

# Mestrado em Engenharia Informática (MEI)

# Mestrado Integrado em Engenharia Informática

## (MiEI)

Perfil de Especialização **CSI** : Criptografia e Segurança da  
Informação

Engenharia de Segurança

# Tópicos

- Regulamento UE 2016/679 – Regulamento Geral de Proteção de Dados (RGPD)

## Motivação

- Desde 25/Maio/2018 que os dados pessoais têm que ser tratados de acordo com o Regulamento EU 2016/679.

# Proteção de dados pessoais – Histórico

**Seis funcionários de operadoras recebiam dinheiro por cada lista de informações pessoais que passavam à concorrência**

Um esquema que vendia dados pessoais de clientes de telecomunicações e que envolveu duas redes criminosas montadas em operadoras foi agora desmontado pela Polícia Judiciária de Lisboa. Seis funcionários de empresas que comercializam pacotes de televisão, internet e telemóveis foram apanhados no esquema e detidos pelos inspetores da PJ.

GOVERNO

## Fisco: acesso a dados terá de ser justificado

22/6/2015, 9:16 1

O fisco quer introduzir um mecanismo informático que obriga a que os colaboradores justifiquem previamente a consulta à informação fiscal dos contribuintes. Vai também ser limitado o acesso externo.



# Proteção de dados pessoais – Histórico

**Seis funcionários de operadoras recebiam dinheiro por cada lista de informações pessoais que passavam à concorrência**

Um esquema que vendia dados pessoais de clientes de telecomunicações e que envolveu duas redes criminosas montadas em operadoras foi agora desmontado pela Polícia Judiciária de Lisboa. Seis funcionários de empresas que comercializam pacotes de televisão, internet e telemóveis foram apanhados no esquema e detidos pelos inspetores da PJ.

GOVERNO

## Fisco: acesso a dados t

22/6/2015, 9:16 1

O fisco quer introduzir um mecanismo informático que justifiquem previamente a consulta à informação fiscal dos contribuintes. Vai também ser limitado o acesso externo.

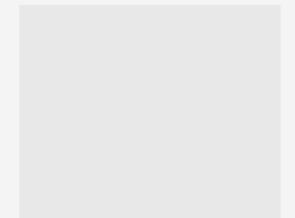
## Facebook: Nova fuga terá exposto dados pessoais de 267 milhões de utilizadores

 Jéssica Sousa 20 Dezembro 2019, 17:31

É aconselhável que, além de reverem a informação acessível no Facebook, os utilizadores fiquem especialmente atentos à receção de mensagens suspeitas ou outro tipo de comunicações não solicitadas ou que possam parecer estranhas.



O Facebook está a investigar relatórios de que um banco de dados que contém mais de 267 milhões de registos de informações pessoais de utilizadores, incluindo nomes e números de telefone, terá sido exposto online e partilhado por hackers. Com esta quantidade de informação, os investigadores alertam para a possibilidade de um aumento dos esquemas de "phishing", especialmente através de mensagens de texto ou chamadas telefónicas.



+ LIDAS

+ PARTILHADAS

Warning: Invalid argument supplied for foreach() in  
 /var/www/vhosts/jornaleconomico.sapo.pt/httpdocs/wp-  
 content/themes/theme-  
 jeconomico/lib/Blocks/MostViewed.php on line 32

# Proteção de dados pessoais – Histórico

**Facebook: Nova fuga terá exposto dados pessoais de 267 milhões de utilizadores**

Seis funcionários de operadoras recebiam

dinheiro r **Expostos dados pessoais de mais de 10 milhões de que passa clientes dos hotéis MGM**

Um esquei JN  
20 Fevereiro 2020 às 14:33



**COMENTAR**

TÓPICOS

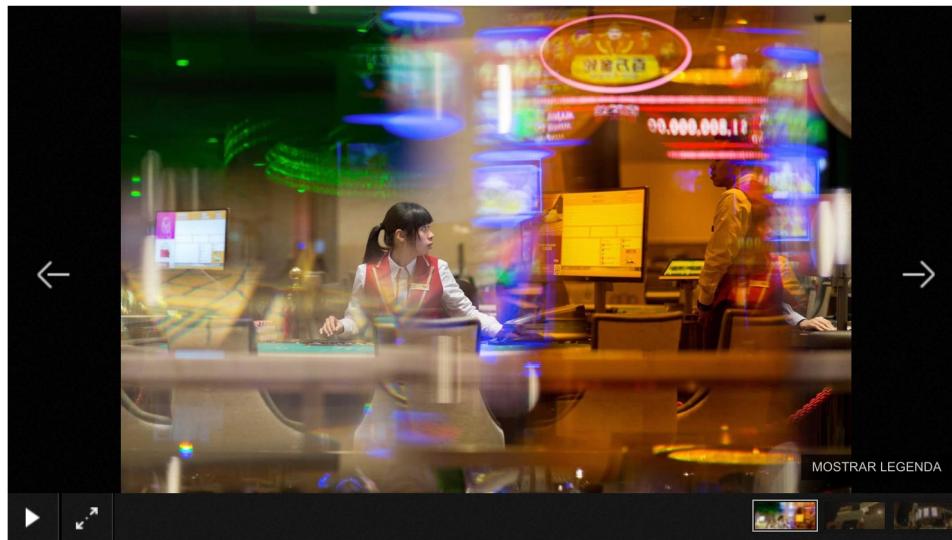
Mundo  
Pirataria  
Pirataria informática  
MGM

GOVERNO

## Fisc

22/6/2015, 5

O fisco q  
justifique  
limitado

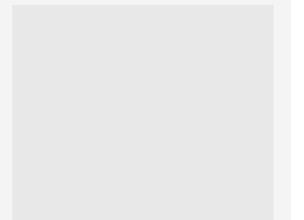


Os dados pessoais de 10,6 milhões de clientes que ficaram hospedados em hotéis MGM Resorts foram expostos depois de um ataque informático no verão do ano passado.

O site [ZDNet informou](#) que as informações pessoais roubadas foram publicadas num fórum de "hackers" esta semana. A MGM confirmou o ataque informático à [BBC](#).

Os dados expostos incluem nomes, moradas e números de passaporte de antigos hóspedes. A MGM disse estar "confiante" de que nenhuma informação financeira foi divulgada. A rede norte-americana de resorts e casinos diz não ser possível saber exatamente quantas pessoas foram afetadas porque as informações expostas podem ser duplicadas.

s utilizadores fiquem especialmente atentos à das ou que possam parecer estranhas.



PUB

**+ LIDAS** **+ PARTILHADAS**

Warning: Invalid argument supplied for foreach() in /var/www/vhosts/jornaleconomico.sapo.pt/httpdocs/wp-content/themes/theme-jeconomico/lib/Blocks/MostViewed.php on line 32

hóspedes  
á sido  
res  
avés de

# Proteção de dados pessoais – Histórico

Seis funcionários de operadoras recebiam dinheiro r Expostos dados pessoais de mais de 10 milhões de que passa clientes dos hotéis

Um esquecer clientes de redes criminosas agora desembarca em Lisboa. Seja comerciali telemóveis detidos pelo Estado

GOVERNO

## Fisc

22/6/2015, 5

O fisco quer justificar o seu limitado



Os dados pessoais dos hóspedes dos hotéis MGM Redo do ano passado

O site ZDNet info é um fórum de "hacker"

Os dados expostos hóspedes. A MGM divulgada. A rede exatamente quando duplicadas.

Facebook: Nova fuga terá exposto dados pessoais de 267 milhões de utilizadores

**Descoberta base de dados com 49 milhões emails e outras informações pessoais**



A base de dados de contactos da Straffic.io com 140 GB de informação foi protegida com uma password que podia ser facilmente encontrada

**A** Straffic.io é uma empresa de marketing israelita fundada em 2017 e a responsável por ter deixado desprotegida uma base de dados com 140 GB de informações – e que contém nomes, género, moradas, endereços de email e números de telefone de pessoas dos EUA e da Europa. A descoberta da base de dados foi feita por um investigador de segurança que se fartou de receber SMS indesejadas durante dois anos e foi investigar a origem.

# Proteção de dados pessoais – Histórico

## Virgin Media data breach affects 900,000 people

© 5 March 2020

     Share



GETTY IMAGES

A Virgin Media database containing the personal details of 900,000 people was left unsecured and accessible online for 10 months, the company has admitted.

The information was accessed "on at least one occasion" by an unknown user.

The database, which was for marketing purposes, contained phone numbers, home and email addresses.

# Proteção de dados pessoais – Histórico

## Press Release

26 July 2017 - h 08:56 | PRICE SENSITIVE

Financial

UniCredit today announced it has been the victim of a security breach in Italy due to unauthorised access through an Italian third party provider to Italian customer data related to personal loans only.

A first breach seems to have occurred in September and October 2016 and a second breach which has just been identified in June and July 2017. Data of approximately 400,000 customers in Italy is assumed to have been impacted during these two periods. No data, such as passwords allowing access to customer accounts or allowing for unauthorised transactions, has been affected, whilst some other personal data and IBAN numbers might have been accessed.



**A Virgin Media database containing the personal details of 900,000 people was left unsecured and accessible online for 10 months, the company has admitted.**

The information was accessed "on at least one occasion" by an unknown user.

The database, which was for marketing purposes, contained phone numbers, home and email addresses.



# Proteção de dados pessoais – Histórico

## Press Release

26 July 2017 - h 08:56 | PRICE SENSITIVE

Financial

UniCredit today announced it has been the victim of a security breach in Italy due to unauthorised access through an Italian third party provider to Italian customer data related to personal loans only.

A first breach seems to have occurred in September and October 2016 and a second breach which has just been identified in June and July 2017. Data of approximately 400,000 customers in Italy is assumed to have been impacted during these two periods. No data, such as passwords allowing access to customer accounts or allowing for unauthorised transactions, has been affected, whilst some other personal data and IBAN numbers might have been accessed.



## Cathay Pacific Fined £500,000 for Data Breach | Avast



by Avast Blog on March 6, 2020

International airline Cathay Pacific, based in the UK, was issued a £500,000 fine by the Information Commissioner's Office (ICO) for a data breach that occurred continuously between October 2014 and May 2018. According to the ICO's [notice](#), approximately 9.4 million data subjects were affected by the breach, which leaked information such as names, nationalities, birth dates, phone numbers, email addresses, and passport numbers for Cathay Pacific customers around the world.

# Over 120 million Decathlon accounts hacked

By Jitendra Soni 18 days ago

P Employee and user data leaked due to unsecured server



(Image credit: Shutterstock.com / Tharnapoom Voranavin)

Sporting company Decathlon has suffered a massive data breach exposing records of over 123 million users and employees.

According to researchers at [vpnMentor](#), more than 9GB of data was leaked from an unsecured ElasticSearch server.

The leaked information, which primarily pertains to the Spanish arm of the company, was found on February 12th, with Decathlon informed on 16th February, with the company saying the server was fixed the next day itself.

- [Slickwraps hit by customer data breach](#)
- [US Defence agency reports data breach](#)
- [Estée Lauder suffers massive breach, 400m records exposed](#)



International airline Cathay Pacific suffered a data breach that occurred on February 2017, affecting over 9 million data subjects worldwide. The breached data includes names, email addresses, telephone numbers, and passport numbers.

## Decathlon hack

According to Decathlon, the majority of the data was related to its employees, with very few customers affected.

The leaked files contained information including employee user names, unencrypted passwords, official email addresses, employee contract information, API logs and API credentials.

# Brasil – Histórico

Financial

through an Italian third party provider to Italian customer data related

It been identified in June and July 2017. Data of approximately 123 million users and employees, including names, email addresses, and passwords allowing access to customer accounts or allowing for their accounts to be reset have been accessed.



## Data Breach | Avast

by the Information Commissioner's Office (ICO) for Avast Software. According to the ICO's [notice](#), approximately 9.4 million individuals in the UK had their personal data breached, such as names, nationalities, birth dates, phone numbers, email addresses, and IP addresses around the world.



# Over 120 million Decathlon accounts hacked

By Jitendra Soni 18 days ago

P Employee and user data leaked due to unsecured server



by Brandon Vigliarolo in Security on March 5, 2020, 10:43 AM PST

A study finds that ID fraud is a greater concern than murder for 47% of Americans.



A report from Atlas VPN finds that one in three Americans worries about identity theft, while only 20% are concerned about becoming a murder victim. Along with being concerned about identity theft, 72% say they are worried about having personal information stolen by hackers. This may indicate a separate fear of stolen information not being used for ID theft, or the two concerns could be conflated.

## More about cybersecurity

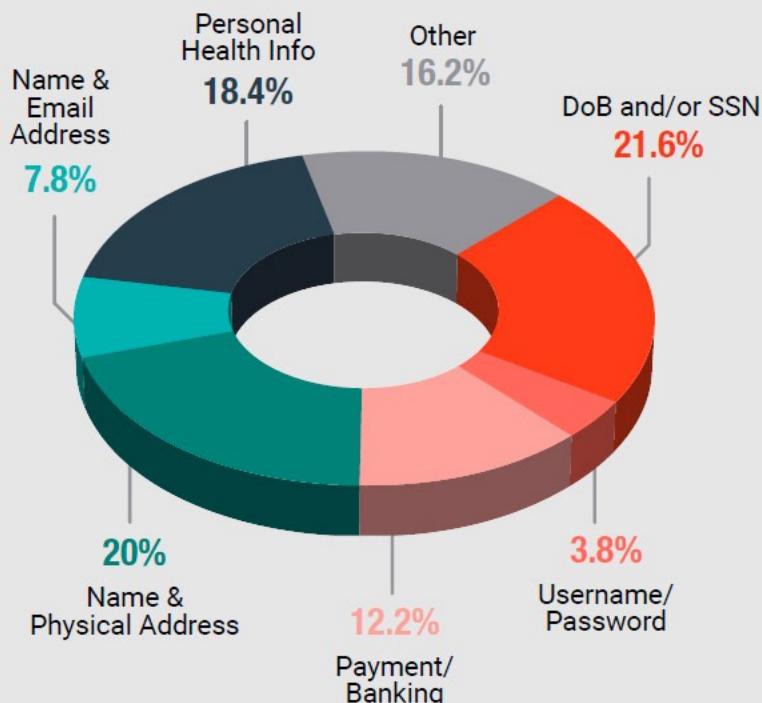
- Cybersecurity in 2020: Eight frightening predictions
- The 10 most important cyberattacks of the decade
- How to become a cybersecurity pro: A cheat sheet

# Proteção de dados pessoais – Histórico

In 2019 the total number of records exposed increased by 284% compared to 2018, according to Risk Based Security.

## Breach Types

Types of Data Exposed in Every Breach



<https://www.helpnetsecurity.com/2019/06/05/2018-data-breaches-cost-usa/>

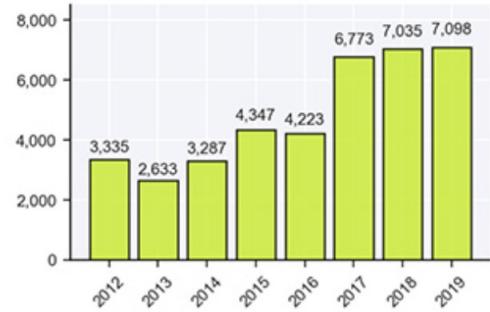


Figure 1: Number of breaches reported each year

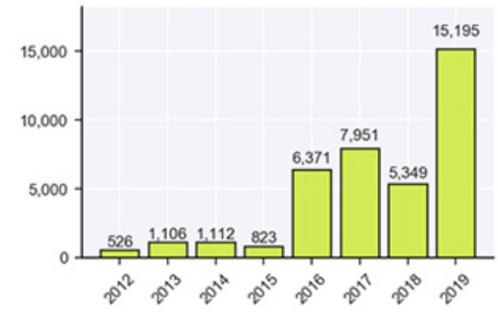
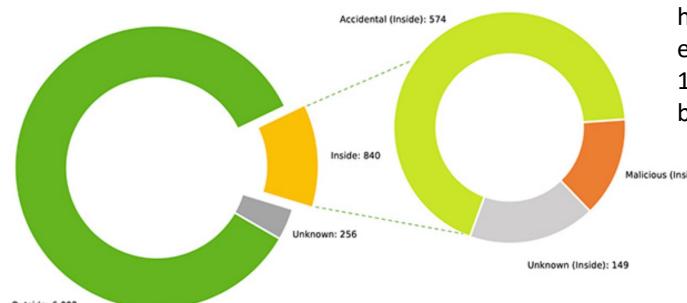


Figure 2: Number of records lost (in millions) each year

## 2019: The worst year on record

However, 2019 has lived up to its reputation for being “the worst year on record” for breach activity with more breaches reported, more data exposed, and more credentials dumped online.

Since the release of the report three months ago, 7.2 billion records were compromised, with only four events accounting for 93.5% of those records. The cause? Open and misconfigured databases that were made publicly accessible to anyone motivated to seek them out.

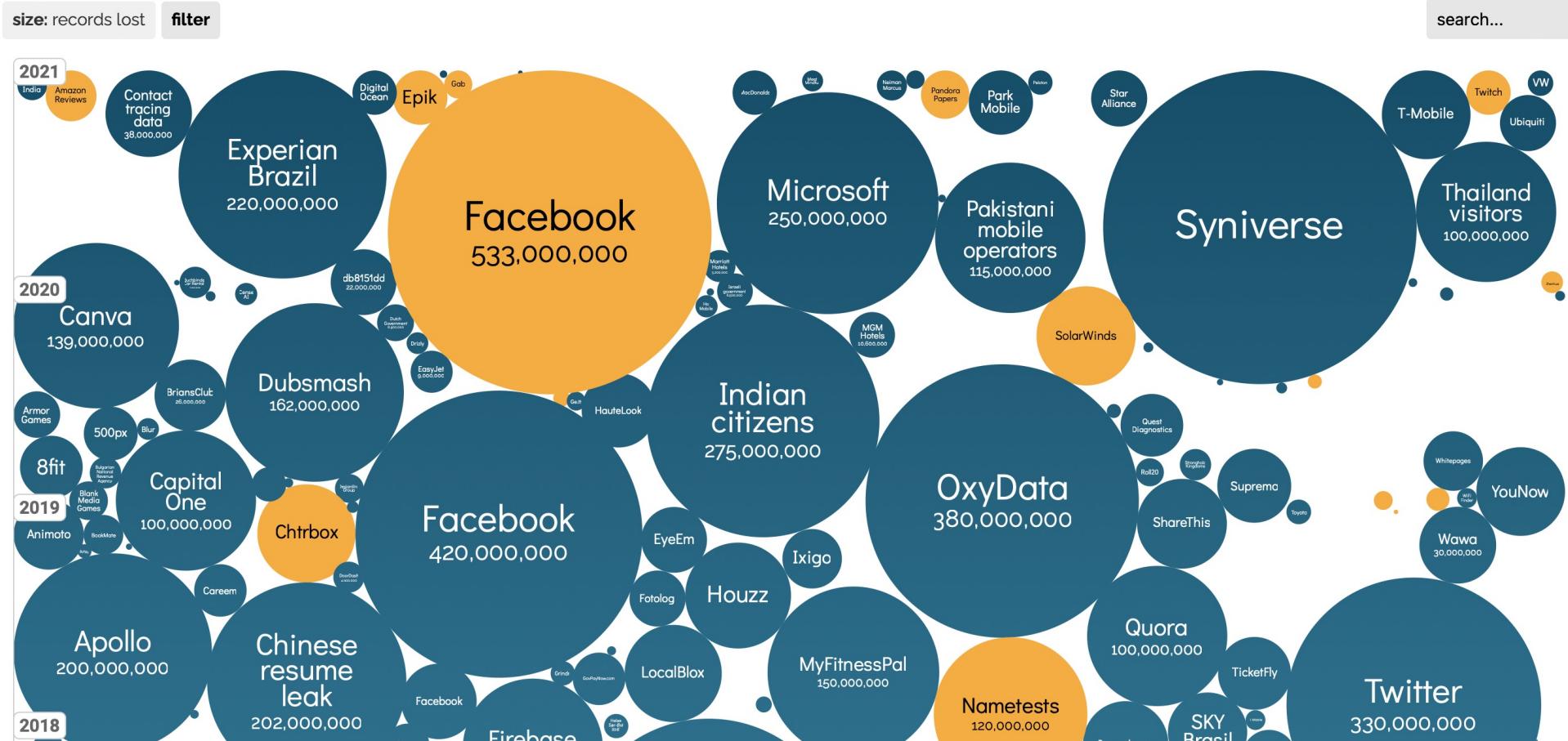


<https://www.helpnetsecurity.com/2020/02/11/2019-reported-breaches/>

# Proteção de dados pessoais – Histórico

Selected events over 30,000 records  
UPDATED: Oct 2021

<http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>



# Regulamento Geral de Proteção de Dados (RGPD)

- Regulamento UE 2016/679 – Regulamento Geral de Proteção de Dados (RGPD)
- A sua aplicação entrou “em vigor” a 25/Maio/2018.
- Substitui a atual “Lei de Proteção de Dados Pessoais”, introduzindo mudanças significativas.
- As empresas (e organizações públicas e privadas) passam a ser responsáveis pela proteção de dados pessoais à sua guarda, pelo que terão de tomar medidas para ficar em conformidade com a Lei, sob pena de pesadas multas.
- Tem reflexos nas empresas, independentemente da sua área de negócio ou dimensão, que vão ter **impacto no desenvolvimento de software**.



# Regulamento Geral de Proteção de Dados (RGPD)

## Sanções por incumprimento

- Podem chegar aos 20 milhões de euros para grandes empresas (ou até 4% da faturação anual mundial do exercício financeiro anterior, o que for maior), por incumprimento do RGPD.
- Adicionalmente, as empresas podem ser responsabilizadas e penalizadas por eventuais danos causados pela indevida aplicação do RGPD, podendo ser condenadas a indemnizar os cidadãos afetados, seja por danos materiais ou imateriais.

**Google fined €50 million for GDPR violation in France**

*The CNIL said Google's data consent policies aren't easily accessible or transparent*

By Jon Porter | @JonPorty | Jan 21, 2019, 11:16am EST

**HOSPITAL DO BARREIRO FINED BY COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS IN 400,000 EURO FOR ALLOWING IMPROPER ACCESS TO CLINICAL FILES**

INDUSTRIAL PROPERTY

Published by Sónia Queiróz Vaz / 30 October, 2018

**UK's ICO fines British Airways a record £183M over GDPR breach that leaked data from 500,000 users**

Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach

# Regulamento Geral de Proteção de Dados (RGPD)

## Objetivo do RGPD

- Objetivo de **garantir** aos cidadãos maior **segurança**, em termos dos seus **dados pessoais**, no âmbito da globalização e das evoluções tecnológicas verificadas nos tempos mais recentes.
  - Obriga a vigilância mais apertada quanto à **origem, armazenamento, tratamento e acesso** a dados pessoais.
- Objetivo de harmonizar as normas e procedimentos relativamente à informação preservada pelas empresas em todos os Estados-membro da União Europeia (UE).
  - Tem também implicações nas empresas fora da UE, que prestem serviços ou vendam bens a cidadãos residentes na UE.

# Regulamento Geral de Proteção de Dados (RGPD)

## Âmbito de aplicação do RGPD

- **Tratamento de dados pessoais de cidadãos da UE:**
  - Independente de onde more ou da nacionalidade do cidadão;
  - Que estejam preservados em ficheiros e que sejam tratados, de forma manual ou automática, no âmbito
    - da actividade de uma empresa,
    - das tarefas de um responsável dessa empresa ou
    - de um sub-contratado ("Data Processor") pela mesma,
  - Em que o tratamento é feito dentro ou fora da UE.

# Regulamento Geral de Proteção de Dados (RGPD)

- O que engloba os **dados pessoais** a serem protegidos?
  - Qualquer **informação relativa a uma pessoa singular que possa ser utilizada para identificar diretamente ou indiretamente o titular dessa informação.**
  - Pode ser, entre outros, nome, foto, endereço de e-mail, número de telefone, dados bancários, mensagens (em sites de redes sociais ou outras), informações médicas ou, endereço IP de computador. (fonte: [www.eugdpr.org](http://www.eugdpr.org))



# GDPR – Direitos do titular dos dados

- **Notificação de violação de dados pessoais** (violação da segurança que provoque, de modo accidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento)
  - Comunicação, sem demora, ao titular dos dados;
  - Comunicação à autoridade de controlo (CNPD), no prazo de 72 horas.
- **Direito de acesso**
  - O titular dos dados tem o direito de obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe dizem respeito estão ou não a ser objeto de tratamento, onde e com que objetivo.
  - Adicionalmente, a pedido do titular dos dados, o responsável pelo tratamento deve fornecer uma cópia dos dados pessoais objeto de tratamento, gratuitamente, de forma eletrónica.
- **Direito de retificação**
  - O titular dos dados tem o direito de obter a retificação dos dados pessoais inexatos que lhe digam respeito.

# GDPR – Direitos do titular dos dados

- **Direito a ser esquecido**

- O titular dos dados tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais.
- Excepções relacionadas com obrigações legais e/ou o interesse público e/ou a saúde pública.

- **Direito de oposição**

- O titular dos dados tem o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito.

- **Direito de portabilidade**

- Objetivo é facilitar a transmissão de dados pessoais entre prestadores de serviços,
- Deve implicar a implementação de medidas para permitir o *download* direto desses dados.

# Regulamento Geral de Proteção de Dados (RGPD)

## O que fazer para cumprir com o RGPD?

- Sistema de Registo de Dados
  - O RGPD determina que todos as ações de tratamento dos dados sejam registadas, de forma detalhada, num ou mais dos seguintes casos:
    - empresas que tenham mais de 250 trabalhadores;
    - se esse tratamento implicar riscos para os titulares dos dados;
    - se não for um tratamento ocasional;
    - se os dados forem sobre condenações ou infrações.
  - Esses registos devem incluir:
    - toda a informação sobre o processo onde são recolhidos,
    - nomes do responsável pelo tratamento e do encarregado de proteção de dados (DPO – *Data Protection Officer*),
    - finalidade do tratamento,
    - categoria de dados (quanto ao risco de proteção e conservação),
    - destinatários dos dados (com quem são partilhados).



# Regulamento Geral de Proteção de Dados (RGPD)

## O que fazer para cumprir com o RGPD?

- Consentimento do titular dos dados para o tratamento dos mesmos
  - Feito de forma clara,
  - Por via oral ou escrita,
  - Com conhecimento informado do titular dos dados, do tratamento que os dados pessoais irão ter.

# Regulamento Geral de Proteção de Dados (RGPD)

## O que fazer para cumprir com o RGPD?

- Encarregado de Proteção de Dados (DPO – *Data Protection Officer*)
  - Empresas podem ter necessidade de uma pessoa com a função de DPO;
  - Visa centralizar todas as questões relacionadas com o RGPD;
  - É obrigatória para:
    - Entidades públicas (excepto tribunais);
    - Atividades onde haja um controle sistemático e frequente dos titulares dos dados e em larga escala (e.g., empresas de telecomunicações, bancos);
    - Casos de tratamento de dados especiais, como genéticos, biométricos e de saúde, ou ainda de condenações penais e infrações.



# Regulamento Geral de Proteção de Dados (RGPD)

## O que fazer para cumprir com o RGPD?

- “Princípio de Risco”
  - Ter sempre em conta que o Regulamento adopta o “princípio de risco” para o tratamento de dados pessoais e livre circulação desses dados.
- “*Privacy by Design*”
  - Empresas têm de adoptar medidas internas, técnicas e organizacionais, que definam, de forma transparente e criteriosa, todo o processo de tratamento dos dados pessoais “desde a concepção”.
- “*Data Minimization*”
  - Empresas têm de assegurar, por via de procedimentos técnicos claros, que só registam e tratam os dados pessoais estritamente necessários para cada fim estipulado;
  - Abrange a quantidade dos dados, a forma do seu tratamento, o prazo de conservação e o acesso a esses mesmos dados.



# “Princípio de risco” no Regulamento

- O Regulamento adopta o “**princípio de risco**” para o tratamento de dados pessoais e livre circulação desses dados, e tem duas abordagens diferentes do conceito:
  - Vê o **risko** para os direitos e liberdades das pessoas singulares **como um continuum** e, espera que as empresas façam mais à medida que o processamento de dados pessoais aumenta a possibilidade de danos para o titular desses dados;
  - Divide o **risko** para os direitos e liberdades das pessoas singulares em **dois escalões**, "risko" e "risko elevado", que desencadeiam obrigações distintas.
- O "**princípio de risco**" (“*risk principle*”) baseia-se na ideia de que:
  - As organizações que processam e utilizam dados pessoais devem **dedicar mais recursos às actividades que levantam as ameaças mais significativas**, e
  - A lei deve **promover uma abordagem diferenciada** em vez de impor uma regulação única.

# Proteção de dados desde a conceção (*Privacy by Design*)

- ***Privacy by Design*** (PbD) é um conceito existente há cerca de 20 anos;
- Conjunto de princípios bem intencionados, para que a segurança e privacidade dos dados dos consumidores seja levada mais a sério;
- Fornece diretrizes e práticas relativas ao acesso dos consumidores aos seus dados;
- Defende políticas de privacidade abertas e transparentes;
- Resume os conselhos gerais sobre segurança de dados numa palavra: minimizar
  - **Minimizar** os dados recolhidos, **minimizar** com quem partilha os dados, **minimizar** quem tem acesso aos dados (apenas a quem tem direito de os conhecer, i.e., existe um objetivo de negócio para aceder aos dados), **minimizar** o tempo que guarda os dados. **Menos é mais**: menos dados para o *hacker* aceder, significa um ambiente mais seguro.

# Proteção de dados desde a conceção (*Privacy by Design*) – Princípios

## 1. Proactivo e não Reativo; Preventivo e não Reparador

- Pensar sobre privacidade dos dados no início do processo de planeamento da segurança de dados – não após uma violação de dados.
- *Always be thinking privacy* (ABTP)!

## 2. Privacidade/Proteção de dados por defeito

- Tem por base dar aos consumidores a máxima proteção à sua privacidade. Por exemplo, consentimento explícito, salvaguardas para proteger dados, acesso restrito, minimizar dados recolhidos, políticas de retenção de dados bem definidas.
- Reduz o perfil de risco de segurança dos dados: quanto menos dados tiver, menor é o dano provocado por uma violação de dados.
- Princípio mais complicado para as empresas

## 3. Privacidade incorporada na concepção (*design*)

- Privacidade é incorporada na concepção de sistemas de TI e nas práticas do negócio.
- Ou seja, técnicas de segurança de dados, como criptografia e autenticação, assim como testes de vulnerabilidades e outras tecnologias para garantir a privacidade, são uma característica central do produto.

# Proteção de dados desde a conceção (*Privacy by Design*) – Princípios

## 4. Segurança ponto a ponto – proteção completa do ciclo de vida

- Proteções da privacidade seguem os dados, nos vários estados.
- Princípios PbD aplicam-se quando os dados são criados, partilhados com outros e, arquivados.
- Técnicas de criptografia e autenticação apropriadas devem proteger os dados desde a criação até que sejam apagados.

## 5. Visibilidade e transparência – Aberta

- Princípio cujo objetivo é construir a confiança com os consumidores.
- Informação sobre as práticas de privacidade devem estar publicadas e escritas em linguagem comum (não em legalês).

## 6. Respeito pela privacidade do titular dos dados

- O titular dos dados é dono dos dados.
- Os dados recolhidos devem ser precisos, e o titular deve ter o poder de fazer correções.
- O titular é o único que pode conceder e revogar o consentimento na utilização dos dados.

# Proteção de dados desde a conceção (*Privacy by Design*) – GDPR

- Com a GDPR, a PbD passou a ser **lei** para quem fizer negócios na EU.
  - “[...] o responsável pelo tratamento aplica [...] as medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento [...] .”
  - “O responsável pelo tratamento aplica medidas técnicas e organizativas para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento. Essa obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade.”  
(artigo 25º, Proteção de dados desde a concepção e por defeito)

**No que se refere aos dados pessoais, limitar e minimizar é agora lei na EU.**

# Regulamento Geral de Proteção de Dados (RGPD)

## O que fazer para cumprir com o RGPD?

- Requisitos técnicos previstos
  - Pseudonimização (substituir campos de identificação por identificadores artificiais) e a cifragem (ou codificação) dos dados pessoais;
  - Garantia da confidencialidade, integridade, disponibilidade e resiliência permanentes das infraestruturas tecnológicas e dos serviços de tratamento;
  - Restabelecimento atempado dos dados em caso de incidentes físicos ou técnicos;
  - Realização de Avaliações de Impacto de Protecção de Dados (DPIAs), nos casos de dados de "risco elevado".

# Avaliação de impacto sobre a proteção de dados

*“Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais.”* in Artigo 35º do Regulamento

- A avaliação de impacto sobre a proteção de dados (AIPD ou DPIA - *Data Protection Impact Assessment*) é um **processo sistemático** para avaliar os riscos de privacidade para as pessoas singulares na obtenção, utilização e divulgação dos seus dados pessoais.
- O Regulamento introduz a AIPD como um **meio para identificar os “riscos elevados”** para os direitos de privacidade das pessoas singulares, no processamento dos seus dados pessoais.
- Quando esses “riscos elevados” são identificados, o Regulamento espera que o processador **aplique medidas que permitam reduzir os riscos** para os titulares desses dados e que ajude o processador a cumprir as suas obrigações de proteção de dados.
- Essas medidas podem assumir, entre outras, a forma de controlos técnicos, tais como a encriptação, a pseudonimização ou a anonimização dos dados.



# Cifragem e pseudonimização dos dados pessoais - GDPR

- GDPR é um regulamento que se aplica apenas à proteção dos dados pessoais.
- E se remover esses dados pessoais de todo o conteúdo que a sua empresa guarda?
  - Fica livre do GDPR (e das suas multas),
  - Não tem que implementar os princípios do PbD,
  - A propriedade intelectual da empresa – software, planos de negócio, ... – não são dados pessoais, pelo que não tem que reportar a violação desses dados à autoridade de controlo.
- Contudo, a maioria das empresas não pode simplesmente eliminar os dados pessoais do conteúdo guardado ...

# Cifragem dos dados pessoais - GDPR

- A **cifragem** é uma maneira de lidar com o conteúdo que contém dados pessoais e diminuir algumas das obrigações do GDPR.
- Ao abrigo do GDPR, a cifragem de dados proporciona alguns benefícios:
  - É explicitamente mencionada como uma forma legítima de abordar a segurança do processamento de dados pessoais - um dos principais requisitos da lei;
  - Os dados podem ser processados para um fim diferente daquele para que foram recolhidos;
  - Adicionalmente, as empresas que cifram os dados pessoais não têm de notificar os titulares dos dados em caso de violação dos mesmos (teriam porém de notificar a autoridade de controlo).

# Cifragem dos dados pessoais

- Para cifrar os dados,
  - Escolher o tipo de cifra – simétrica ou assimétrica
  - Escolher o tamanho da chave – depende do período de tempo durante o qual os dados forem guardados

Primitive	Classification	
	Legacy	Future
AES	✓	✓
Camellia	✓	✓
Three-Key-3DES	✓	✗
Two-Key-3DES	✓	✗
Kasumi	✓	✗
Blowfish $\geq$ 80-bit keys	✓	✗
DES	✗	✗

Scheme	Classification		See t
	Legacy	Future	
Public Key Encryption,			
RSA-OAEP	✓	✓	See t
RSA-KEM	✓	✓	See t
PSEC-KEM	✓	✓	See t
ECIES-KEM	✓	✓	See t
RSA-PKCS# 1 v1.5	✗	✗	

Fonte: ENISA Algorithms, key size and parameters report

# Cifragem dos dados pessoais

- Para cifrar os dados,
  - Escolher o tipo de cifra – simétrica ou assimétrica
  - Escolher o tamanho da chave – depende do período de tempo durante o qual os dados forem guardados
  - Decidir se o modo de cifrar/decifrar dados será por hardware (HSM) ou software (SSM)
  - Alterar toda as plataformas informáticas, de modo a cifrarem os dados pessoais e, decifrarem sempre que alguém (com as permissões devidas) o peça.

# Cifragem dos dados pessoais

- Quem pode aceder aos dados pessoais cifrados?
- Para aceder aos dados pessoais cifrados, é necessário acesso à chave de decifra (ou ter autorização para pedir ao HSM/SSM para decifrar os dados).
- Necessidade de implementar um política de controlo de acesso à chave de decifra.

**A cifragem não é o melhor método para proteger todos os dados pessoais.**



# Pseudonimização dos dados pessoais - GDPR

- **Pseudonimização** = substituir dados pessoais por códigos, por exemplo através da adição de uma tabela mestra com relação dados – códigos.
- A pseudonimização é uma técnica para codificar dados pessoais e diminuir algumas das obrigações do GDPR.
- Ao abrigo do GDPR, a pseudonimização de dados proporciona alguns benefícios:
  - É explicitamente mencionada como uma forma legítima de abordar a segurança do processamento de dados pessoais - um dos principais requisitos da lei;
  - É mencionada como sendo a técnica a utilizar para processar dados pessoais para fins científicos, históricos e estatísticos;
  - É explicitamente mencionada como uma técnica de PbD;
  - É também considerada como uma técnica para minimizar dados pessoais – muito importante no GDPR;
  - Os dados podem ser processados para um fim diferente daquele para que foram recolhidos;
  - Se não for possível identificar a pessoa a partir dos seus dados pessoais, não é necessário garantir os direitos de acesso, retificação, oposição e, ser esquecido;
  - Adicionalmente, também não têm que necessariamente notificar os titulares dos dados em caso de violação dos dados pessoais pseudonimizados (teriam porém de notificar a autoridade de controlo), desde que a partir dessa informação não seja possível identificar a pessoa.



# Pseudonimização dos dados pessoais

- Exemplo simples – todos os dados pessoais são substituídos por códigos, com uma estrutura nos códigos refletida na tabela mestra.

**Substituição**

+351123456789	#3.3
jose.miranda@devisefutures.com	#2.2
José Miranda	#2.1
204.23.76.98	#3.6
A XPTO realiza a conferência "Novo Quadro Regulamentar sobre Dados Pessoais" no dia 1 de Fevereiro	#5.7

**Tabela mestra**

#1	{1: 'João Silva', 2: 'js@gmail.com', 3: '333444666'}
#2	{1: 'José Miranda', 2: 'jose.miranda@devisefutures.com'}
#3	{1: 'Ana Teixeira', 2: 'ateixeira@mail.pt', 3: '+351123456789'}
#4	...
#5	...

# Pseudonimização dos dados pessoais

- Exemplo avançado – os dados pessoais são substituídos por resumos criptográficos (por exemplo Hash – SHA256 –), sem necessidade de tabelas adicionais.
  - Note-se que a partir de um Hash não é possível obter os dados originais, mas  $\text{hash}(a) == \text{hash}(b)$  se e só se  $a == b$

João Silva, js@gmail.com, 333444666	c66337b130a60774fb8c64e5026bc 27e0ee7c188b1bc965b7dd623696 7bbd314
José Miranda, jose.miranda@devisefutures.com, +351123456789	cff7f6dc577f22a421e9d69f7e7c099 a6449226ff7e1a0ae95a0ca30c946a f1b
Ana Teixeira, ateixeira@mail.pt, +351978654345	078ed5ecb63ef7ebade099c9322a 4c908ea7da7c3632a74a4376132aa 6e9561

# Cifragem e pseudonimização dos dados pessoais - GDPR

- GDPR encoraja a pseudonimização dos dados pessoais.
- Cifragem dos dados pessoais tem também a sua aplicação (por exemplo, cifrar mensagens com uma chave só conhecida pelo titular dos dados)

**Necessário analisar para chegar ao melhor mix de técnicas de cifragem e pseudonimização, de modo a obter os maiores benefícios do GDPR.**



# Regulamento Geral de Proteção de Dados (RGPD)

## O que fazer?

- Transferências transfronteiriças de dados
  - RGPD também se aplica às empresas que não integram a UE, sempre que estejam em causa dados pessoais alusivos a cidadãos que residem no espaço comunitário europeu.
  - Responsabilidade dessa aplicação é tanto dos responsáveis pelo tratamento dos dados, como dos sub-contratantes.



# Regulamento Geral de Proteção de Dados (RGPD)

- As empresas têm de adaptar os seus produtos (aplicações, apps, sites, ...) que tratam dados pessoais para estarem de acordo com o regulamento RGPD relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.
- Foco para a “Engenharia de Segurança”:
  - **Proteção de dados desde a conceção** (do produto);
  - **Proteção de dados por defeito;**
  - **Cifragem e pseudonimização dos dados pessoais.**



# Regulamento Geral de Proteção de Dados (RGPD)

## Síntese final

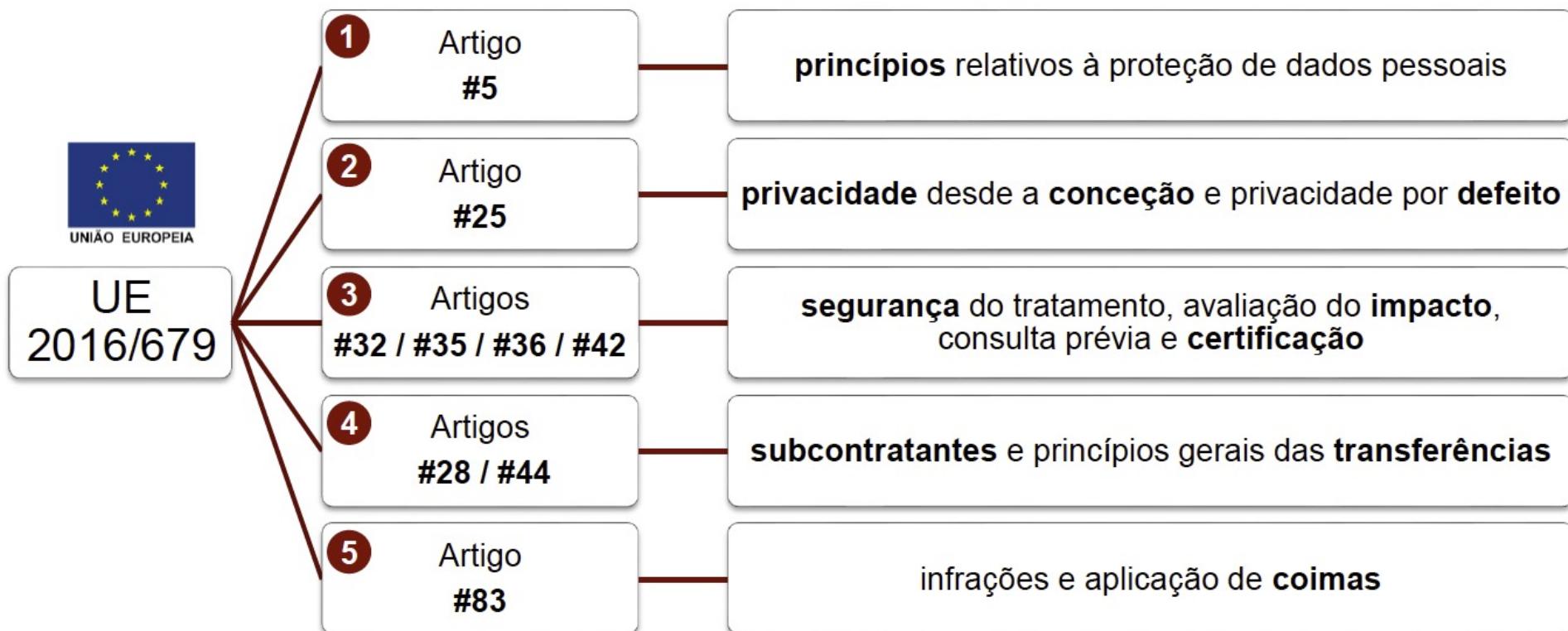


Imagen: Critical Software



# Regulamento Geral de Proteção de Dados (RGPD)

## Síntese final

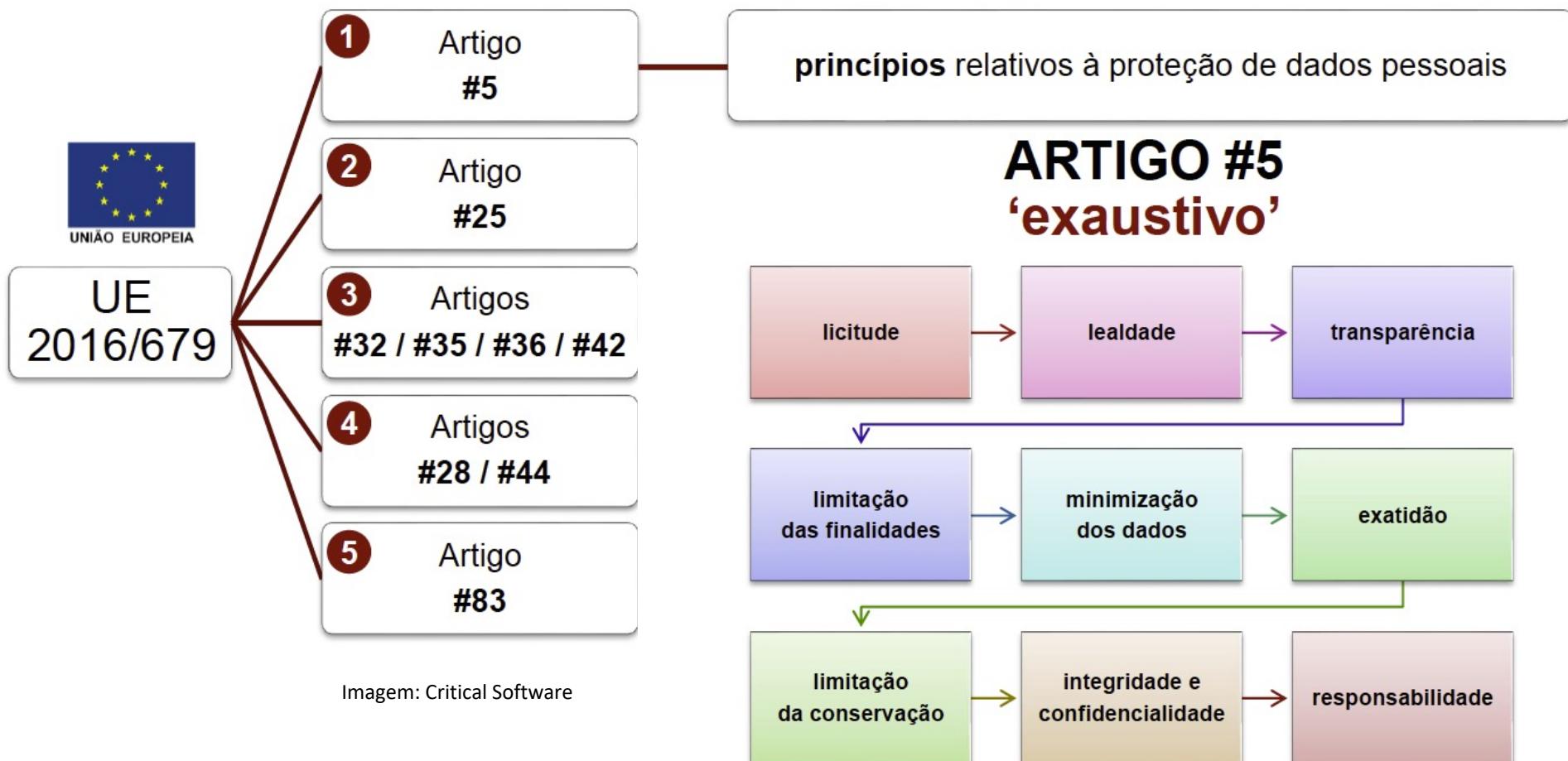


Imagen: Critical Software

# Regulamento Geral de Proteção de Dados (RGPD)

## Síntese final



# Regulamento Geral de Proteção de Dados (RGPD)

## Síntese final



UE  
2016/679

- 1 Artigo #5
- 2 Artigo #25
- 3 Artigos #32 / #35 / #36 / #42
- 4 Artigos #28 / #44
- 5 Artigo #83

## ARTIGOS #32 / #35 / #36 / #42 'auditável'

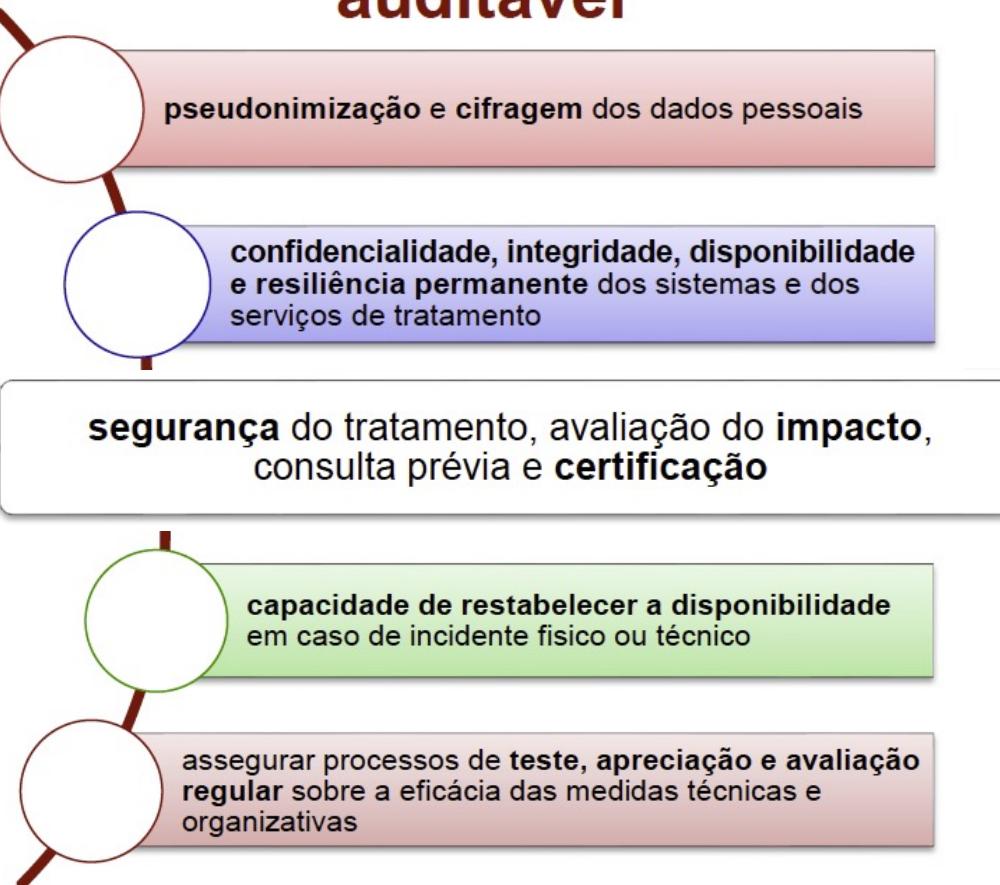


Imagen: Critical Software

# Regulamento Geral de Proteção de Dados (RGPD)

## Síntese final

### ARTIGOS #28 / #44 'extensível'

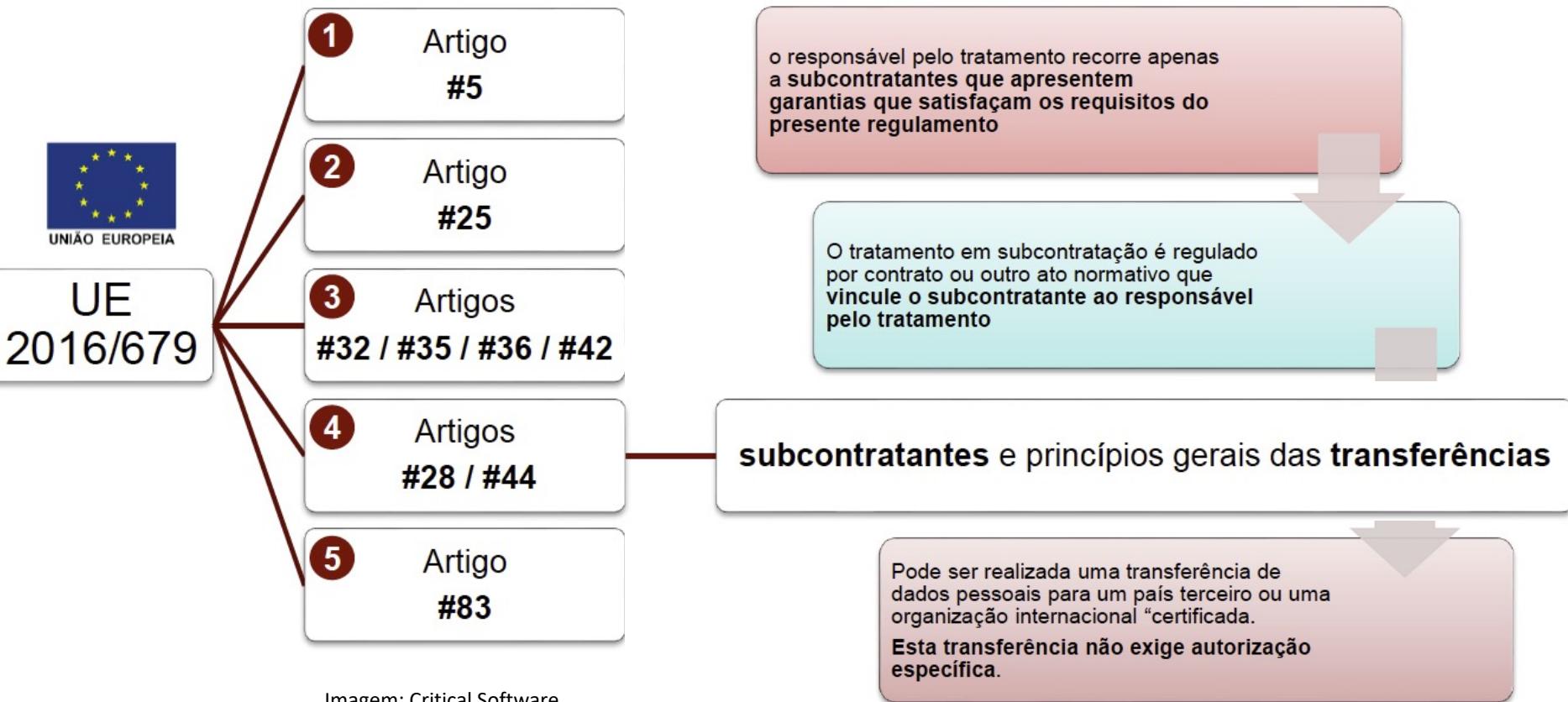


Imagen: Critical Software

# Regulamento Geral de Proteção de Dados (RGPD)

## Síntese final

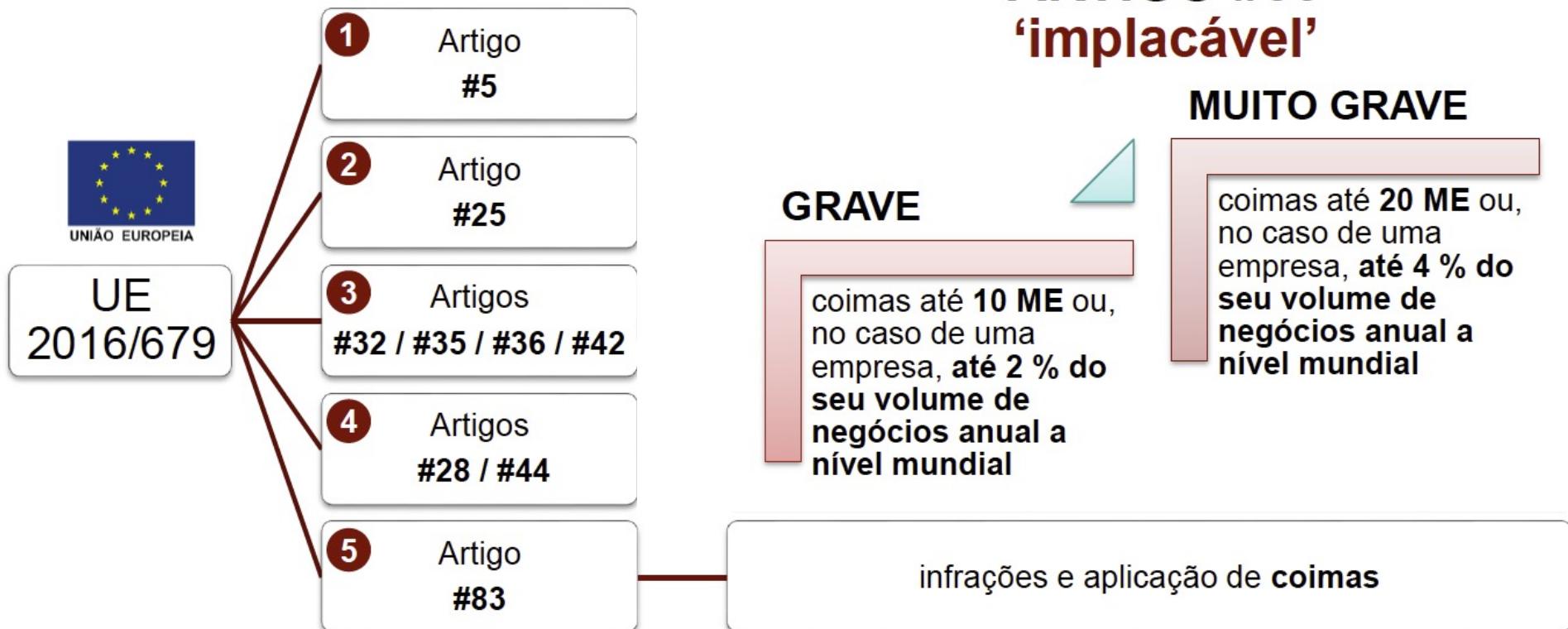


Imagen: Critical Software

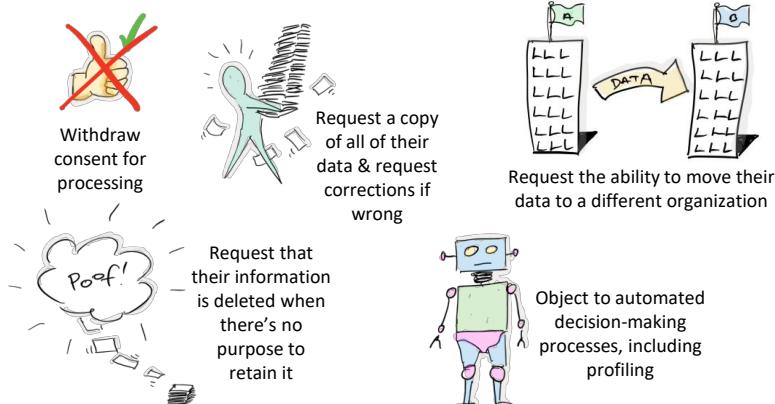
# Regulamento Geral de Proteção de Dados (RGPD)

## High level view of the GDPR

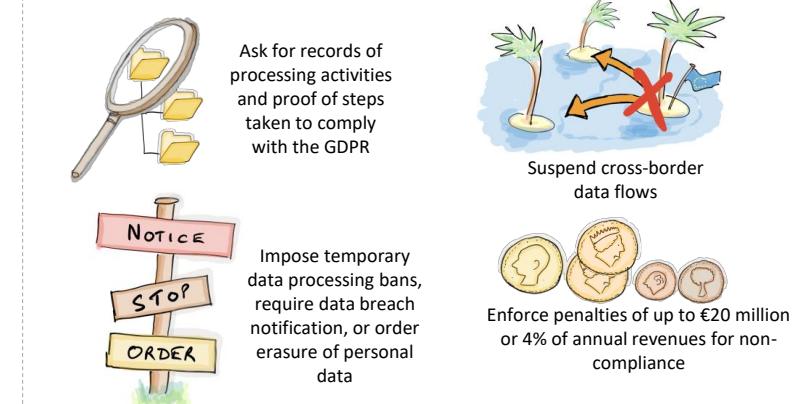
### What organizations have to do



### What individuals can do



### What regulators can do



Inspired by IAPP's GDPR Awareness Guide. Please credit Tim Clements & IAPP if you use this