GDPR compliance

FAS Certification
DPO Certification

EU GDPR INSTITUTE

Agenda

Time	Topic
09:00 - 09:25	Introduction to the The GDPR Institute GDPR roadmap
09:25 - 10:30	Plan - General definitions & DPO
10:30 - 10:45	☕
10:45 - 11:05	Plan - Project scope
11:05 - 12:00	Plan - Data inventory
12:00 - 12:30	🍽
12:30 - 13:30	Do - Accesses, consents & requests
13:30 - 14:20	Do – Transfers & breaches
14:20 - 14:35	☕
14:35 - 15:35	Improve - Data Protection Impact Assessments
15:35 - 16:00	Closing and certification

Access to the presentation

https://www.eugdpr.institute/dpo-gdpr-day-ii/

GDPR areas

organizational
01
02
Legal
03
Technical

Our journey today

- From legal to practice
- Toolkit
- Coordinate changes
- DPO challenges
- Privacy culture

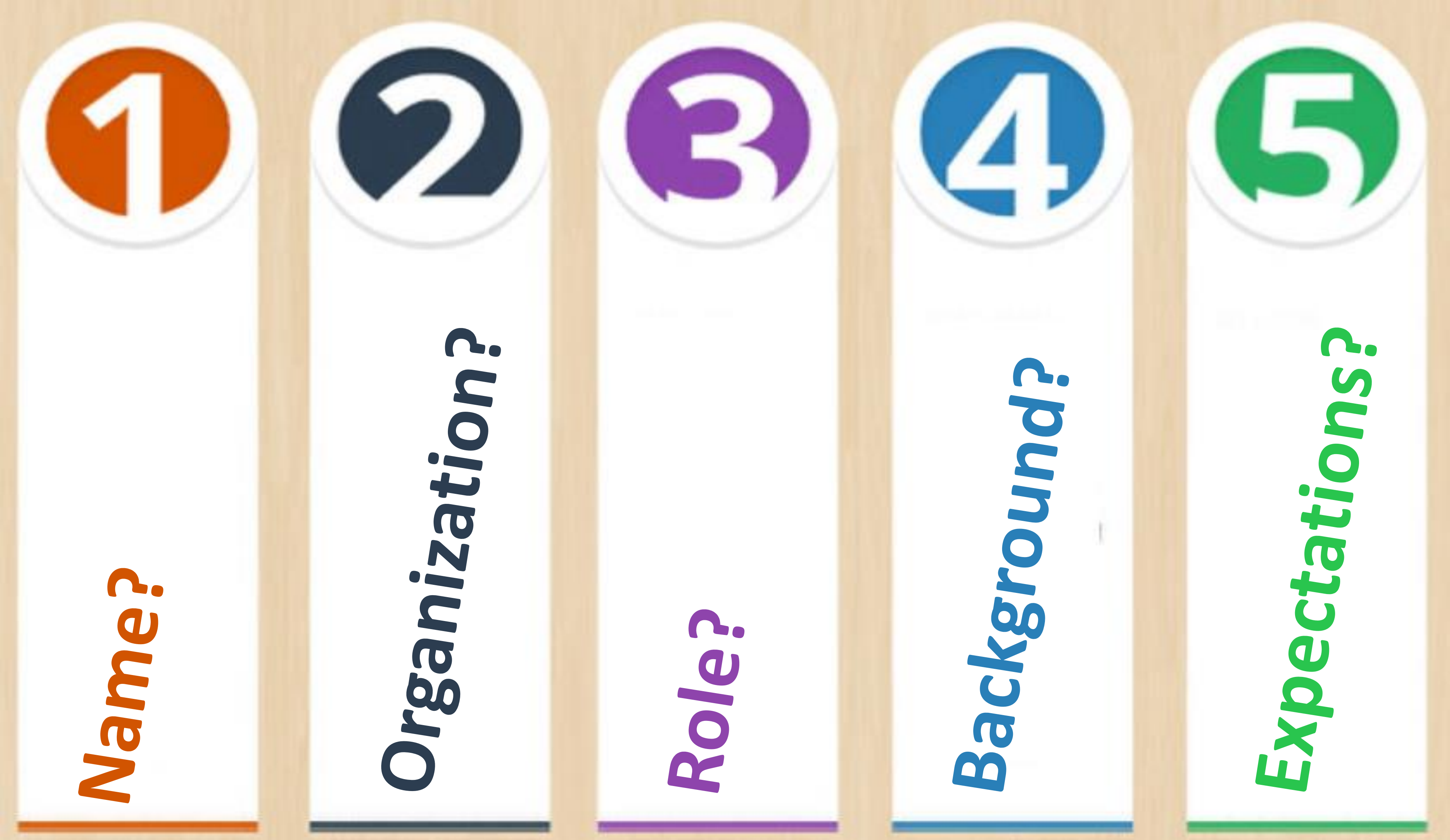
We will focus on issues

… not organizations

- ***"When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed."***

The GDPR Institute
GDPR Roadmap and Framework

Introductions



1 Name?

2 Organization?

3 Role?

4 Background?

5 Expectations?

What you will receive?

http://www.eugdpr.institute/gdpr-compliance/

Does the GDPR applies to me?

- □ Does my Organization offer goods or services to EU residents?
- □ Does my Organization monitor the behavior of EU residents such as apps and websites?
- □ Does my Organization have employees in the EU?

Why GDPR is important?

Fines!

NEW

20M EUR up to 4% global revenue in the last year

Failure to implement core principles, infringement of personal rights and the transfer of personal data to countries or organizations without adequate protection

10M EUR up to 2% global revenue in the last year

Failure to comply with technical and organizational requirements such as impact assessment, breach communication and certification

Reduced with appropriate technical and organizational measures

Why GDPR is important?

Privacy is a competitive advantage

- **Protect the reputation**
- **Organize and control data**
- **Remove unnecessary data**
- **Identify privacy vulnerabilities at an early stage**
- **Focus the client and customer contact lists**

It is all about the reputation!

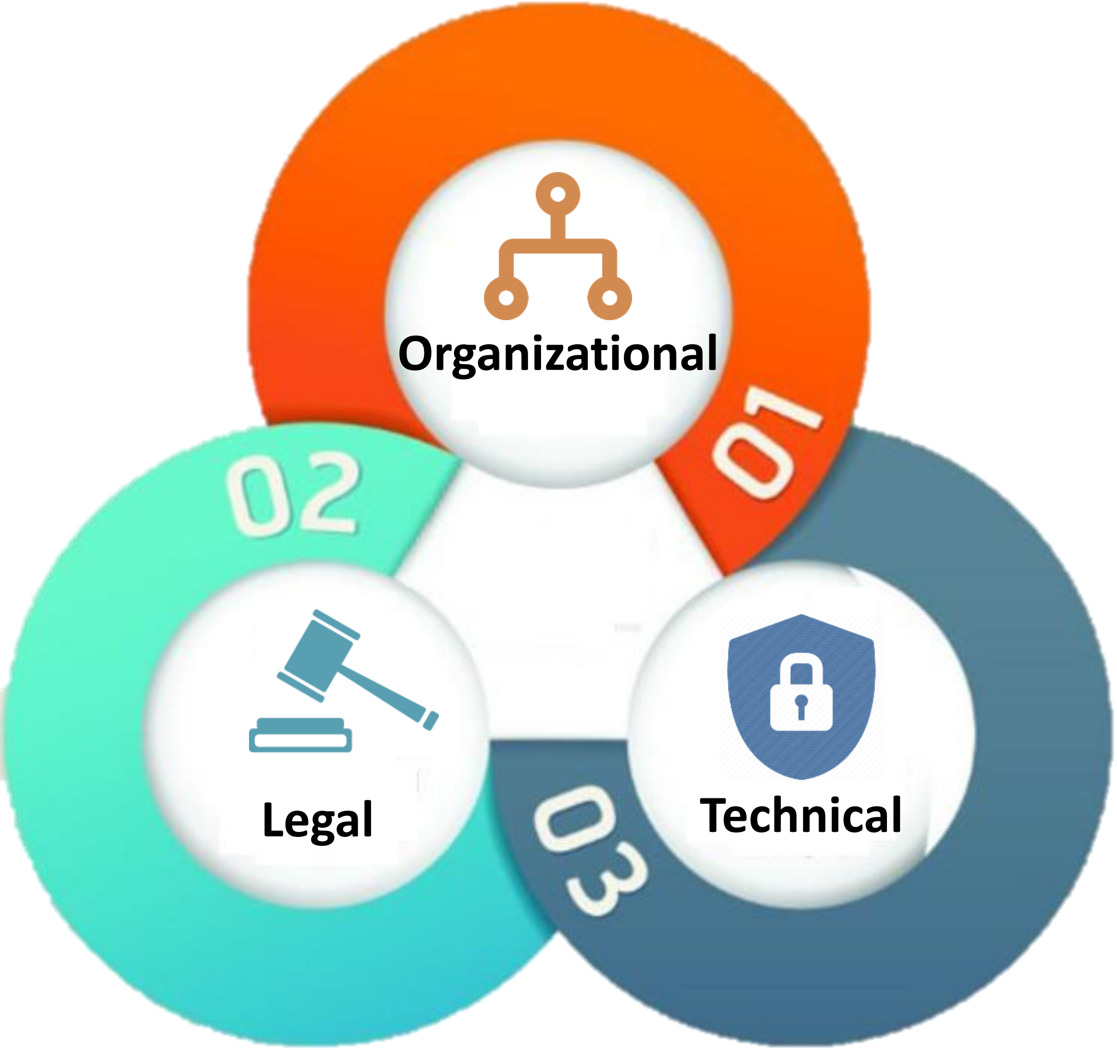
SAFETY WARNING!
Opening this box will result in Death by Electrocution & a £20 Fine.

Info Security and boards

2017 Security and Privacy Survey by Protiviti

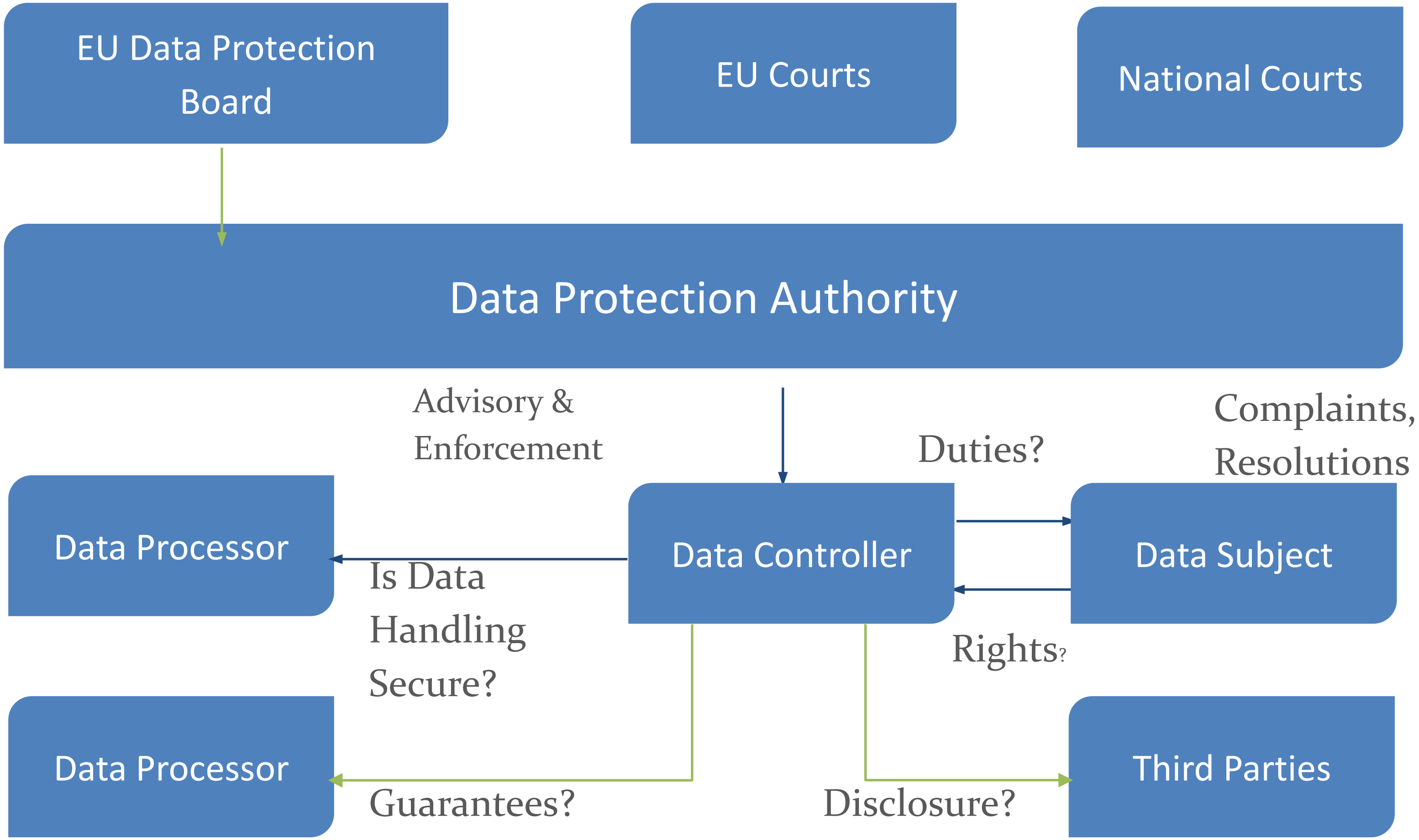
- 87% of FTSE 100 companies disclosed cyber as a principal risk
- Only 33% with a high board engagement in cyber risks
  - Boards are not discussing cyber risks
  - Directors more prepared for compliance risks than cyber risks
  - Weak cybersecurity controls and preparedness
- 38% with all core infosec policies
  - Big impact on security, distinguishing top performers
- 31% with an excellent understanding of critical information
  - Many companies unable to identify the most valuable data assets
- 60% with mandatory training on security to all employees

GDPR areas

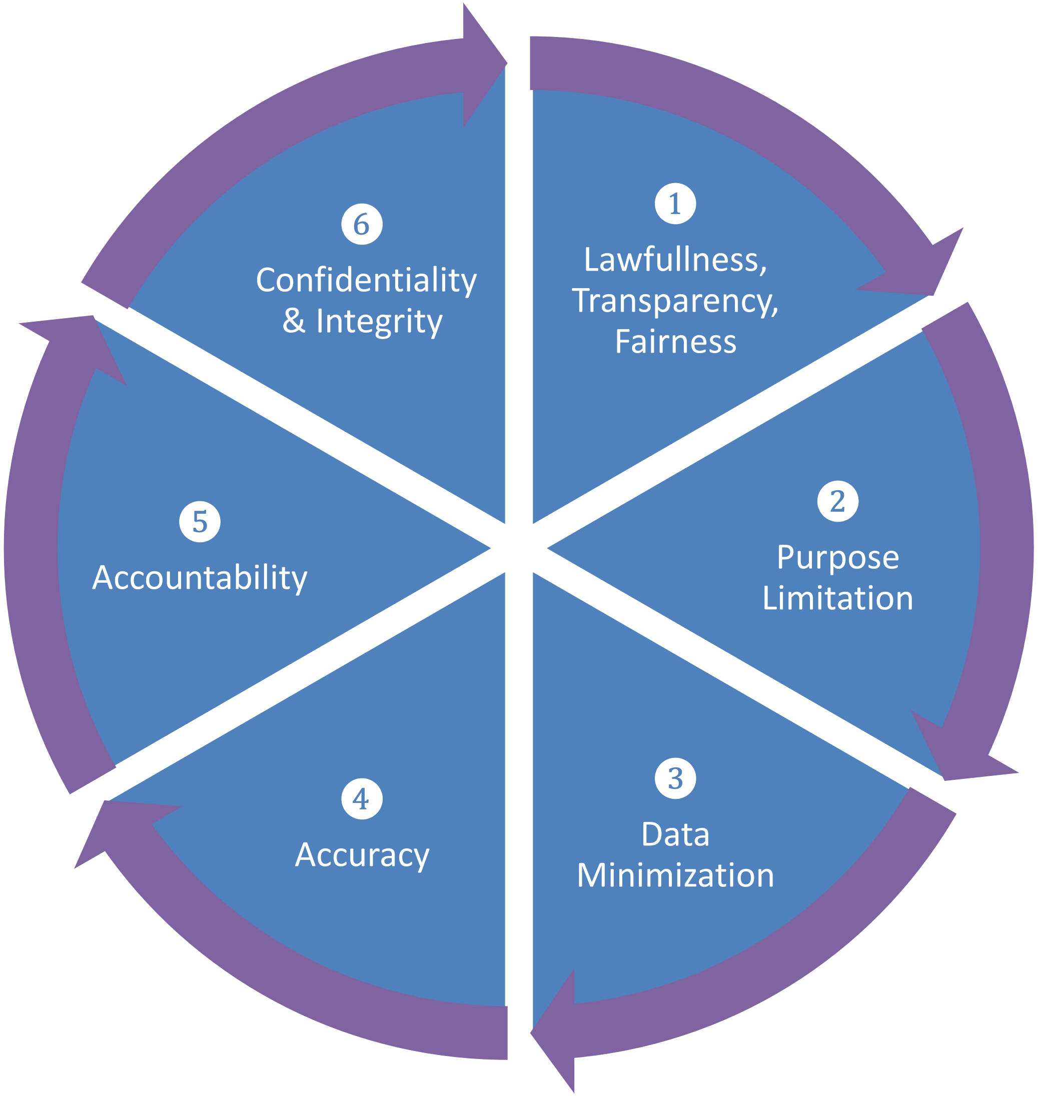


- DPO challenges
- Privacy culture
- GDPR compliance journey
- Organise changes
- Legal to practice

The GDPR Overview



The GDPR Guiding Principles



1 Lawfullness, Transparency, Fairness

2 Purpose Limitation

3 Data Minimization

4 Accuracy

5 Accountability

6 Confidentiality & Integrity

Guiding principles Solutions

GDPR Principles	Typical Challenges	Solution and Capabilities
Integrity & Confidentiality	Applying industry standard IT security controls to prevent unauthorised access	Strong Encryption, Fine-grained authorisation
Accountability	Demonstrating compliance, detecting and analysing breaches in 72 hours	Comprehensive, inescapable audit trail Cybersecurity solutions
Lawfulness, Fairness and Transparency	Implement a way to keep track of personal data	Classifying and tracking lineage of personal data elements
Purpose Limitation	Track consent and data usage	DPO can audit precisely how data was used, Keep data governed
Data Minimization	Removing or anonymising data where possible Preventing unlawful data transfers outside the EU while still enabling outsourcing	Data can be tagged to indicate allowed purpose, time limit Redacted views
Accuracy	Finding a low overhead way to fix data	Fast updates of individual records

ISO 27001 Info Security

EU GDPR INSTITUTE

Context

- Understand the organization
- Understand needs and expectations
- Determine scope

Leadership

- Leadership and commitment
- Policy
- Roles, responsibilities and authorities

Planning

- Actions to address risk
- Info sec risk assess.
- Info sec risk treatment
- Info sec plans

Support

- Resources
- Competence
- Awareness
- Communications
- Documented information

Operation

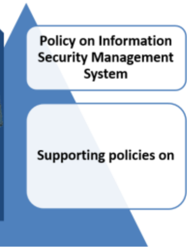
- Operational planning and control
- Info sec risk assess
- Info sec risk treatment

Perfor-mance

- Monitoring, measurement, analysis and evaluation
- Internal audit
- Management review

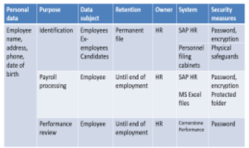
Improve-ment

- Nonconformity and corrective actions
- Continual improvement

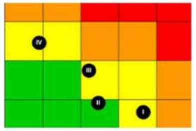


Policy on Information Security Management System

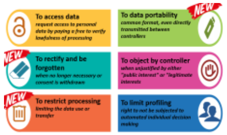
Supporting policies on



Personal data	Purpose	Data subject	Retention	Owner	System	Security measures
Employee name, address, phone, date of birth	Identification	Employees Ex-employees Candidates	Permanent file	HR	SAP HR	Password, encryption
					Personnel filing cabinets	Physical safeguards
	Payroll processing	Employee	Until end of employment	HR	SAP HR	Password, encryption
					MS Excel files	Protected folder
	Performance review	Employee	Until end of employment	HR	Cornerstone Performance	Password



Train your people



To access data *request access to personal data by paying a free to verify lawfulness of processing*

To data portability *common format, even directly transmitted between controllers*

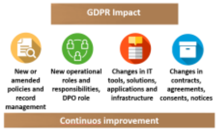
To rectify and be forgotten *when no longer necessary or consent is withdrawn*

To object by controller *when unjustified by either "public interest" or "legitimate interests*

To restrict processing *limiting the data use or transfer*

To limit profiling *right to not be subjected to automated individual decision making*

Audit compliance



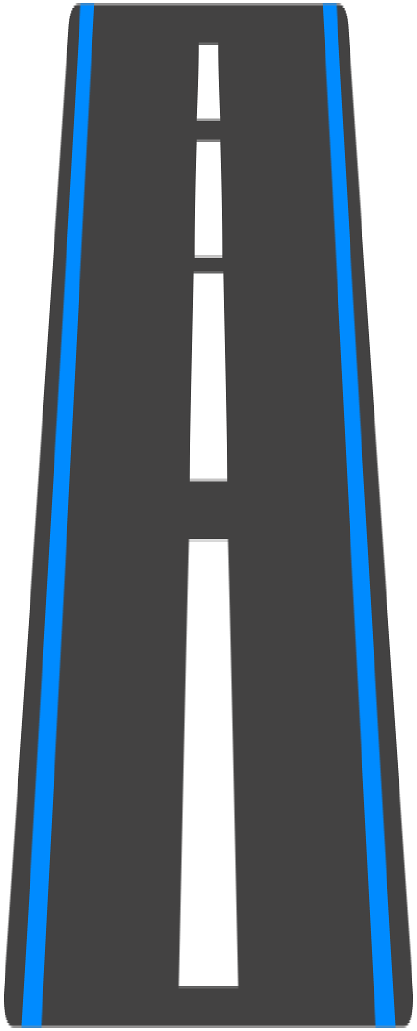
GDPR Impact

- New or amended policies and record management
- New operational roles and responsibilities, DPO role
- Changes in IT tools, solutions, applications and infrastructure
- Changes in contracts, agreements, consents, notices

Continuos improvement

Data protection (ISO 27001) is needed for privacy (GDPR)

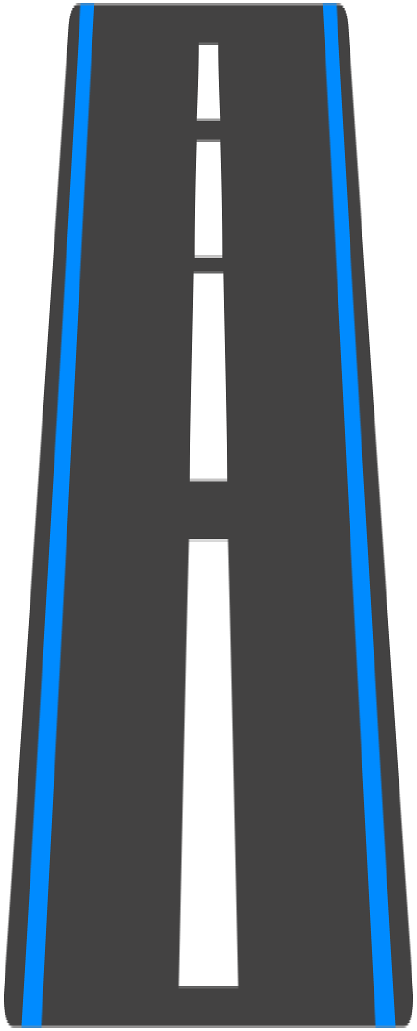
Roadmap



A- Plan

- 1- Obtain the buy-in from stakeholders
- 2- Get a team
- 3- Identify relevant processes and third-party activities
- 4- Compile a data inventory
- 5- Clean the house: data minimization
- 6- Create a privacy policy

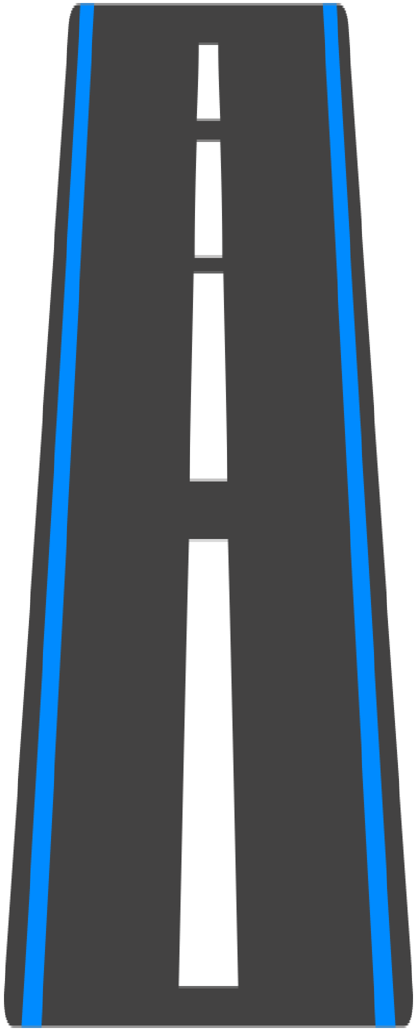
Roadmap



B- Do

- 1- Limit accesses
- 2- Review consents
- 3- Process access requests
- 4- Validate data transfers outside the EU
- 5- Report data breaches

Roadmap



C- Improve

- 1- Train the staff
- 2- DPIAs for business chances
- 3- Audits
- 4- Certifications

A - Plan

Step 1: Obtain the buy-in

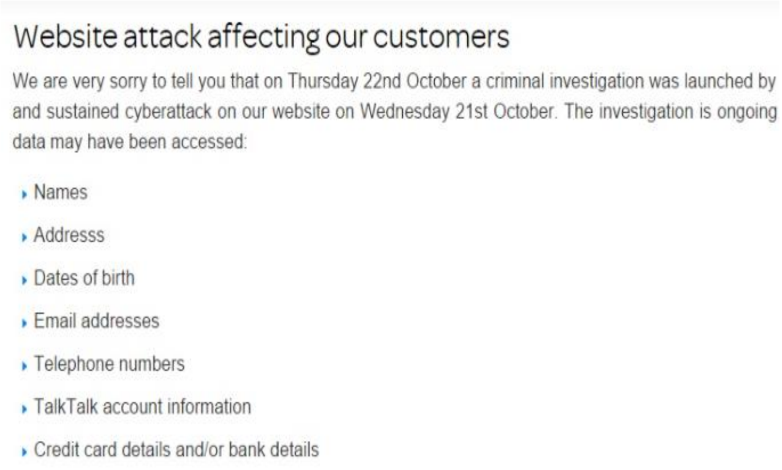
EU GDPR INSTITUTE

Key factor for success

Fines + Reputation

Board members
Senior managers
Chief compliance officer
Chief risk officer
Chief legal officer
Chief information offices
Chief security information officer

Step 1: Discussion case



Website attack affecting our customers

We are very sorry to tell you that on Thursday 22nd October a criminal investigation was launched by
and sustained cyberattack on our website on Wednesday 21st October. The investigation is ongoing
data may have been accessed:

- Names
- Addresss
- Dates of birth
- Email addresses
- Telephone numbers
- TalkTalk account information
- Credit card details and/or bank details

- **TalkTalk exposed the names, addresses, dates of birth, phone numbers and email addresses of more than 150k customers**
- **U.K. the Information Commissioner's Office fined at 400k GBP**
- **TalkTalk appeared in headlines associated with a lack of security and lost more than 100k customers**

Step 1: Tips

- Educate about GDPR to key stakeholders
  - Explain the privacy risks for their own career
  - Invite them to conferences and training
  - Communicate the link between GDPR and cyber risks
- Propose a plan adjusted to the Organization culture
  - Efficient and clear plan
  - Plan adjusted to available resources
  - GDPR project linked to strategies
    - e.g. better use of data, update marketing databases, protect patents and trade secrets
- Share cases about data breaches
  - “Good privacy is good business”

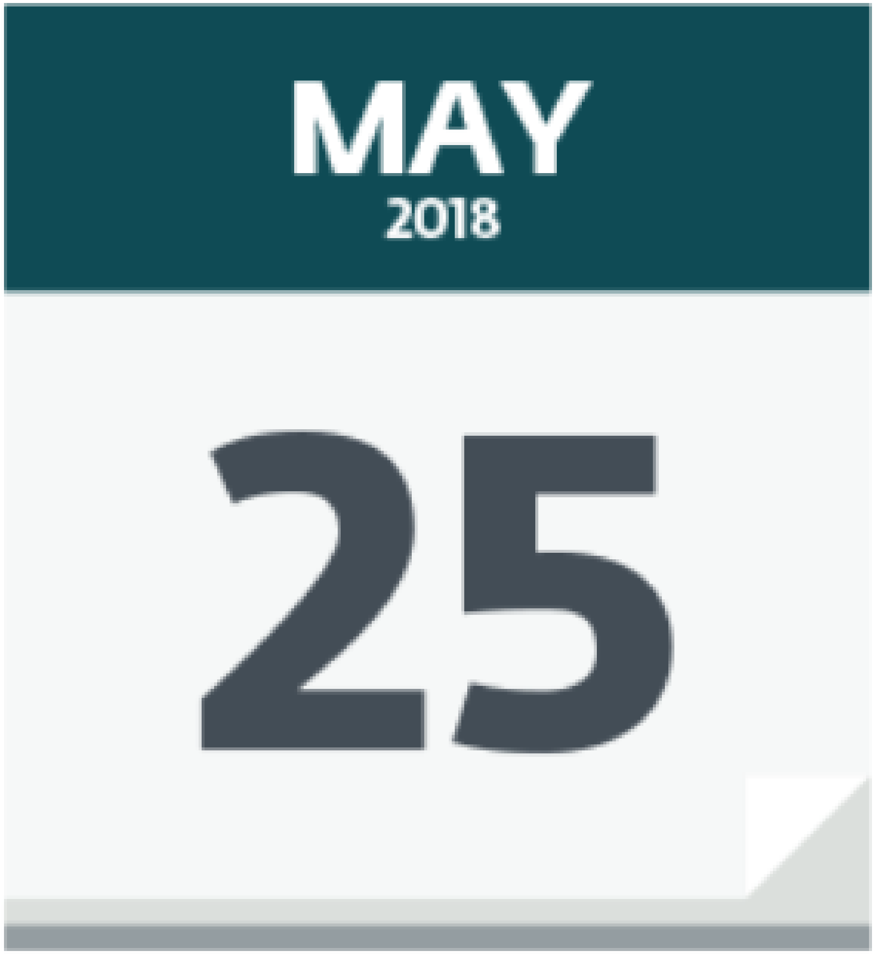
Step 2: Get a team

One man army?

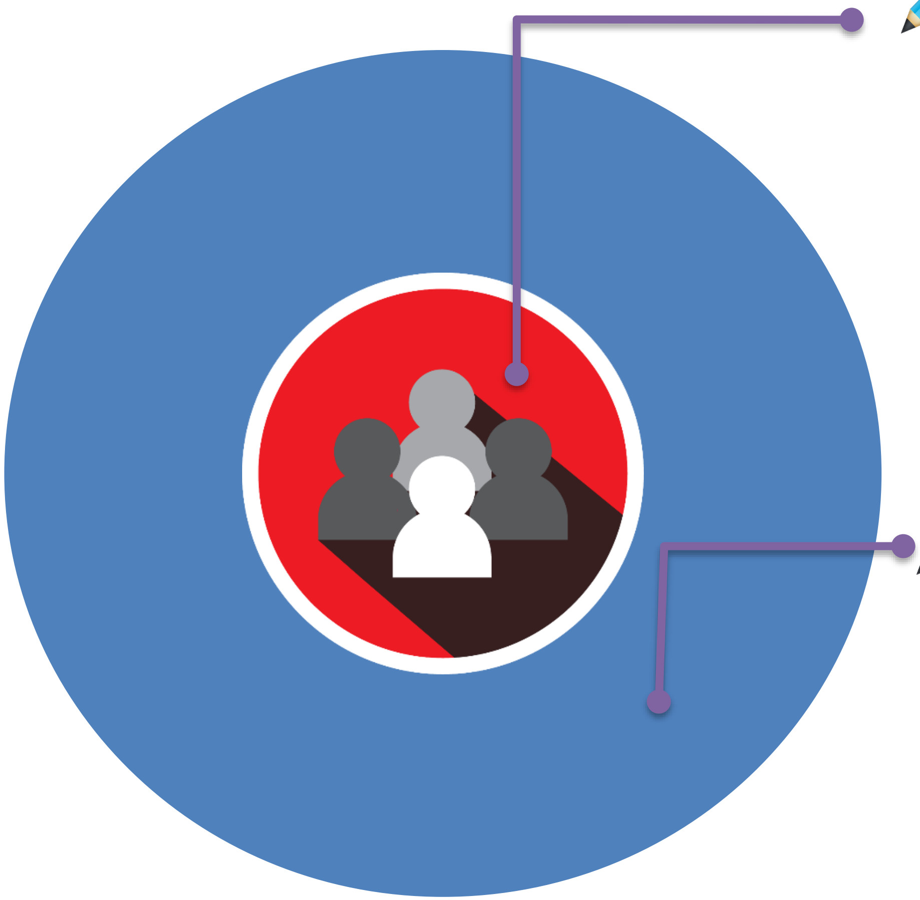
Data protection officer

Implementation team <> Maintenance team
Define a clear objective and responsibilities
Be a leader
Experience in project management, security, training and legal
Commit time of process subject experts
Document all the project activities

Be ready…

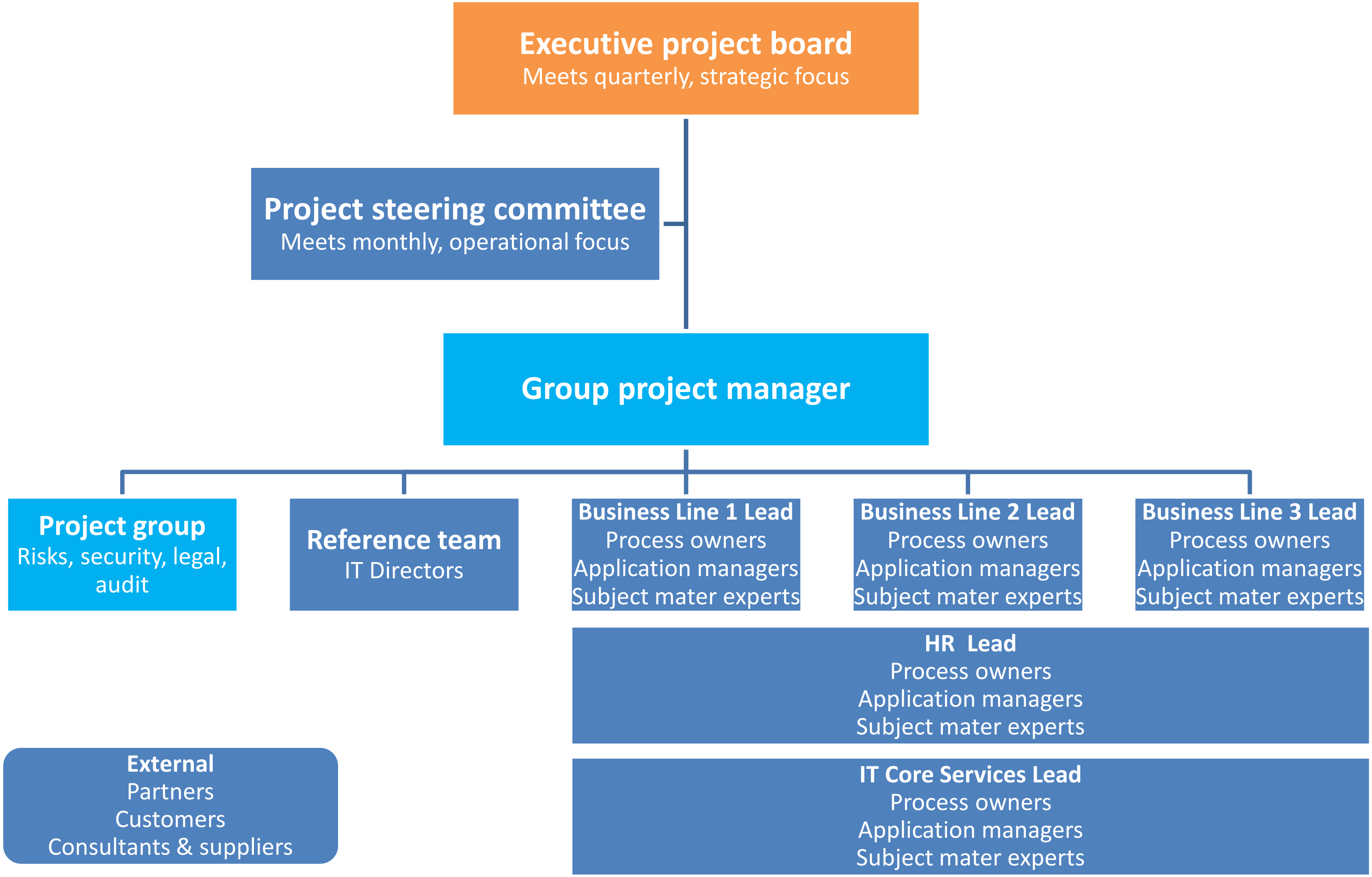


Get the team early



- Core team
  - Lead the implementation efforts
  - Knowledge of GDPR compliance, privacy controls, data security and change management
- Subject matter experts
  - IT, compliance, HR, marketing, procurement, customer support

Step 2: Example



Executive project board
Meets quarterly, strategic focus

Project steering committee
Meets monthly, operational focus

Group project manager

Project group
Risks, security, legal, audit

Reference team
IT Directors

Business Line 1 Lead
Process owners
Application managers
Subject mater experts

Business Line 2 Lead
Process owners
Application managers
Subject mater experts

Business Line 3 Lead
Process owners
Application managers
Subject mater experts

HR Lead
Process owners
Application managers
Subject mater experts

External
Partners
Customers
Consultants & suppliers

IT Core Services Lead
Process owners
Application managers
Subject mater experts

Step 3: Relevant processes

Scope

Business functions

Understand areas dealing with personal information

3rd parties processing personal information

Get priorities

Define deadlines in the roadmap

Step 3: Repair or replace

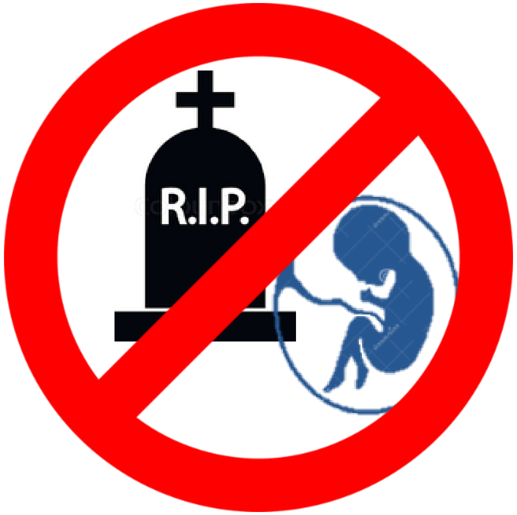
What is personal information?

Any information

… relating to an identified or identifiable …

natural person

the data subject!



How data is identifiable?

A Bulgarian **+7 M**

How data is identifiable?

A Bulgarian female **3.5M**

How data is identifiable?

A Bulgarian female born in 2000 **29k**

How data is identifiable?

…. born 8th January 1942 comes from the Rhodope Mountains, born in Arda, Smolyan Province, singing Rhodopean folk songs

1

How data is identifiable?

1 identifier

Name
ID, passport, driver, social security and tax numbers
Cookies and online IDs
Phone numbers
Location data
Genetic

NEW

1 or + factors

Physical
Physiological
Economic
Cultural
Social
Mental

How data is identifiable?

NEW

Key or Pseudonymous

1 identifier

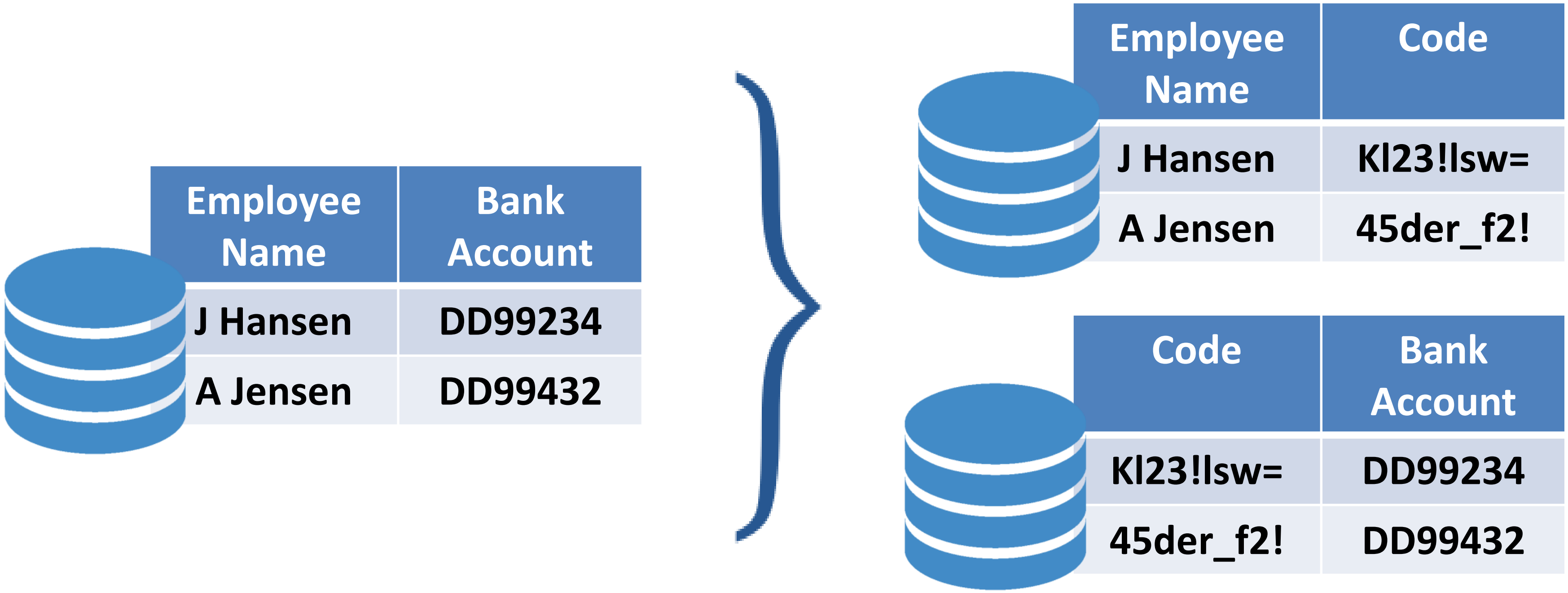
NEW

Pseudonymous

Coded data linked by a secure and separated key to re-identify a data subject

1 or + factors

What is pseudonymisation?



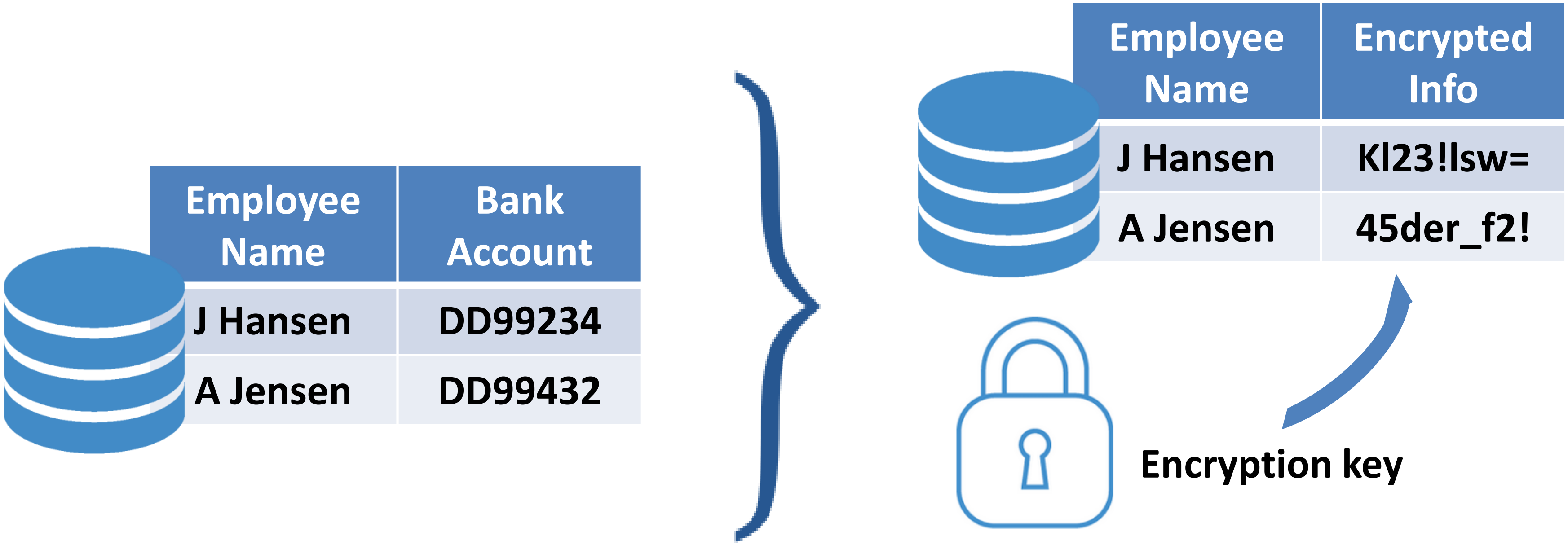
Employee Name	Bank Account
J Hansen	DD99234
A Jensen	DD99432

Employee Name	Code
J Hansen	Kl23!lsw=
A Jensen	45der_f2!

Code	Bank Account
Kl23!lsw=	DD99234
45der_f2!	DD99432

- Replacing the sensitive data by a random code
- Using a table in a separated server to link the random code to the original sensitive data

What is encryption?



Employee Name	Bank Account
J Hansen	DD99234
A Jensen	DD99432

Employee Name	Encrypted Info
J Hansen	Kl23!lsw=
A Jensen	45der_f2!

- It is an algorithm to scramble and unscramble data
- Transforming the original data with an encryption key

Which data is sensitive?

Health

Biometric

NEW

Genetic

NEW

Trade union

Racial

Political

Religion

Sex life

Special categories → generally cannot be processed, except given explicit consent and necessary for employment and other well defined circumstances

Personal data stored in an ERP/CRM?

- **Employee and candidates tables for payroll: address, bank account, health, civil and military status, disabilities, related people, timesheets, criminal records and tax info, travel expense reports**
- **Customers, prospects and payment: credit card numbers, invoices**
- **Suppliers tables: contractors, vendors, partners**

In productive and other environments

Backups and legacy systems

Other personal data stored?

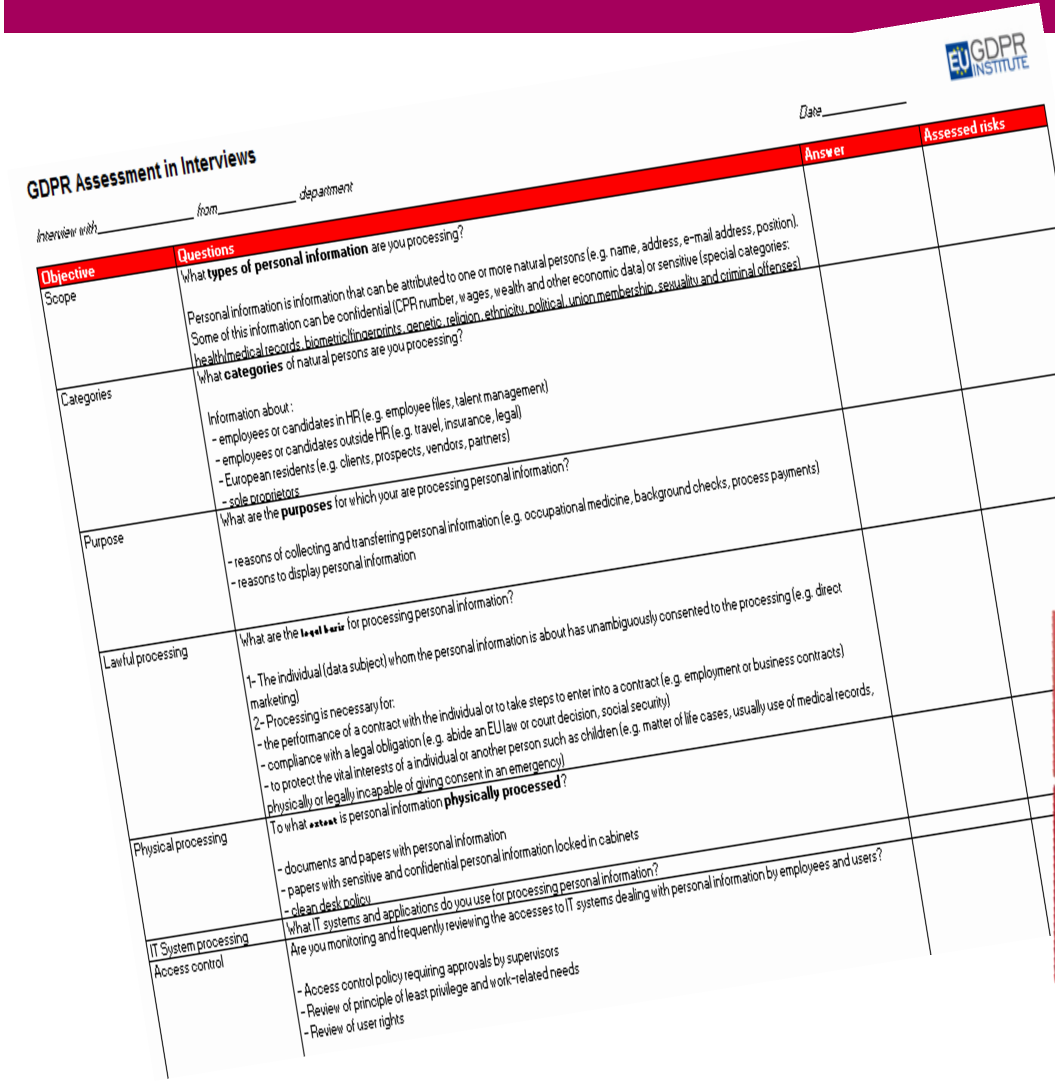
- **Website visitors**
- **Email servers**
- **Marketing databases (call centres), client complains**
- **Customer loyalty programs**
- **Patient/client databases**
- **Personnel files and performance reviews, IQ tests, diplomas, training**
- **Legal documents, contract management and due diligence checks for new partners**
- **Credit card statements**
- **Cameras and fingerprints for access control**
- **Parking permits, visitor and access management**
- **Phone books**
- **End-user apps, downloads, shared folders**

Sources: structured and unstructured (emails, documents, presentations, spreadsheets, dropbox)

How do I identify personal data?

- Interviews
  - Follow a process or a list of assets (applications/servers)
  - Identify activities managing personal information with an expert
- Workshops
- Questionnaires
- Data discovery
  - Data, application and user discovery

Interviews



GDPR Assessment in Interviews

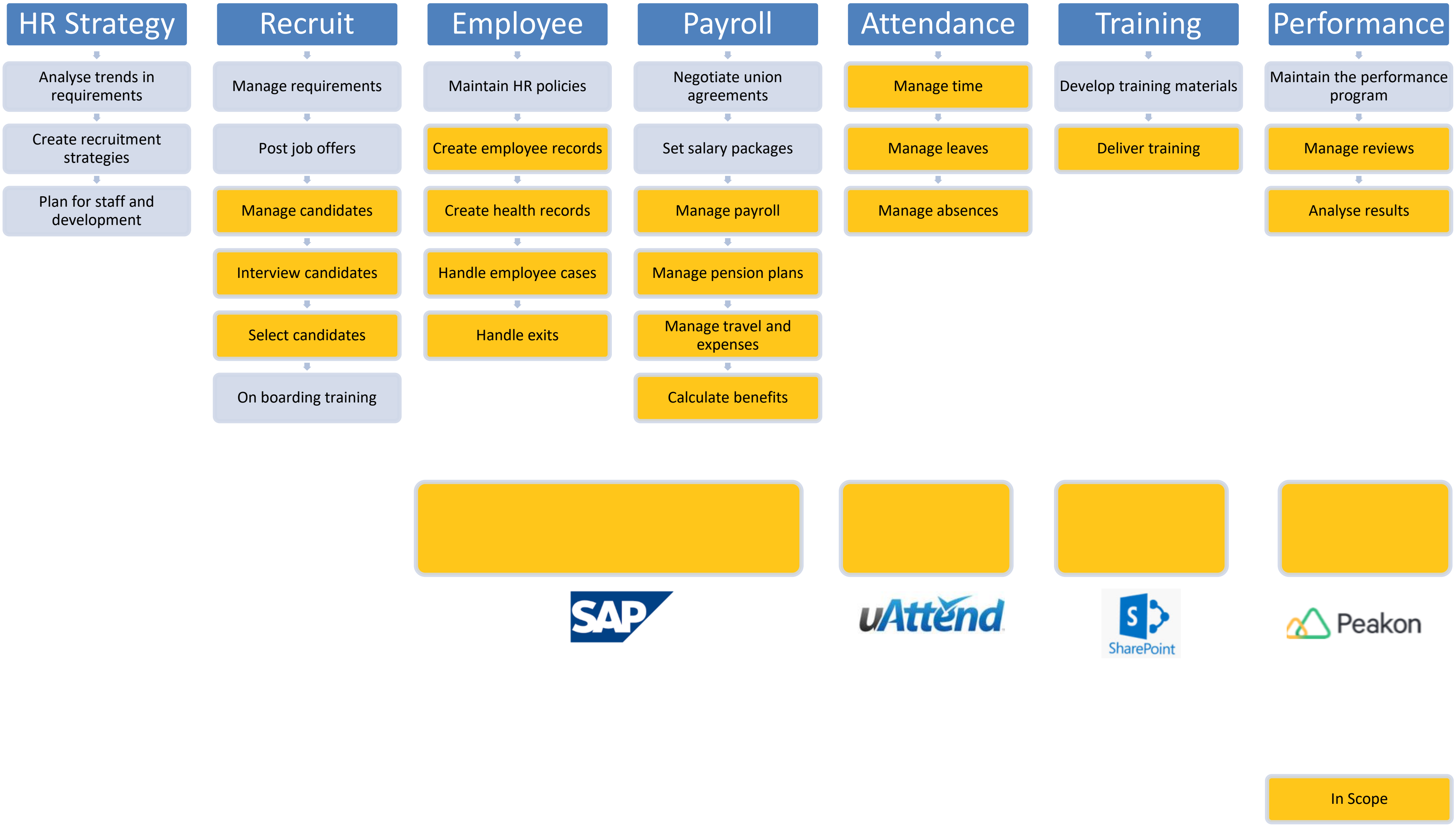
*Interview with*____________ *from*__________ *department*

*Date*__________

Objective	Questions	Answer	Assessed risks
Scope	What **types of personal information** are you processing? Personal information is information that can be attributed to one or more natural persons (e.g. name, address, e-mail address, position). Some of this information can be confidential (CPR number, wages, wealth and other economic data) or sensitive (special categories: health/medical records, biometric/fingerprints, genetic, religion, ethnicity, political, union membership, sexuality and criminal offenses)		
Categories	What **categories** of natural persons are you processing? Information about : - employees or candidates in HR (e.g. employee files, talent management) - employees or candidates outside HR (e.g. travel, insurance, legal) - European residents (e.g. clients, prospects, vendors, partners) - sole proprietors		
Purpose	What are the **purposes** for which your are processing personal information? - reasons of collecting and transferring personal information (e.g. occupational medicine, background checks, process payments) - reasons to display personal information		
Lawful processing	What are the **legal basis** for processing personal information? 1- The individual (data subject) whom the personal information is about has unambiguously consented to the processing (e.g. direct marketing) 2- Processing is necessary for: - the performance of a contract with the individual or to take steps to enter into a contract (e.g. employment or business contracts) - compliance with a legal obligation (e.g. abide an EU law or court decision, social security) - to protect the vital interests of a individual or another person such as children (e.g. matter of life cases, usually use of medical records, physically or legally incapable of giving consent in an emergency)		
Physical processing	To what **extent** is personal information **physically processed**? - documents and papers with personal information - papers with sensitive and confidential personal information locked in cabinets - clean desk policy		
IT System processing	What IT systems and applications do you use for processing personal information?		
Access control	Are you monitoring and frequently reviewing the accesses to IT systems dealing with personal information by employees and users? - Access control policy requiring approvals by supervisors - Review of principle of least privilege and work-related needs - Review of user rights		

- Interview template in the toolkit

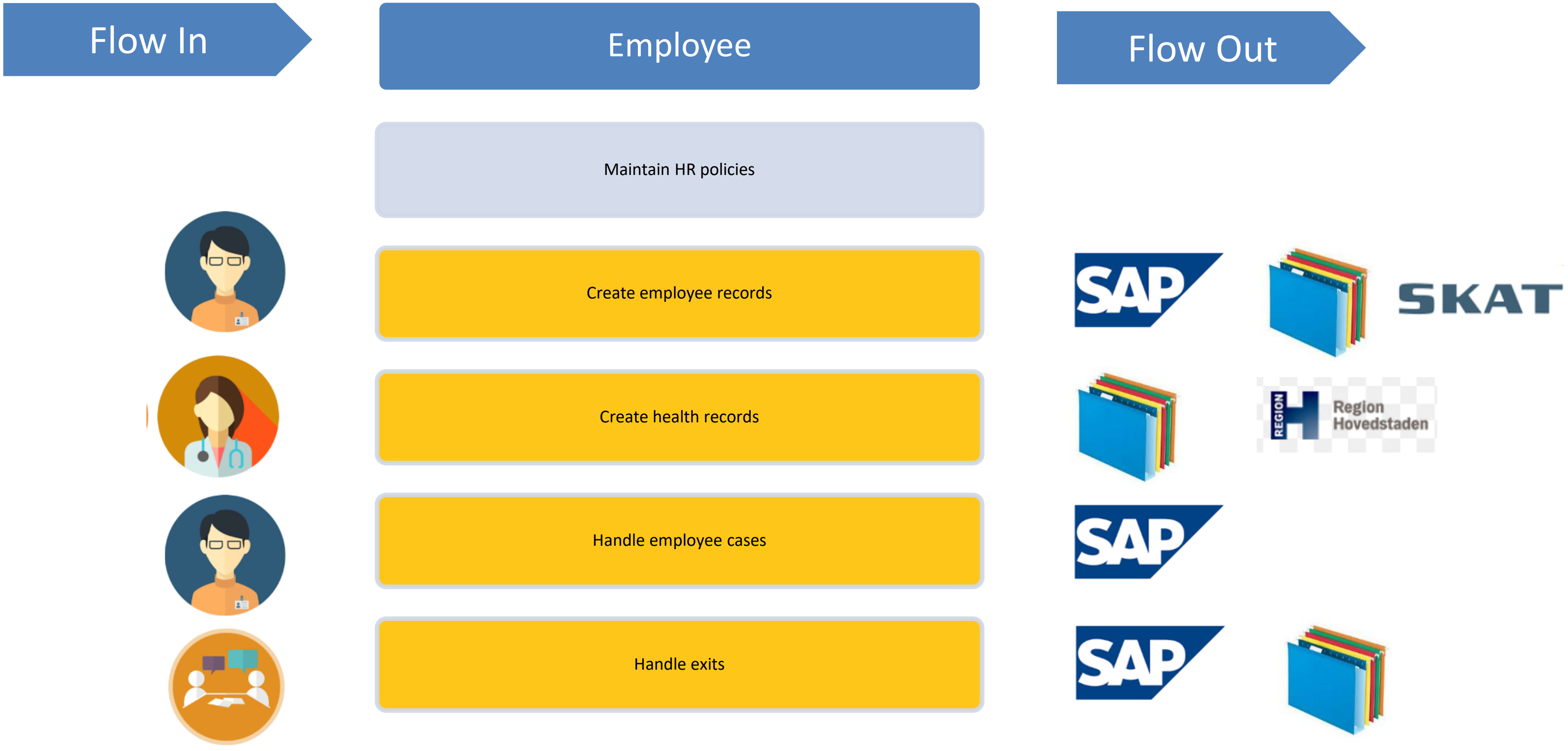
Step 3: Scope example



HR Strategy	Recruit	Employee	Payroll	Attendance	Training	Performance
Analyse trends in requirements	Manage requirements	Maintain HR policies	Negotiate union agreements	🟨 Manage time	Develop training materials	Maintain the performance program
Create recruitment strategies	Post job offers	🟨 Create employee records	Set salary packages	🟨 Manage leaves	🟨 Deliver training	🟨 Manage reviews
Plan for staff and development	🟨 Manage candidates	🟨 Create health records	🟨 Manage payroll	🟨 Manage absences		🟨 Analyse results
	🟨 Interview candidates	🟨 Handle employee cases	🟨 Manage pension plans			
	🟨 Select candidates	🟨 Handle exits	🟨 Manage travel and expenses			
	On boarding training		🟨 Calculate benefits			

🟨 In Scope

Step 3: Scope example


Flow In

Employee

Flow Out

Maintain HR policies

Create employee records

Create health records

Handle employee cases

Handle exits

In Scope

Group discussion

- Which departments hold most of the personal data in your organization?

Step 4: Compile a data inventory

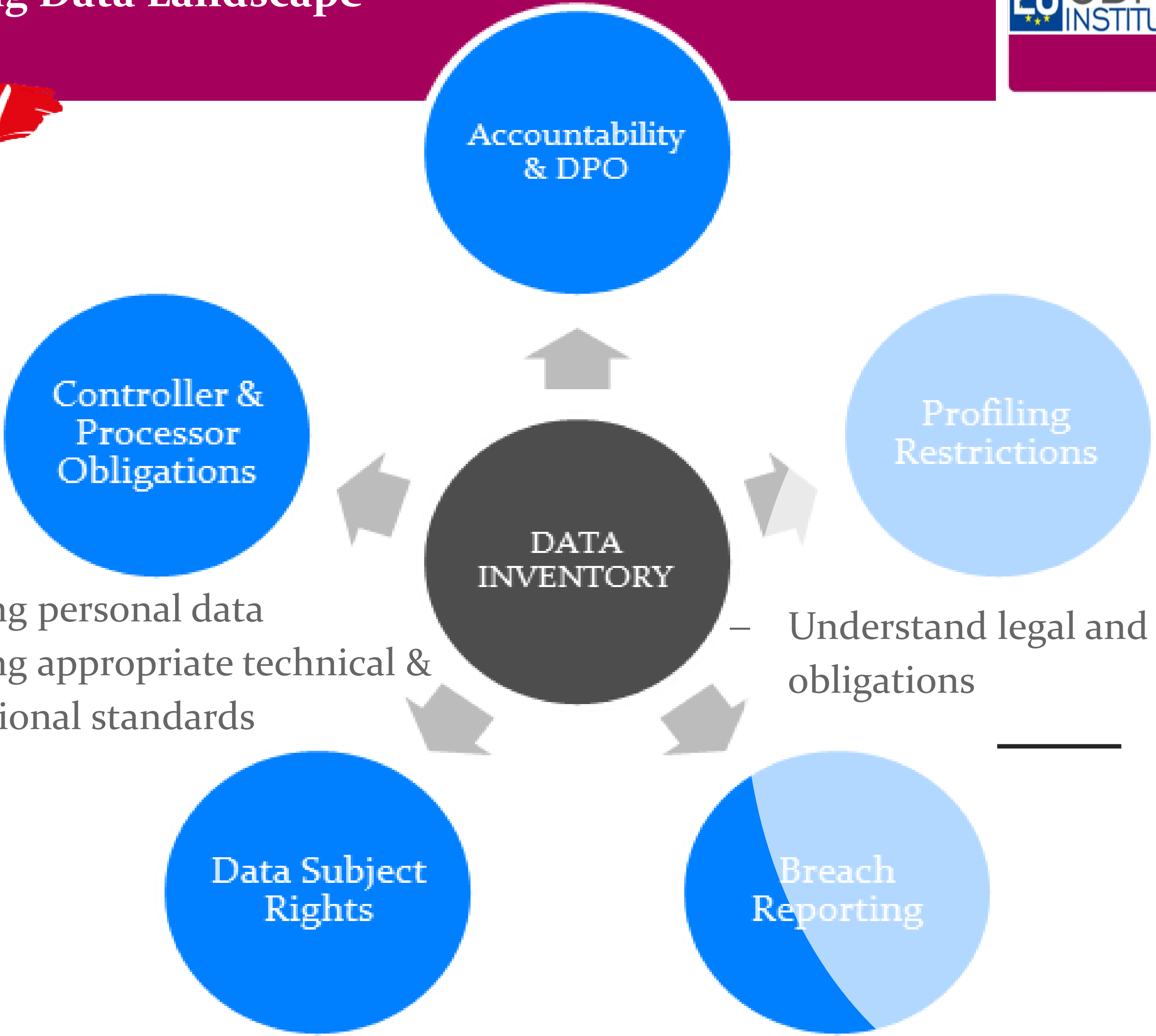
NEW

- **What personal data do we hold?**
- **Where is it?**
- **What is it being used for?**
- **How secure is it?**

Data Landscaping: A value-based approach to document what data is held, why, for how long, where, where it came from, & with whom it will be shared, when and where.

Analysing Data Landscape

NEW



- Identifying personal data
- Identifying appropriate technical & organisational standards

- Understand legal and regulatory obligations

Step 4: Compile a data inventory

Departments to cover

- Commercial, marketing, advertising, customer care, complains system
- HR, payroll, health & pension insurance, recruitment
- Procurement, A/R and treasury
- Legal, including the whistleblowing line

Support: compliance, IT, process experts

Tip: Data changes. Plan who will update the inventory

Step 4: Compile a data inventory

EU GDPR INSTITUTE

Who

- are the data subjects?
- has access to their personal data?

Where

- the personal data is stored?
- the personal data is transfered?

Why

- the personal data is under the Organization control?

When

- the personal data is kept until?
- Is shared with third-parties?

What

- safety mechanisms and controls are is place?

We had finally identified all the privacy risks! Yeah, keep trying

EU GDPR INSTITUTE

Step 4: Template & example

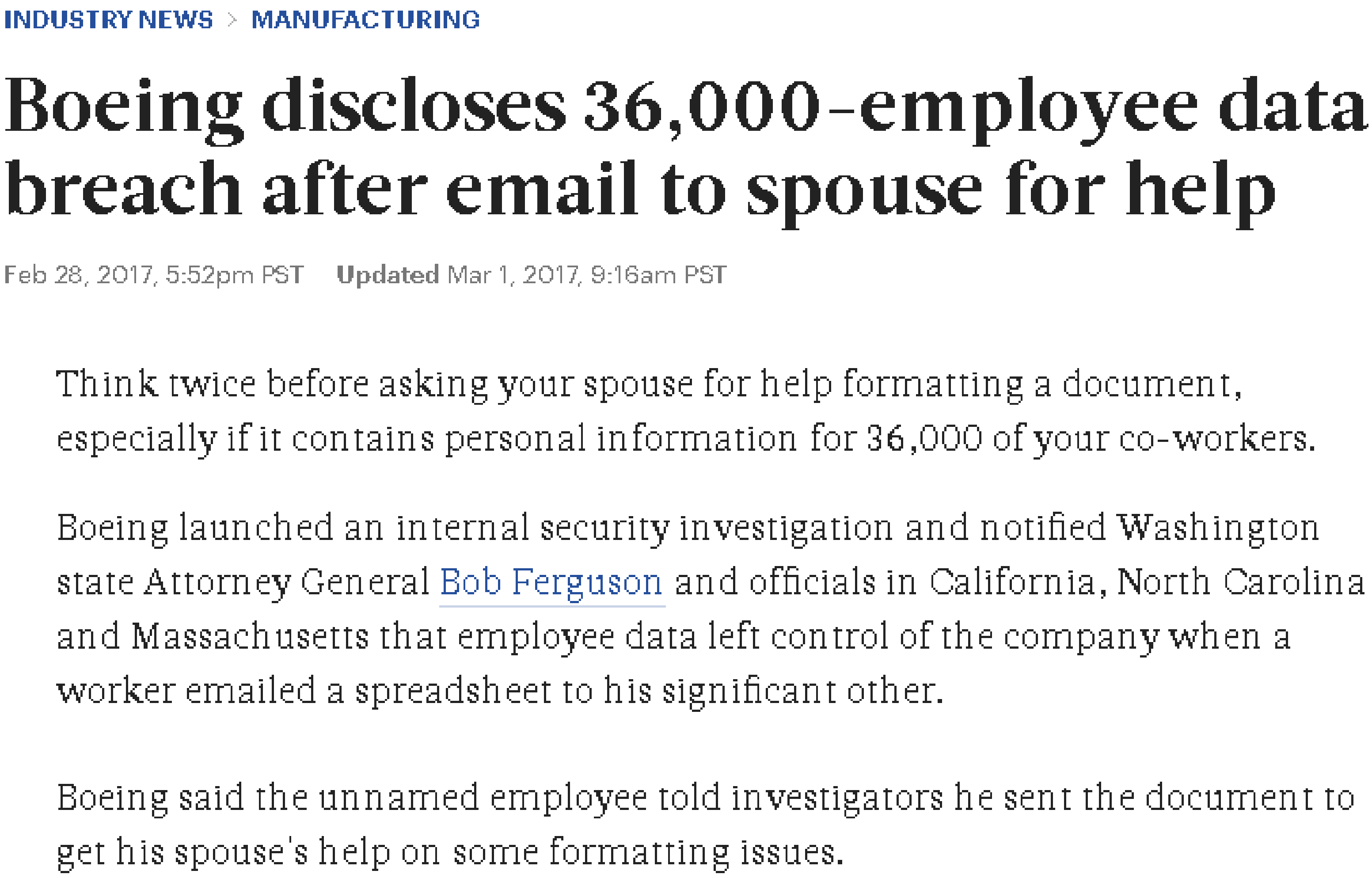
Personal data	Purpose	Data subject	Retention	Owner	System or service	Security measures
Employee name, address, phone, date of birth	Identification	Employees Ex-employees Candidates	Permanent file	HR	SAP HR	Password, encryption
					Personnel filing cabinets	Physical safeguards
	Payroll processing	Employee	Until end of employment	HR	SAP HR	Password, encryption
					MS Excel files	Protected folder
	Performance review	Employee	Until end of employment	HR	Cornerstone Performance	Password

Step 4: Template & example

Other information to consider

- Notice, choice and consent
- Collection mechanism
- Technical information of data: format, structure
- Storage location: paper archive, cloud, in-house, server, networks, email / country
- Storage medium
- Security classification: confidential, restricted
- Source: system generated, input
- Collected by
- Used by
- Disclosed to (expand disclosure to other parties)
- Retention period
- Deletion type
- Volume (gigas, records)
- Transfer to ("data processing inventory", recipients, countries, processor/controller relationship)
- Privacy risk rating

Step 4: A bad example



INDUSTRY NEWS > MANUFACTURING

Boeing discloses 36,000-employee data breach after email to spouse for help

Feb 28, 2017, 5:52pm PST **Updated** Mar 1, 2017, 9:16am PST

Think twice before asking your spouse for help formatting a document, especially if it contains personal information for 36,000 of your co-workers.

Boeing launched an internal security investigation and notified Washington state Attorney General Bob Ferguson and officials in California, North Carolina and Massachusetts that employee data left control of the company when a worker emailed a spreadsheet to his significant other.

Boeing said the unnamed employee told investigators he sent the document to get his spouse's help on some formatting issues.

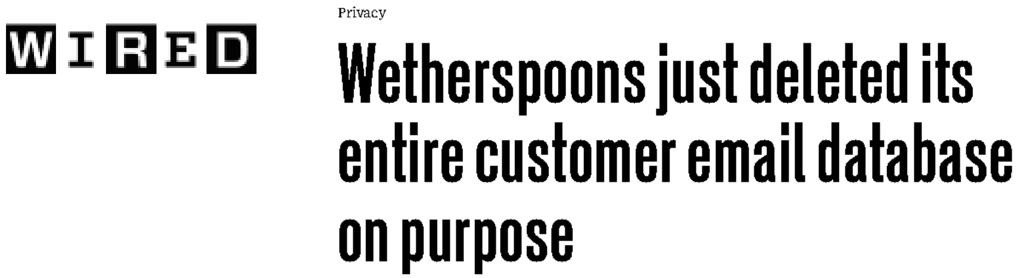
Step 5: Clean the house!

The GDPR is an opportunity to improve data practices

De-risk! Start clean!

- **Stop asking for personal data which is not needed**
- **Delete personal data after it is not longer needed**
- **Restructure databases to avoid redundancies in personal data**
- **Centralize channels to receive personal information**
- **Anonymize data, erasure copies and links**
- **Opt out in email lists**
- **Remove duplicate, out-of-date or inaccurate records**
- **Be conservative: there are not fines for over-deleting**

Step 5: Discussion case

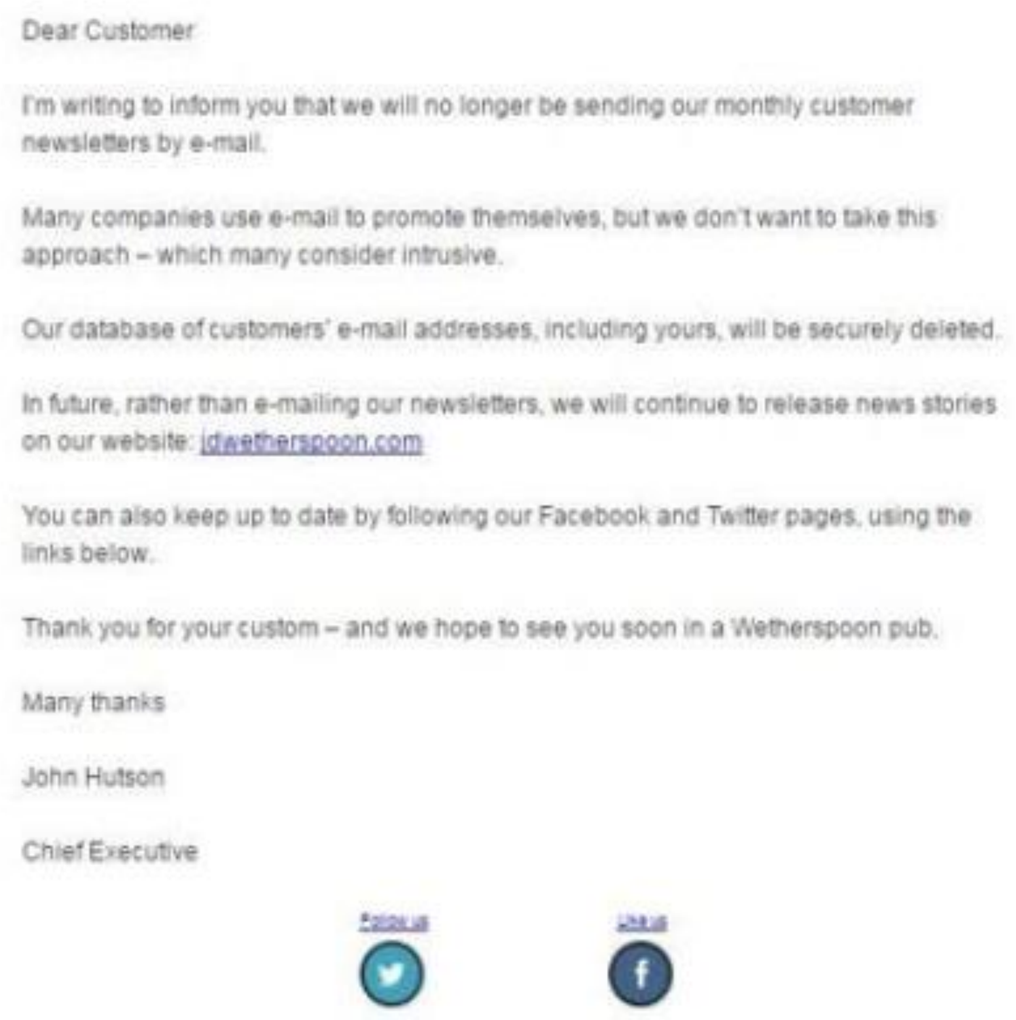

WIRED

Privacy

Wetherspoons just deleted its entire customer email database on purpose

- UK pub chain deleted their customer emails from marketing database in Jun 2017
- Contacts are now by Twitter and Facebook
- They suffered a breach of 665k emails in 2015

Step 5: Discussion case



Dear Customer

I'm writing to inform you that we will no longer be sending our monthly customer newsletters by e-mail.

Many companies use e-mail to promote themselves, but we don't want to take this approach – which many consider intrusive.

Our database of customers' e-mail addresses, including yours, will be securely deleted.

In future, rather than e-mailing our newsletters, we will continue to release news stories on our website: jdwetherspoon.com

You can also keep up to date by following our Facebook and Twitter pages, using the links below.

Thank you for your custom – and we hope to see you soon in a Wetherspoon pub.

Many thanks

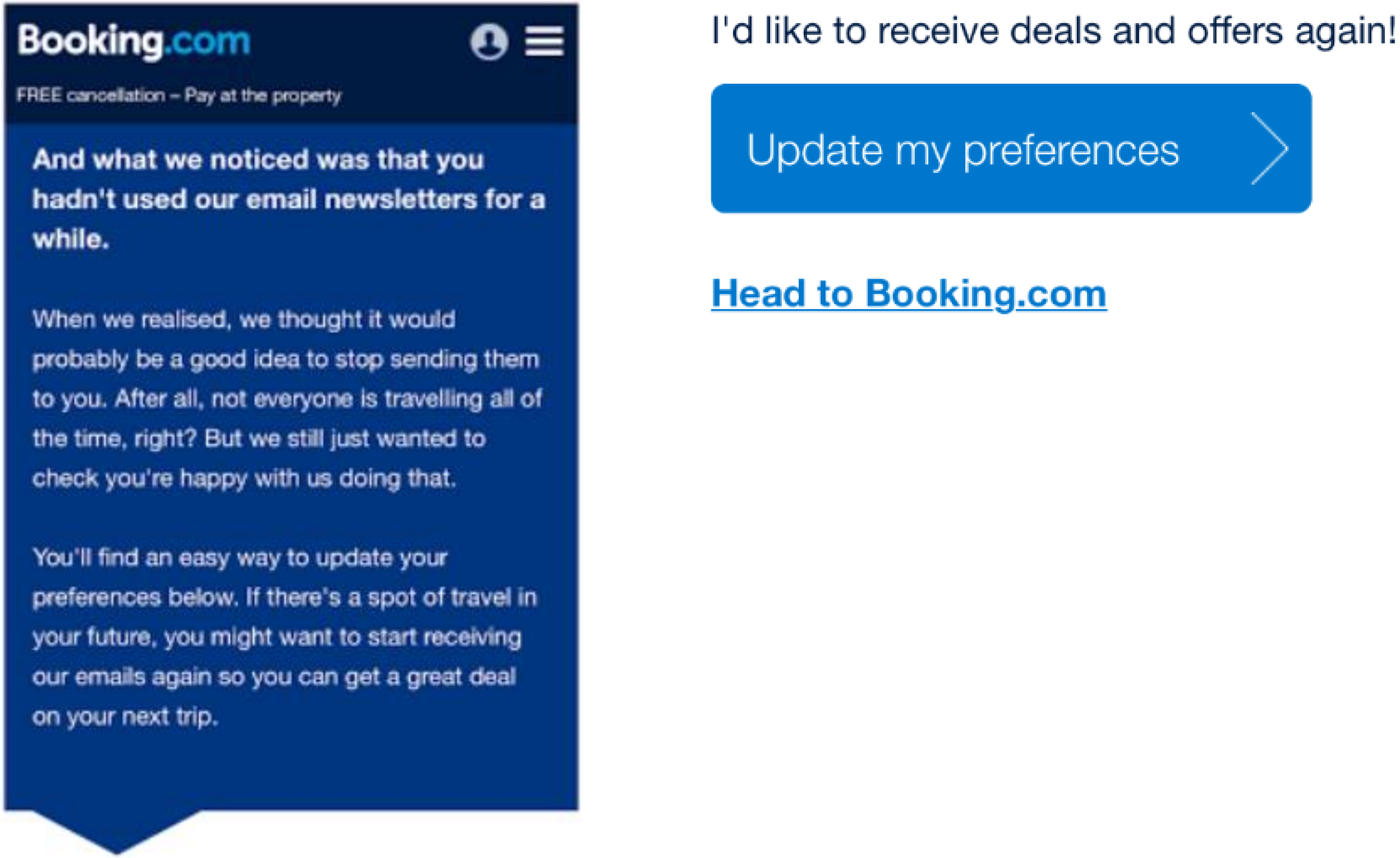
John Hutson

Chief Executive

Follow us Like us

- Pros
  - Less intrusive?
  - No need to keep track of consents?
- Cons
  - Communication of offers

Step 5: An example



FREE cancellation – Pay at the property

And what we noticed was that you hadn't used our email newsletters for a while.

When we realised, we thought it would probably be a good idea to stop sending them to you. After all, not everyone is travelling all of the time, right? But we still just wanted to check you're happy with us doing that.

You'll find an easy way to update your preferences below. If there's a spot of travel in your future, you might want to start receiving our emails again so you can get a great deal on your next trip.

I'd like to receive deals and offers again!

Step 6: Create a privacy policy

Best practices based on the ISO 27001

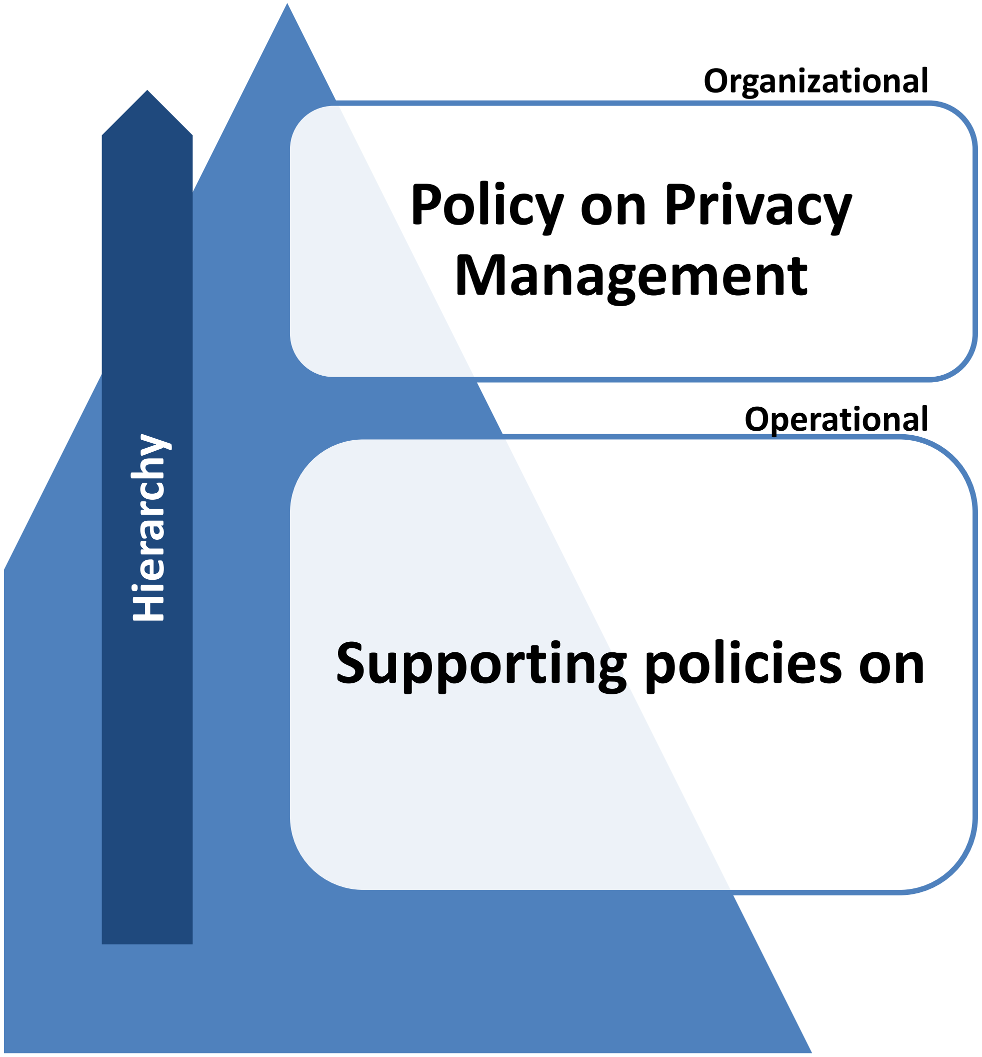
- **Set the information security objectives**
  - **provide access of information only to authorized employees and 3rd parties**
  - **protect the confidentiality, availability and integrity of information assets**
  - **implement annual information security awareness trainings**
- **Support from upper management**
  - **Policy approved by CEO, IS compliance reports to board**
- **Responsibilities to data owners, data users, IT, risk management and internal audit**
- **Communicated across the Organization and 3rd parties**
- **Regularly updated**

Step 6: Create a privacy policy

Recommended chapters

- **Organization privacy vision**
- **Define data categories**
- **Organization of applicable policies**
  - **Data retention, information security, recognize GRPD rights**
- **Define general principles and roles to limit:**
  - **the collection**
    - **how the consents are ensured, when risk impacts are done**
  - **the use**
    - **how data is secured and given access to**
  - **the disclosing**
    - **define circumstances for disclosure, complains and requests, notification of breaches**

Step 6 : Create a privacy policy



Hierarchy

Organizational

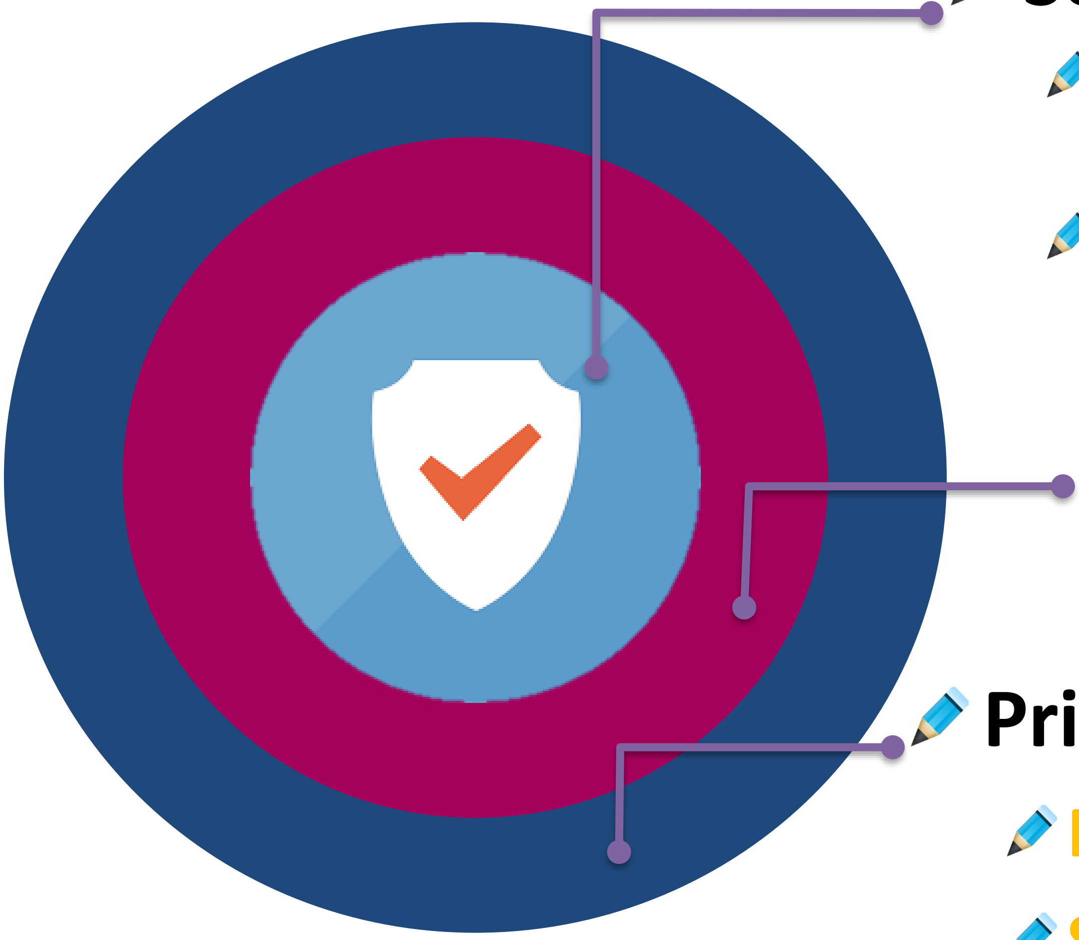
Policy on Privacy Management

Operational

Supporting policies on

- data breach incident management
- duty of disclosure
- classification and acceptable use of information assets
- backup & business continuity
- access control y password
- handling international transfers
- clear desk and clear screen policy
- use of network services
- software development
- data processing agreements

Privacy policy



- Security strategy
  - Part of the business ethics
  - Risk tolerance based on the customer trust
- Data security policy
  - Objectives
- Privacy policy
  - Privacy program
  - Supporting policies

Step 6: Create a privacy policy

- Privacy policy template by the GDPR Institute
- Please ask us if you need further templates for additional policies

Supporting policies

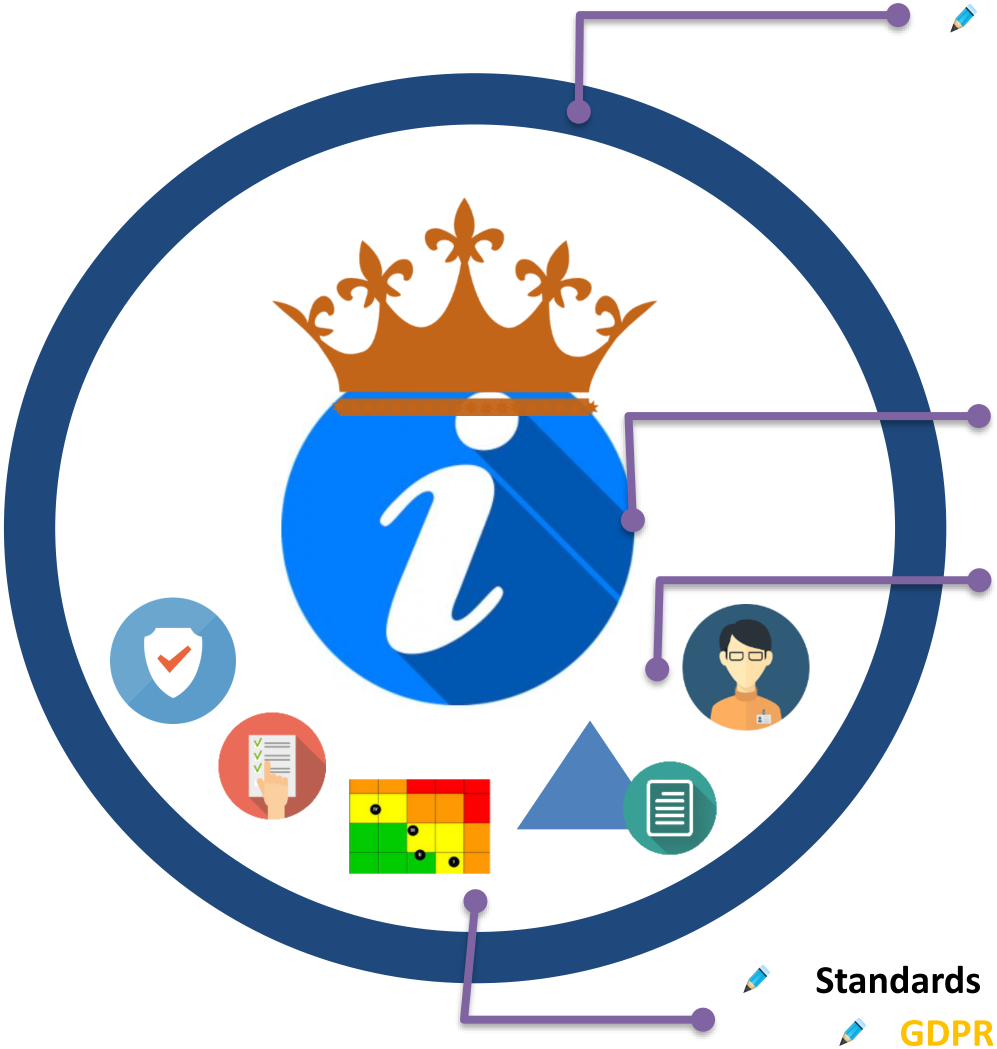
Specific policies

- records retention
- access control and delegation of access to employees' company e–mail accounts (vacation, termination)
- acceptable collection and use of information resources incl. sensitive personal data
- obtaining valid consent
- collection and use of children and minors’ personal data
- secondary uses of personal data
- maintaining data quality
- destruction of personal data
- the de–identification of personal data in scientific and historical researches

Policies to add privacy controls

- use of cookies and tracking mechanisms
- telemarketing, direct and e–mail marketing
- digital advertising (online, mobile)
- hiring practices and conducting internal investigations
- use of social media
- Bring Your Own Device (BYOD)
- practices for monitoring employee (CCTV/video surveillance)
- use of geo–location (tracking and or location) devices
- e–discovery practices
- practices for disclosure to and for law enforcement purposes

Data Protection Management System



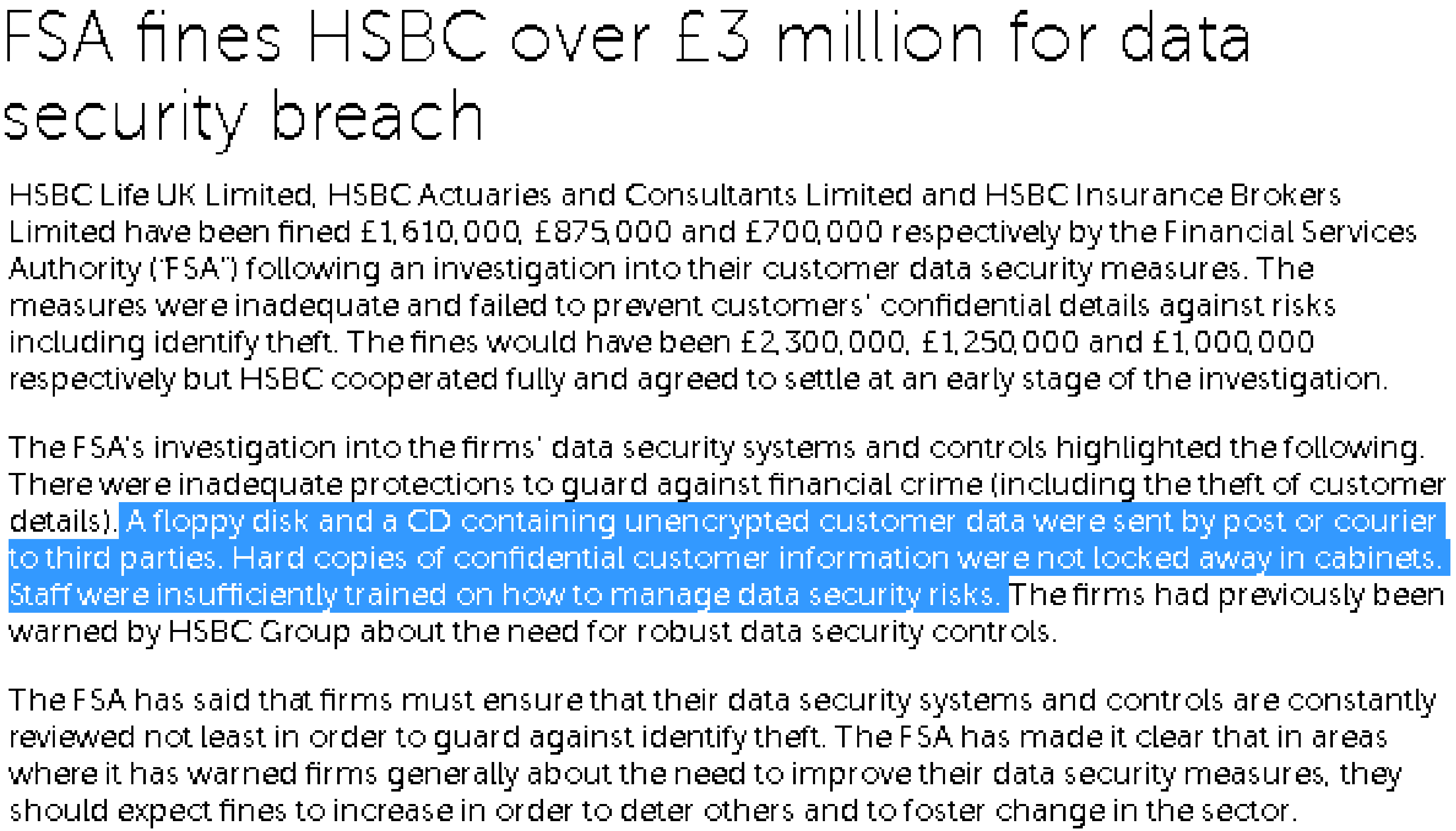
- Compliance system
  - Risk-based
  - Nature, scope, context and purposes of the data processing
  - Integrated to other compliance systems
  - Synergies for training, documenting, managing risks, auditing
- “Crown Jewels” Personal Data
  - Objective to prevent a data breach
  - Identify critical personal data
- Elements
  - Personal data policy
  - Additional supporting policies
  - Data protection officer
  - DPIA
  - IT security controls
  - 3rd party contracts
  - Reporting and dashboard
- Standards
  - GDPR Requirements
  - ISO 27001/2

Step 6: Removable media

Removable media is a common route for the introduction of malware and the accidental or deliberate export of sensitive data

- Employees should not use removable media as a default mechanism to store or transfer information → offer alternatives
- Media ports should be approved for few users
- All removable media should be provided by the Organization
- Sensitive information should be encrypted at rest on media
- Educate employees to maintain awareness

Step 6: Discussion case



FSA fines HSBC over £3 million for data security breach

HSBC Life UK Limited, HSBC Actuaries and Consultants Limited and HSBC Insurance Brokers Limited have been fined £1,610,000, £875,000 and £700,000 respectively by the Financial Services Authority ("FSA") following an investigation into their customer data security measures. The measures were inadequate and failed to prevent customers' confidential details against risks including identify theft. The fines would have been £2,300,000, £1,250,000 and £1,000,000 respectively but HSBC cooperated fully and agreed to settle at an early stage of the investigation.

The FSA's investigation into the firms' data security systems and controls highlighted the following. There were inadequate protections to guard against financial crime (including the theft of customer details). A floppy disk and a CD containing unencrypted customer data were sent by post or courier to third parties. Hard copies of confidential customer information were not locked away in cabinets. Staff were insufficiently trained on how to manage data security risks. The firms had previously been warned by HSBC Group about the need for robust data security controls.

The FSA has said that firms must ensure that their data security systems and controls are constantly reviewed not least in order to guard against identify theft. The FSA has made it clear that in areas where it has warned firms generally about the need to improve their data security measures, they should expect fines to increase in order to deter others and to foster change in the sector.

B - Do

Step 1: Limit access

- Ensure the minimum access based on the employees' **need to know** to perform their job
- May require to update the access control policy
- Restrict the rights to enter, display, alter and remove personal information
- Include any cloud hosted files
- Access management solutions and using controls access roles are useful
- Limit super user roles, DBAs and third parties
- Single sign-on, control under the active directory

Step 1: Tips

- Keep all user credentials secure and centralized
- Enforce strong, unique and often-changed passwords
- Implement dual controls for key personal information
- Closely restrict access for 3rd parties and monitor their activity
- Audit all access to privileged accounts
- Eliminated hard-coded credentials in scrips and application
- Log sessions for forensic audits

Step 2: Review consents
How consents should be given?

Plain language

- Explicit purpose of processing
- Scope and consequences
- List of rights
- Separated from other

Opt-Out

- Genuine choice to withdraw any time
- Affirmative actions: silence, pre-ticked boxes and inactivity are inadequate

Updated

- Reviewed when the use of data change
- When the data controller changes (or the contact details)
- Being able to demonstrate

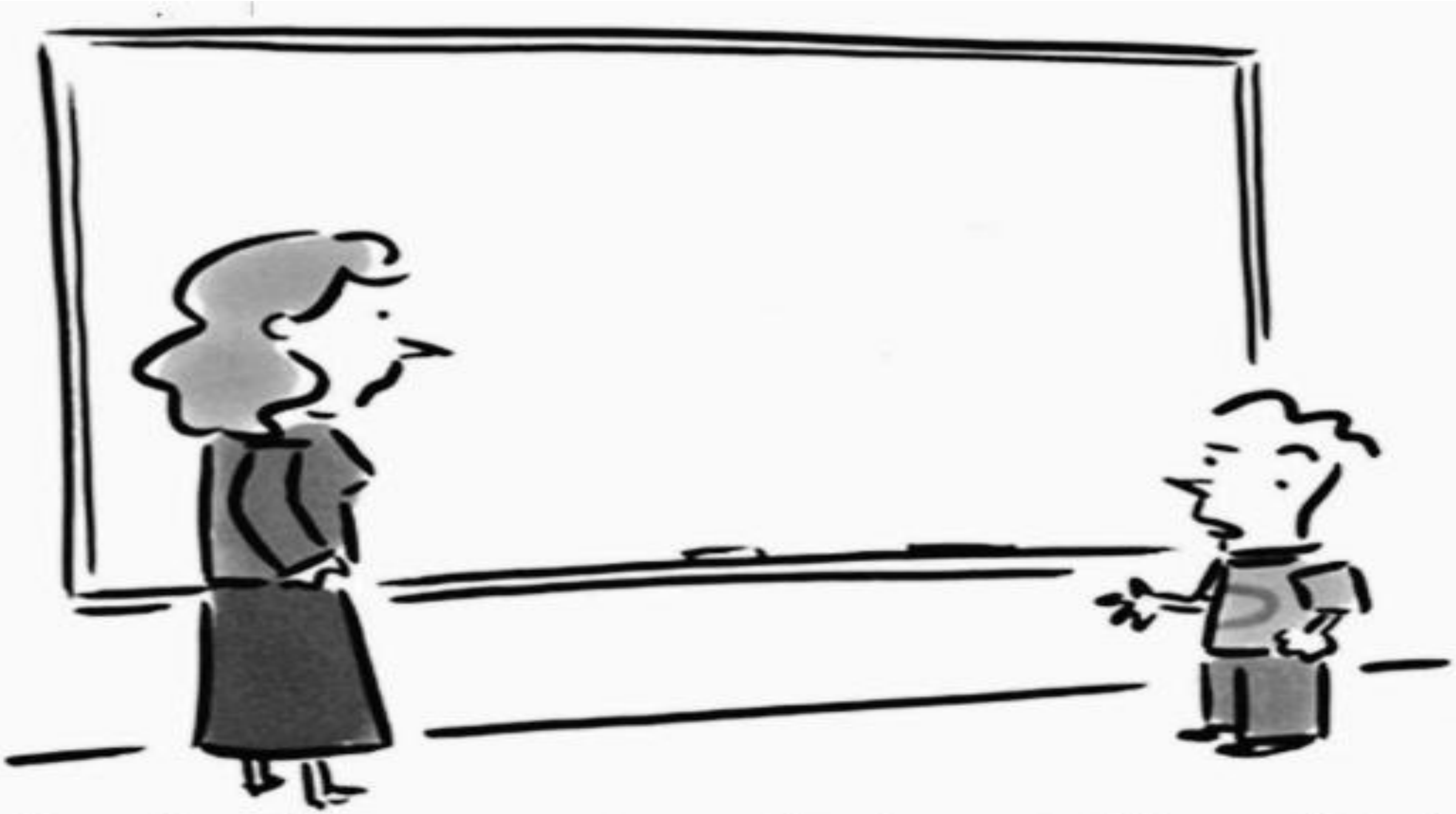
Minors

- Parental authorization for children bellow the age of 16
- Reasonable means to verify parental consent

Step 2: Tips

- Focus on ‘explicit consents’ for sensitive data and international transfers
- Link the consents to the personal data inventory
- Confirm that the consents are clear and transparent
- Update the data subject rights
- Audit how the consents are documented and retained
- Audit if the op-outs are processed on time

Step 2: Review consents



"Before I write my name on the board, I'll need to know how you're planning to use that data."

Step 3: Prepare to deal with requests

NEW

- 1 month to comply with requests from data subjects
- Many requests are received → extended to 2 months more
- Flood of data requests post-GDPR?
- Request are a key part of the implementation strategy
  - Prepare a protocol, train caseworkers and test how it works
  - Tool to copy insulated personal data in standard format
- All info: electronic + on paper + archived data
- Understandable format
  - Structured, common and machine-readable → CVS, HTML, PDF, MPEG/videos, TIFF
  - Add reference tables when parameters and codes are used
- Format "in writing"
  - Letter, email, customer contact, social media → use a standard form
- **Reasonable requests** → free
- **Repetitive or unreasonable requests** → fee based on administrative costs
- **Disproportionate or expensive requests** (proven) → refuse

Step 3: Tips

- Before acting, control that data requests are
  - accurate and fully completed,
  - fees are paid, and
  - identity of data requesters (and representative) are validated
- Once controlled, act promptly
  - In particular, when third parties have personal data
- Refine the scope: offer to focus the research when the request is extremely wide and involve large volume of data
- Centralize and prioritize requests according to complexity
- Use a document management system

Step 4: Validate data transfers

Flows-in the organization

- Who input the personal information
- Collected personal data fields
- Storage location

Flows-out (data transfer or display)

- Categories of recipients in EU or non-EU countries
- Security measures on the transfer (e.g. encryption standard)

Step 5: Review contracts

Controller

Processor

Data exporter when processing is outside de EU

Review data processing agreements: clear responsibilities and use of sub-contracts

Audits and certifications

There are “model clauses” for data exports

Negotiate the cost of GDPR compliance in fees

Foresee dispute resolutions and compensation clauses

Data controller responsibilities

- able to NEW demonstrate compliance with the GDPR
- ensure personal data is:
  - processed fairly and lawfully and in accordance with the principles of the GDPR
  - is carried out under a contract
  - processed by the data processor only on clear and lawful instructions based on the contract
- exercise overall control
  - – Data protection by design and by default NEW
- notify breaches

Data processor responsibilities

- process personal information on behalf of the data controller client
- act only on instructions from the data controller
  - comply with a clear standard
  - impose a confidentiality obligation to its employee dealing with controller`s information
- provide sufficient guarantees to demonstrate compliance NEW
  - in respect of the technical and organizational security measures governing the processing
- Allow a data controller audits NEW
  - on premises, systems, procedures, documents and staff
- Delete or return data at the end of the contract

Principles

Processed lawfully, fairly and transparently

Processed in a manner that ensures appropriate security

Collected for specified, explicit and legitimate purposes

Accurate and, where necessary, kept up to date

Adequate, relevant and limited to what is necessary

Kept for no longer than is necessary

Rights

EU GDPR INSTITUTE

To access data

request access to personal data to verify lawfulness of processing

NEW

To data portability

common format, even directly transmitted between controllers

NEW

To rectify and be forgotten

when no longer necessary or consent is withdrawn

To object by controller

when unjustified by either "public interest" or "legitimate interests

NEW

To restrict processing

limiting the data use or transfer

To limit profiling

right to not be subjected to automated individual decision making

Difference

Privacy notices

Data subject right to be **informed** on fair collection

Legal basis, type of information, 3rd parties recipients and retention period

Consents

Formal **permit** to process personal information by the data subject

Step 2: Review consents
How should consents be given?

Plain language

- Explicit purpose of processing
- Scope and consequences
- List of rights
- Separated from other

Opt-Out

- Genuine choice to withdraw any time
- Affirmative actions: silence, pre-ticked boxes and inactivity are inadequate

Updated

- Reviewed when the use of data change
- When the data controller changes (or the contact details)
- Being able to demonstrate

Minors

- Parental authorization for children bellow the age of 16
- Reasonable means to verify parental consent

Step 6: Notify a data breach

Data breach

- Accidental or unlawful…
- unauthorized disclosure or access + destruction, loss, alteration …
- of personal data transmitted, stored or processed

When to notify

- Not latter than 72 hours after having become aware of it
- Undue delays should be justified

What to notify

- Type and number of data records and subjects compromised (aprox)
- DPO contact info
- Likely consequences and mitigation measures

Whom to notify

- Supervising authority
- Each data subject is likely to result in a high risk for the right of unencrypted data

Step 7: Data security program

Encryption of personal data

- Key element in GDPR standard
- No always feasible: depending on costs and risks, impact on performance
- Encryption of stored (eg. hard disk) and in transit data (e.g. calls)

Security measures

- Ongoing review (e.g. access audis)
- Importance of two-factor authentication, ISO 27001, compartmentalization and firewalls
- Patches for malware & ransomware

Resilience

- Restore data availability and access in case of breach
- Redundancy and back and facilities
- Incidence response plan

Regular security testing

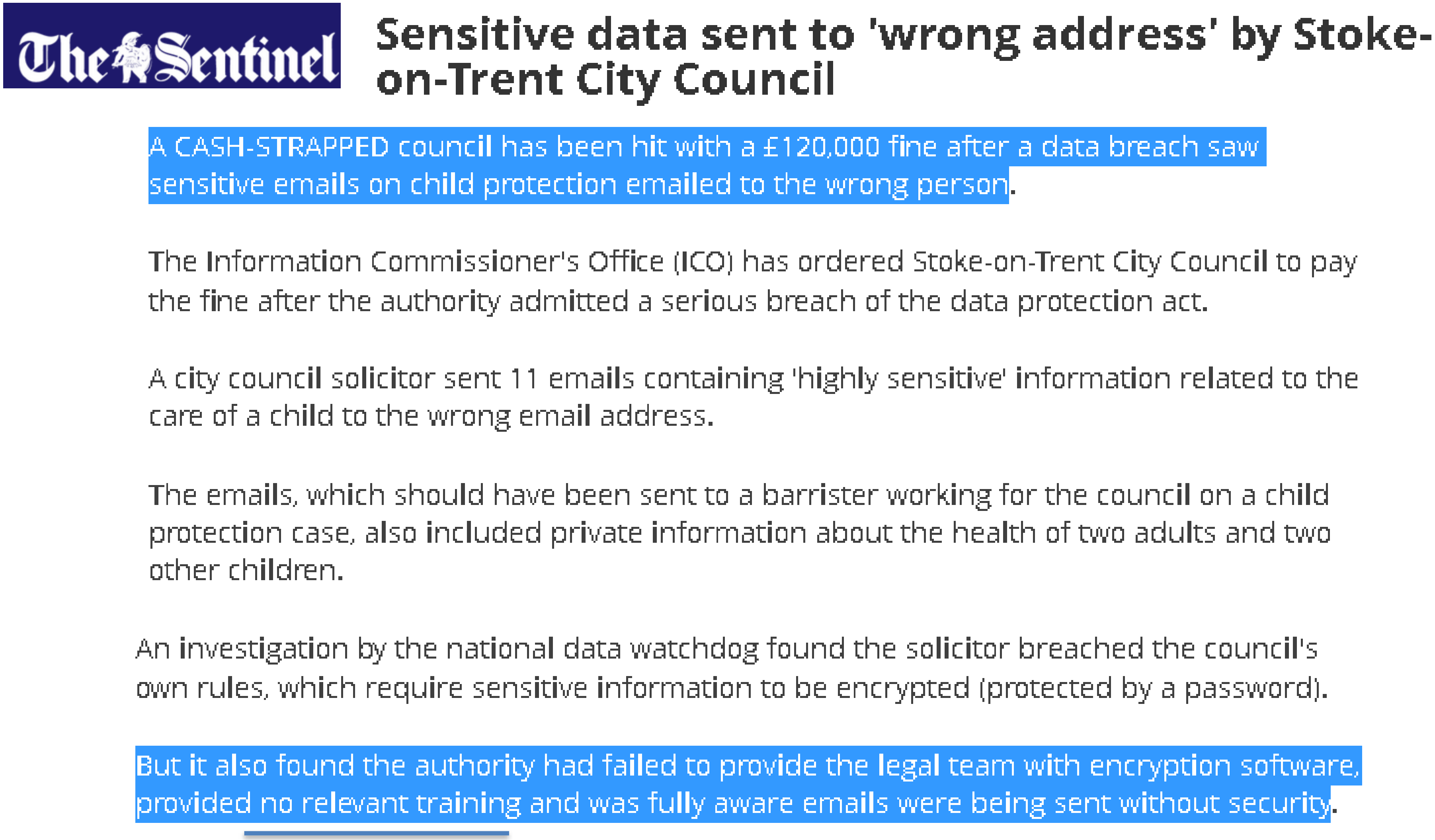
- Assessment of the effectiveness of security practices and solutions
- Penetration, network and application security testing

C – Improve and Maintain

Step 1: Train your people

- Employees from the top to the bottom
  - Clear message: there are disciplinary actions for mishandling personal information
  - Face to face or on-line? How repetitive? Security and/or fraud risks?
- Privacy awareness campaings
  - Promote the privacy culture
- Explain how to deal with personal data for specific purposes
  - How employees can detect and prevent a data breach
  - Be relevant to each target audience, how the GRPD changed privacy practices to each group
  - Avoid legal terms of the GDPR , allow questions
  - Discuss real life cases: I missed a memory stick, I sent an email to the wrong person, my laptop was stolen, I received a call from the “insurance Organization” asking for a HR database (phishing), I received a “google” request to install an app (virus prevention)
- Both electronic and on paper

Step 1: Discussion case



The Sentinel

Sensitive data sent to 'wrong address' by Stoke-on-Trent City Council

A CASH-STRAPPED council has been hit with a £120,000 fine after a data breach saw sensitive emails on child protection emailed to the wrong person.

The Information Commissioner's Office (ICO) has ordered Stoke-on-Trent City Council to pay the fine after the authority admitted a serious breach of the data protection act.

A city council solicitor sent 11 emails containing 'highly sensitive' information related to the care of a child to the wrong email address.

The emails, which should have been sent to a barrister working for the council on a child protection case, also included private information about the health of two adults and two other children.

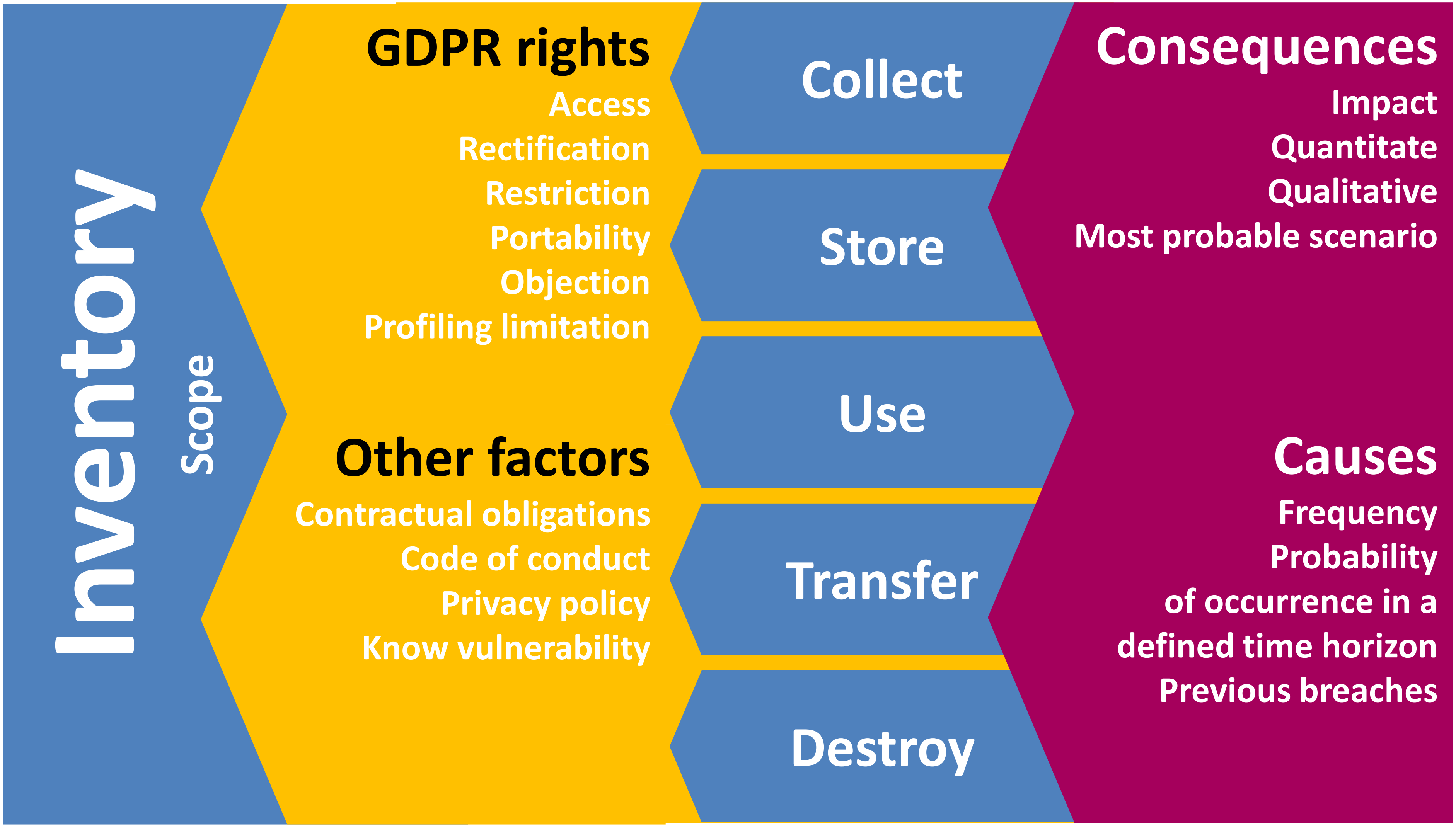
An investigation by the national data watchdog found the solicitor breached the council's own rules, which require sensitive information to be encrypted (protected by a password).

But it also found the authority had failed to provide the legal team with encryption software, provided no relevant training and was fully aware emails were being sent without security.

Step 2
Data Protection Impact Assessment

- Process to identify, analyse, evaluate, consult, communicate and plan the treatment of potential privacy impacts with regard to the processing of personal information (ISO 29134:2017 Guidelines for DPIA) → Goal: avoid a data breach
- Framed within the general risk management framework of the organization
- Mandatory for the data controller to early identify required control measures
- Only for new and high-risk activities or projects in processing personal data:
  - large sensitive data,
    - e.g. healthcare providers and insurance companies
  - extensive profiling, or
    - automated-decision making (e.g. by scoring) with legal or similar significant effect
    - e.g. financial institutions for automated loan approvals, e-recruiting, online marketing companies, and search engines with target marketing facilities
  - monitoring public places
    - e.g. local authorities, CCTV in all public areas, leisure industry operator
- One DPIA for each type of processing

Tips for risk identification



Inventory

Scope

GDPR rights

Access
Rectification
Restriction
Portability
Objection
Profiling limitation

Other factors

Contractual obligations
Code of conduct
Privacy policy
Know vulnerability

Collect

Store

Use

Transfer

Destroy

Consequences

Impact
Quantitate
Qualitative
Most probable scenario

Causes

Frequency
Probability
of occurrence in a
defined time horizon
Previous breaches

Generic risks and controls

EU GDPR INSTITUTE

Objective	Risk	Lifecycle	Component	Controls
Availability	Loss, theft or authorized removal Loss of access rights	Processing Transfer	Data, systems, processes	Redundancy, protection, repair & back ups
Integrity	Unauthorized modification	Processing Transfer	Data	Compare hash values
			Systems	Limit access, access review
Confidentiality	Unauthorized access	Storage	Data, systems	Encryption
			Processes	Rights and roles, training, audits
Ensuring unlinkability	Unauthorized or inappropriate linking	Processing	Data	Anonymity, pseudoanymity
		Processing	Systems	Separation of stored data
Compliance	Excessive or authorized collection	Collection	Data	Purpose verification, opt-out, data minimization, DPIAs
	Processing, sharing or re-purposing without consent	Processing	Data	Review of consents, logs workflow for consent withdrawals
	Excessive retention	Storage	Data	Data retention policy

Risks to the data subject

- Discrimination
  - Loss of opportunities
    - job, loan, insurance and visa applications
    - denial to access to public services
  - Other social disadvantages and exclusion (i.e. religion)
  - Key: special categories of personal data (i.e. health data)
- Fraud/Impersonation
  - Identity theft in applying for loans, new credit cards and government benefits
  - Exposition to scams and risks (i.e. phishing, espionage, DDoS attacks, social-engineering)
  - Counterfeit (i.e. passport, ID card, drive license)
  - Illegal selling of contact data (i.e. spam, marketing calls)
- Financial losses
  - Stolen money by illegal credit card purchases
  - Fraudulent wire transfers
- Reputation damage
  - Public embarrassment: remember Ashley Madison!
- Physical harm
  - Being kidnapped

Key: Higher risks involving personal data of children or other vulnerable people (i.e. handicapped)

Impacts

- Legal
  - fines and punishments resulting from non-compliance with GDPR obligations
- Financial
  - claims for damages to data controller
  - costs for the remediation
- Operational
  - business reputation
  - loss of clients and contracts
  - failure to achieve business goals
  - overwhelming workload

Example of risk registry

Event	Root cause	Consequen-ces	Impact	Probability	Treatment	Monitoring	Owner and due date
Customer personal information breached	Failures to design privacy in CMS applications Espionage Lack of maturity in privacy program	Loss of clients GDPR enforcement Business interruption Requests to delete data Loss of commercial opportunities	High 100 M EUR	Medium 15% in 3 years	Insurance policy Training Security scanning MS integrations project	Action plan progress	Noah Nilsen Mkt Director Q3 2017

Follow-up

Communicate to stakeholders, bottom-up and top-down

Advance with action plans and document implementation measures (IT and non-IT changes)

Regular post-implementation reviews to assess if risks are mitigated and to ensure that solutions identified have been adopted. Re-assess the DPIAs at least every 3 years

Toolbox

- Data Protection Impact Assessment template by the GDPR Institute

- Please ask us if you need further templates for additional policies

Privacy…

By default

- The protection of personal data must be a default property of systems and services
- Strictest privacy settings automatically must be applied once a customer acquires a new product or service
- Personal information must by default only be kept for the amount of time necessary to provide the product or service

By design

- Privacy and data protection must be a key consideration in the early stages of any project and then throughout its lifecycle
- Proactively control adherence to GRPD principles when designing for new products, services or business processes
- Appropriate technical and organizational measures
- Design compliant policies, procedures and systems

Group discussion

- **What privacy by default and by design means to you?**

Step 3: Audit compliance

- Ensure that data protection processes and procedures are being adhered to
- Implement the management reviews
- Simulate incidents (e.g. data breach) to audit protocols
- Independent testing and quality assurance
- Formalize non-compliance and remediation
- Escalate concerns and risks
- Identify compliance metrics and trends

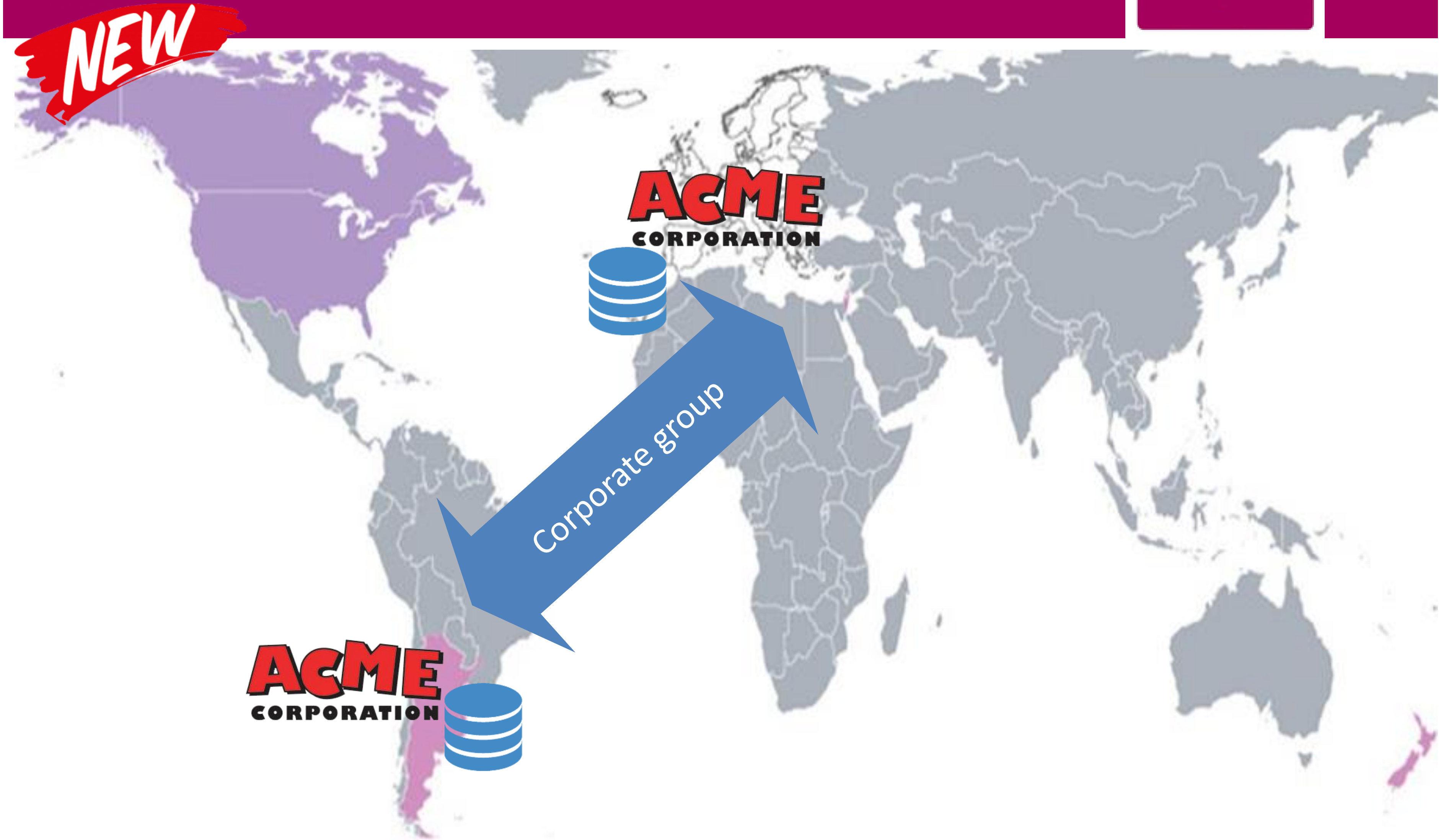
Step 4: Code of conduct & certification

- Platform for data controllers, processors and stakeholders
  - to ensure a structured and efficient means for GDPR compliance
- Significant administrative and documentation burdens
- Establish and maintain compliance with code of conduct or earning certification status
- These costs can be offset by reducing audit costs and automation

Step 4: Code of conduct & certification

- Certification can serve as marketing tool, allowing data subjects to choose controllers to signal GDPR compliance
- Plays a significant role in facilitating cross-border data transfers
- Certification mechanisms can create business opportunities for new third party administrators and programs as effective means for determining binding promises by controllers and processors

Binding corporate rules



National Supervisory Authorities

- Competent on their own state
- Single contact point: one-stop-shop
- Contribute to consistent application of the GDPR
- Powers exercised impartially, fairly and with a reasonable time
- Able to impose a limitation (or ban) on data processing
- Power to conduct investigation

In general

Roadmap

Key definitions
Clarify the bands of penalties and range of awards for breaches
Review the timeline to reflect the application of GDPR
Role of the DPO (data protection officer)
Six data protection principles, lawfulness and consent
Define sensitive data
Rights of data subjects (a number of national deviations)
Controllers and processors
Data protection by design
Securing personal data
Procedure on reporting data breaches
Transferring personal data outside the EU
How to perform a DDPIA (data protection impact assessment)
Powers of supervisory authorities
Lead supervisory authority
Role of the EDPB (European Data Protection Board)
Importance of certifications

The GDPR Law

- ✏ General provisions
  - ✏ Chapter 1 (Art. 1 – 4)
- ✏ Principles
  - ✏ Chapter 2 (Art. 5 – 11)
- ✏ Data subject rights
  - ✏ Chapter 3 (Art. 12 – 23)
- 🌐 Controller and processor
  - 🌐 Chapter 4 (Art. 24 – 43)
- ✏ Transfers
  - ✏ Chapter 5 (Art. 44 – 50)
- 🌐 Supervisory authorities
  - 🌐 Chapter 6 (Art. 51 – 59)
- ✏ Cooperation and consistency
  - ✏ Chapter 7 (Art. 60 – 76)
- 🌐 Remedies, liability & penalties
  - 🌐 Chapter 8 (Art. 77 – 84)
- ✏ Specific processing situations
  - ✏ Chapter 9 (Art. 85 – 91)
- ✏ Other rules
  - ✏ Chapters 10/12 (Art. 92 – 99)

✏ Direct obligation

🌐 Meta rule

🔗 https://gdpr-info.eu

Change management

GDPR Impact

New or amended policies and record management

New operational roles and responsibilities, DPO role

Changes in IT tools, solutions, applications and infrastructure

Changes in contracts, agreements, consents, notices

Continuous improvement

Change management

GDPR Impact

Create a protection impact assessment policy
Improve the access management policy
Review processes dealing with personal information

Identify owners of personal data
Assess key staff skills
Create and conduct learning and awareness programs
Communicate the GDPR changes

Determine the need for DPIAs
Follow-up remediation plans for IT solutions
Incident management

Document compliance efforts
Get approvals for changes
Metrics for GDPR compliance

Change management

	Privacy (DPO)	IT InfoSec	Legal	Procurement	Compliance	Business	HR
Data breach notification	●	●	●	◑	●	◔	
Data lifecycle mgmt.	●	●	◔	◑	◔	◕	◑
3rd-party disclosures	●	◔	◔	◕		●	◔
Governance	◕	◕	◔	◔	●	◔	◔
DPIA	●	◔	◔	◑	◔	◑	◑
Data transfers	●		●	◕			◔
Rights for data subjects	●	●	●				◑
Privacy by design	●	◔	◔	◔	◔	◕	◔
Data security	◔	●	◔	◑	◔	◑	
Monitoring	◔	◕		◔	●		◑

Roadmap schedule

Plan

Do

Improve

	Month 1	Month 2	Month 3	Month 4	Month 5	Month 6		Month 7	Month 8 +
CORE TEAM	Governance and change management risk management (key risks, gaps, control design)						GDPR Effective	Risk reviews	
	Team kick-off	Gap analysis	DPO role in place	Data processor agreement template	Data deletion rules	Breach notification procedure		Compliance audits	Review and update of policies
	Data inventory and flows	Privacy strategy and policy	Training needs analysis	Privacy by design guidelines	DPIA Process	Monitoring and reporting		Privacy impact assessments	Training and awareness
	Privacy in Code of Conduct	DPMS tools / mechanisms	Mapping info. Sec. controls to GDPR	Role-based training materials	Awareness campaigns	Biding corporate rules		Improve security services (authentication, data loss prevention, real time monitoring, threat intelligence)	
BUSINESS FUNCTIONS	Business kick-off meetings	Application, data and flow mapping							
	Assessment of competences								

Process	Information Documents	Organization	Technology

Steering committee meetings

How to demonstrate compliance?

Why documentation?

“If something is not documented, it is not done”

- *My auditor*

Extensive documentation efforts for GDPR

Discussions about the right level of documentation

Formalizing operational procedures

Need to integrate privacy practices in policies

Controllers must be able to prove their compliance with the GDPR under the accountability principle and upon request of Supervisory Authority

Objectives

Management

- Privacy is part of the general management system
  - Documentation is the evidence of accountability and good governance
- Privacy policy
  - Supported by: document retention and destruction, info classification, breach management,…
  - Assess and manage the impact of changes in policies
  - Available to all the staff (training)

Corporate defense

- Demonstrate compliance efforts (implementation measures, control improvement)
  - Records of processing activities under your responsibility (art. 30)
  - When needed, data protection impact assessment (art. 35)
  - Records of consent from data subjects and guardians (arts. 7 and 8)
  - Actions taken during a data breach (arts. 33 and 34)
  - Purposes for collecting information (art. 13)
- Document legal basis for the processing (art. 5)
- Privacy clauses in contracts, bidding corporate rules,…

Audits

- Outsourcer/data processor must prove technical and organizational controls (art. 28, ISAE 3000 type 1, data protection seals and certifications)

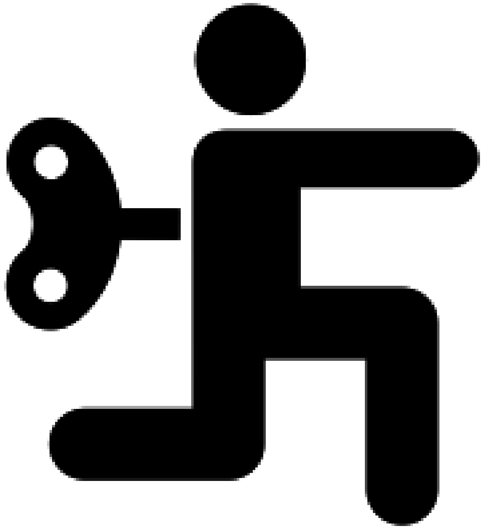
Demonstrate compliance

- Evidence of board engagement in privacy (art. 5)
  - Unclear evidence: approving a privacy program, board agendas and minutes covering GDPR issues, evaluation of privacy reports, action plans involving board members, list of project stakeholders, budgets, approval
  - Nice to have: job roles assigning privacy responsibilities, privacy core team and experts, meetings and guidance with other internal functions dealing with personal data
  - General: ISO/IEC 27001 compliance certificate

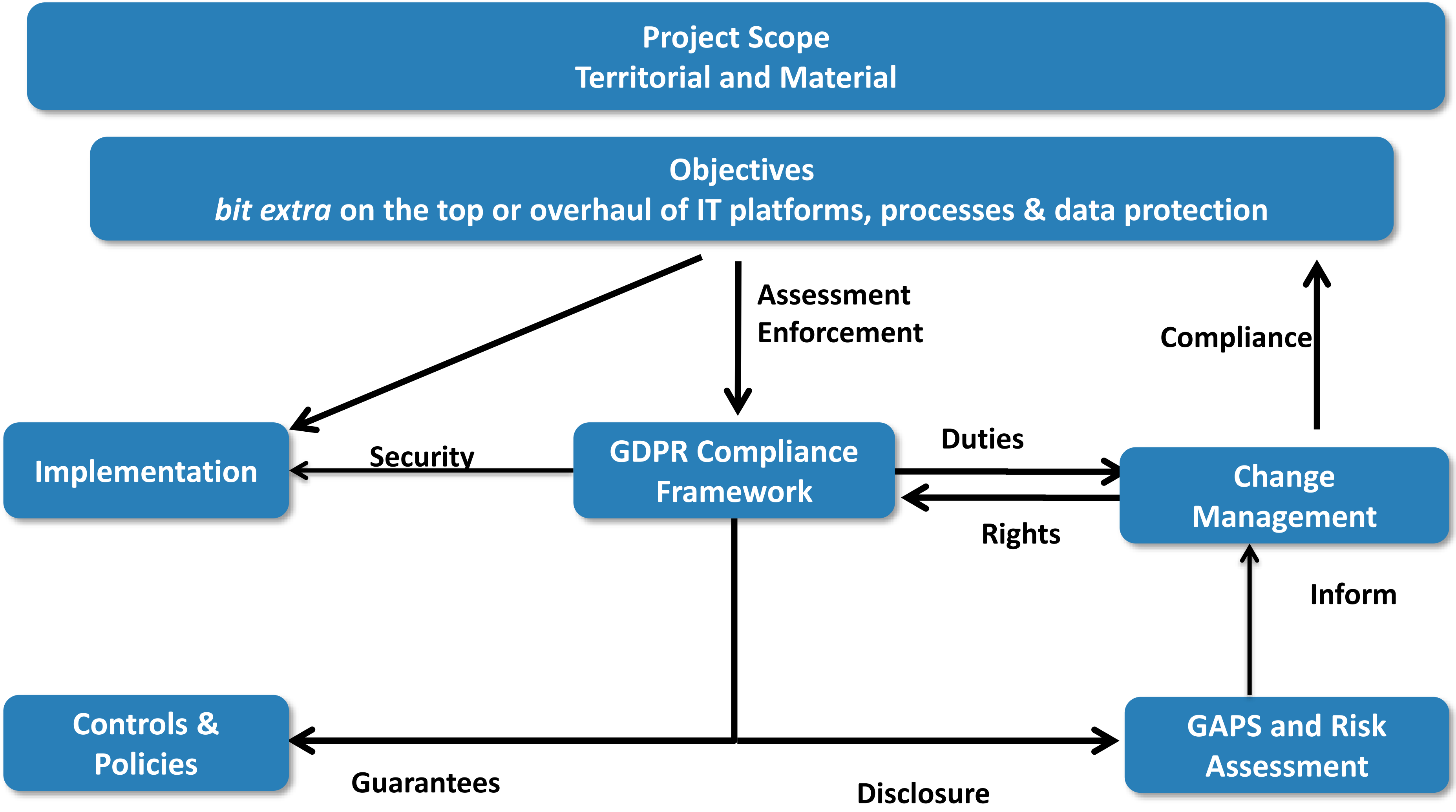
Demonstrate compliance

- Responsibility of the controller (art 24)
- Responsibility of the controller in outsourcing (art 28)
- Records of processing activities (art 30)
- Records of data transfers (arts 45 to 49)
- Security of processing (art 32)
- Data protection impact assessment (arts 35 and 36)
- Data breach notification (art 33)
- Privacy by design and by default (art 25)
- Protocol for a data breach notification
- Procedure to obtain valid data privacy notices

What you have received?



Summary



Project Scope
Territorial and Material

Objectives
bit extra on the top or overhaul of IT platforms, processes & data protection

Assessment
Enforcement

Compliance

Implementation

Security

GDPR Compliance Framework

Duties

Rights

Change Management

Inform

Controls & Policies

Guarantees

Disclosure

GAPS and Risk Assessment

The GDPR Institute

EU GDPR INSTITUTE

Connecting IT Security to Governance, Risk and Compliance

www.copenhagencompliance.com

HR Riskability

Human Capital Assessment Framework

CERTIFICATION ★ EXERCISES ★ RESEARCH ★ TRAINING

IMPROVE ★ ORGANIZATION ★ NEEDS

COPENHAGEN COMPLIANCE

Global GRC Solutions

Corporate Governance
Risk Management
& Compliance
Certification

IN CONTROL ★ FACILITATION

INSTRUCTION ★ COURSES ★ AUTHORITY ★ TRACKING

The GDPR Institute® is the global Governance, Risk Management, Compliance and IT Security (GRC) think tank. As a privately held professional services firm, the mission is the advancement of the corporate ability to govern across the borders, sector, geography, and constituency. The primary aim is to help companies and individuals achieve integrated GRC management that unlocks the Organization ethics, cultures and value by optimising GRC issues to IT-Security & automation thru templates, roadmaps, & frameworks.

The GDPR Institute provides global end-to-end GRC platform, with a comprehensive & proven advisory based on; giving priority to transparency, accountability and oversight issues. Our focus is on GRC Intelligence, Internal Controls, Audit, CSR, Compliance & Policy Management, IT-GRC, Sustainability Management, Bribery Fraud, Corruption (BFC), IT &- Cyber Security Issues

The GDPR Institute® has dedicated resources for consultancy and research in Good Governance, Risk Management and Compliance issues involving corporations, universities and business schools and GRC organizations on four continents.

Useful GDPR links

EU GDPR INSTITUTE

Privacy Shield Framework

https://www.privacyshield.gov/article?id=Privacy-Policy-FAQs-1-5

- **GDPR Official Text (English, pdf)**
  http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
- **EU GDPR Home Page**
  http://ec.europa.eu/justice/data-protection/
- **Working Party 29 Guidance**
  http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083
- **Guidelines on "Right to Portability" (pdf)**
  http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf
- **Guidelines on Data Protection Officers (pdf)**
  http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf
- **Guidelines for identifying a controller or processor's lead supervisory authority (pdf)**
  http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp244_en_40857.pdf
- **Bulgarian data protection authority** Www.cpdp.bg
- **UK ICO – 12 Steps to take now (pdf)**
  https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf
- **EUGDPR INSTITUTE**
  http://www.eugdpr.institute/faq/
  http://www.eugdpr.institute/gdpr-thought-leadership/

Bulgaria: *as is* or *to be*

- 52 articles leave room for national legislation
- GDPR rules apply today with ‘low’ level of fines
- **CPDP – the Bulgarian Data Protection Authority**
  - The only public authority whose main task is to ensure privacy and personal data protection in Bulgaria.
    - an office of over 80 people, the main activities are;
    - adequate prevention and effective control.
      - The CPDP will host an international conference of data protection authorities in 2018 within the framework of the Bulgarian Presidency.
      - https://www.cpdp.bg/en/index.php?p=news_view&aid=756.

Certification exam

http://www.eugdpr.institute/gdpr-fas/

Copyright notice