”)

conclusões:

#1 - o RGPD é muito mais “aberto” que a directiva 95

#2 - o RGPD é muito mais “aberto” que a LGPD 98 (a vida privada!!!!!!!!)

#3 - a posição das instituições europeias é mais “aberta” do que a da CNPD

#4 - “ignorar” “pequenas” regras é essencial

é o RGPD que vai permitir salvar a condição humana

QUESTÕES*

https://www.youtube.com/playlist?list=PLAOIEYezmy6koQwo1cTuYpazJPHSQs7BM

QUESTÃO 1

"Falou-se que o RGPD não se aplica às relações entre os Estados membros e os EUA, fiquei com dúvidas sobre o que cabe no âmbito do RGPD e o que não cabe."

RESPOSTA

1:10:14 a 1:12:18

https://www.youtube.com/watch?v=XT4La_cATbc#t=1h10m14s

QUESTÃO 2

«Até onde deve ir a atuação do advogado em matéria de segurança da informação? Será que enquanto advogado e até DPO, compete-nos apenas explicar as exigências do RGPD aos nossos clientes e deixar os departamentos de IT ou empresas especializadas para o efeito fazer o seu trabalho, sempre com a nossa supervisão? Ou é nos exigível ir mais longe e ser um verdadeiro "agente de cibersegurança"?»

RESPOSTA

53:19 a 1:00:22

https://www.youtube.com/watch?v=jUhlG2FTl-k&t=3227s#t=53m19s

* A presente compilação transcreve, sem revisão, as questões colocadas pelos advogados aos oradores relativamente a cada temática.

FICHA TÉCNICA

Título

Ciclo de Conferências sobre o Regulamento Geral de Proteção de Dados

Edição

Conselho Regional de Lisboa da Ordem dos Advogados

Rua dos Anjos, 79

1050-035 Lisboa

T. 21 312 98 50 E. crlisboa@crl.oa.pt

www.oa.pt/lisboa

Coordenação

João Massano

Centro de Publicações

Ana Dias

Marlene Teixeira de Carvalho

Colaboradores

Isabel Carmo

Susana Rebelo

Sofia Galvão