



GENERAL
DATA
PROTECTION
REGULATION



FAS
Foundation

DPO
Masterclass

CEP
Practitioner



Overview of the GDPR sessions



abc

Foundation. FAS

- Introduction to GDPR
- GDPR in practice
- Changes Management
- Principles for data processing
- Roadmap for implementation



Workshops

- The key components of third-party compliance
- Assessing GRC, cyber and GDPR vulnerabilities
Creating A Data Privacy Culture
- Leadership, PR and social media for crisis management
- How To Effectively Deal With Cyber Security Breaches



DPO




- DPO rule and functions
- Binding corporate rules
- Data protection impact assessment
- ISO 27001



Practitioner. CEP

- Best practices and methodology
- Managing the privacy compliance program
- Study cases
- Definitions

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



Agenda

Day 1



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

Day 2



How to implement and Execute GDPR

Key roles and responsibilities: controller, processor and data protection

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

The Role and responsibility of the DPO

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 3



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

Certification



Access to the presentation

<https://eugdpr.institute/fas>



All Links




- FAS Presentation - <https://www.eugdpr.institute/fas/>
- FAS Exam - <https://www.eugdpr.institute/gdpr-fas-exam/>
- DPO Presentation - <https://www.eugdpr.institute/dpo/>
- DPO Exam - <https://www.eugdpr.institute/gdpr-dpo-exam/>
- CEP Presentation - <https://www.eugdpr.institute/cep/>
- CEP Exam - <https://www.eugdpr.institute/gdpr-cep-exam/>
- pdf links
 - FAS: <https://www.eugdpr.institute/wp-content/uploads/2019/06/day1.pdf>
 - DPO: <https://www.eugdpr.institute/wp-content/uploads/2019/06/day2.pdf>
 - CEP: <https://www.eugdpr.institute/wp-content/uploads/2019/06/day3.pdf>

We will focus on issues

... not organisations



 ***“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.”***

Does the GDPR applies to me?



Does my organization offer goods or services to EU residents?

Does my organization monitor the behaviour of EU residents such as apps and websites?

Does my organization have employees in the EU?

Introductions

Name?

1

Organization?

2

Role?

3

Background?

4

Expectations?

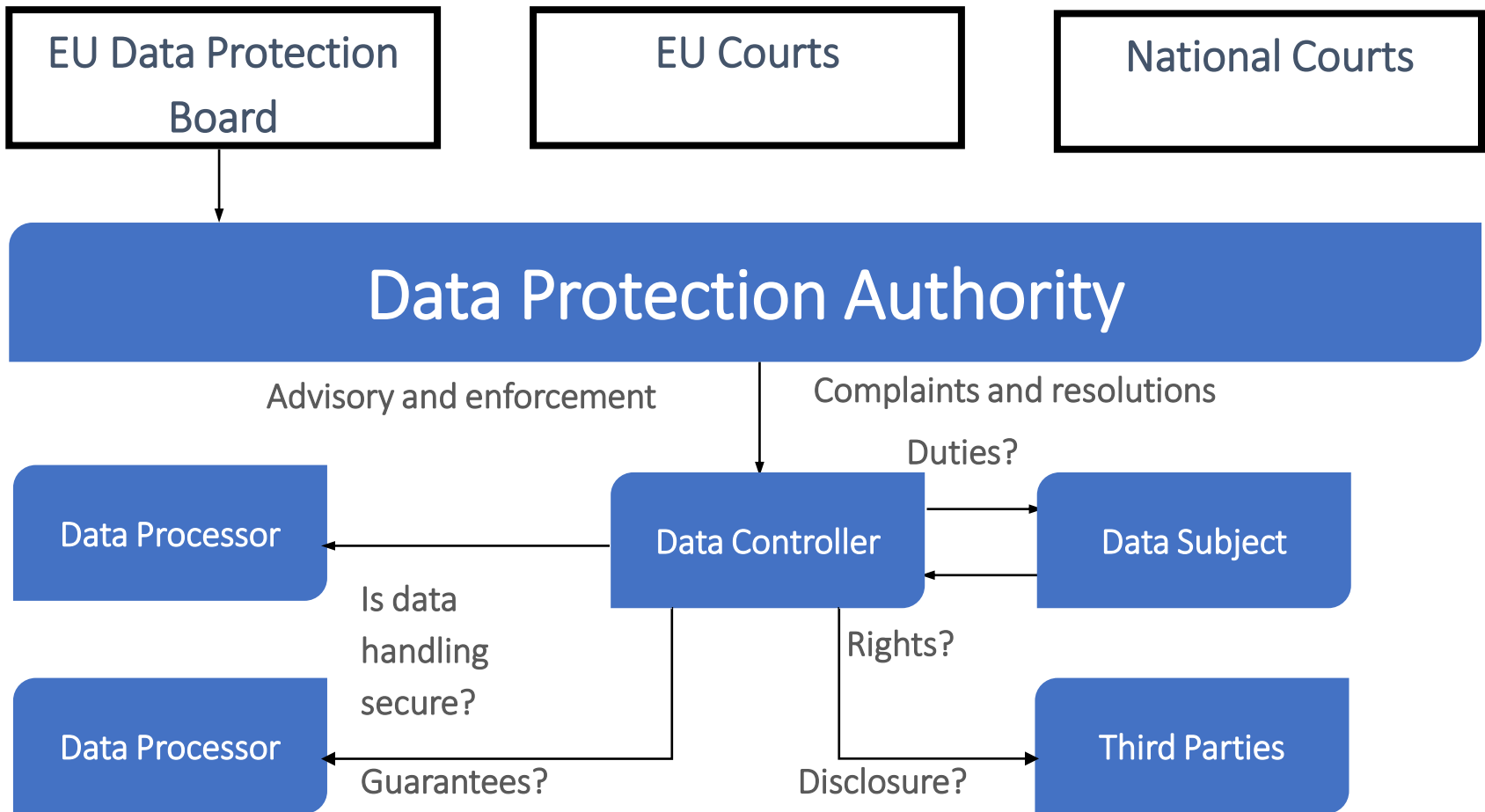
5

GDPR areas



- ✎ **GDPR challenges**
- ✎ **Privacy culture**
- ✎ **GDPR compliance journey**
- ✎ **Organise changes**
- ✎ **Controller/Processor /DPO Challenges**
- ✎ **Legal to practice**
- ✎ **Data Transfers**
- ✎ **Oversight Authorities**

Organization



Basic definitions



Privacy data

information that can uniquely identify a person, can be public or private

Data subject

person whose personal information is being referred to



Sensitive personal information

related to medical treatment, genetic data, sex life and +

Data controller

organization that determines the means and purpose of data processing



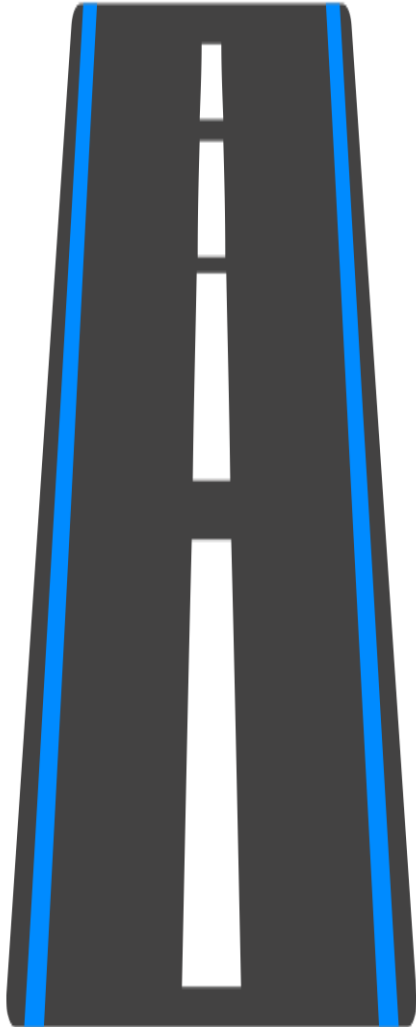
PHI *Protected Health Information*

PFI *Personal Financial Information*

Data processor







organization that processes personal information based on instructions

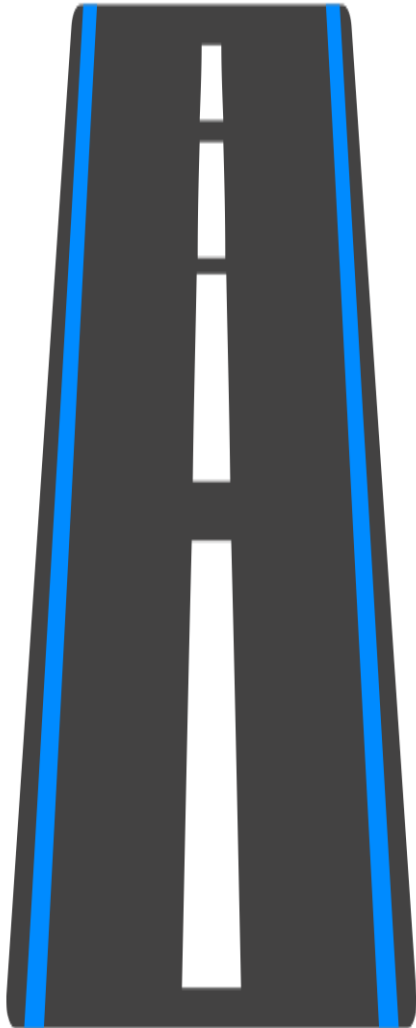




A- Plan







-  **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- Review contracts**
-  **6- Report data breaches**



C- Improve

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



Seminar content and topics covered will include:



- The background of EU GDPR and important
- An overview of the regulatory framework of local, regional and global privacy laws
- How to document the data mapping process to identify personal data items, formats, transfer methods and locations;
- The data subject's rights to an individual's personal
- The hidden challenges of third-party vendor risk management
- Consent management and cookie compliance
- Procedure for Processing Efficient and effective management of subject access requests
- Privacy by Design and Default
- The What, When and How of Data Privacy Impact Assessments (DPIA)
- Incident identification response and the response
- The lifecycle of a data breach and breach reporting
- GDPR and Sales and marketing requirements and the execution issues of post-implementation monitoring and controls
- How GDPR works with third parties and the impact on International data transfers
- The multijurisdictional & territorial scope of the EU GDPR
- Updating the Privacy Shield, Codes of Practice, Standard Contractual Clauses, Binding corporate rules
- Conducting Data audits and certification
- Awareness training and competence requirements
- We will also discuss the recent case studies for non-compliance and explore the global best practices that can lead to excellence in GDPR, data protection, privacy, IT and cybersecurity progress.

Overview

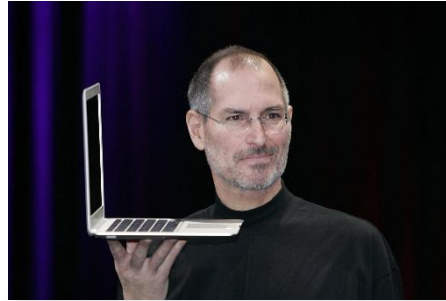


History of GDPR

Data privacy and protection



**What the
friends
think**



**What
the mom
thinks**



**What
society
think**



**What
the boss
thinks**



**What the
family
thinks**



**What
we think**

What is happening in the world?

There are data breaches everywhere, everyday.



*Facebook Security Breach Exposes
Accounts of 50 Million Users*

FINANCE • EQUIFAX

**Equifax Data Breach, One Year Later: Obvious
Errors and No Real Changes, New Report Says**

Cathay Pacific faces probe over massive
data breach

Under Armour

- 150 million records breached
- Date disclosed: May 25, 2018

Evolving information landscape



We are in a rapidly evolving information age

- Big Data, Mobile and the Internet of Things are rapidly transforming how information is collected, processed, used and shared.



Industry is in a digital transformation

- Mobile finance, digital payments and currency, driverless cars and a host of other rapidly emerging information services are re-shaping traditional business models.



Old laws don't fit; new framework is emerging

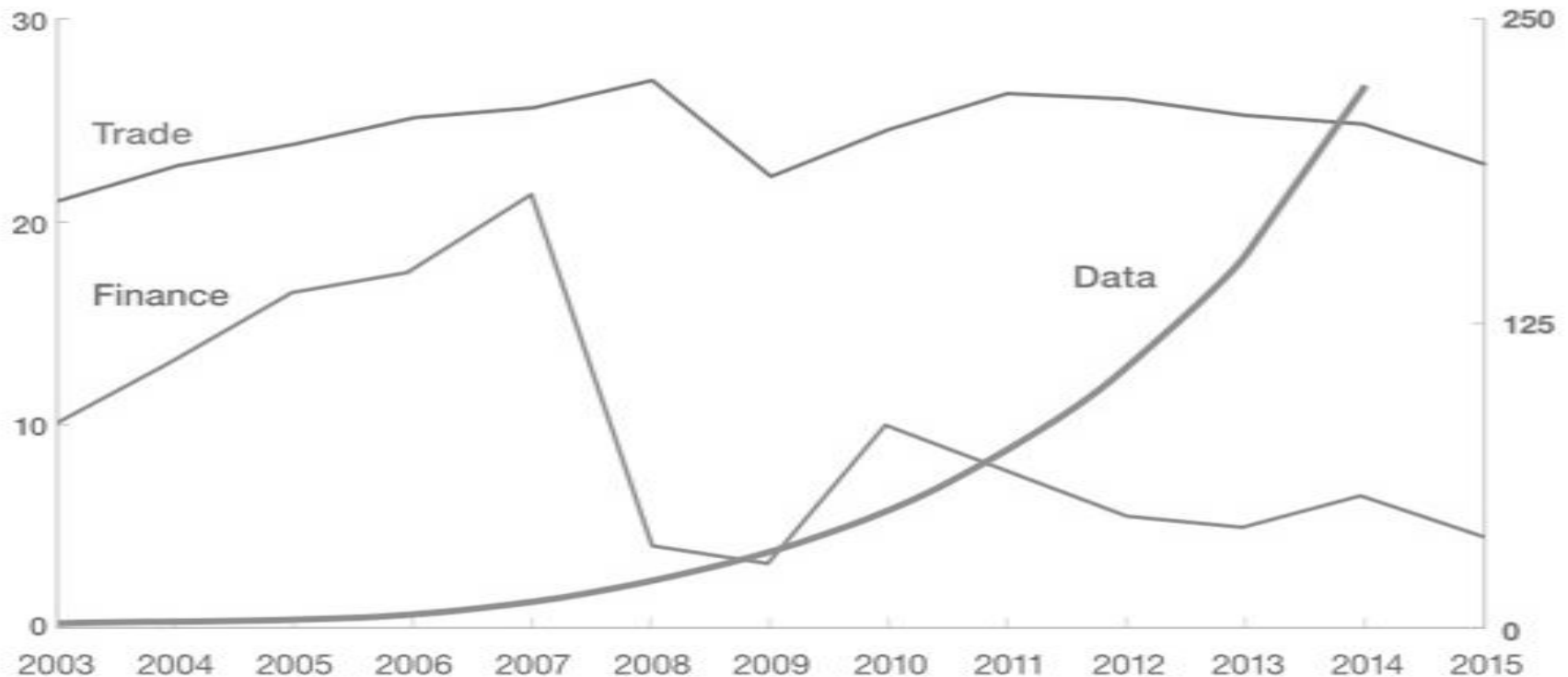
- Information-related global laws and regulations are struggling to adapt to new technologies and new data uses, requiring a new approach to managing information-related risks.

What an opportunity

Global flows of data have outpaced traditional trade and financial flows.



Flows of trade and finance,¹
% of GDP

Flows of data,¹
terabits per second





Earlier regulations and laws (October 1995)

EU Data Protection Directive

-  Protection of rights of individuals in data processing activities
-  Ensure the free flow of personal data between EU Member States

Issues

-  Legal differences arose as a consequence of the implementing acts adopted by the EU Members
-  Data processing activities that were allowed in one EU Member State could be unlawful in another one

Drivers to Privacy Laws

- ✎ Common Understanding
 - ✎ Standardize what is acceptable, setting common expectations, requirements, obligations & enforcement
- ✎ Data Collection
 - ✎ Safeguards to protect against incessant data collection
- ✎ Data Processing
 - ✎ Protection against incessant processing
- ✎ Technology advancement & Enhanced connectivity
 - ✎ Safeguards against excessive collection & processing must be implemented in the world of IoT and connected devices
- ✎ Context availability & processing
 - ✎ Safeguards against misuse of context built through mobile, sensor & location based technologies

Drivers to Privacy Laws

- ✎ Trans border data flows & Cloud services
 - ✎ Vulnerabilities due to data in different geo locations must be prevented by enacting laws
- ✎ Analytical Profiling
 - ✎ Big data analytics has enabled the collation of scattered bits of PI & manufacture information. Laws must be built to safeguard against misuse of such information
- ✎ Products & Services
 - ✎ Laws to prevent misuse of information in different contexts
- ✎ Supply chain, hyper specialization & global sourcing
 - ✎ Business focus on core competency and outsourcing the rest.
 - ✎ Laws must be made to prevent damage from loss of data

Timeline

Directive 95/46/EC is adopted

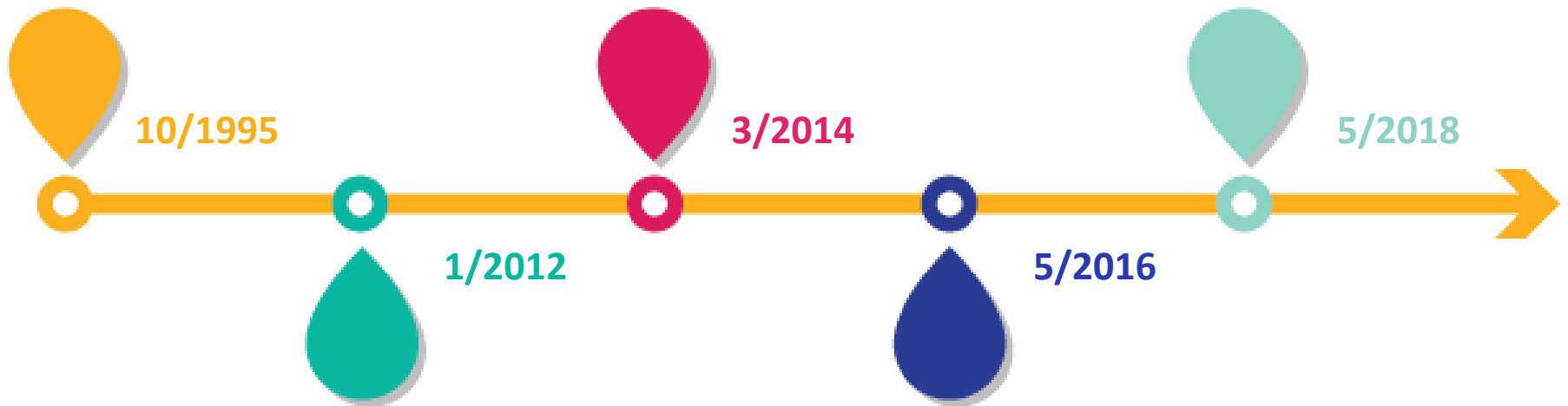
Processing of personal data
Free movement of personal data

GDPR draft is adopted

Personal data protection as a
fundamental right
Voted overwhelmingly in favor

GDPR is effective

So now?...



10/1995

1/2012

3/2014

5/2016

5/2018

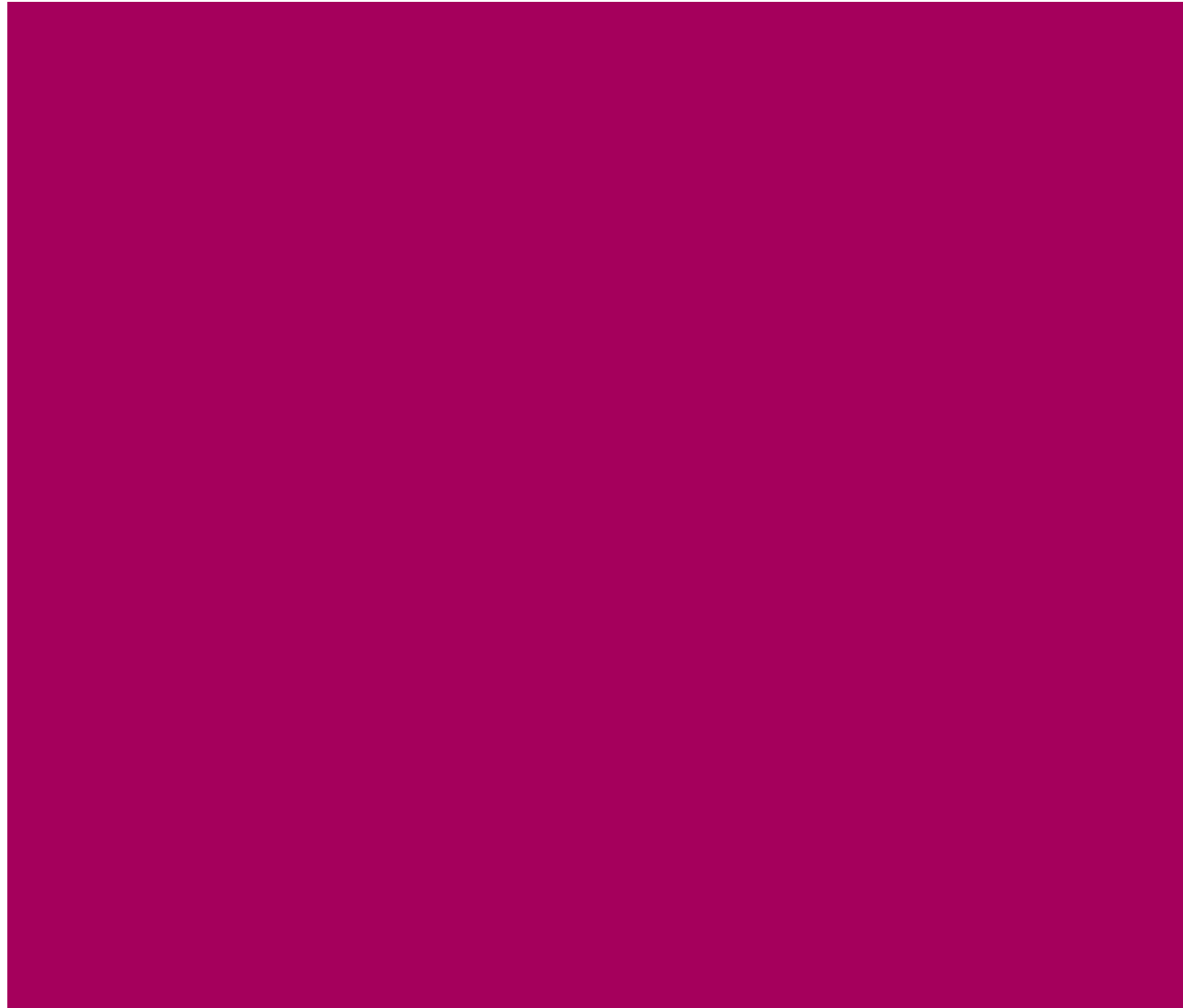
EC proposal reform

Strengthen online privacy rights
and digital economy

GDPR enters into force

Published in the EU Official Journal

A - Plan



ISO 27001 Info Security



Context

Leadership

Planning

Support

Operation

Performance

Improvement

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

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

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

- Resources
- Competence
- Awareness
- Communications
- Documented information

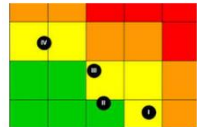
- Operational planning and control
- Info sec risk assess
- Info sec risk treatment

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

- Nonconformity and corrective actions
- Continual improvement



Personal Data	Purpose	Data Subject	Retention	Owner	System	Security Mechanisms
Employee name, address, phone, date of birth	Identification	Employees	Permanent file	HR	SAP HR	Password, encryption, Physical safeguards
Payroll processing	Employee	Until end of employment	HR	SAP HR	MS Excel files	Password, encryption, Physical folder
Performance review	Employee	Until end of employment	HR	Compass Performance		Password



Train your people

Audit compliance

- To access data: request access to personal data by using a form to verify the identity of requester.
- To data portability: request access to personal data in a structured, commonly used and machine-readable format.
- To verify and be forgotten: request deletion or removal of personal data.
- To restrict processing: request the data not to be used.
- To object by controller: when authorized by other legal provisions or legitimate interests.
- To track profiling: request to opt out of targeted advertising or profiling.

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, notices

Continual Improvement

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

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

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.



Step 2: Get a team



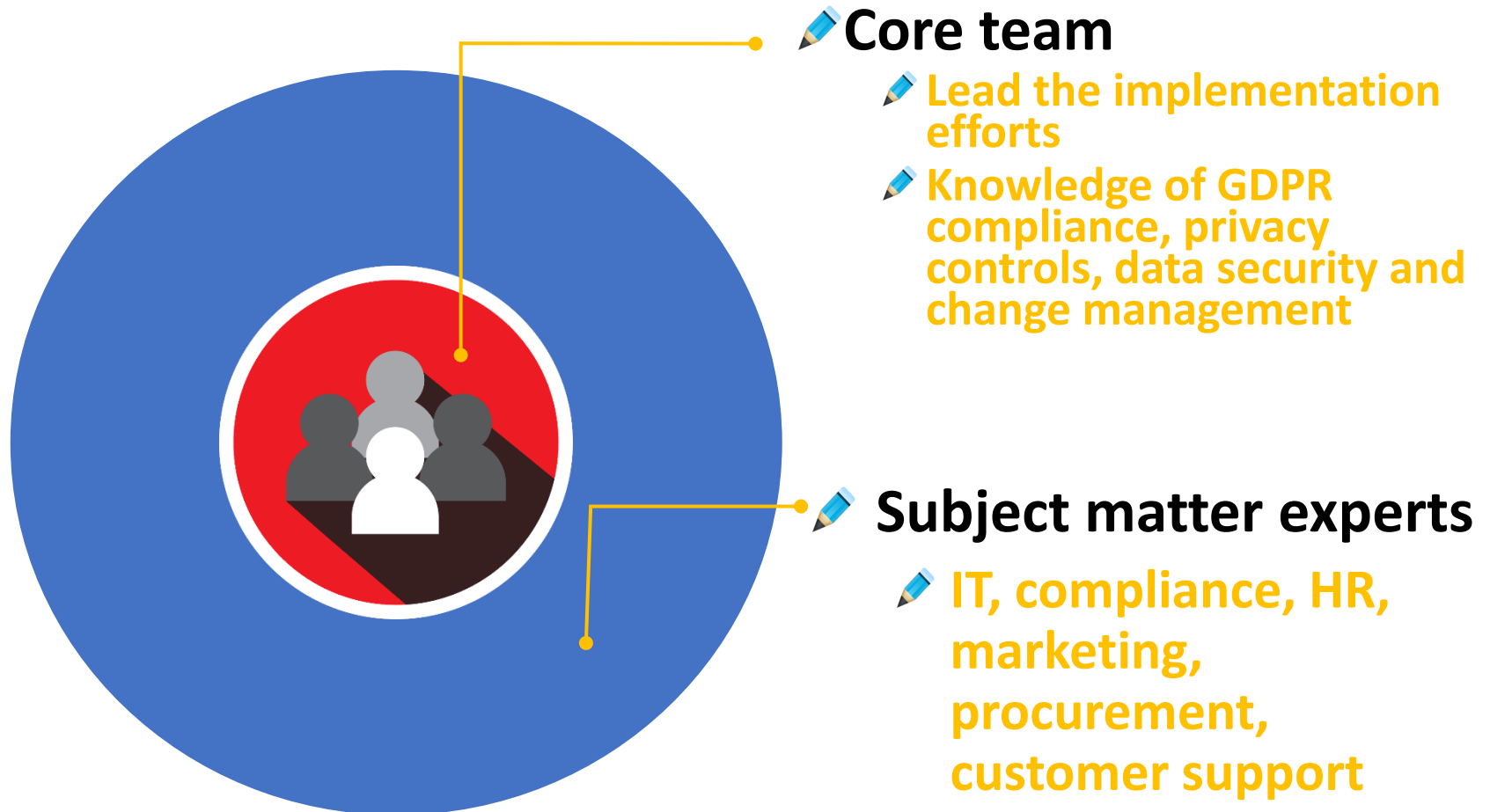
One man army?

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

Step 2: Get the team

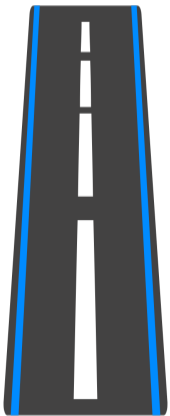


Step 3: Relevant processes



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 is data identifiable?

A British person **65,5M**



How is data identifiable?

A British female **33,2M**



How is data identifiable?

A British female born in 1950 **6,2M**



How is data identifiable?

.... Living in Buckingham Palace **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

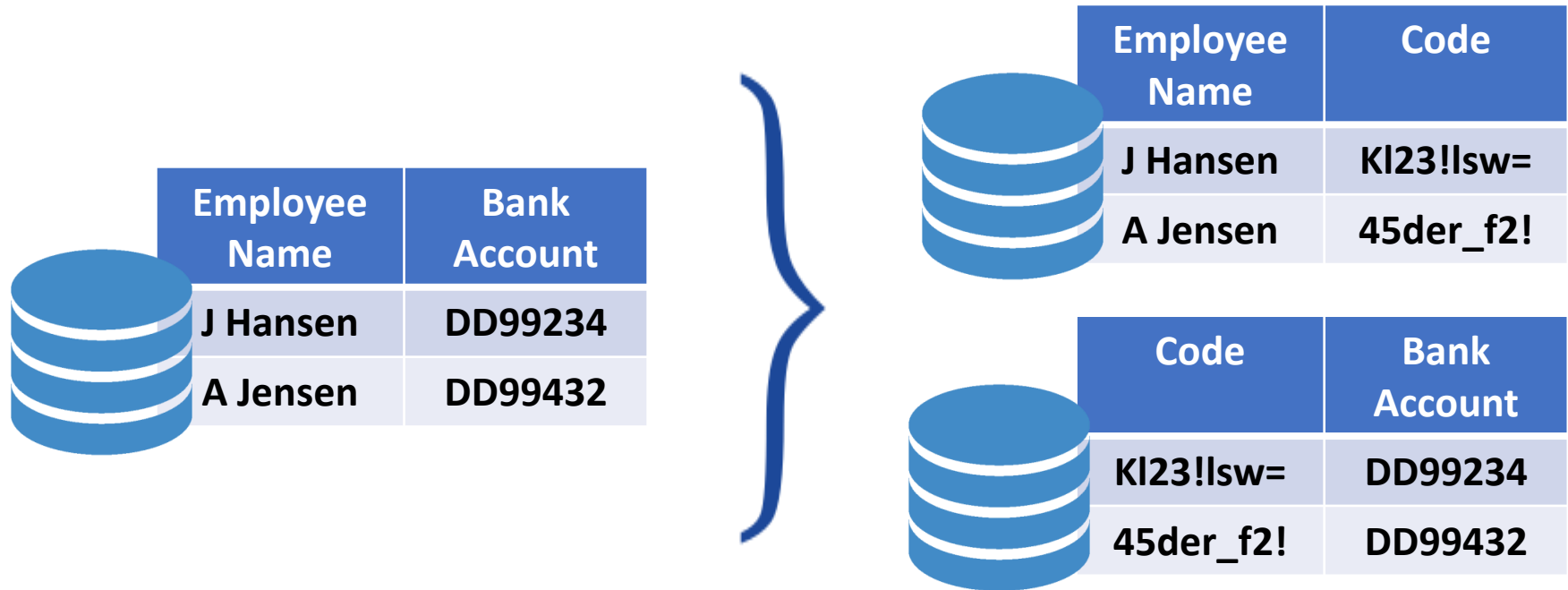
NEW

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

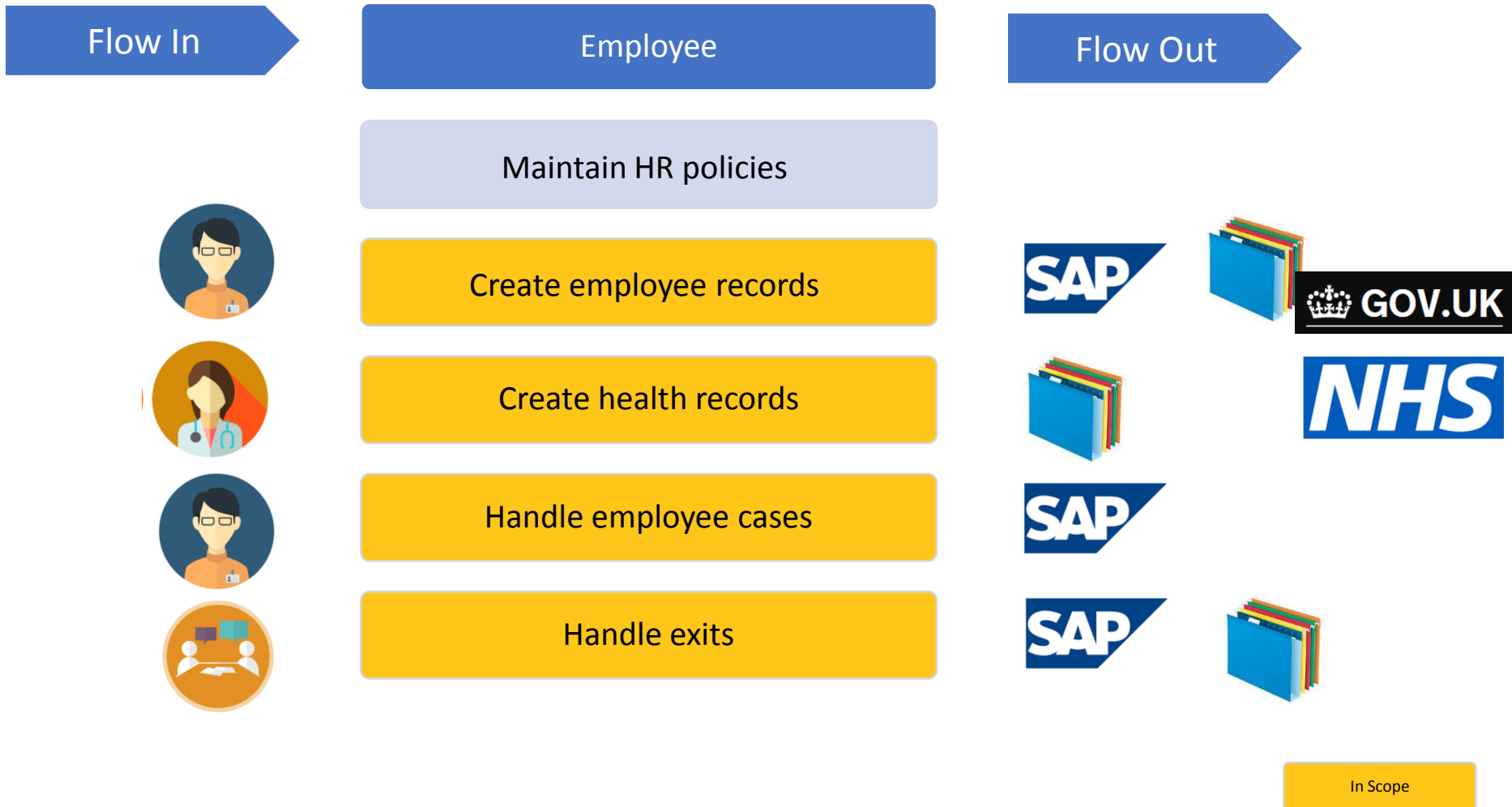
Political

Religion

Sex life

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

Step 3: Scope example



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?

Step 4: Compile a data inventory

Who

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

Where

- the personal data is stored?
- the personal data is transferred?

Why

- the personal data is under the organization control?

When

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

What

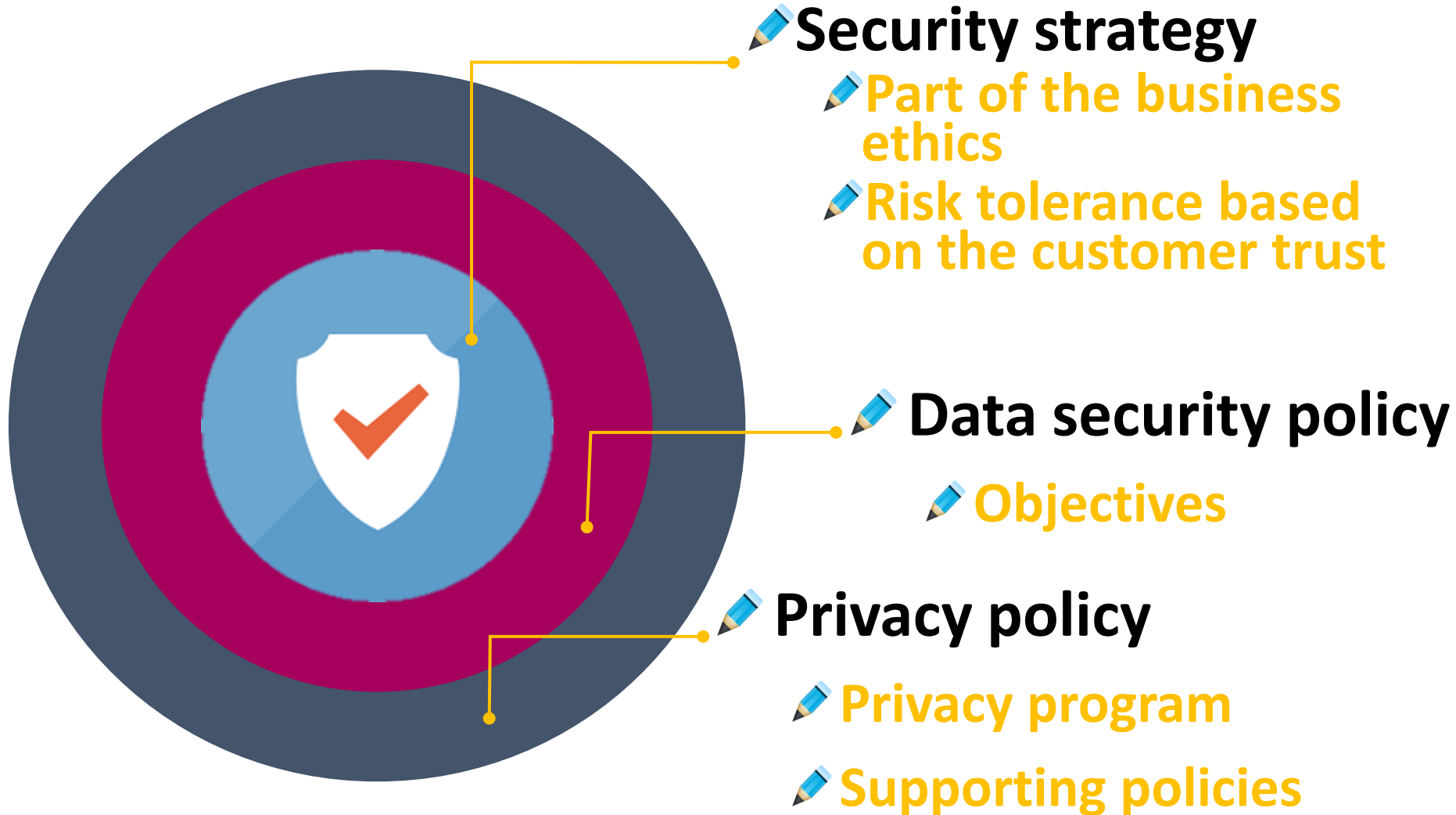
- safety mechanisms and controls are in place?

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 6: Privacy policy



Step 6: Documentation requirements



- ✎ **Policies**
- ✎ **Objectives**
- ✎ **Scope**
- ✎ **Procedures**
- ✎ **Controls**
- ✎ **Risk assessment methodologies**
- ✎ **Risk treatment plan**
- ✎ **Documents protection and control**

Step 6: Privacy Policy



Accountability and Transparency

Controllers

Processors

Subjects

Consent

Uses

Transfers

Purpose

Retention



Marketing



HR



Customers



Vendors



Cloud



Government



Analytics



Support



R&D



IT



Minors



Employees



M&A



Vendors

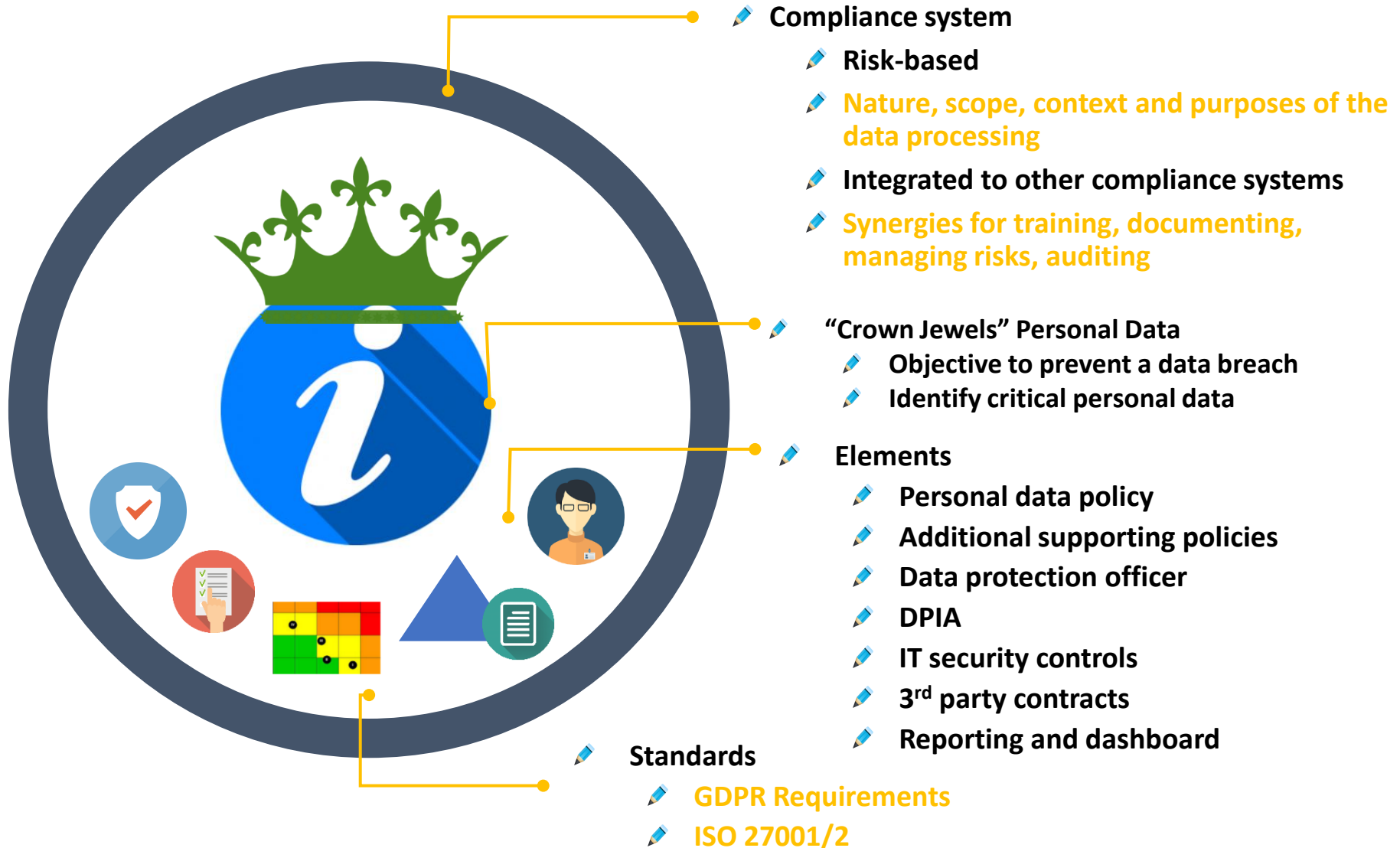


Operations



Backups &
Testing




Data Protection Management System



Step 6: Create a privacy policy

Best practices based on the ISO 27001

Set the information security objectives

-  provide access to information only to authorized employees and 3rd parties
-  protect the confidentiality, availability and integrity of information assets
-  implement annual information security awareness training

Support from upper management

-  Policy approved by CEO, IS compliance reports to the 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, recognise GRPD rights

- ✎ Define general principles and roles to limit:

 - ✎ the collection

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

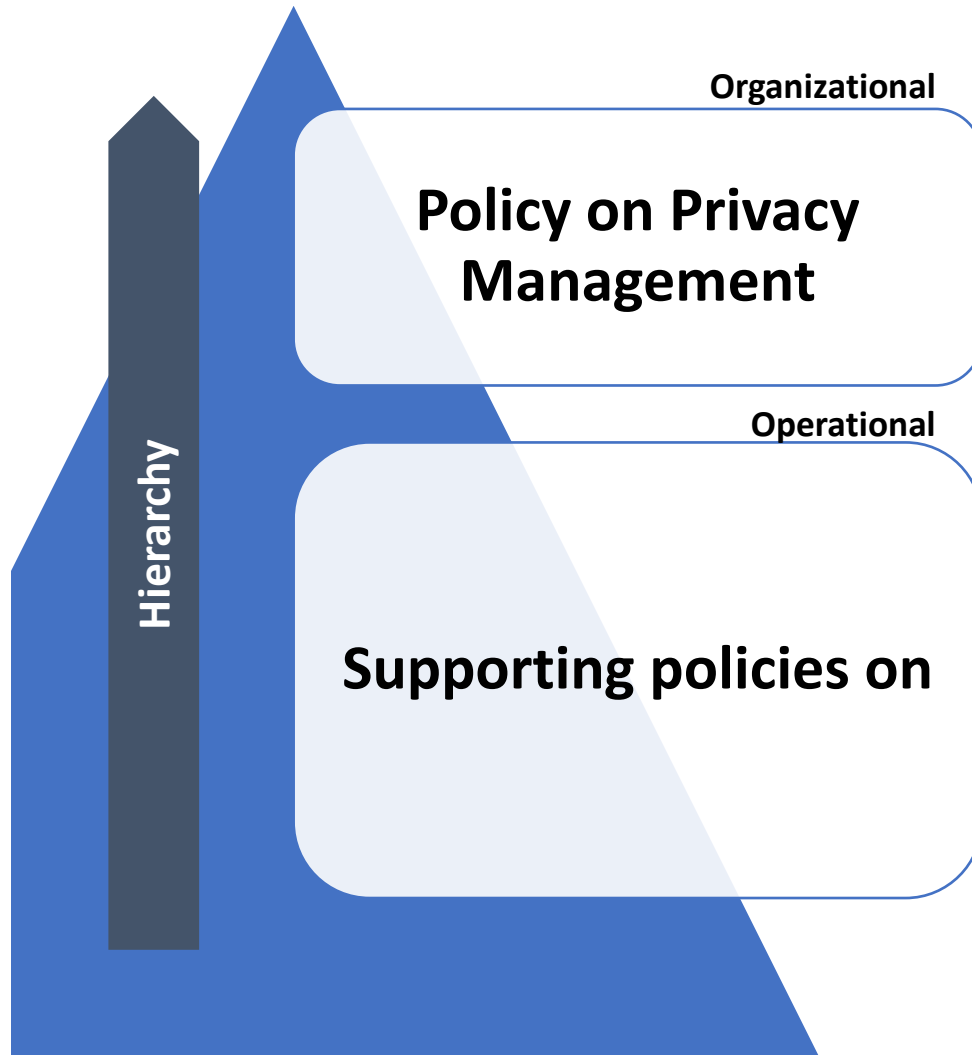
 - ✎ the use

 - ✎ 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



- 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

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

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**



Step 1: Principles



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

Step 1: Rights



To access data

request access to personal data to verify lawfulness of processing

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

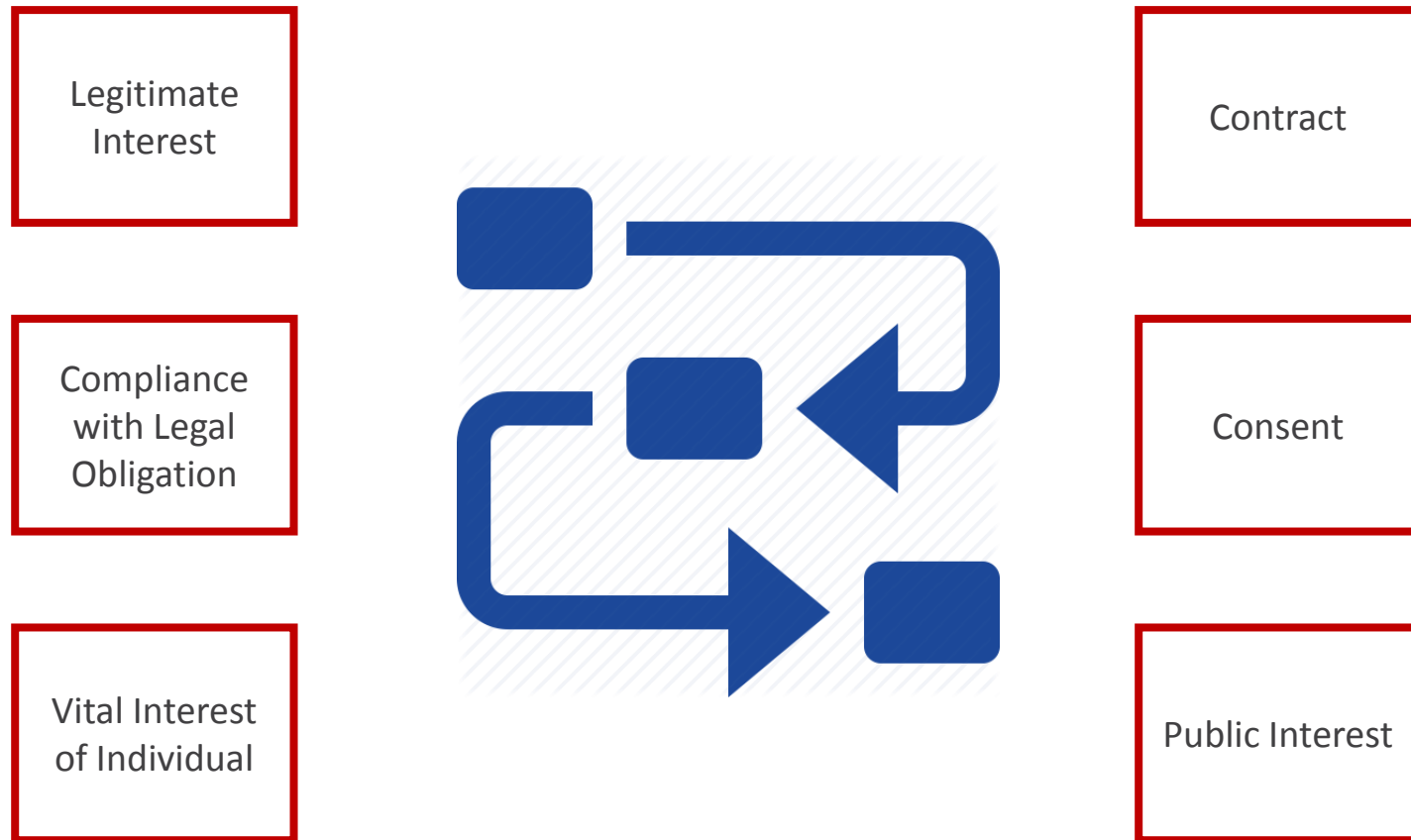


NEW

How to react after receiving a data subject request?

- ✎ How and when you got the consent
- ✎ What the consent covers
- ✎ How to demonstrate the processing according to the consent
- ✎ Where the data was stored and how it was accessed

Legal Bases for Processing Personal Data



If it is hard to obtain a valid consent, this probably means that another more appropriate legal basis should be used

Difficulties collecting consent – more appropriate legal basis should be used

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

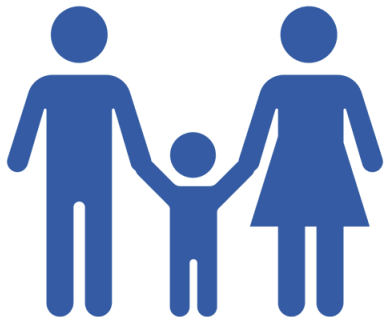
- Parental authorization for children below the age of 16
- Reasonable means to verify parental consent

Step 2: Verify age and parental authorisation

Consider requirements before relying on consent to justify processing of children's data.

Mechanism Requirements

- Appropriate age verification
- Parental authorisation
- Comply with Privacy by Design
- Limit risk to individuals
- Cannot be easily circumvented



Step 2: Difference

Privacy notices

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

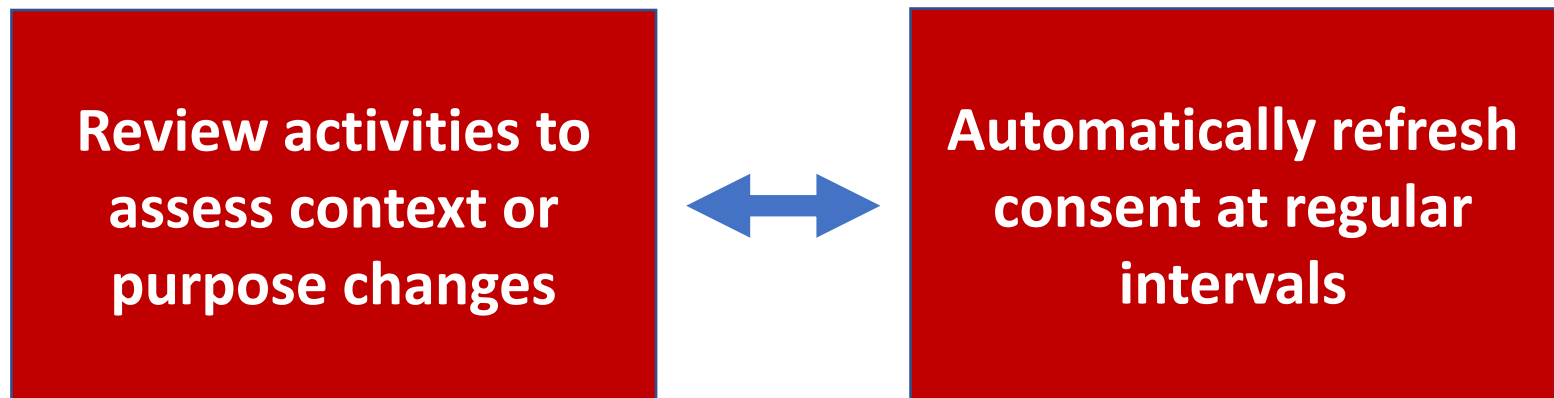
Legal basis, type of information, 3rd parties recipients and retention period

Consents

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

Step 2: Consent renewal

- Make sure consent does not degrade over time.
- When purpose or activities evolve beyond the initial purpose, new consent will be required.



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.”

What are your responsibilities if you buy an email database of potential clients from a marketing company?

✎ Do you need to have consent(s)

✎ How do you assess the legitimate interests

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?
- ✦ Requests 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 → CSV, 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


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
- notify breaches


NEW

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
 - in respect of the technical and organizational security measures governing the processing
- Allow a data controller audits 
 - on premises, systems, procedures, documents and staff
- Delete or return data at the end of the contract

Group discussion

 **Are you a data processor or a data controller?**



... but, where?

in the EU

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

outside the EU

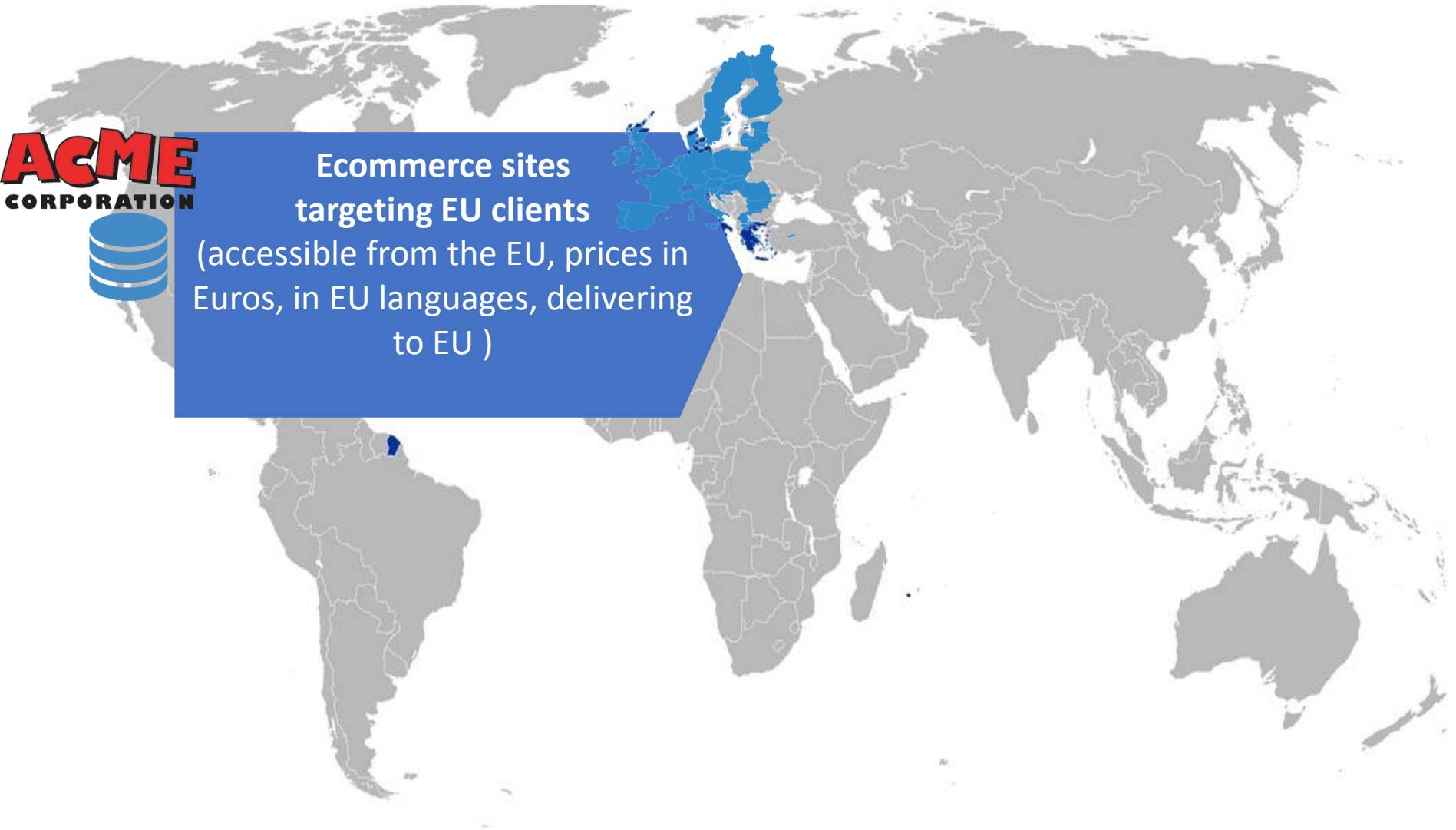
When personal data of EU citizen is processed by a non-EU organization **offering goods and services** in the EU (not paid in the EU)

Extra-territorial application

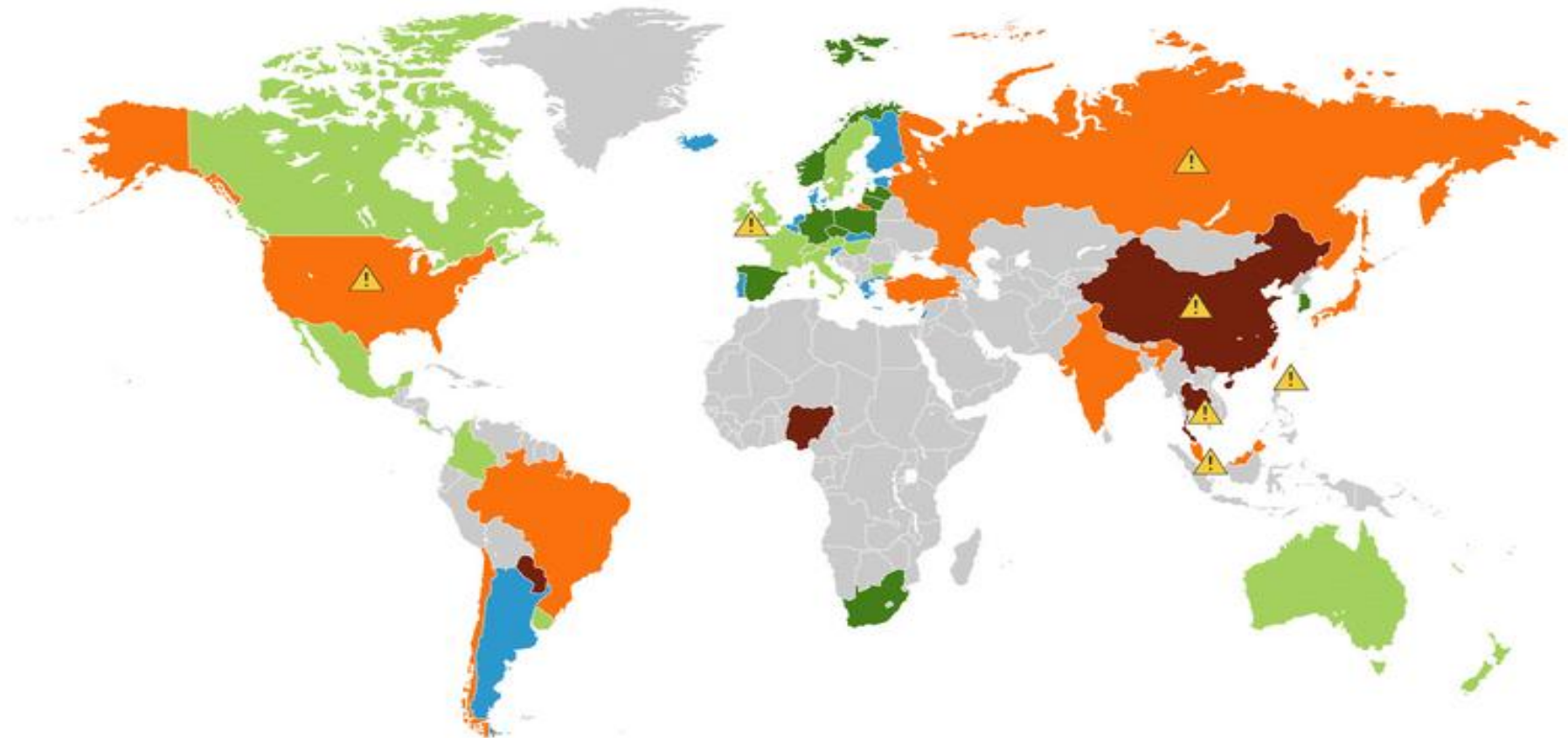
ACME
CORPORATION



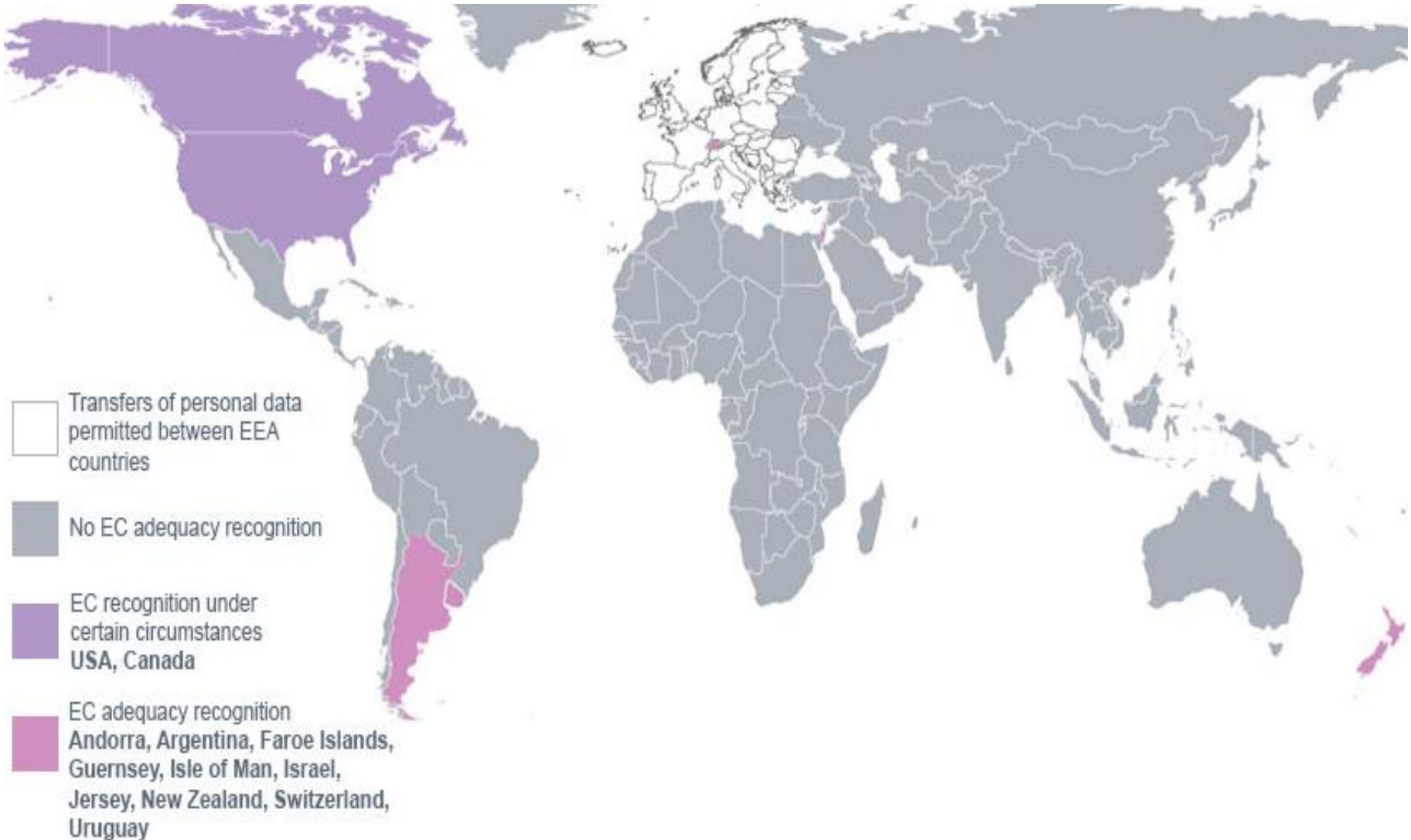
Ecommerce sites
targeting EU clients
(accessible from the EU, prices in
Euros, in EU languages, delivering
to EU)



Views on privacy



International transfers

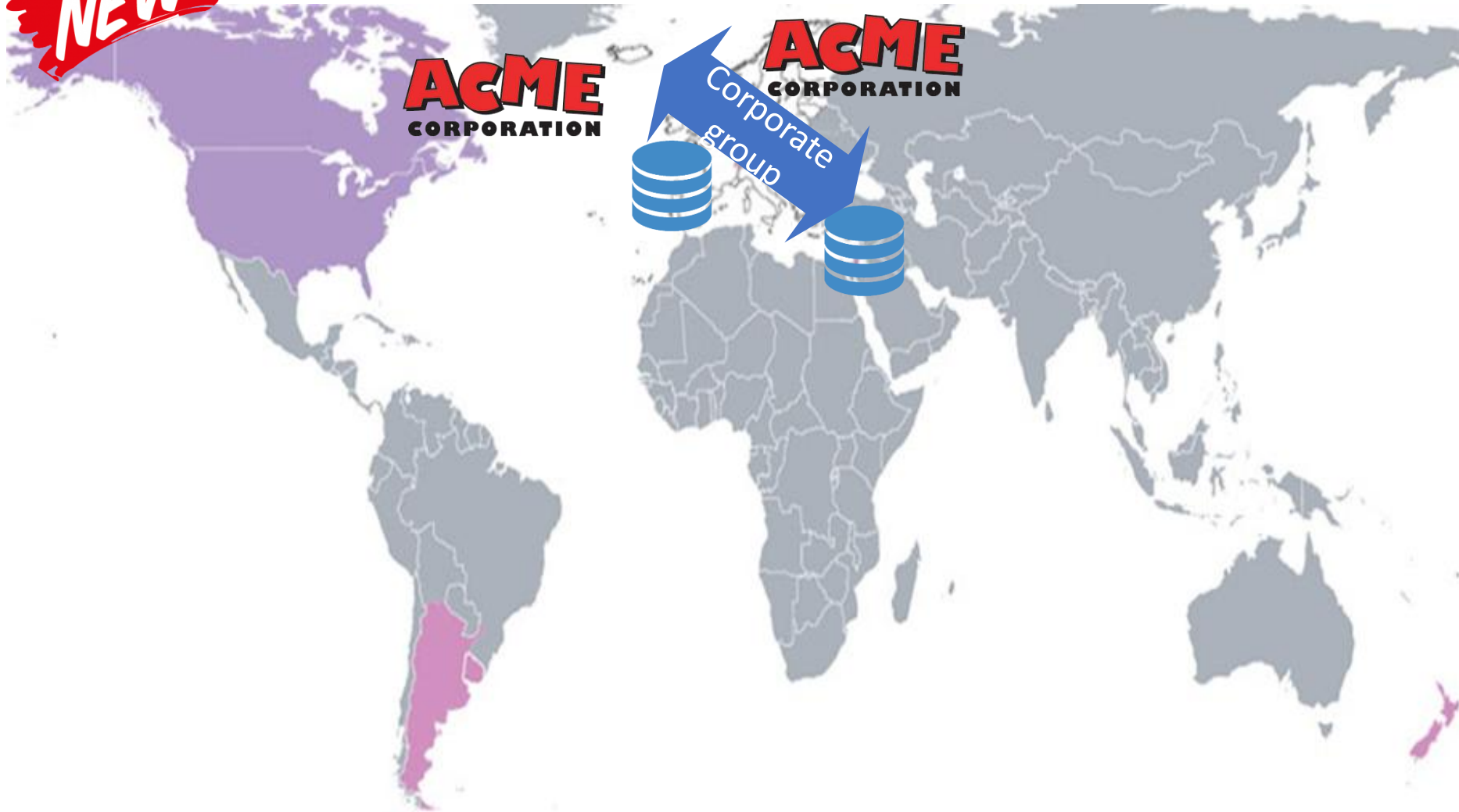


Adequate safeguards

- Controllers and processors may only transfer personal data to third countries that do not provide for adequate protection (non-adequate countries),
 - if the controller or processor has provided adequate safeguards
- The data transfer provisions require processors/controllers to implement adequate safeguards, with full GDPR scope
 - The interpretation of this requirement means that processors should provide “adequate safeguards” insofar as their own obligations are concerned.
 - The DPAs interpret the transfer requirement on the controller “to offer adequate safeguards.”
 - The current provision is that both controllers processors are required to impose “adequate safeguards” in case of transfers to all third parties in a non-adequate country

Binding corporate rules

NEW



Contract between group companies to transfer information, covering

- ✎ specify the purposes of the transfer and affected categories of data
- ✎ reflect the requirements of the GDPR
- ✎ confirm that the EU-based data exporters accept liability on behalf of the entire group
- ✎ explain complaint procedures
- ✎ provide mechanisms for ensuring compliance (e.g., audits)

Model pre-approved clauses to reduce compliance burden

Standard data processor clause



The controller or processor can use standard data-protection clauses adopted by the Commission or by a supervisory authority


- Standard data-protection clauses between the processor and another processor
- To avoid any prejudgment of the fundamental rights or freedoms of the data subjects, controllers and processors
- Encouraged to provide additional safeguards via contractual commitments that supplement standard protection clauses
- Regulators have new rights to audit your compliance for businesses that operate in sectors where complaints to the regulators are frequent
- Identification of 'high risk' areas in processor contracts
 - creating a 'processor inventory' and identifying the high risk issues in the contracts based on, e.g. volume of personal data processed, where it might be accessed from and by how many sub-contractors/people, and how sensitive the data is.

Privacy shield



- The premise of GDPR is the ‘harmonization’ of data protection laws across EU
- The U.S.-EU Safe Harbor, then the EU-U.S. Privacy Shield, and later U.K. Privacy Shield Shouldn’t other countries be subject to the same security with respect to compliance with EU data protections laws, with major countries like China, India and Russia.
- Five-step checklist:
 1. Develop and maintain a privacy policy based on Privacy Shield principles.
 2. Validate security safeguards with a customized security questionnaire deployed to system, application and interface owners who handle data that are subject to the certification.
 3. Address onward transfers by review and revising existing contracts for third-party vendors and other onward transferees.
 4. Update training for employees who have access to EU citizen data.
 5. Compile within a single compliance binder documentation that supports the company’s Privacy Shield certification—such as policies, a gap assessment report, and contract addendums.
- If firms wish to transfer HR data, they will have to indicate that separately in their self-certification submission and include details, such as their HR privacy policy.
- <https://www.bbb.org/EU-privacy-shield/privacy-shield-principles/>

Group discussion

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



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

Step 5: Tips for clauses

Ensure that the contracts with 3rd parties include the obligations to:

- ✎ comply with the GRPD and other privacy principles and best practices
- ✎ comply with the organization's privacy policy and other supporting procedures
- ✎ notify your DPO in the event of data breach, privacy complaint, or near miss
- ✎ agree to regular privacy audits of personal information handling practices
- ✎ indemnify in the event of personal data losses
- ✎ ensure their staff undertake privacy training



Step 6: 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 6: 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

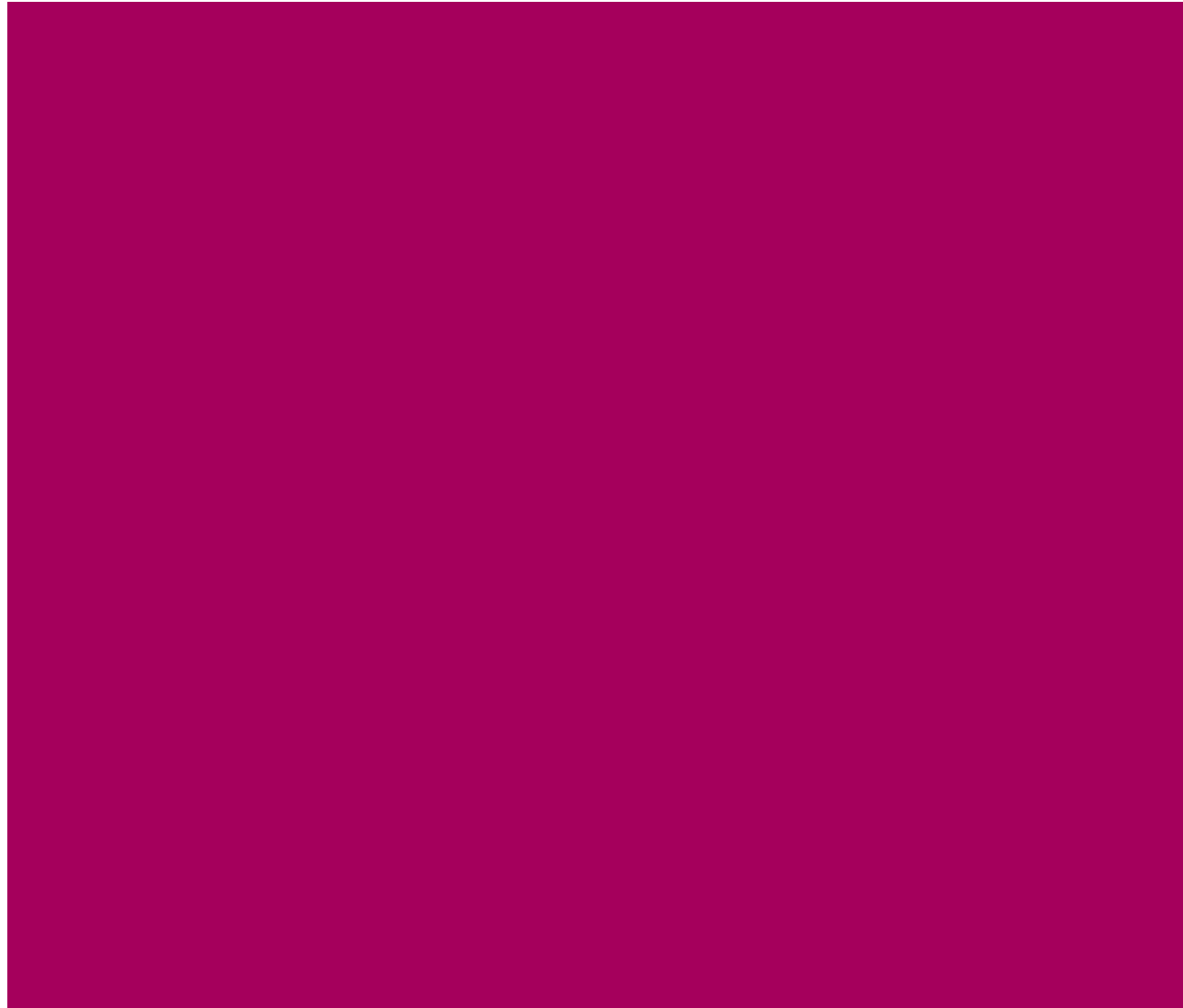
- Restore data availability and access in case of breach
- Redundancy and back and facilities
- Incidence response plan



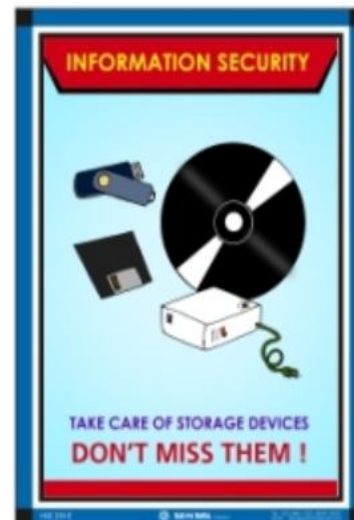
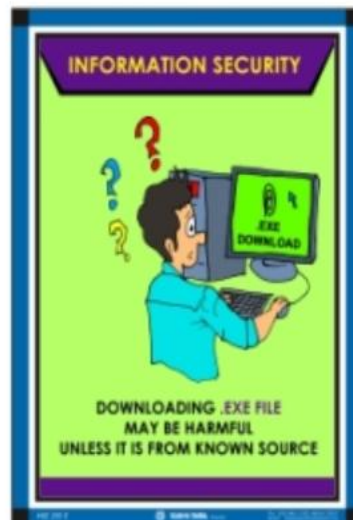
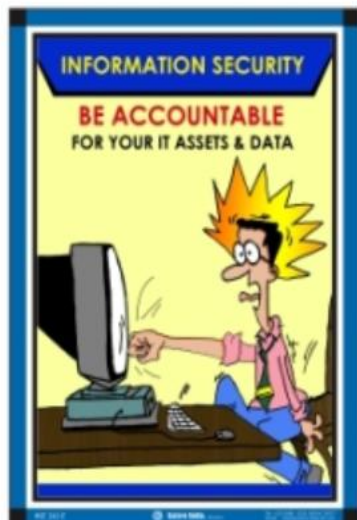
Regular security testing

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

C - Maintain



Step 1: Train your people



Step 1: Discussion case

 **How could you develop training for this risk?**

 **How could you document your training efforts?**



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

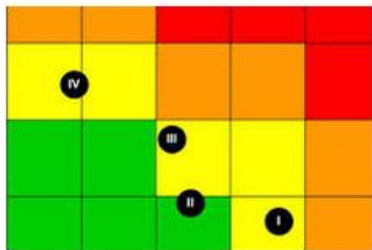
3- Consult on risks and controls



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!

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, pseudoanonymity
		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

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

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 3: Audit compliance



Process	KPI example
Training	% of staff (or hours) trained on privacy policies (participated/passed, type of program, levels)
Incident	# of privacy incidents (by system, location, repeated or new) # reported data breaches
Audits	# non conformities # action plans on-going (and past due)
Consents	% consents obtained
Access control	% of credential validated
Compliance	# requests # complains # new projects with DPIA

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

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


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)

GDPR *as is or to be*



✎ 52 articles leave room for national legislation

✎ GDPR rules apply today with low level of fines

✎ June 2017 guidance from oversight

✎ Intense debates for the levels of fines, obligations to appoint a DPO and specific regulations for banks and pharma

✎ Draft legislative proposals

✎ Act formally presented

✎ Final approval

✎ Art. 88 - Employment Data: MS laws and collective agreements

All Links



- FAS Presentation - <https://www.eugdpr.institute/fas/>
- FAS Exam - <https://www.eugdpr.institute/gdpr-fas-exam/>
- DPO Presentation - <https://www.eugdpr.institute/dpo/>
- DPO Exam - <https://www.eugdpr.institute/gdpr-dpo-exam/>
- CEP Presentation - <https://www.eugdpr.institute/cep/>
- CEP Exam - <https://www.eugdpr.institute/gdpr-cep-exam/>
- pdf links
 - FAS: <https://www.eugdpr.institute/wp-content/uploads/2019/06/day1.pdf>
 - DPO: <https://www.eugdpr.institute/wp-content/uploads/2019/06/day2.pdf>
 - CEP: <https://www.eugdpr.institute/wp-content/uploads/2019/06/day3.pdf>

Data Privacy and Protection is a Team Sport, which needs Super Powers!

