

GDPR Foundation, DPO, Practitioner and Executive Training Seminars with certification



by

COPENHAGEN
COMPLIANCE

Example of the
Foundation seminar

Agenda



Full presentations , templates and available during our seminars

workshop exercises are only

Overview of Privacy

Privacy principles

Definition of privacy and private data

Global data privacy laws

Organizational requirements

GDPR Basics

The legal evolvement

Key components and provisions

Best practices and standards

ISO27001, PCI DSS, NIST Guidance

Scope and application

Legal implications of violation:
penalties, liabilities and exemptions

How to implement

Key roles and responsibilities: controller, processor and data protection officer

Implementation steps: gap analysis, data mapping, risk assessment

Privacy by Design and Privacy by Default

Legitimate interests

Rights of data subjects and consent

Workforce awareness



Agenda



Day 3



Operation of GDPR compliance
Incident management and reporting
Need for data protection impact assessment
How to Conduct a DPIA
BS10012 - The PIMS standard for
How to use standards to comply with GDPR
ISO29100, ISO27018, COBIT 5
GDPR Best Practices
GDPR, the Cloud Services, IoT and Cyber security
Data transfers to third countries

Day 4



Monitoring GDPR Compliance
Enforcement
Demonstrating compliance
Lifecycle management
GDPR compliance checklist
GDPR action plan
Certification



What you will receive?



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?

GDPR areas



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

The GDPR Institute

GDPR roadmap



Available during the seminar










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 (RoPA Record of processing activities)
- ✎ 5- Clean the house: data minimization
- ✎ 6- Create a privacy policy







B- Do

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



C- Improve

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



ISO 27001 Info Security



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

Performance

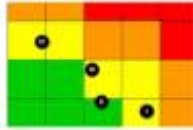
- Monitoring, measurement, analysis and evaluation
- Internal audit
- Management review

Improvement

- Nonconformity and corrective actions
- Continual improvement



Asset	Owner	Class	Classification	Retention	Disposal
Customer data	Marketing	Confidential	High	10 years	Securely delete
Employee records	HR	Confidential	High	5 years	Securely delete
Financial reports	Finance	Confidential	High	7 years	Securely delete
Product development	R&D	Confidential	High	3 years	Securely delete
Internal communications	HR	Confidential	Medium	3 years	Securely delete
Supplier contracts	Procurement	Confidential	Medium	5 years	Securely delete
Marketing materials	Marketing	Public	Low	2 years	Archive or delete
Website content	Marketing	Public	Low	2 years	Archive or delete
Customer support logs	Customer Service	Confidential	Medium	3 years	Securely delete
IT system logs	IT	Confidential	High	1 year	Securely delete



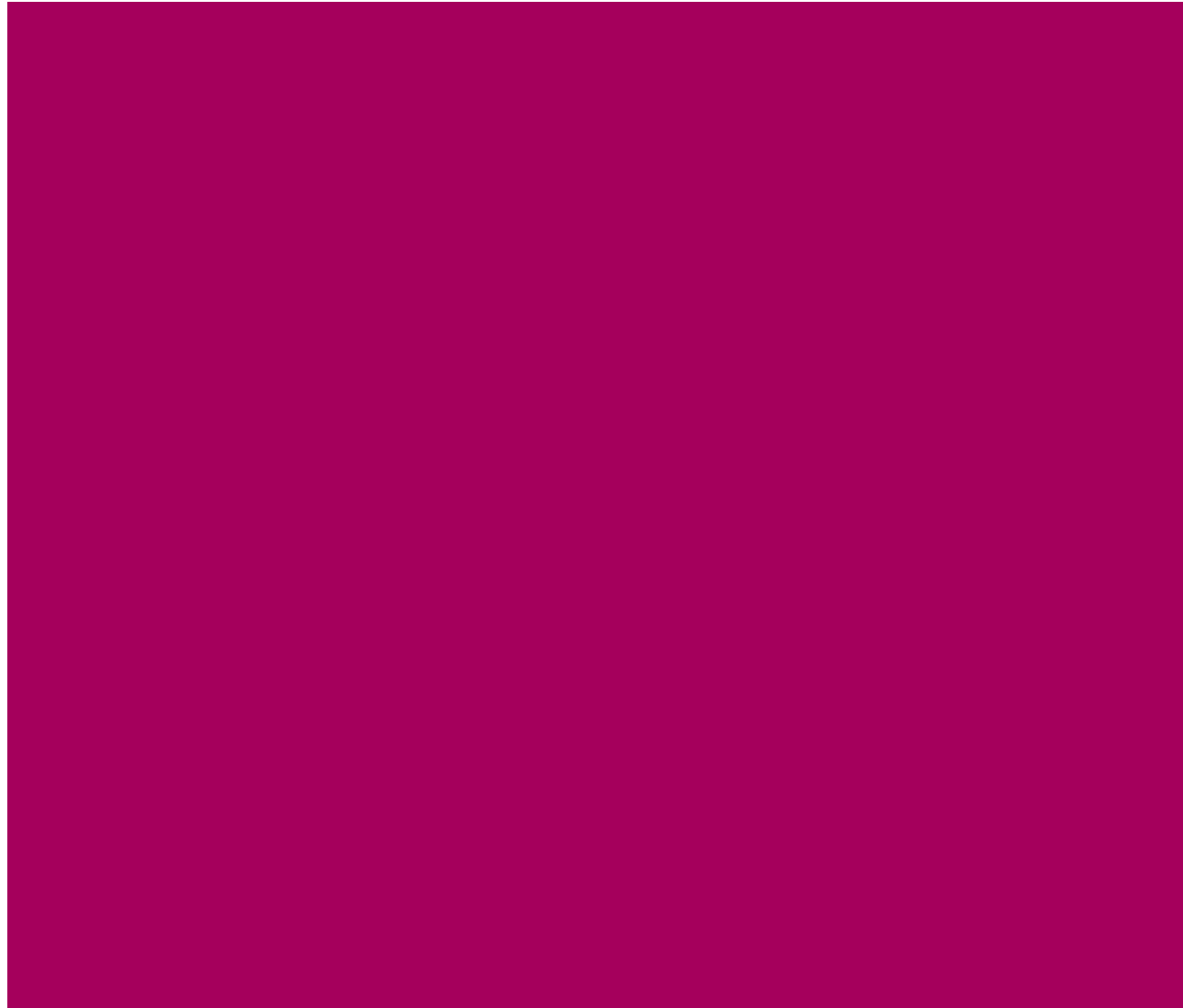
Train your people

Audit compliance



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

A - Plan



Step 1: Obtain the buy-in



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: Selling the project



- ✎ How to sell GDPR to the IT function?
 - ✎ Save money by identifying storage redundancy
 - ✎ Reduce the IT complexities by clarifying data accountability
 - ✎ Improve the access controls
- ✎ How to sell GDPR to the risk and control functions?
 - ✎ Understand where relevant data is stored and managed
 - ✎ Plan improve the technical and operational controls
- ✎ How to sell GDPR to the operational functions?
 - ✎ Better use of data
 - ✎ Understand data flows with third parties
 - ✎ Clear responsibilities with IT vendors

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!




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 2: Get a team



One man army?

Data protection officer

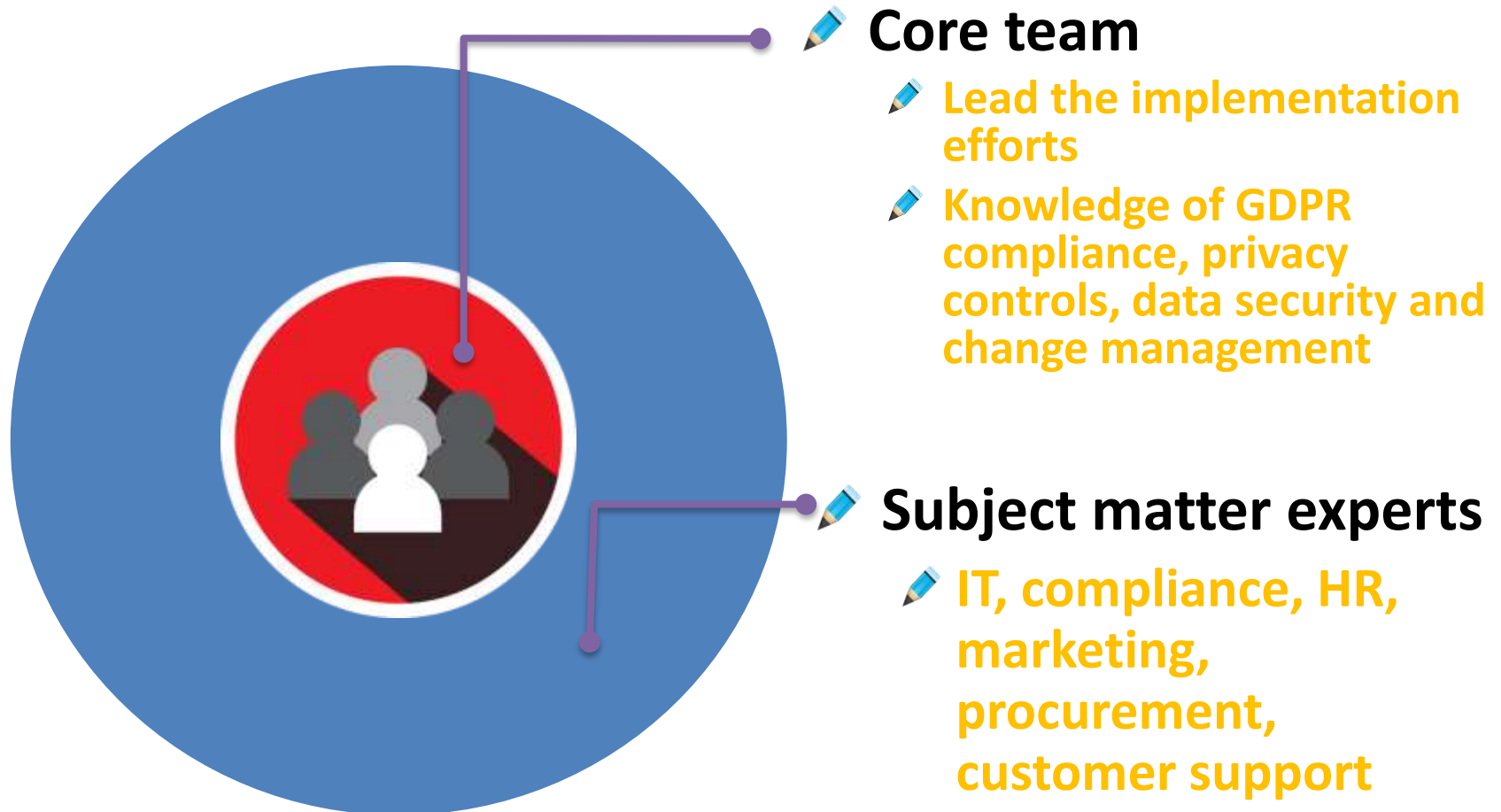


Implementation team <> Maintenance team
Define a clear objective and responsibilities
Be a leader
Experience in project management, security,
training and legal
Commit time of process subject experts
Document all the project activities

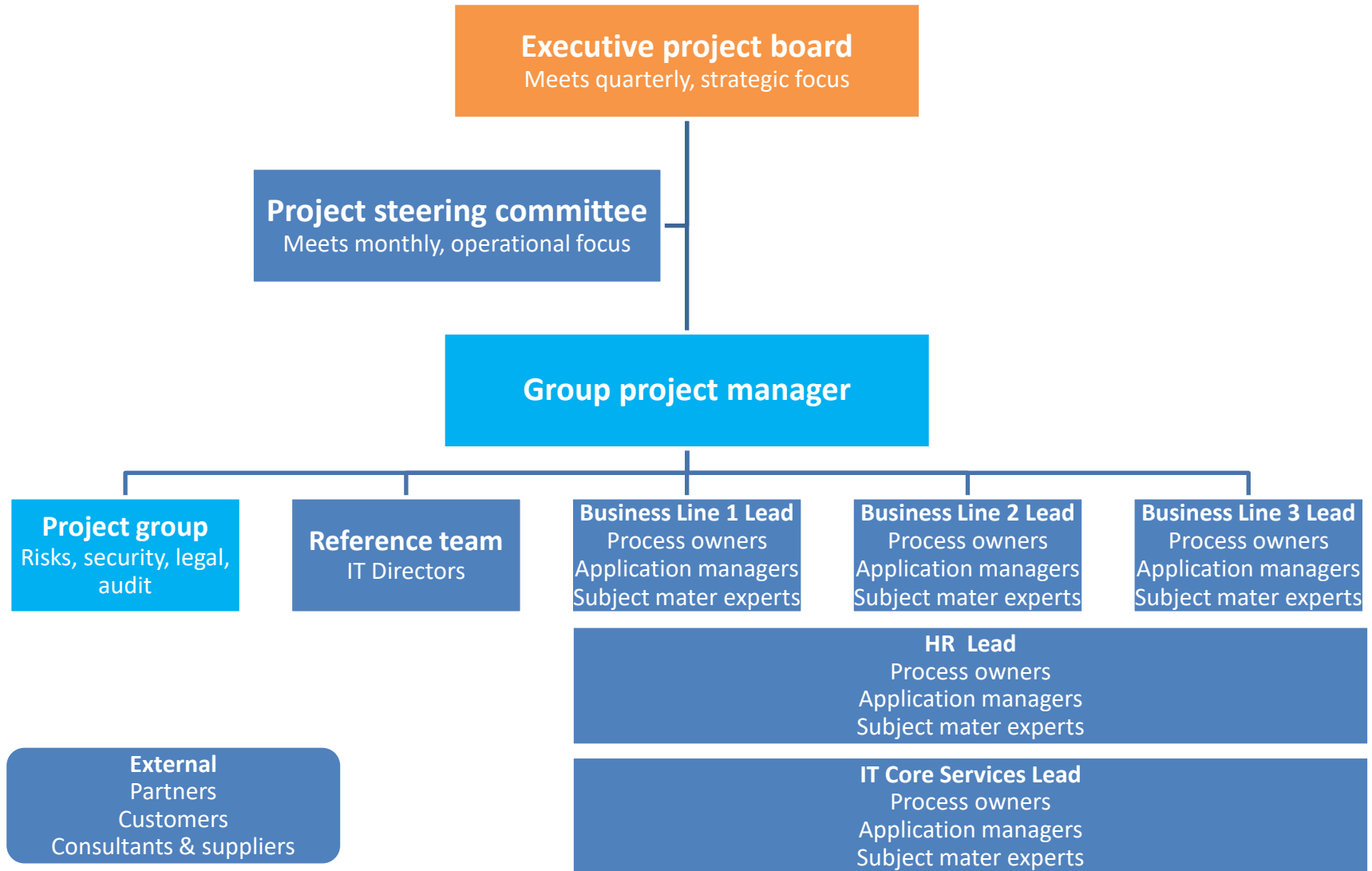
How many were ready by...



Get the team early



Step 2: Example



Who needs a DPO?



The controller

AND

The processor

1. Processing is carried out by public authority

2. Required by a national law (eg. Germany)

3. Business with a core activity

- Processing operations requiring monitoring of personal data at large scale
 - Included hospitals for health data, marketing agency for customer web data, surveillance companies
 - Excluded payroll for a commercial organization, health data by a single doctor
- Processing operations requiring monitoring of sensitive personal data at large scale relating to criminal convictions and offences

What does a DPO?



- ✎ Fosters the data protection culture
- ✎ Guide the GDPR implementation and monitor its compliance
- ✎ Make recommendations in meetings where decisions with data protection implications are taken
- ✎ Cooperate and liaison with the supervisory authorities

Independence to ensuring compliance

Employee or external consultant based on a service contract

Expertise in national and European data protection laws

Knowledge of the business sector and of the organization of the controller

Professional ethics and lack of conflict of interests

Groups may designate a single DPO

Group discussion



 **Who can be a DPO? The chief risk officer, the compliance officer, the chief information security officer...**



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 Danish **+5M**



How data is identifiable?



A Danish female **2.5M**



How data is identifiable?



A Danish female born in 1940 **20k**



How data is identifiable?



.... Living in Amalienborg **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

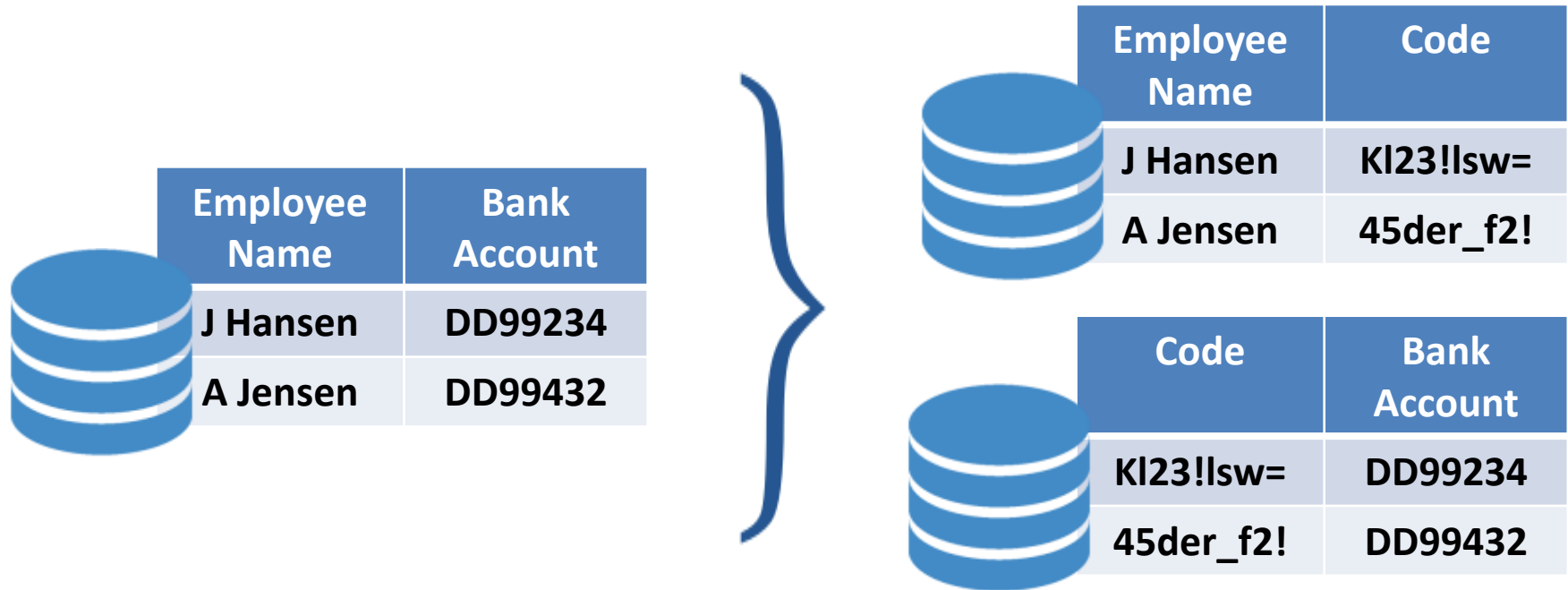
NEW

Pseudonymous

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

**1 or +
factors**

What is pseudonymisation?



- ✎ 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?



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

Which data is sensitive?



Health

Biometric

Genetic

NEW

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 _____

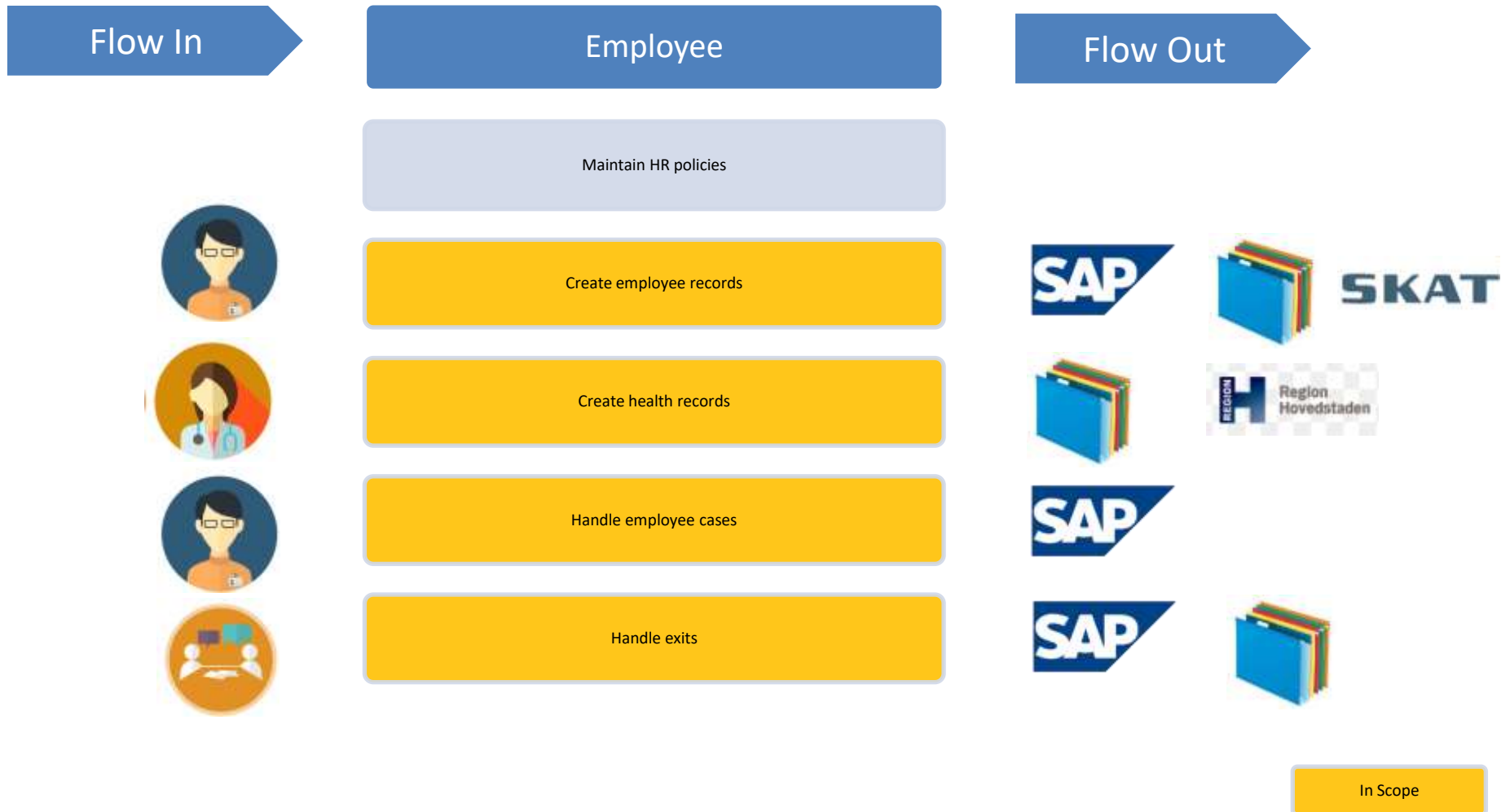
Objective	Questions	Answer	Assessed risks
Scope	What types of personal information are you processing? Personal information is information that can be attributed to one or more natural persons (e.g. name, address, e-mail address, position). Some of this information can be confidential (IDPR number, wages, wealth and other economic data) or sensitive (special categories: health/medical records, biometric/ fingerprints, genetic, religion, ethnicity, political union membership, sexuality and criminal offences).		
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 you 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) To what extent is personal information physically processed ?		
Physical processing	- documents and papers with personal information - papers with sensitive and confidential personal information locked in cabinets - clean desk policy What IT systems and applications do you use for processing personal information? Are you monitoring and frequently reviewing the accesses to IT systems dealing with personal information by employees and users?		
IT System processing Access control	- Access control policy requiring approvals by supervisors - Review of principle of least privilege and role-related needs - Review of user rights		

 Interview template in the toolkit

Available during the seminar




Step 3: Scope example



Group discussion



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



Step 4: Compile a data inventory



NEW

RoPA Record of Processing Activities



What personal data do we hold?



Where is it?



What is it being used for?



How secure is it?

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



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 Personnel filing cabinets	Password, encryption 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	

Available during the seminar

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: jdawetherspoon.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

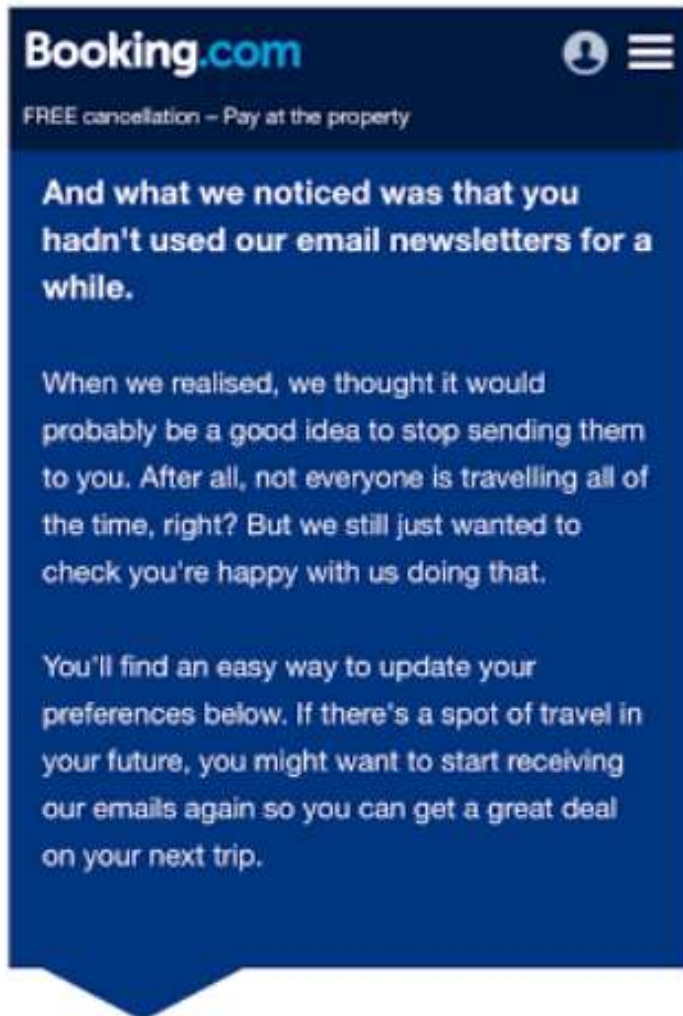
 Less intrusive?

 No need to keep track of consents?

Cons

 Communication of offers

Step 5: An example



I'd like to receive deals and offers again!




[Head to Booking.com](https://www.booking.com)

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

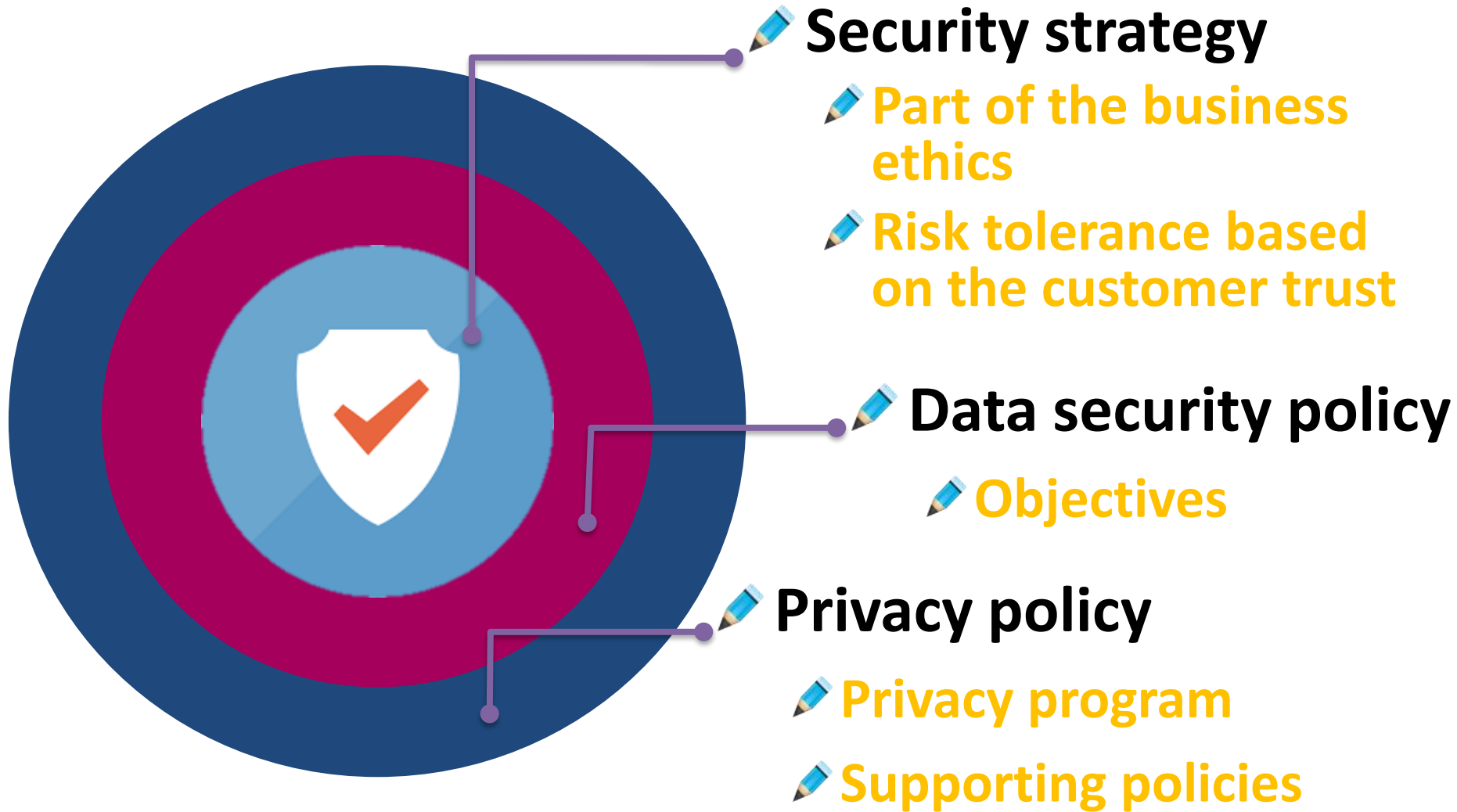
Support from upper management

-  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 and choices**

- ✎ **Define general principles and roles to limit:**

 - ✎ **the collection**

 - ✎ **how the consents are ensured, when risk impacts are done**

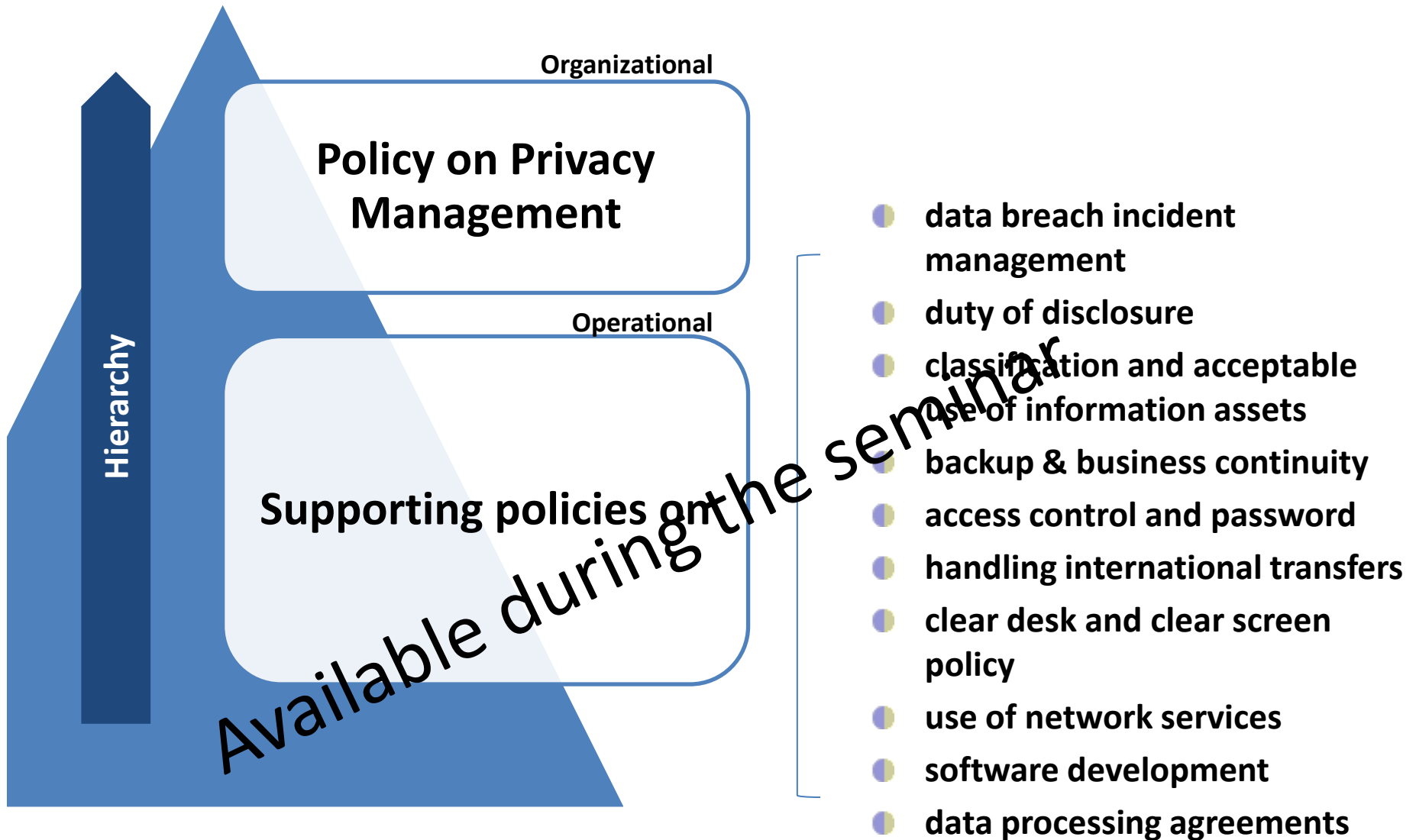
 - ✎ **the use**

 - ✎ **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



Step 6: Create a privacy policy



✎ Privacy policy template by the GDPR Institute

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

Available during the seminar

Supporting policies



Specific policies

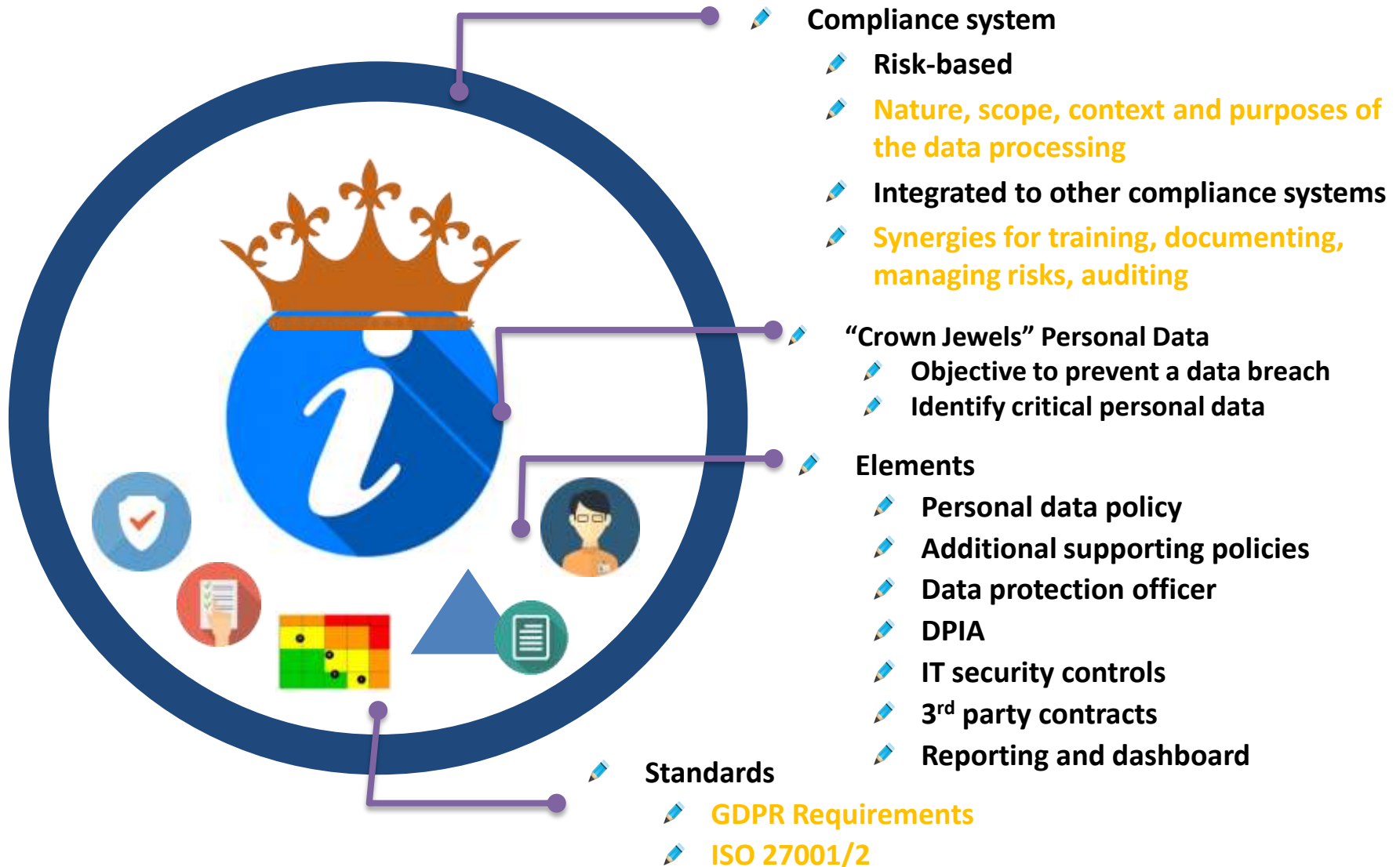
- ✎ records retention
- ✎ access control and delegation of access to employees' company e-mail accounts (vacation, termination)
- ✎ acceptable collection and use of information resources incl. sensitive personal data
- ✎ obtaining valid consent
- ✎ collection and use of children and minors' personal 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

Available during the seminar

Data Protection Management System



Step 6: Discussion case



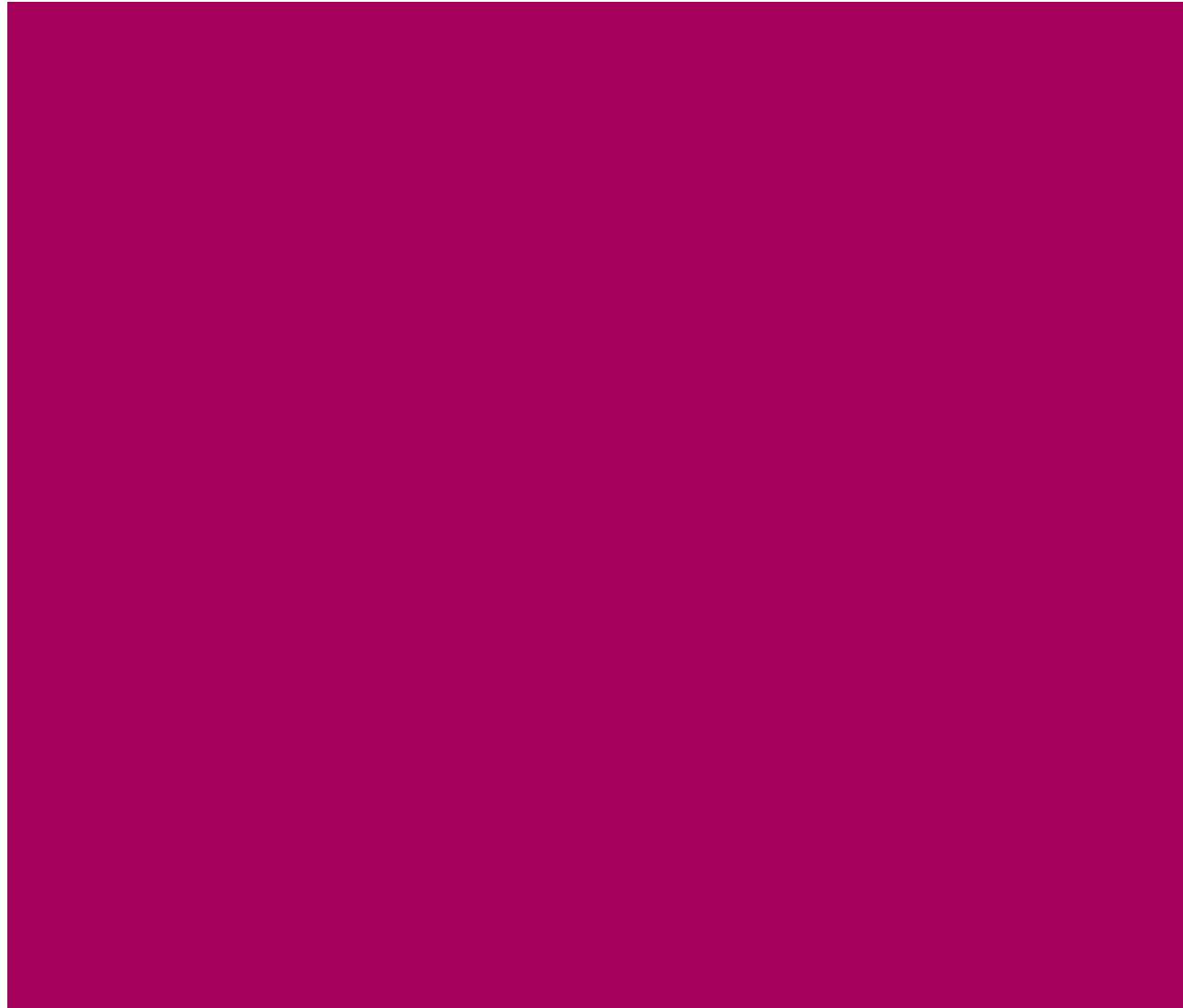
FSA fines HSBC over £3 million for data security breach

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



Level	Scope	Access
Confidential	Sensitive information, bank details, payroll data, passwords, large directories with names, addresses and phone numbers, Also: board reports, business plans and budgets	Significant scrutiny
Restricted	Personal data, reserved reports and papers, ERP/CRM systems	Approved by data owners
Internal use	Internal emails and communication	Employees and contractors
Public	Intranet, public reports	

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**



the controller be able to demonstrate **accountability**

- ✎ Being able to demonstrate **best efforts** to comply with the GDPR principles
- ✎ Proactive approach to properly manage personal data and to address privacy risks by a **structured privacy management program**



Proportionality

processing only if necessary for the attainment of the stated purpose

- ✎ Personal data must be adequate, relevant and not excessive in relation to the purposes
- ✎ By the data processor and controller
- ✎ Requires to use the less intrusive means of processing

When processing is lawful?



- ✎ Data subject gives consent for one or more specific purposes
- ✎ Processing is necessary to meet contractual obligations entered into by the data subject
- ✎ Processing is necessary to comply with legal obligations of the controller
- ✎ Processing is necessary to protect the vital interests of the data subject
- ✎ Processing is necessary for tasks in the public interest or exercise of authority vested in the controller
- ✎ Purposes of the legitimate interests pursued by the controller

Rights



To access data

request access to personal data 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

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



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 consents should be given?



A

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 below the age of 16
- Reasonable means to verify parental consent

Step 2: Review consents

How consents should be given?



signing a consent statement on a paper

I agree to

I agree to the Google Terms of Service and Privacy Policy

ticking an opt-in box on paper or electronically (no pre-ticked)



clicking an opt-in button or link online



selecting from equally prominent yes/no options

Data Protection:

- Email
- Post
- Telephone

choosing technical settings or preference dashboard settings



responding to an email requesting consent

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: Deal with data subject 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 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)

How personal data is processed?



Collect

Use

Destroy

Record

Transmit

Restrict



Change

Display



Electronically

Manually

GDPR covers personal information processed wholly or partly by automated means

... but, by who?



Controller

Who decides
why the personal
data is needed

Processor

Who processes
the data
Service provider, cloud
services, outsourcing firms,
e-commerce platforms

Natural or legal person
including the government

... but, where?



in the EU

When personal data of individual living in the EU (citizens or not) is processed

outside the EU

When personal data of EU citizen is processed by a non-EU organization **offering goods and services** in the EU (not paid in the EU)

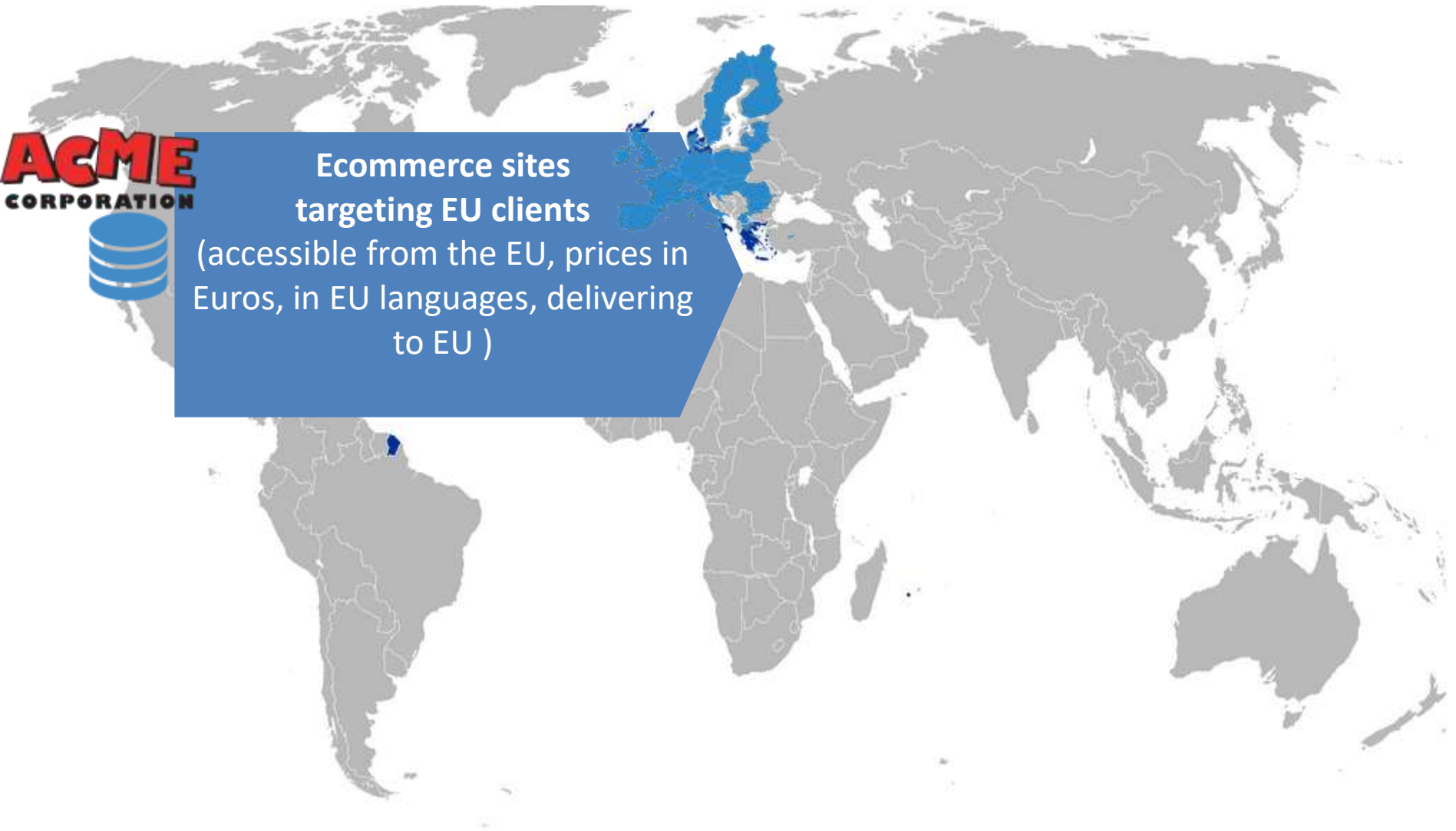
Extra-territorial application



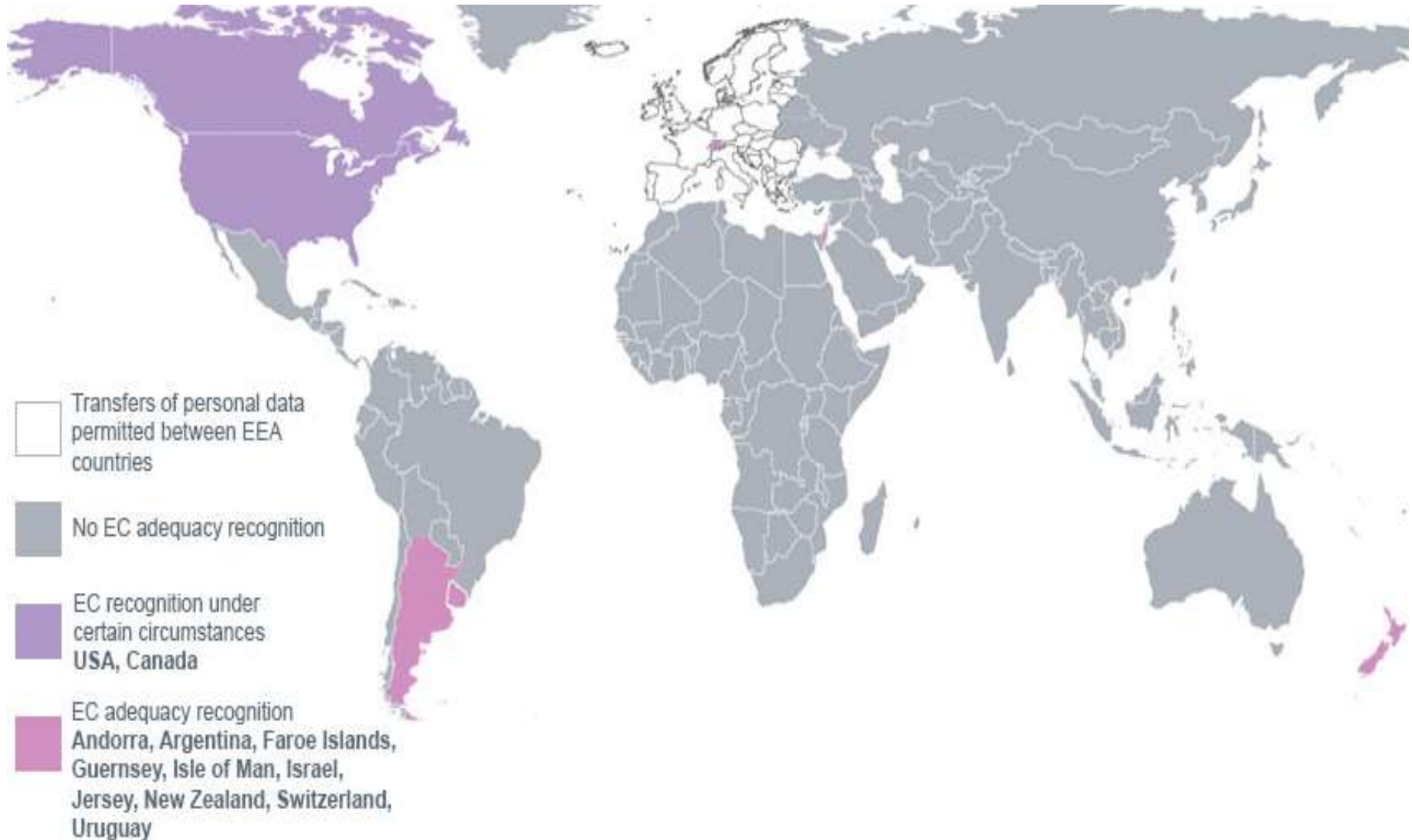
ACME
CORPORATION



Ecommerce sites
targeting EU clients
(accessible from the EU, prices in
Euros, in EU languages, delivering
to EU)

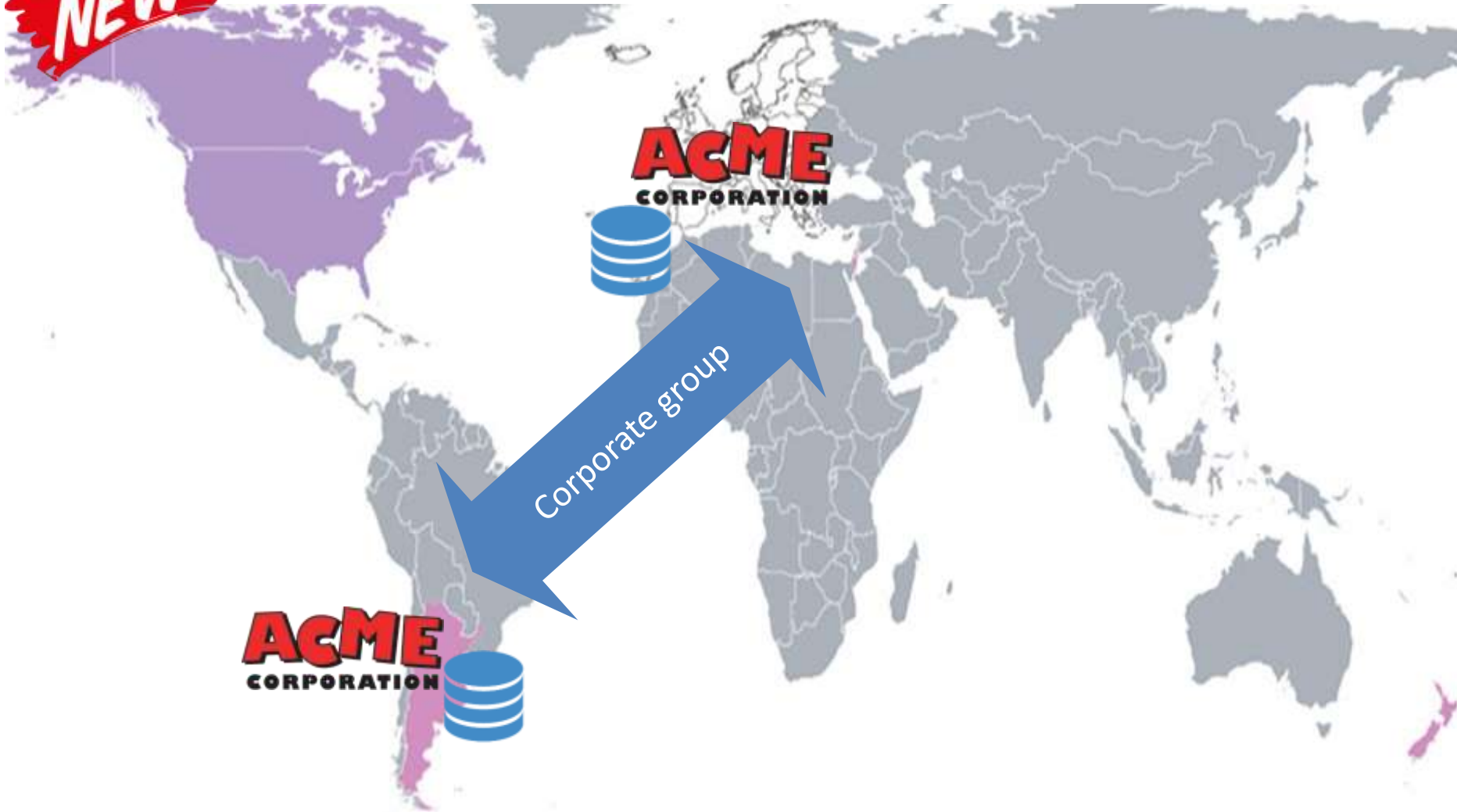


International transfers




Binding corporate rules

NEW



Group discussion



 **How would you link the dataflow map with the cross-border transfers?**



Step 4: 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

Step 5: How to 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 later 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 5: How detect a data breach?



Indication of compromise

- ✎ notification from public authorities
 - ✎ FBI knocks at the door
- ✎ from users
 - ✎ oops, I opened a “funny attached file”
- ✎ alerts from 3rd parties
 - ✎ hosting vendor informed they had a malware
- ✎ continuous monitoring solutions
 - ✎ this server is transferring out a lot of amount of data

Incident response protocol

- ✎ Investigate “when” the breach was done
- ✎ Get the investigation team
- ✎ Investigate the level of compromise

Step 5: Scenario planning



Before the breach

- ✎ **Address IT risks and vulnerabilities**
 - ✎ all potential threats are identified and defendable (e.g. penetration testing, vulnerability scanning)
 - ✎ multi-layer cyber security defenses
- ✎ **Plan scenarios for responses**
- ✎ **Improve breach detection**
- ✎ **Require patches on DNS servers**

After the breach

- ✎ **Plan actions to the contain damage**
 - ✎ business continuity, disaster recovery and reputation management (e.g. company crisis protocols)
- ✎ **Resilience! Plan how to move on from the breach**
 - ✎ Minimize the risk of future occurrence
 - ✎ Feedback from the incident response teams and affected people
 - ✎ Enhance and modify information security policies and training programs

Step 5: Discussion case



They even
sell data
breach
services

- ✎ Equifax, main credit reporting agency
- ✎ Hackers exploited a security vulnerability in a US-based application
- ✎ Exposed names, social security numbers, birth dates, addresses of 143M US consumers and 200K credit card numbers!
- ✎ Required customers to freeze their credit files, offered free credit monitoring and paid new credit cards
- ✎ Equifax had problems with data security before
- ✎ 41 days between discovery and disclosure
- ✎ Significant internal failure to communicate
- ✎ Executives sold 2M in shares just before disclosing
- ✎ Future class action suits

How can we manage the need to investigate a breach with the 72 hours rules to disclose a breach under GDPR?

Step 5: 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 audits)
- 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

Step 5: Discussion case



Popular restaurant app Zomato says the records of about 17 million users have been stolen in a security breach.

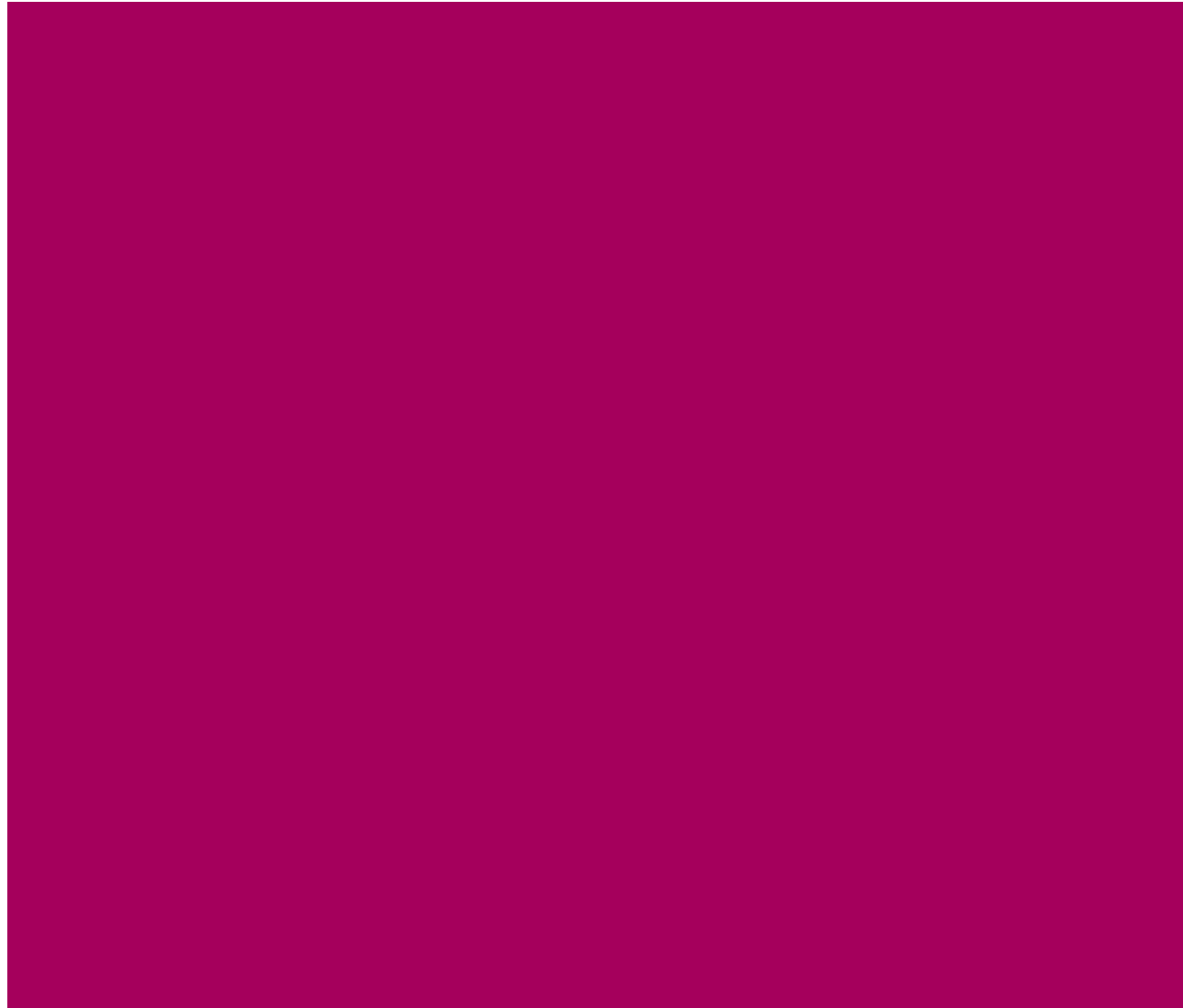
The Indian startup, which covers more than one million eateries across 24 countries, [said Thursday](#) that names, email addresses and encrypted passwords were taken from its database.

The company, which competes with Yelp ([YELP](#)), reassured affected customers that no payment information or credit card details were stolen.

Zomato said the security measures it uses ensure the stolen passwords can't be converted back into normal text, but it still urged users who use the same password on other services to change them. It also logged the affected users out of the app and reset their passwords.

"So far, it looks like an internal (human) security breach - some employee's development account got compromised," the company said in [a blog post](#), without providing further details. It didn't immediately respond to a request for more information.

C - Improve

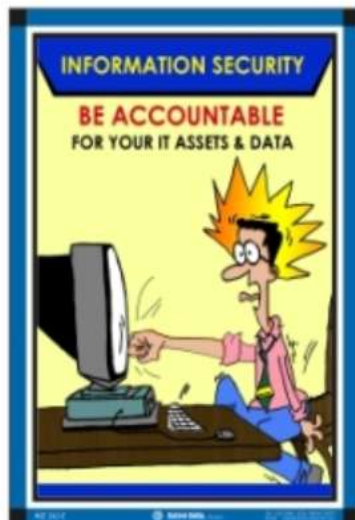
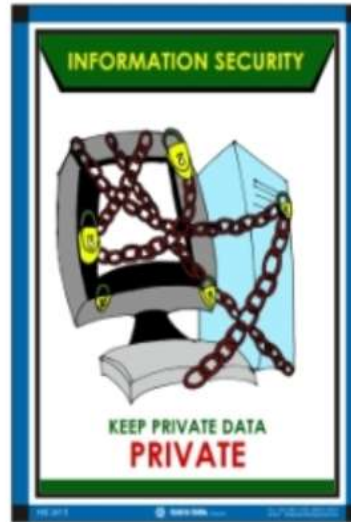


Step 1: Train your people



- ✎ 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 campaigns
 - ✎ 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: Train your people



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.

NEW

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

1 – Identify the need



Early before **new** projects or revision of existing processes

for example, when considering a

- ✦ new system to store personal data
- ✦ change the use of already collected personal data
- ✦ new video surveillance system
- ✦ vulnerable data subjects (e.g. children)
- ✦ new database consolidating tables with personal information from other systems
- ✦ new algorithm to profile a particular type of client
- ✦ proposal to share personal data with a business partner
- ✦ impact of a new legislation

Existing processes → Recommended initial assessment

Doubts if needed → consult the Supervisory Authority and beg for mercy!

2 – Identify the flows



Process map start from the process or project documentation



Identify personal information in the process map



Consult with experts how personal information is collected, transferred, used and stored

 for existing and future purposes

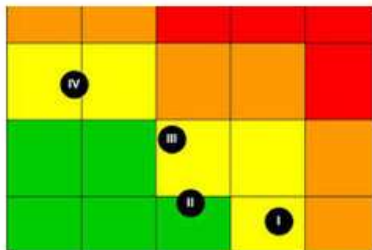
3- Consult on risks and controls



Consult all involved parties to have a 360° view, link risks to owners



Include current controls in the process map












Assess the impact and frequency in a heat map (recommended), risk assessment in ISO 27001 (under 29100)

- ✎ Impact: fines, business continuity costs, loss of clients, reputational damage
- ✎ Risk must be assessed from the view of the data subject, not the business!

People to consult



Internal

-  Data protection officer (usually leading the DPIA)
-  Project management leaders and developers
-  CIO, CISO and other IT experts
-  Compliance officer
-  Legal department
-  Internal audit executive
-  Risk management officer
-  Future or current users
-  Senior managers

External

-  Potential data processors and vendors
-  Experts

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





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







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	Consequences	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

Available during the seminar

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)


Direct obligation

Meta rule


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)

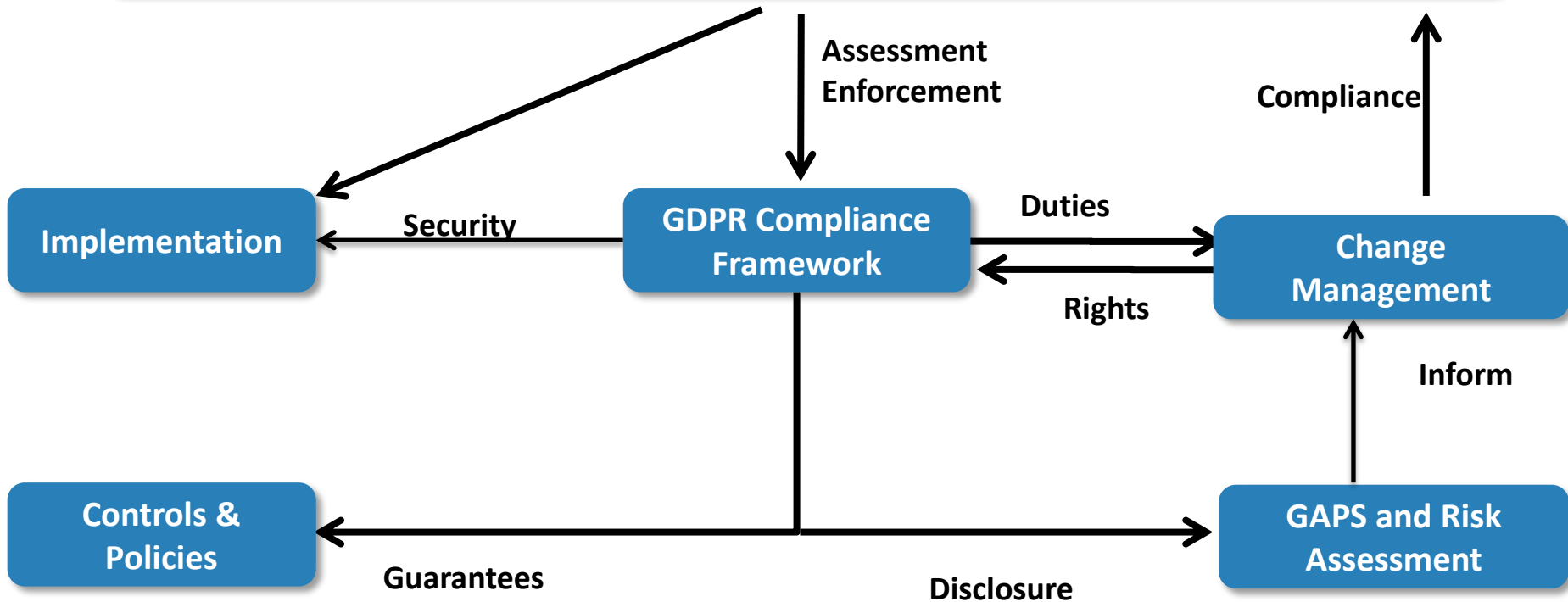
Summary



Project Scope
Territorial and Material

Objectives

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



The GDPR Institute



www.copenhagencompliance.com



Human Capital Assessment Framework



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



<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
- **Datatilsynet DK Oversight**
<https://www.datatilsynet.dk/forside/>
- **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/>





Kersi F. Porbunderwalla is the Secretary General of Copenhagen Compliance and President of The EUGDPR Institute and Riskability IT Tools. Kersi is a global consultant, teacher, instructor, researcher, commentator and practitioner on good Governance, Risk Management, Compliance and IT-security (GRC), Bribery, Fraud and anti-Corruption (BFC) and Corporate Social Responsibility (CSR) issues. Kersi lectures at The Govt. Law College (Thrissur, India) Georgetown University (Washington) Cass Business School, (London) and at Fordham University (New York) and Renmin Law School (Beijing). Kersi has conducted several hundred workshops, seminars and international speaking assignments on Regulatory Compliance, GDPR, GRC, CSR, and BFC issues.

Disclaimer: This presentation is prepared for Triumph. The content together with the links to narratives, brochures and information on our websites, is for general informational purposes only. Please refer to Copenhagen Compliance® for specific advice on regulatory compliance and other GRC issues. As always refer to your counsel for legal advice, we are not licensed to provide legal advice.

Copenhagen Compliance UK Ltd®

Info@copenhagencompliance.com

www.eugdpr.institute

21, Cloudseley Street, London N1 OHX, UK.

Tel. +44 7778 917 133

Tel: +45 2121 0616

Copyright notice



The copyright of this work belongs to The GDPR Institute[®] and none of this presentation, either in part or in whole, in any manner or form, may be copied, reproduced, transmitted, modified or distributed or used by other means without permission from The GDPR Institute[®]. Carrying out any unauthorized act in relation to this copyright notice may result in both a civil claim for damages and criminal prosecution.

© Copenhagen Compliance®



www.copenhagencompliance.com

Copenhagen Compliance® 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 company ethics, cultures and value by optimising GRC issues to IT-Security & automation.



Human Capital Assessment Framework

Copenhagen Compliance provides a global end-to-end GRC and IT security 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 , IT &- Cyber Security Issues



Copenhagen Compliance® has dedicated resources for consultancy and research in Good Governance, Risk Management and Compliance issues involving corporations, universities and business schools and GRC organisations on four continents. Email; info@copenhagencompliance.com Tel. +45 2121 0616

As ever, always have your legal advisors review and advise on any legal guidance or on any contractual obligation. The EUGDPR Institute by Copenhagen Compliance Group is neither a Law Firm nor are we licensed to provide legal advice.