ORDINA

# INFORMATION SECURITY AWARENESS & GDPR

TOM DEGOL & JELLE DAUWE

HOGESCHOOL PXL

# WHO ARE WE?

## Security & Privacy Consultants

Tom obtained both a Bachelor of Applied Information Technology and a Master of Business Information Management. Additionally, he also achieved the ISO 27001 Lead Implementer, ITIL service management and Prince2 project management certificates. Through his combination of knowledge from both the Business and IT world, supplemented with his communicative and organizational skills, he is always able to develop a pragmatic approach tailored to the needs and wishes of the client. Tom therefore has a strong focus on bringing together Information Security with day-to-day operations and their related processes.

Jelle is a Security Consultant with a passion for Security and Privacy. His interest for both themes, and especially the combination of the two, was discovered during his Bachelor education Information Management & Security. This education was the right way for entering the world of Security and Privacy. For his bachelor thesis Jelle researched the various risks concerning the processing of personal data. This is elaborated through various audits at an organization that incorporates the processing of personal data into its business plan.

ORDINA


Introduction

# ONLINE DANGERS

## Identity theft

- Identity theft
- Access to assets
  - Financial
  - Purchases
  - Crimes
- This information can be accessed freely on **social media**!

# ONLINE DANGERS

## Advertisements


- Purchase behavior
- Price inflation
- Misleading ads
- Tracking
- Targeted ads
- Profiling

# ONLINE DANGERS

- Ghost Accounts

- Friend's group
- Collected information
- Identity analyses
- Predictions and suggestions
- Tracking
- **NO Facebook member!**

# ONLINE DANGERS

Cambridge Analytica

# ONLINE DANGERS

## Cambridge Analytica

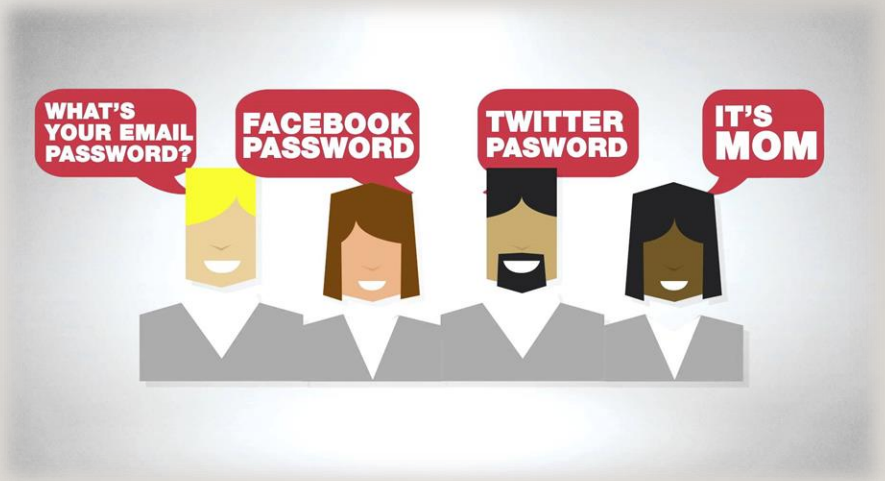
- Social media
- Influence elections
- Facebook likes
- Smartphone data
- Profiling
- Cambridge analytica

# THREAT MAP


ORDINA

# WHAT ABOUT YOUR *"HACKERS MIND"*?

- Social Engineering
- 
- ';--have i been pwned?
- https://haveibeenpwned.com/



# BE CAREFUL!

Who uses their passwords more than once?

# BE CAREFUL!

Who hasn't changed their password in over a year?

# BE CAREFUL!

Who stores their passwords somewhere?

# BE CAREFUL!

Who has a password shorter than eight characters?

# WHAT ABOUT PASSWORDS

1. **123456** (Unchanged)
2. **Password** (Unchanged)
3. **12345678** (Up 1)
4. **qwerty** (Up 2)
5. **12345** (Down 2)
6. **123456789** (New)
7. **letmein** (New)
8. **1234567** (Unchanged)
9. **football** (Down 4)
10. **iloveyou** (New)
11. **admin** (Up 4)
12. **welcome** (Unchanged)
13. **monkey** (New)
14. **login** (Down 3)
15. **abc123** (Down 1)
16. **starwars** (New)
17. **123123** (New)
18. **dragon** (Up 1)
19. **passw0rd** (Down 1)
20. **master** (Up 1)
21. **hello** (New)
22. **freedom** (New)
23. **whatever** (New)
24. **qazwsx** (New)
25. **trustno1** (New)


ORDINA

# MINIMAL DATA PROTECTION MEASUREMENTS


- Passwords
  - At least 8 characters, more than 10 is advisable
  - Special Characters
  - Big and small letters
  - Numbers
  - Password Manager
- Social Media
  - Do not share everything with anyone
  - Be careful on what you share
  - Advertisements
  - Never tell a password to a *"Support Employee"*

# DE BACKER

**De Backer wants to have awareness about Privacy in the final objectives**

De Backer start zijn uiteenzetting in scholen altijd met een privacy-experiment waarvoor hij jongeren uit de aanwezige groep op voorhand op het internet opzocht. "Jongeren beseffen te weinig hoe ze moeten omgaan met sociale media en het is mijn missie om dit aan te pakken", klinkt het. "Belangrijk is dat we hen leren hoe ze zichzelf en vooral hun gegevens, kunnen beschermen. Een groot deel van hun gegevens hebben ze zelf gedeeld en daardoor wordt hun privacy bedreigd. Jongeren moeten nadenken over hoe ze die privacy kunnen beveiligen, want bedrijven zoals Facebook en Snapchat zien al die gegevens als koopwaar, dat is waarom hun diensten voor de gebruiker gratis zijn."

De Backer wil dat die bewustwording onderdeel wordt van de eindtermen. "Sociale media vormen anno 2017 een fundamenteel onderdeel van ons dagelijks leven. In plaats van ze te bannen, moeten we jongeren leren hoe ermee om te gaan."

Dit schooljaar gaat de staatssecretaris zijn scholentournee uitbreiden naar Wallonië. Bedoeling is om minstens één keer per maand een uiteenzetting te geven en daarmee zoveel mogelijk leerlingen te bereiken.

# PRIVACY VS SECURITY

- Privacy
  - Application of rules that govern the collection and handling / use of personal information
- Information Security
  - Protection of information (personal or otherwise) from unwanted intruders


There can be security without privacy, but there cannot be privacy without security!

# IMPLICATIONS FOR COMPANIES AND THEIR CLIENTS

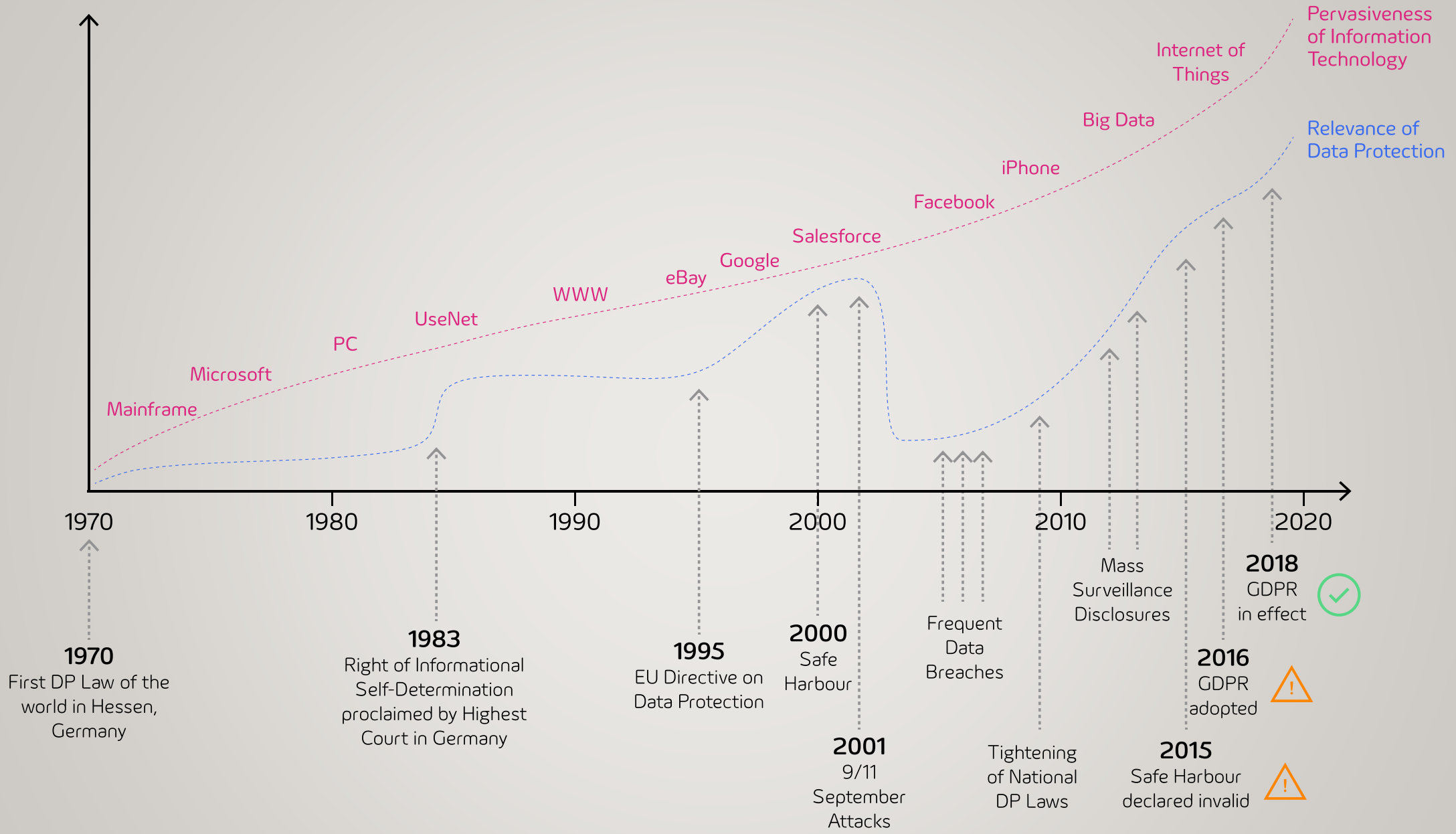
- The company can be a data processor
  - They process data from their clients
- The company can be a data controller
  - For customers and employees
    - Names
    - Addresses
    - Banking information
  - Personal data processing
    - Contractual
    - Legal obligation

ORDINA

# COMPANIES AND THEIR DATA PROTECTION / INFORMATION SECURITY

- Data controllers and processors routinely access sensitive data that is owned by customers
  - Names
  - Health records
  - Financial Information
- Employees are critical in the defense and protection of sensitive data and information systems
  - Awareness sessions on the protection of data and information systems

# General Data Protection Regulation


Pervasiveness of Information Technology
Internet of Things
Big Data
iPhone
Facebook
Salesforce
Google
eBay
WWW
UseNet
PC
Microsoft
Mainframe
Relevance of Data Protection
1970
1980
1990
2000
2010
2020
1970
First DP Law of the world in Hessen, Germany
1983
Right of Informational Self-Determination proclaimed by Highest Court in Germany
1995
EU Directive on Data Protection
2000
Safe Harbour
2001
9/11 September Attacks
Frequent Data Breaches
Tightening of National DP Laws
Mass Surveillance Disclosures
2015
Safe Harbour declared invalid
2016
GDPR adopted
2018
GDPR in effect

ORDINA

# GENERAL INFORMATION

GDPR

- Privacy = Respect for:
  - Private life
  - Family life
  - Home
  - Communications
- Privacy is the right to be left alone and to be forgotten
- In the  privacy is a fundamental right

# GENERAL INFORMATION

GDPR

- Companies in- and outside of the EU
  - Data controllers / Data processors
  - Monitoring behavior of European citizens
- May 25th 2018
- Fines (whichever is the highest)
  - Up to € 20,000,000 or 4 % of total annual turnover (worldwide)

# WHAT IS PERSONAL DATA


- Personal data
  - Name
  - Identification number
  - Location data
  - Online identifier
  - Factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity
- Special categories
  - Racial or ethnic origin
  - Political opinions, religious or philosophical beliefs
  - Trade-union membership
  - Data concerning health or sex life and sexual orientation
  - Genetic data or biometric data

# 6 GENERAL GDPR PRINCIPLES



- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation (retention)
- Integrity and confidentiality

# WHAT IS DATA PROCESSING

GDPR

*Any (set of) operation(s) which is performed on personal data*

# PROCESSING CONDITIONS



- Consent
- Necessary for the performance of a contract
- Legal obligation
- Vital interests
- Public functions
- Legitimate interests

# KEY ITEMS

GDPR

- Increased fines
- Proof of compliance (Accountability)
- Privacy by design / by default
- Transparency
- New rights
- EU and non-EU based organizations

# INFORMATION SECURITY



The protection of information and information systems from unauthorized access, use, disclosure, modification or destruction in order to provide confidentiality, integrity and availability.

# INFORMATION SECURITY



- Information and information processing systems represent a certain value that needs to be appropriately protected
- Objective – to understand, manage and reduce the risk to information under the control of the organization

# THE IMPORTANCE OF SECURITY

*Article 32 – Security of Processing*

- The GDPR requires organizations to take a risk-based approach to data security
- Additional obligation to take steps, where appropriate to risk:
  - **Pseudonymization** and **encryption** of personal data
  - Ensure ongoing **confidentiality**, **integrity**, **availability** and **resilience** of IT Systems
  - Restore the **availability** of personal data in a timely manner, in case of an event or incident
  - Regular **testing**, **assessing and evaluating** the effectiveness of technical and organizational measures

ORDINA

# CIA KEY CONCEPT

Privacy and Information Systems Security


- Confidentiality
  - Protecting information from unauthorized disclosure to people or processes

- Integrity
  - Assuring the reliability and accuracy of information and IT resources


- Availability
  - Ensuring that all systems and applications are available and that users are able to access their information

# CIA EXAMPLE



- Confidentiality
  - What if your account was not kept confidential and a stranger was able to access it when they approach the ATM.
- Integrity
  - Imagine if every time you went to the ATM, the balance that is displayed would be inaccurate.
- Availability
  - What if your bank's ATMs are rarely available when you need them? Would you continue to use that bank?

# PERSONAL IDENTIFIABLE INFORMATION (PII)



Personal Identifiable Information is information which can be used to distinguish or trace an individual's identity, such as their name, Social Security number, biometric records, … Alone or when combined with other personal or identifying information which is linked or linkable to a specific individual.

# PII – INFORMATION LIFE CYCLE



Protecting the PII is very important during each stage of the information life cycle

# PII – INFORMATION LIFE CYCLE



1. Create
   - Validate that you are allowed to collect the PII
2. Store
   - Ensure that stored data is protected with adequate data security controls
3. Use
   - Monitor user activity and apply security controls to prevent data leakages
4. Share
   - Implement a strategy to continuously monitor stored data
5. Archive
   - Ensure archived data is available and protected
6. Destroy
   - Ensure files are deleted appropriately

# QUIZ



- Only PII that can be used to directly identify an individual needs protection?
  - True / false
- What is the goal of information security?
  A. Ensure that employee's passwords contain at least eight characters including numbers, letters and special characters?
  B. Protect the CIA of information and corresponding information systems?
  C. Eliminate all threats to information systems?
  D. Provide a lock for all file cabinets in the building?

# PAUSE

# APPROACH: FRAMEWORK

13 Steps of the Belgian SA

1. Awareness
2. Data Inventory
3. Communication
4. Data Subject Rights
5. Subject Access Request
6. Lawfulness of Data Processing
7. Consent Strategy
8. Children
9. Data Breaches
10. Privacy by Design & DPIA
11. International Data Transfers
12. DPO
13. Existing Contracts


ORDINA

# APPROACH: FRAMEWORK

## Awareness

- Privacy
  - First: the key stakeholders of the organization
  - Then: make all the other employees aware

    (e.g. e-learning, outsourcing, etc.)
- Security
  - Security awareness is equally important
  - End users are often the weakest link in the chain
  - Create security topics relating to the needs of the organization

# APPROACH: FRAMEWORK

## Data Inventory

- Privacy
  - Document what and whose personal data you keep, the reason why, where, until when and how.
  - Replacement of the former ‘notification’ duty
- Security
  - Importance of a well documented CMDB
  - (Security of) Data flows

# APPROACH: FRAMEWORK

## Communication

- Privacy
  - Privacy- and cookie policy (external)
  - Privacy policy (internal)
- Security
  - Ensure that Security Awareness is created through different channels (e.g., e-mail, intranet, e-learnings, etc.)

# APPROACH: FRAMEWORK

## Data Subject Rights

- Privacy
  - Access, information, rectification, erasure, restriction, portability, objection, automated-decision making (e.g. profiling)
  - Focus on which rights can be exercised by customers – make processes & guidelines
- Security
  - Ensure that proper User Access controls are in place so that only authorized employees have access to personal data

# APPROACH: FRAMEWORK

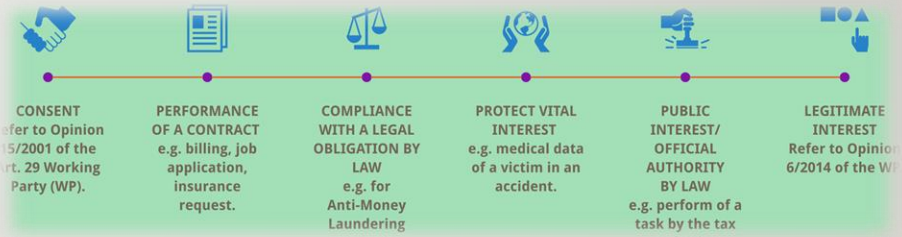
Subjects Access Request

- Privacy
  - Drawing up a procedure (indicate in privacy notices & policies)
  - Note: management is crucial
  - Criteria of non-exercise are just as important!

# APPROACH: FRAMEWORK

## Lawfulness of Data Processing

- Privacy
  - Be careful with specific categories of personal data (e.g. art. 9 GDPR)
  - Basis: data inventory
  - Why need personal data when it is not lawful to process it?
- Security
  - Importance of security of data flows



# APPROACH: FRAMEWORK

## Consent Strategy

- Privacy
  - Be careful to use consent as only lawful basis
  - Only develop it when necessary
  - Be aware: children, right to erasure, ‘opt-in’ and ‘opt-out’, explicit vs unambiguous

# APPROACH: FRAMEWORK

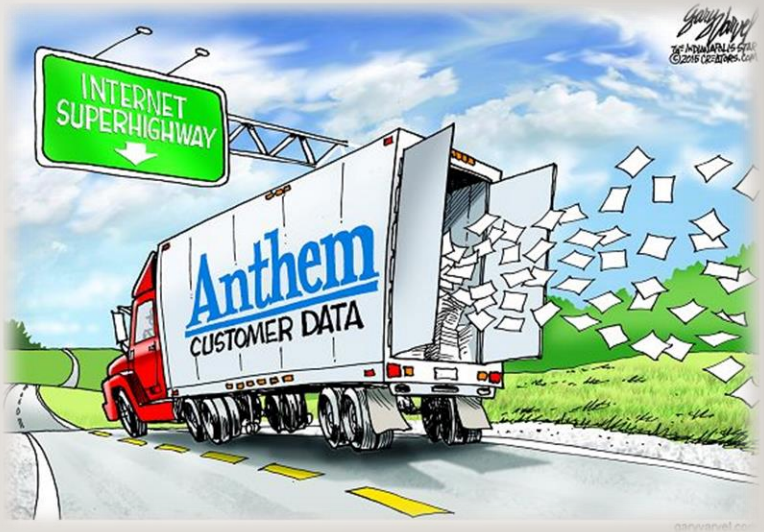
Children

- Privacy
  - Consent of parents: how do you verify it?
  - Only when targeted by ‘information society services’ – simplify privacy notice/policy

# APPROACH: FRAMEWORK

Data Breaches

- Privacy
  - Establish a procedure and template
  - Define Roles & Responsibilities (e.g. through a RACI)
  - Make people aware **when** there is data breach
- Security
  - Possibility to integrate the Data Breach procedure with the (Security) Incident Management procedure
  - Encryption of sensitive fields in Security Incidents or Breach tickets



# APPROACH: FRAMEWORK

Privacy by Design & DPIA

- Privacy
  - DPIA ⟷ PIA ⟷ Risk Analysis
  - Establish a DPIA framework and benchmarking standards (cf. PIA from the CNIL)
  - Incorporate this in your data processing agreements
- Security
  - Security Risk Assessments can incorporate Data Protection to a certain degree

# APPROACH: FRAMEWORK

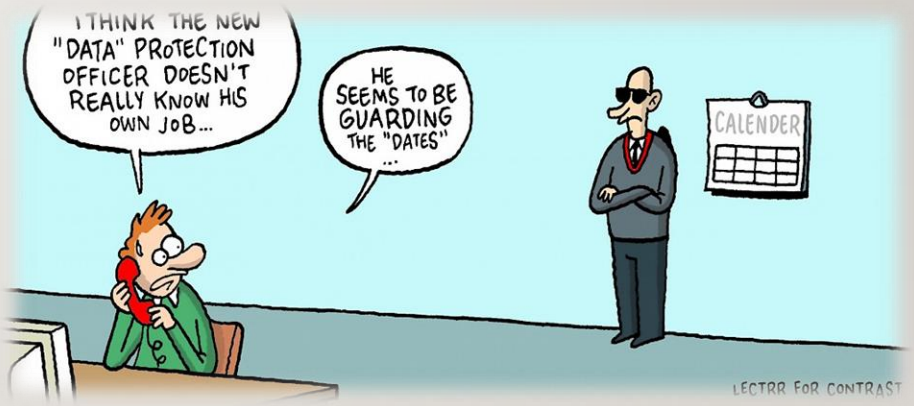
## International Data Transfers

- Privacy
  - Assess when this is done (cf. inventory)
  - Incorporate this in the data processing agreements
  - Make vendor questionnaires
- Security
  - Special attention to cross-border data flows

# APPROACH: FRAMEWORK

DPO

- Privacy
  - Assess if it is legally required: if not, do not appoint an official DPO
  - Document your assessment
  - Write a job description (if needed)
- Security
  - CISO ≠ DPO
  - Need for Segregation of Duties



# APPROACH: FRAMEWORK

Existing contracts

- Privacy
  - Focus on the contracts after the 25th of May 2018
  - Procurement/tenders: additional step in the procedure
  - Template: controller-processor, controller-controller
- Security
  - Security considerations in contracts
  - Third Party due diligence (e.g. through Third Party Questionnaires)

# GDPR: NOT ONLY A PAIN IN THE ASS


ORDINA

# GDPR: NOT ONLY A PAIN IN THE ASS

- Privacy remains a fundamental and constitutional right and is important
- Getting privacy right is a competitive advantage
- Compliancy proves a business to act as a reliable economic partner
- Gain consumer confidence


YAHOO!

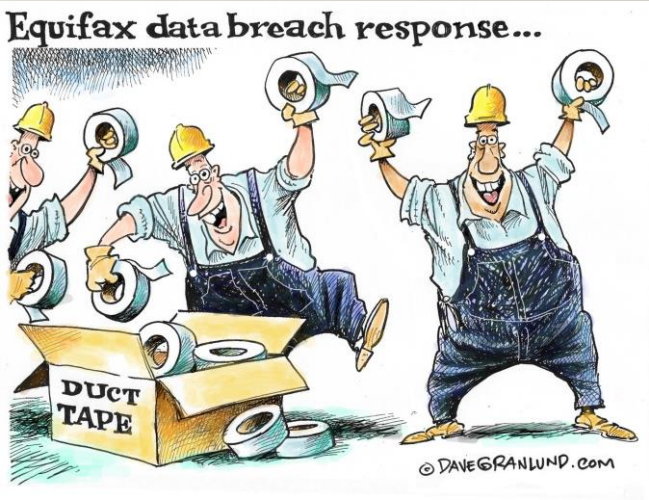
# DATA BREACH FACTS H1 2018

Data Breaches H1 2018

- 4,553,172,708 records breached in first half of 2018

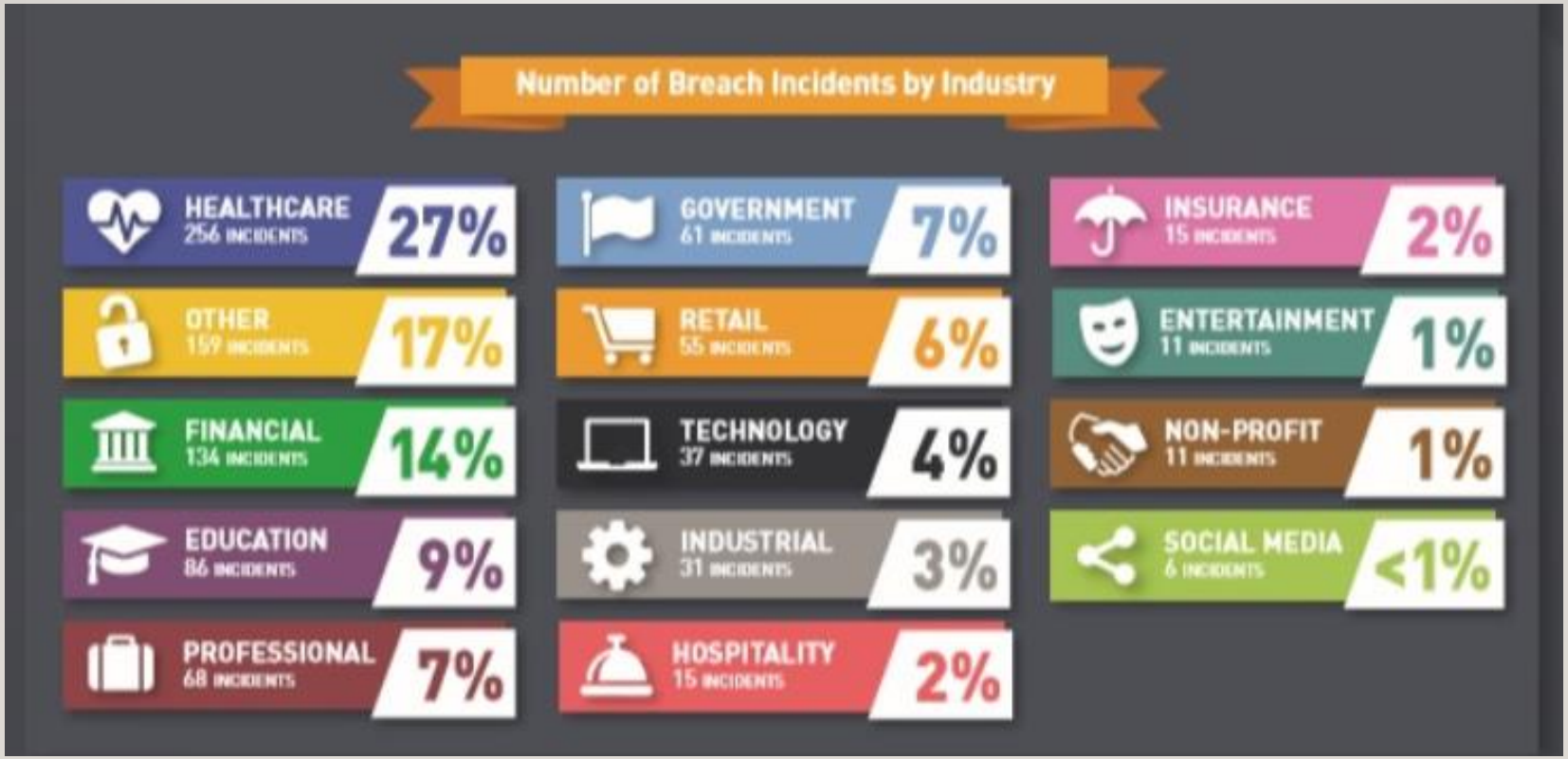
| 24 155 650 every day | 1 048 152 every hour | 17 469 every minute | 291 every second |
|---|---|---|---|

- 945 breach incidents
- 65% of the breaches are identity theft



# NUMBER OF BREACH INCIDENTS BY INDUSTRY

Data Breaches overview




ORDINA

# IMPACT ON AN INDIVIDUAL

Data Breaches

Lost information = risk

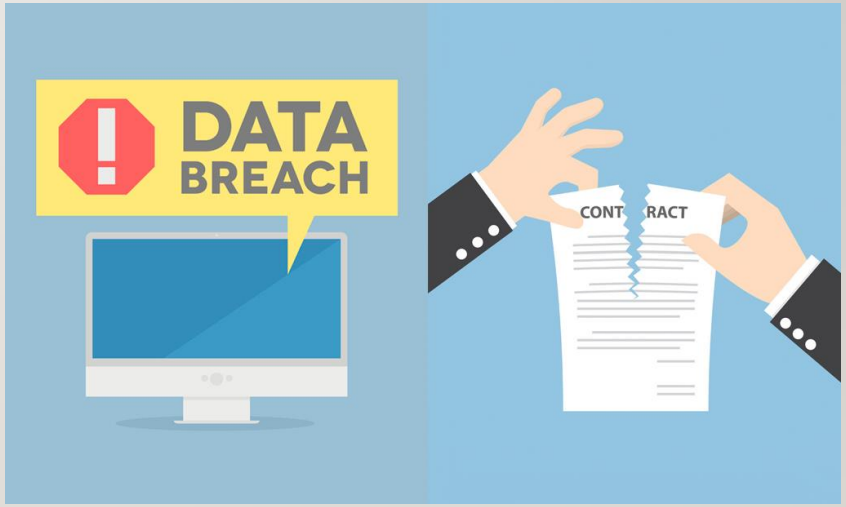
- Identification
- Embarrassment
- Endangerment
- Jeopardizing

# IMPACT ON AN ORGANIZATION

Data Breaches

- Reputational damage
- Lost productivity
- Mandatory breach notifications
- Costs, costs and… costs

- Lost business revenue is the biggest financial consequence of a data breach



# HOW DATA BREACHES OCCUR



- Human error
- Document leakages
- Theft
  - Documents
  - Unencrypted devices
- Phishing emails
- Insecure web pages

# EXAMPLES

## Data Breaches

- 2013
  - 1 billion Yahoo user accounts affected
- 2014
  - 500 million Yahoo user accounts affected
- Data Breach due to unauthorized third party access

# EXAMPLES

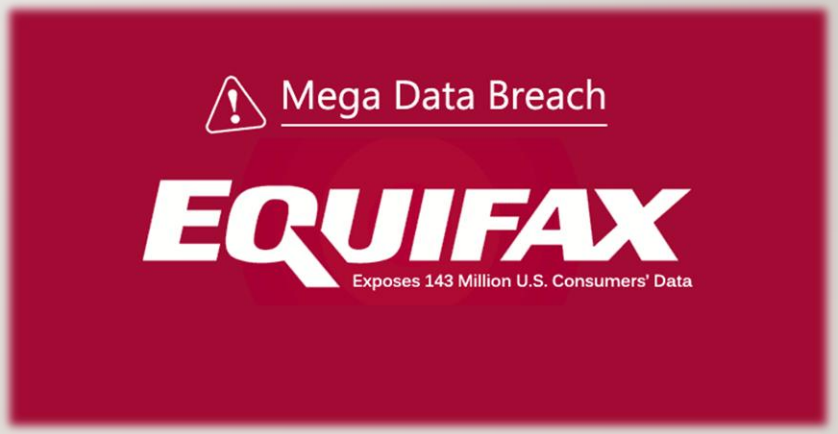
## Data Breaches


- 2014
  - 145 million records containing encrypted passwords, name, email addresses, phone numbers, …
- Data Breach due to a malicious outsider

# EXAMPLES

## Data Breaches

- 2017
  - 143 million US customers financial information including **social security numbers**
- Equifax is one of the nation's three major US credit reporting agencies
- Data Breach due to a security flaw in one of their custom made tools and unauthorized access to the Equifax servers



# EXAMPLES

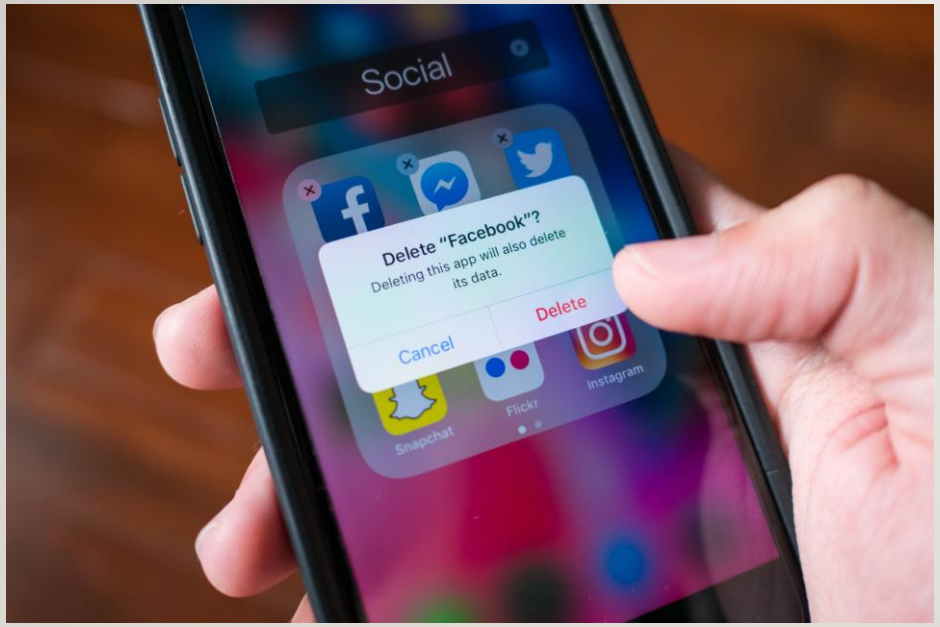
Data Breaches

Deloitte.

- 2017
  - Confidential information, including private emails and documents of some of its clients
- Data Breach due to a malicious outsider gaining access through an administrator account on the Deloitte's email server.
  - The server was not secured using two-factor authentication (2FA)

# EXAMPLES

## Data Breaches




- 2018
  - Highly sensitive data, including locations, contact details, relationship status, recent searches, and devices used to log in.
  - The hackers were able to exploit vulnerabilities in Facebook's code to get their hands on 'access tokens

# USER SECURITY AWARENESS

# IMPORTANCE OF AWARENESS



- Important to understand and be aware of the constant risks facing
  - Individuals
  - Organizations
- Awareness campaigns can reduce the overall organization's risk

# AWARENESS

## Passwords

- Easy passwords can be easily cracked or guessed
- Important to choose a password easy to remember but difficult to crack
- Use passphrases instead of passwords
  - Example: Take me out to the ballgames
    → "Tmo2tBGs"

| number of Characters | Numbers only | Upper or lower case letters | upper or lower case letters mixed | numbers, upper and lower case letters | numbers, upper and lower case letters, symbols |
|---|---|---|---|---|---|
| 3 | Instantly | Instantly | Instantly | Instantly | Instantly |
| 4 | Instantly | Instantly | Instantly | Instantly | Instantly |
| 5 | Instantly | Instantly | Instantly | 3 secs | 10 secs |
| 6 | Instantly | Instantly | 8 secs | 3 mins | 13 mins |
| 7 | Instantly | Instantly | 5 mins | 3 hours | 17 hours |
| 8 | Instantly | 13 mins | 3 hours | 10 days | 57 days |
| 9 | 4 secs | 6 hours | 4 days | 1 year | 12 years |
| 10 | 40 secs | 6 days | 169 days | 106 years | 928 years |
| 11 | 6 mins | 169 days | 16 years | 6k years | 71k years |
| 12 | 1 hour | 12 years | 600 years | 108k years | 5m years |
| 13 | 11 hours | 314 years | 21k years | 25m years | 423m years |
| 14 | 4 days | 8k years | 778k years | 1bn years | 5bn years |
| 15 | 46 days | 212k years | 28m years | 97bn years | 2tn years |
| 16 | 1 year | 512m years | 1bn years | 6tn years | 193tn years |
| 17 | 12 years | 143m years | 36bn years | 374tn years | 14qd years |
| 18 | 126 years | 3bn years | 1tn years | 23qd years | 1qt years |

# AWARENESS



- Most attacks take place via email or malicious websites
- Confirm that websites use https instead of http and that the website has a lock icon
- Be extra careful when using public WIFI's
  - Use a VPN
  - Communicate using encrypted applications and networks

# AWARENESS

## Email and Internet Security

- Do not use your private email for work related goals
- Do not use your work email for private related goals
- Never provide your passwords to anyone
- Do not open suspicious URL's
- Email attachments are a potential source of contamination


ORDINA

# AWARENESS

## Phishing

- = Social engineering
- Fake emails, text messages or website created to look like the original. They are distributed by criminals in order to capture personal information about individuals
  - Usernames
  - Passwords
  - Credit card information

# AWARENESS

## Physical Security

- Shoulder surfing
- Tailgating
- Unauthorized users
- Stolen equipment
- Secure printing
- Clean / clear desk policy
- Common sense

# QUIZ



- A phishing email:
  A. Is a type of social engineering attack
  B. Can be from an organization that you recognize, like a professional association
  C. Contains a link to a web site that asks you for personal information
  D. All of the above
- Which password is most secure? (and why)
  A. Linda12
  B. 123Abs
  C. Big_Apples
  D. BH17**Plus

# QUIZ

Awareness

- How can you tell if an email is fake or a phishing email?
  A. The email is sent at night?
  B. It asks you to do something you wouldn't do, such as respond with your username, full password and credit card details?
  C. You weren't expecting an email from the company that sent it to you?
- Which of these is a tell-tale sign that a website isn't real, and in fact is designed to trick you into giving away your private information
  A. The website address looks unusual?
  B. It looks loss professional than you expect?
  C. It is impossible for most people to sport a well-designed fake website?


ORDINA