Master in Computer Engineering (MEI)
Integrated Master in Informatics Engineering (MiEI)

Specialization Profile **CSI**: Cryptography and Information Security

Engenharia de Segurança

Tópicos

- Regulation UE 2016/679 – General Data Protection Regulation (GDPR)

Motivation

- Since 25 May 2018 personal data must be processed in accordance with EU Regulation 2016/679.

Protection of personal data - History

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

Seis funci
dinheiro
que passa

Um esque
clientes d
redes crin
agora des
Lisboa. Se
comercial
telemóvei
detidos p

GOVERNO

Fisc

22/6/2015,

O fisco
justifiqu
limitado

Dois homens detidos por tráfico de milhões de dados pessoais informáticos

As autoridades dos Países Baixos apreenderam equipamentos relacionados com o site www.weleakinfo.com.

Por Lusa
17 Janeiro, 2020 • 23:40

PARTILHAR

Facebook
Twitter
WhatsApp
E-mail
Comentar

O site www.weleakinfo.com agora apresenta uma mensagem na página inicial a referir que aquele domínio foi apreendido pelo FBI

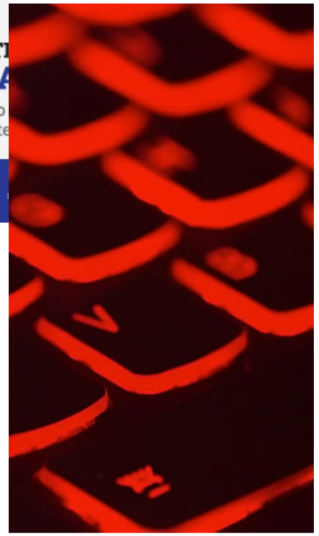
Dois homens foram detidos, nos Países Baixos e na Irlanda do Norte, por tráfico de milhões de dados pessoais informáticos, incluindo palavras-passe de endereços eletrónicos, na sequência de uma investigação internacional, anunciaram esta sexta-feira as autoridades holandesas.

hospedes. A MGM
divulgada. A rede
exatamente quan
duplicadas.

s com 49
nformações

DETETÁMOS QUE PODE T
ADBLOCKER LIGA
Apoie o jornalismo, desative o
ad blocker para o nosso site

OBRIGADO



nação foi protegida com uma

1 2017 e a responsável por ter

A 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.

Over 120 million Decathlon accounts hacked

By Jitendra Soni 18 days ago

Employee and user data leaked due to unsecured server

ata - History

by **Brandon Vigliarolo** in **Security**

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.

(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

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

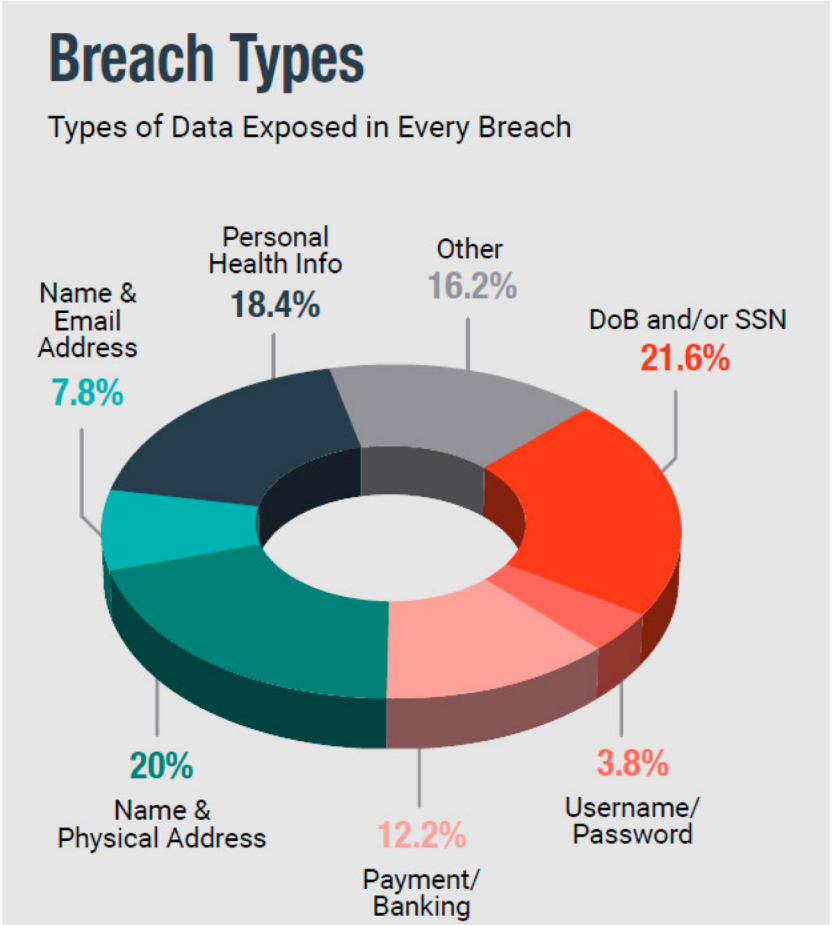
by Avast Blog on March 6, 2020

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.

API logs and API credentials.

Protection of personal data - History

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



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

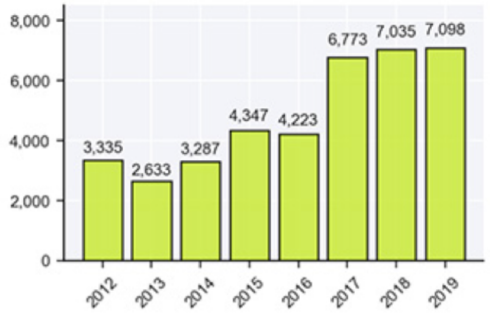


Figure 1: Number of breaches reported each year

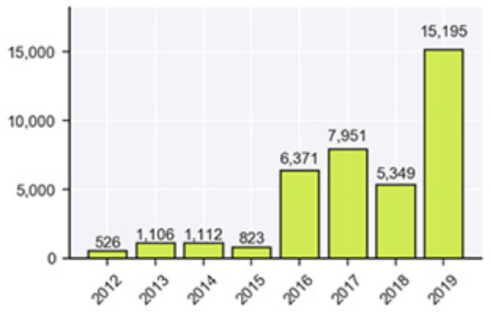
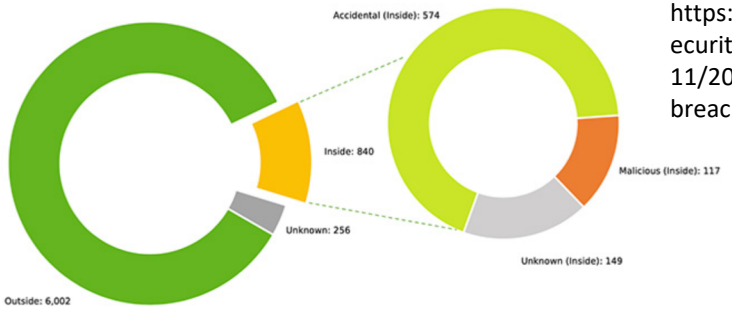


Figure 2: Number of records lost (in millions) each year

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.

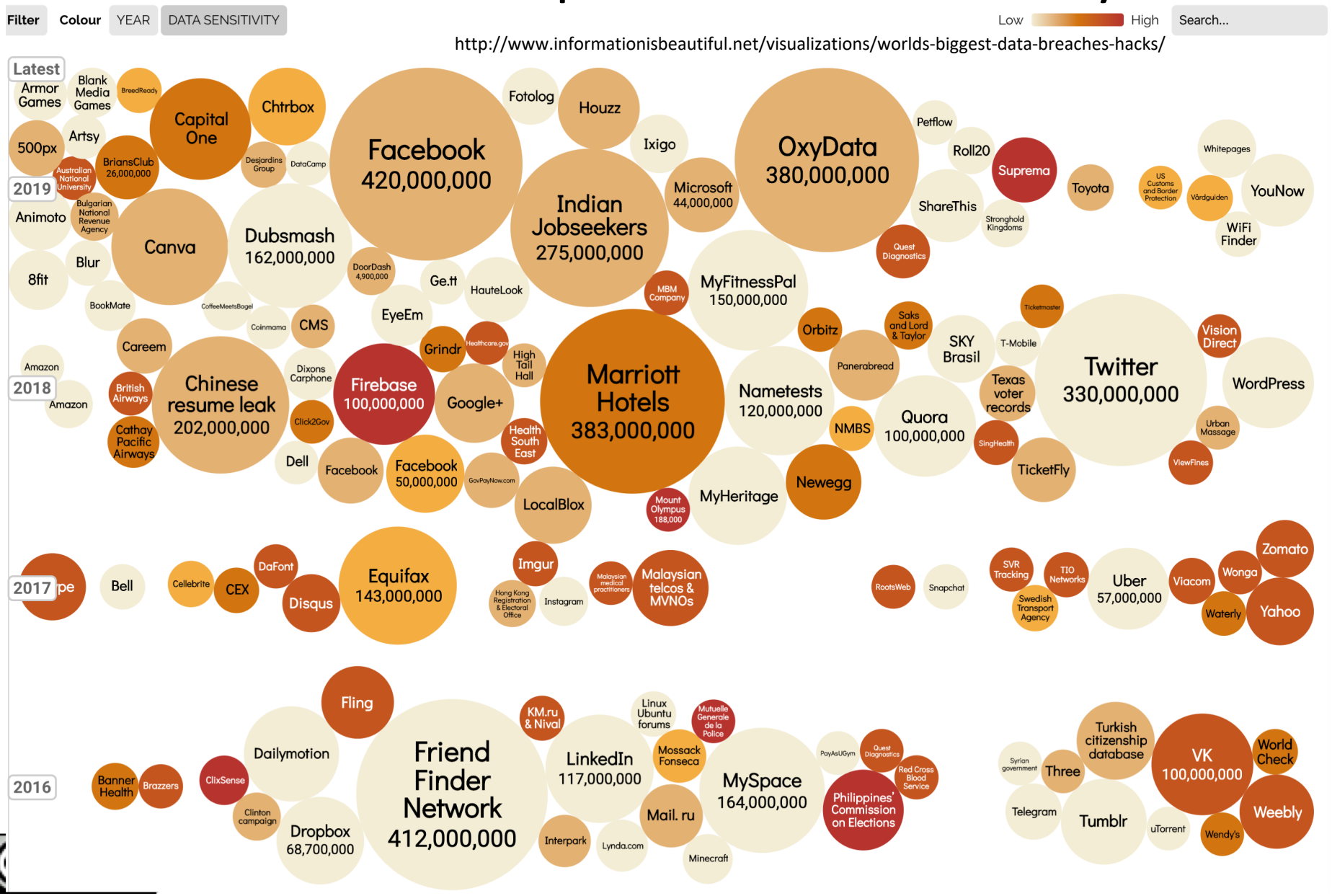
Since the release of the report three months ago, 7.2 billion records were compromised, with only four events accounting for 93.5% of those records. The cause? Open and misconfigured databases that were made publicly accessible to anyone motivated to seek them out.



2019: Number of reported breaches by attack vector

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

Protection of personal data - History



General Data Protection Regulation (GDPR)

- Regulation UE 2016/679 – General Data Protection Regulation (GDPR)
- Its use has entered "into force" on 25 / May / 2018.
- Replaced, in Portugal, the Portuguese Law "Personal Data Protection Act", introducing significant changes.

General Data Protection Regulation (GDPR)

- Regulation UE 2016/679 – General Data Protection Regulation (GDPR)
- Its use has entered "into force" on 25 / May / 2018.
- Replaced, in Portugal, the Portuguese Law "Personal Data Protection Act", introducing significant changes.
- Companies (and public and private organizations) are responsible for the protection of personal data held in their custody, and they will have to take steps to comply with the Regulation, under penalty of heavy fines.
- It has repercussions on companies, regardless of their area of business or size, that will have a major **impact on software development**.

General Data Protection Regulation (GDPR)

GDPR purpose

- Aim to **guarantee** greater **security** to citizens' personal data, in the context of globalization and technological developments.
  - Requires tighter surveillance regarding the **origin**, **storage**, **processing** and **access** to personal data.
- Aim to harmonize standards and procedures with regard to information preserved by companies in all EU Member States.
  - It also has implications for companies outside the EU that provide services or sell goods to citizens residing in the EU.

General Data Protection Regulation (GDPR)

Scope of the GDPR

- **Processing** of EU citizens' **personal data:**
  - Regardless of where the citizen's live or citizen's nationality;
  - Which are preserved in files and which are processed, either manually or automatically, within the
    - company's business,
    - duties of an oficial/employee of the company, or
    - duties of a of a sub-contractor ("Data Processor") of the company,
  - Where the processing is done inside or outside the EU.

General Data Protection Regulation (GDPR)

- What encompasses the **personal data** to be protected?
  - Any **information relating to a natural person** that can be **used to directly or indirectly identify the owner of such information**.
  - It can be, among others, name, photo, email address, phone number, bank details, messages (on social networking sites or other), medical information or computer IP address. (source: www.eugdpr.org)

“Risk Principle” in the GDPR

- The GDPR adopts the "**risk principle**" concept for the processing of personal data and free movement of personal data, and has two different approaches to this concept:
  - Sees the **risk** to the rights and freedoms of natural persons **as a continuum** and expects companies to do more as the processing of personal data increases the possibility of damage to the data subject (owner of such data);
  - Divides the **risk** to the rights and freedoms of natural persons into **two tiers**, "risk" and "high risk", which trigger different obligations.

- The "**risk principle**" is based on the idea that:
  - Organizations that process and use personal data should d**evote more resources to activities that raise the most significant threats**, and
  - Law should **promote a differentiated approach** rather than impose the same approach to diferente levels of risk.

General Data Protection Regulation (GDPR)

Penalties for non-compliance

- Can reach 20 million euros for large companies (or up to 4% of the annual worldwide turnover of the preceding financial year, whichever is greater), due to non-compliance with the GDPR.
- In addition, companies may be liable and penalized for any damages caused by the undue application of the GDPR, and may be convicted to compensate affected citizens, whether for material or immaterial damages.

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

INDUSTRIAL PROPERTY

Publicado por Sónia Queiróz Vaz / 30 October, 2018

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

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

Ingrid Lunden @ingridlunden / 11:35 am WEST • July 8, 2019

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

Date **09 July 2019**

GDPR – Rights of the data subject

- **Notification of personal data breach** (breach of security that causes, accidentally or unlawfully, the unauthorized destruction, loss, modification, disclosure or access to personal data transmitted, stored or otherwise processed)
  - Communication to the data subject without delay;
  - Communication to the supervisory authority within 72 hours.
- **Right of access**
  - The data subject has the right to obtain confirmation from the controller that the personal data concerning him or her are being processed, where and for what purpose.
  - In addition, at the request of the data subject, the controller must provide, free of charge, an electronic copy of the personal data processed.
- **Right of rectification**
  - The data subject has the right to obtain rectification of the inaccurate personal data concerning him.

GDPR – Direitos do titular dos dados

- **Right to be forgotten**
  - The data subject has the right to obtain from the controller the erasure of his or her personal data.
  - Exceptions are related to legal obligations and / or the public interest and / or public health.
- **Right of opposition**
  - The data subject has the right to oppose, at any time, on grounds relating to his particular situation, to the processing of their personal data.
- **Portability right**
  - Aim is to favor the transmission of personal data between service providers,
  - Should involve the implementation of features to allow the direct download of this data.

General Data Protection Regulation (GDPR)

What to do to comply with the GDPR?

- Data Logging System
  - GDPR requires that all data processing actions be recorded in detail in one or more of the following cases:
    - companies with more than 250 employees;
    - if such treatment involves risks to data subjects;
    - if it is not an occasional treatment;
    - if the data is about convictions or infractions.
  - The records shall include:
    - all the information about the process where the personal data is collected,
    - names of the controller and data protection officer (DPO),
    - purpose of processing,
    - category of data (regarding the risk of data protection and preservation),
    - recipients of the data (with whom they are shared).

General Data Protection Regulation (GDPR)

What to do to comply with the GDPR?

- Consent of the data subject for the treatment of their personal data
  - Made in a clear and unambiguous manner,
  - Orally or in writing,
  - With informed knowledge of the processing that their personal data will have.

General Data Protection Regulation (GDPR)

What to do to comply with the GDPR?

- DPO – Data Protection Officer
  - Companies may need a person with the role of DPO;
  - Aims to centralize all issues related to the GDPR;
  - Visa centralizar todas as questões relacionadas com o RGPD;
  - It is mandatory for:
    - Public entities (except courts);
    - Activities where there is systematic and frequent control of data owners and on a large scale (eg, telecommunications companies, banks);
    - Cases of special data processing, such as genetic, biometric and health, or criminal convictions and infractions.

General Data Protection Regulation (GDPR)

What to do to comply with the GDPR?

- *"Privacy by Design"*
  - Companies must adopt internal, technical and organizational measures that define, in a transparent and careful manner, the **procedures of processing personal data** "**from design**".
- "*Data Minimization*"
  - Companies must ensure, through clear technical procedures, that they only record and process the personal data strictly necessary for each stipulated purpose;
  - It covers the quantity, the processing, the storage period and the access to personal data.

Data protection from design (*Privacy by Design*)

- ***Privacy by Design*** (PbD) has been around for more than 20 years;
- Well-intentioned set of principles, so that the security and privacy of consumer data is taken more seriously;
- Provides guidelines and practices regarding consumer access to their data;
- Advocates open and transparent privacy policies;
- Summarize the general advice on data security in one word: **minimize**
  - **Minimize** the data collected, **minimize** with whom the data is shared, **minimize** who has access to the data (only those who have the right to know, i.e., there is a business objective to access the data), **minimize** the time that the data is stored. **Less is more**: less data for the hacker to access, means a more secure environment.

Data protection from design (*Privacy by Design*) – Principles

1. Proactive and not Reactive; Preventive and not Repairing
   - Think about data privacy at the beginning of the data security planning process - not after a data breach.
   - Always be thinking privacy (ABTP)!
2. Privacy / Data Protection by default
   - It is based on giving consumers maximum protection of their privacy. For example, explicit consent, safeguards to protect data, restricted access, minimize collected data, well defined data retention policies.
   - Reduces the security risk profile of data: The less data you have, the less damage is caused by a data breach.
   - More complex for business.
3. Privacy embedded in design
   - Privacy is embedded into the design of IT systems and into business practices.
   - That is, data security techniques, such as encryption and authentication, as well as vulnerability testing and other technologies to ensure privacy, are a central feature of the product.

Data protection from design (*Privacy by Design*) – Principles

4. Point-to-point security - complete lifecycle protection
   - Privacy protection follow the data, in its various status.
   - PbD principles apply when data is created, shared with others, and archived.
   - Appropriate encryption and authentication techniques should protect the data from creation to deletion.
5. Visibility and transparency – Open
   - Principle whose goal is to build trust with consumers.
   - Information about privacy practices must be published and written in common language (not legal).
6. Respect for the privacy of the data subject
   - The data subject is the owner of the data.
   - Data collected must be accurate, and the holder must have the power to make corrections.
   - The data subject is the only one who can grant and revoke consent to use their data.

Data protection from design (*Privacy by Design*) – GDPR

- With GDPR, PbD became the **law** for anyone doing business in the EU.
  - *"[...] the controller shall […] implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data* minimisation*, in an effective manner […]."*
  - *"The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility."*

  (GDPR, Article 25, Data protection by design and by default)

With regard to personal data, restrict and minimize it is now law in the EU.

General Data Protection Regulation (GDPR)

What to do to comply with the GDPR?

- Technical requirements set out in GDPR
  - Pseudonymization (replace identification fields with artificial identifiers) and encryption of personal data;
  - Ensure the continued confidentiality, integrity, availability and resilience of technological infrastructures and processing services;
  - Recover of data in the event of physical or technical incidents;
  - Conduct Data Protection Impact Assessment (DPIA) in cases of "high-risk" data.

Data Protection Impact Assessment

"Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data." in RGPD, Article 35 - Data protection impact assessment

- Data Protection Impact Assessment (DPIA) is a **systematic process** for assessing the privacy risks to natural persons in the collection, use and disclosure of their personal data.
- The Regulation introduces the DPIA as a **means to identify the "high risks"** to the privacy rights of natural persons in the processing of their personal data.
- When these "high risks" are identified, the Regulation expects the processor to **implement measures to reduce the risks** to the data subjects and to help the processor to meet its data protection obligations.
- Such measures may take the form, inter alia, of technical controls, such as encryption, pseudonymization or anonymisation of data.

Encryption and pseudonymization of personal data - GDPR

- GDPR is a regulation that applies only to the protection of personal data.
- What if you remove the personal data from all the content your business stores?
  - It is free from GDPR (and its fines),
  - You do not have to implement the principles of PbD,
  - The intellectual property of the company - software, business plans, ... - are not personal data, so you do not have to report the breach of this data to the supervisory authority.
- However, most companies can not simply delete the personal data from stored content ...

Encryption of personal data - GDPR

- **Encryption** is a way to deal with content that contains personal data and lessen some of GDPR's obligations.
- Under the GDPR, data encryption offers some benefits:
  - It is explicitly mentioned as a legitimate way of addressing the security of personal data processing - one of the main requirements of the law;
  - The data can be processed to a different end than the one for which they were collected;
  - In addition, companies that encrypt personal data do not have to notify data subject in the event of a breach (they would have to notify the supervisory authority).

Encryption of personal data

- To encrypt the data,
  - Choose cipher type - symmetric or asymmetric
  - Choose key size - depends on the period of time the data is stored

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

Scheme	Classification		
	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	✗	✗	

Source: ENISA Algorithms, key size and parameters report

Encryption of personal data

- To encrypt the data,
  - Choose cipher type - symmetric or asymmetric
  - Choose key size - depends on the period of time the data is stored
  - Decide whether the data encryption / decryption will be by hardware (HSM) or software (SSM)
  - Change all computer platforms in order to encrypt personal data, and decipher whenever someone (with the necessary permissions) requires it.

Encryption of personal data

Who can access encrypted personal data?

- To access encrypted personal data, you need access to the decryption key (or have authorization to ask the HSM / SSM to decrypt the data).
- Need to implement a key access control policy.

Encryption is not the best method to protect all personal data.

Pseudonymization of personal data - GDPR

- **Pseudonymization** = replace personal data by codes, for example by adding a master table with data - codes.
- Pseudonymization is a technique for coding personal data and reducing some of the GDPR obligations.
- Under the GDPR, the pseudonymization of data offers some benefits:
  - It is explicitly mentioned as a legitimate way of addressing the security of personal data processing - one of the main requirements of the law;
  - It is mentioned as being the technique to be used to process personal data for scientific, historical and statistical purposes;
  - It is explicitly mentioned as a PbD technique;
  - It is also considered as a technique to minimize personal data - very important in GDPR;
  - The data can be processed to a different end than the one for which they were collected;
  - If it is not possible to identify the person from their personal data, it is not necessary to guarantee the rights of access, rectification, opposition and, be forgotten;
  - In addition, processors do not necessarily have to notify data subjects in the event of a breach of the pseudonymised personal data (they would however have to notify the supervisory authority), provided that from that data it is not possible to identify the person.

Pseudonymization of personal data

- Simple example - all personal data are replaced by codes, with a structure in the codes reflected in the master table.

+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

#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	…

Pseudonymization of personal data

- Advanced example - personal data is replaced by cryptographic summaries (eg Hash - SHA256 -), with no additional tables required.
  - Note that from a hash it is not possible to obtain the original data, but hash (a) == hash (b) if and only if a == b

João Silva, js@gmail.com, 333444666	c66337b130a60774fb8c64e5026bc27e0ee7c188b1bc965b7dd6236967bbd314
José Miranda, jose.miranda@devisefutures.com, +351123456789	cff7f6dc577f22a421e9d69f7e7c099a6449226ff7e1a0ae95a0ca30c946af1b
Ana Teixeira, ateixeira@mail.pt, +351978654345	078ed5ecb63ef7ebbade099c9322a4c908ea7da7c3632a74a4376132aa6e9561

Encryption and pseudonymization of personal data - GDPR

- GDPR encourages the pseudonymisation of personal data.
- Encryption of personal data also has its application (for example, encrypt messages with a key only known by the data holder)

It is necessary to analyze the personal data to be processed and the business requirements, to choose the best mix of encryption and pseudonymization techniques, in order to obtain the greatest benefits of GDPR.

General Data Protection Regulation (GDPR)

- Cross-border data transfers
  - GDPR also applies to non-EU companies, where personal data referring to citizens residing in the European Community area are concerned.
  - Responsibility for the processing is for both the data controllers and the sub-contractors.

General Data Protection Regulation (GDPR)

- Companies have to adapt their products (applications, apps, websites, ...) which process personal data in order to comply with the GDPR with regard to the processing of **personal data** and the free movement of personal data.
- Focus to ”Security Engineering”/“Engenharia de Segurança”:
  - **Protection of personal data since design** (of the software product)**;**
  - **Personal data protection by default;**
  - **Encryption and pseudonymization of personal data.**

General Data Protection Regulation (GDPR)

High level view of the GDPR

What organizations have to do


Keep records of all processing of personal information


Institute safeguards for cross-border data transfers

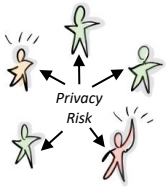

Maintain appropriate data security


Collect personal data lawfully and fairly, and where relevant, get appropriate consent and provide notification of personal data processing activities


Get a parent's consent to collect data for children under 16


Consult with regulators before certain processing activities

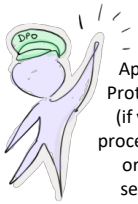

Provide appropriate data protection training to personnel having permanent or regular access to personal data



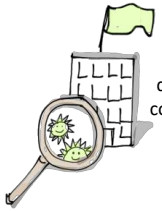
Conduct Data Protection Impact Assessments on new processing activities

Implement Data Protection-by-Design *(Privacy "baked-in")*


Take responsibility for the security and processing activities of third-party vendors



Appoint a Data Protection Officer (if you regularly process lots of data, or particularly sensitive data)

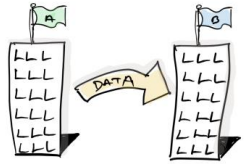

Be able to demonstrate compliance on demand


Notify data protection agencies and affected individuals of data breaches in certain circumstances

What individuals can do

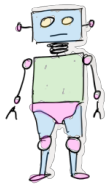

Withdraw consent for processing


Request a copy of all of their data & request corrections if wrong

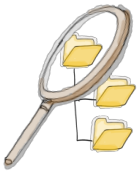


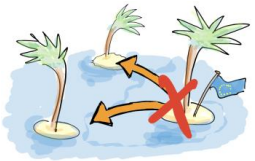
Request the ability to move their data to a different organization

Request that their information is deleted when there's no purpose to retain it


Object to automated decision-making processes, including profiling

What regulators can do


Ask for records of processing activities and proof of steps taken to comply with the GDPR


Suspend cross-border data flows

Impose temporary data processing bans, require data breach notification, or order erasure of personal data


Enforce penalties of up to €20 million or 4% of annual revenues for non-compliance

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