EU GDPR INSTITUTE

GENERAL DATA PROTECTION REGULATION

information security institute

GDPR MASTERCLASS
by Information-security Institute

FAS
Foundation

DPO
Masterclass

CEP
Practitioner

Foundation Training, Day I Budapest November 2019

Overview of the GDPR sessions

GDPR MASTERCLASS

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 Day I and II

GDPR MASTERCLASS

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

Certification Exam

Day 2

How to implement, Document and Execute GDPR Compliance

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

Certification Exam

Agenda Day III

GDPR MASTERCLASS

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 Exam

Seminar content and topics covered will include:

GDPR MASTERCLASS

- The background of EU GDPR ; important components for implementation/execution
- An overview of the regulatory framework of local, regional and global privacy laws
- Data mapping, identify personal data items, formats, transfer methods, locations
- The data subject's rights to an individual's personal data
- Third party and the impact on International data transfers
- The hidden challenges of third-party vendor risk management
- Processing Efficient and effective management of subject Access Requests
- The What, When and How of Data Privacy Impact Assessments (DPIA)
- Incident identification response. The lifecycle of a data breach and breach reporting
- Privacy by Design and Default Consent management and cookie compliance
- Sales and marketing compliance, & post-implementation monitoring and controls
- The multijurisdictional & territorial scope of the EU GDPR
- Privacy Shield, Standard Contractual Clauses, Binding Corporate Rules, certification
- Conducting Data audits ,Awareness training and Competence requirements
- 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.

Access the presentation

GDPR MASTERCLASS

FAS Presentation - https://www.eugdpr.institute/fas/

All Presentation and Exam Links

GDPR MASTERCLASS

- 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/2019/11/day1.pdf
- DPO: https://www.eugdpr.institute/wp-content/uploads/2019/11/day2.pdf
- CEP: https://www.eugdpr.institute/wp-content/uploads/2019/11/day3.pdf

We will focus on issues

… not organisations

GDPR MASTERCLASS

- ***"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."***

Introductions

GDPR MASTERCLASS

Does the GDPR applies to me?

GDPR MASTERCLASS

- ☐ **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?**

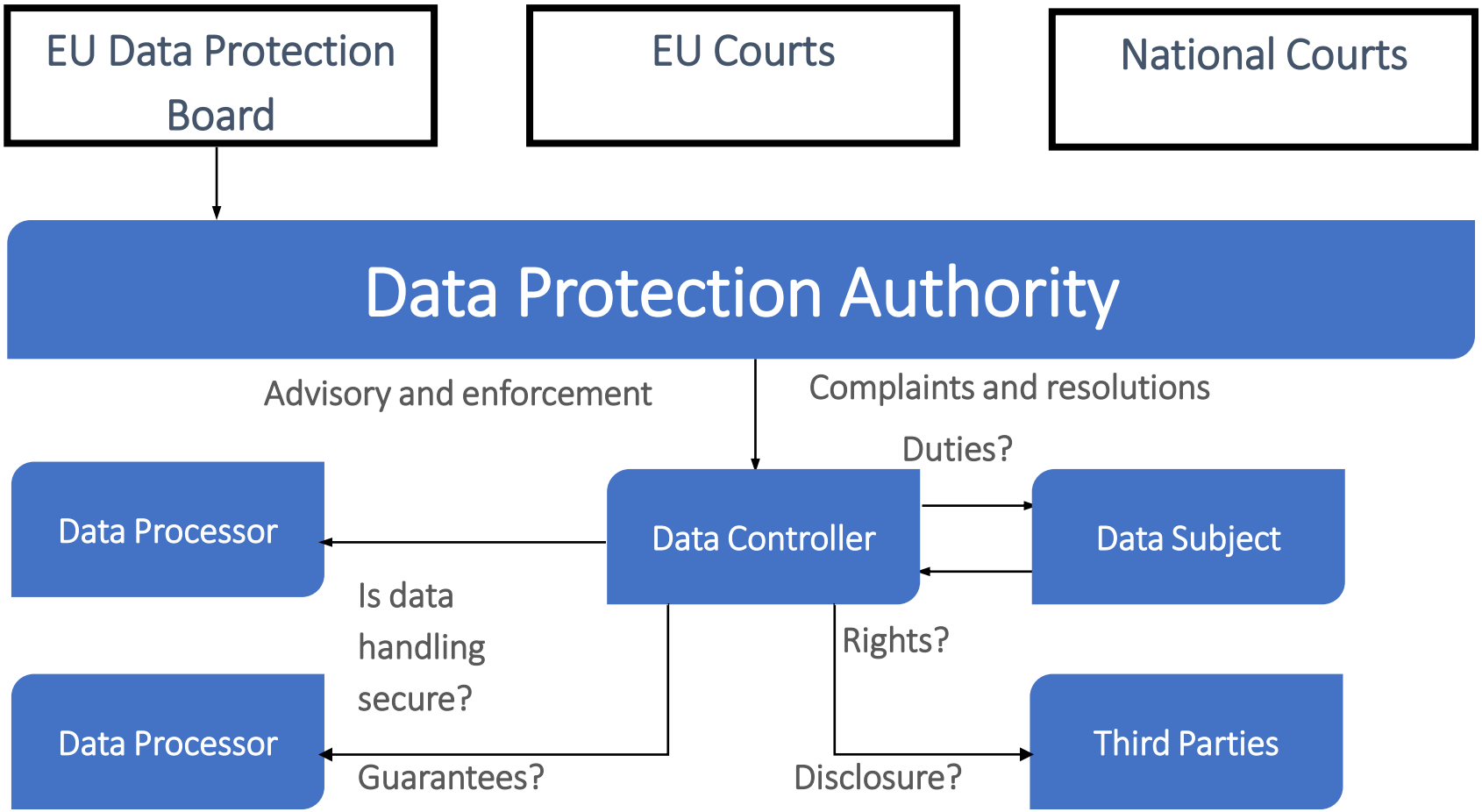
GDPR is out of scope when:

GDPR MASTERCLASS

- When processing of personal data;
- In the course of an activity which falls outside the scope of Union law;
- by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU; (Treaty of European Union)
- by a natural person in the course of a purely personal or household activity;
- by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

Organisation

GDPR MASTERCLASS



GDPR areas. Foundation

GDPR MASTERCLASS

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

Basic definitions

GDPR MASTERCLASS

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 +

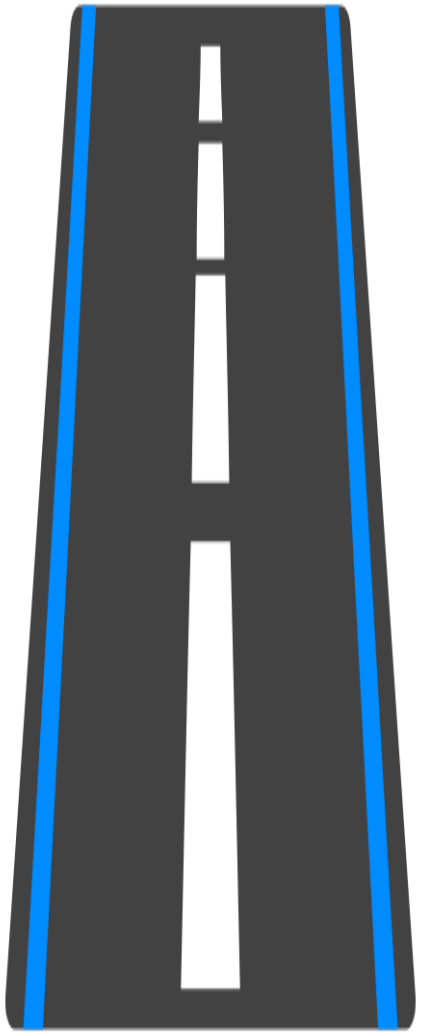
Data controller
organization that determines the means and purpose of data processing

PHI ***Protected Health Information***
PFI ***Personal Financial Information***

Data processor
organization that processes personal information based on instructions

Roadmap

GDPR MASTERCLASS

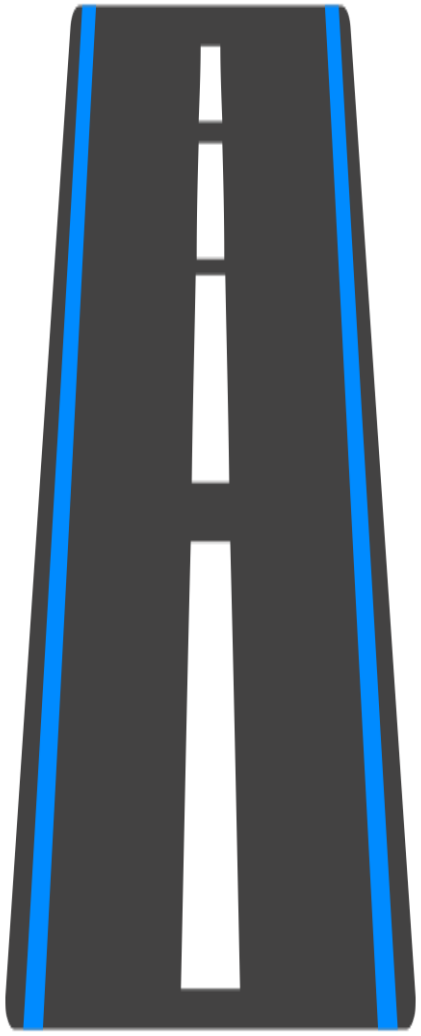


A- Plan

- 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

Roadmap

GDPR MASTERCLASS

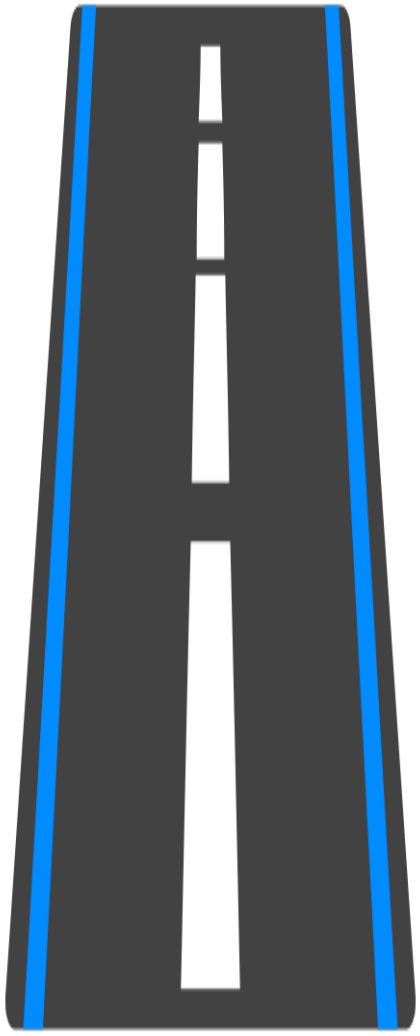


B- Do

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

Roadmap

GDPR MASTERCLASS



C- Improve

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

Overview

GDPR MASTERCLASS

History of GDPR

Data privacy and protection

GDPR MASTERCLASS

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?

GDPR MASTERCLASS

There are data breaches

50 million euros (£44m) by the French data regulator

Facebook Security Breach Exposes Accounts of 50 Million Users

£183.39 million ($230 million).

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

GDPR MASTERCLASS

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.

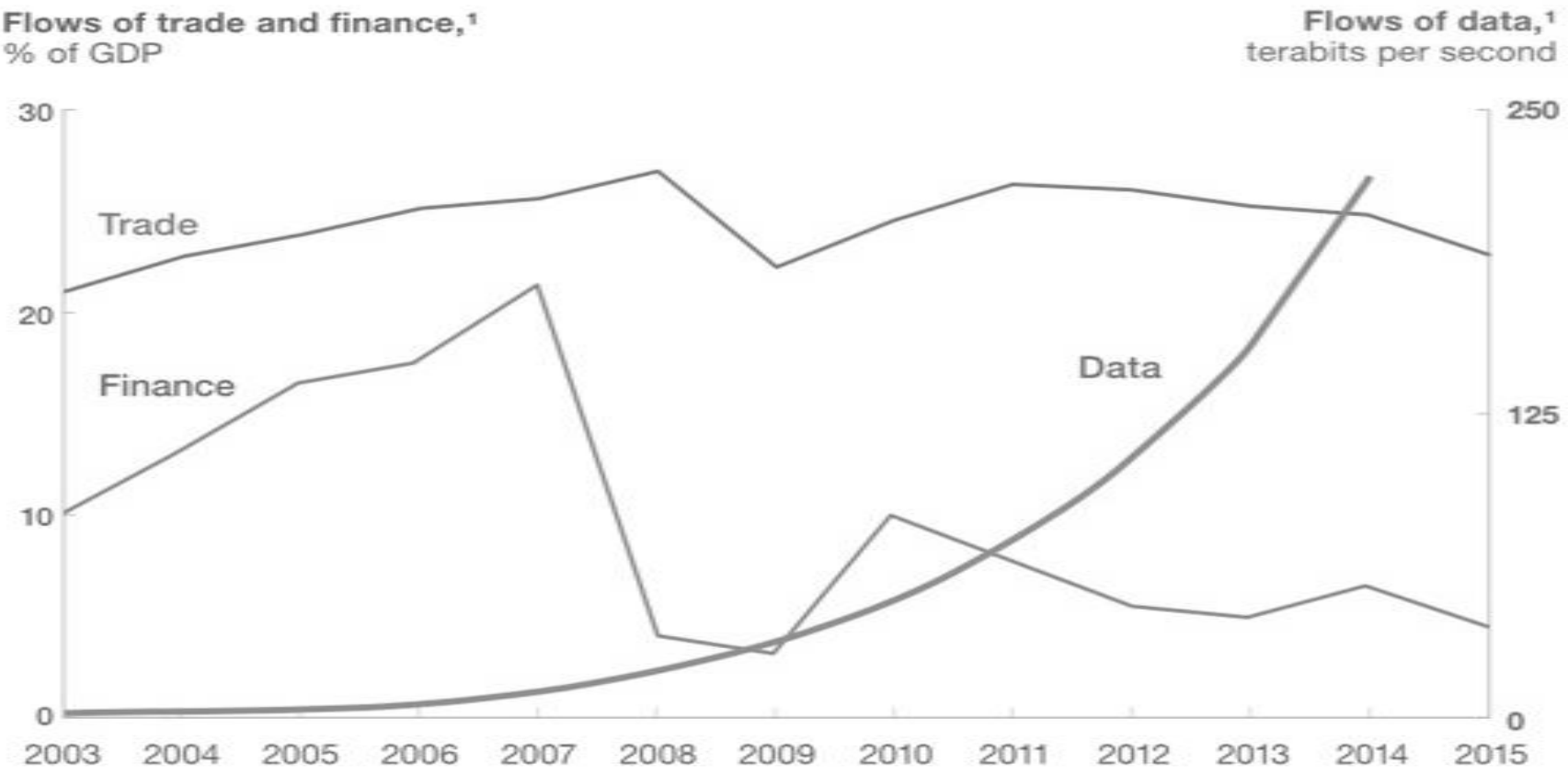
Old laws don’t fit; new framework is emerging

- 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

GDPR MASTERCLASS

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



History of data protection

GDPR MASTERCLASS

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 because 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

Privacy laws and regulations

GDPR MASTERCLASS

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

Privacy laws and regulations

GDPR MASTERCLASS

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

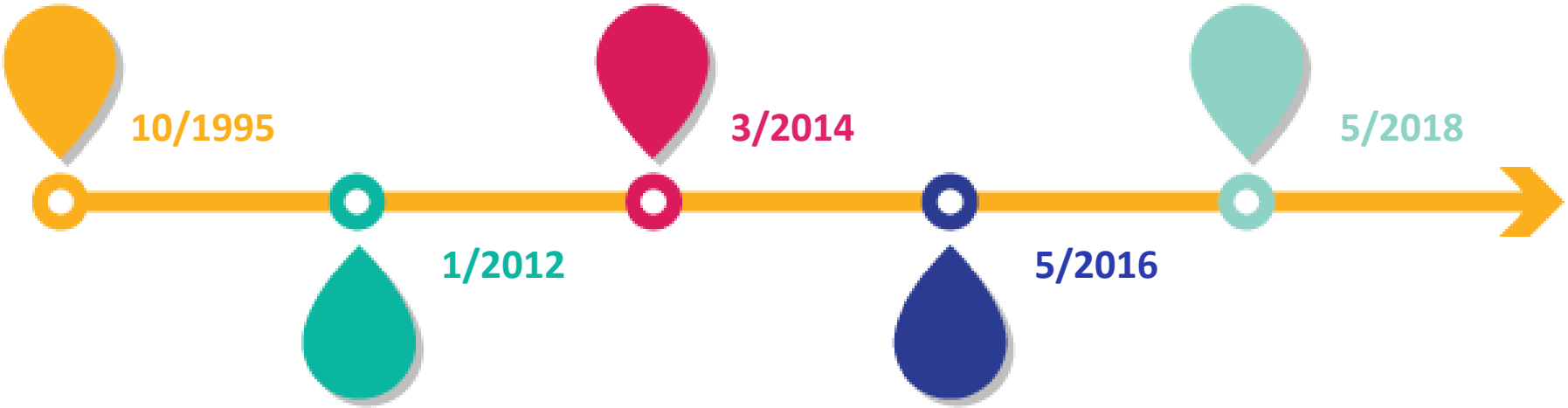
Timeline

GDPR MASTERCLASS

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?...



EC proposal reform
Strengthen online privacy rights and digital economy

GDPR enters into force
Published in the EU Official Journal

A - Plan

GDPR MASTERCLASS

- 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

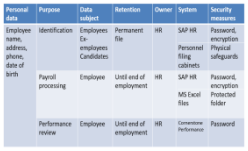
(A- Plan)

ISO 27001 Info Security

GDPR MASTERCLASS

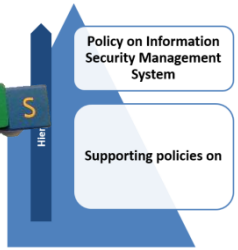
Context

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



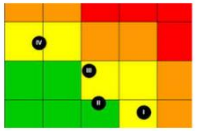
Leadership

- 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

Train your people

Operation

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

Perfor-mance

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

Audit compliance

Improve-ment

- Nonconformity and corrective actions
- Continual improvement

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

(A- Plan / Step 1)

Obtain the buy-in

GDPR MASTERCLASS

Key factor for success

Fines + Reputation

Board members
Senior managers
Chief compliance officer
Chief risk officer
Chief legal officer
HR/Sales
IT Security officers
Chief security-information officer

(A-Plan / Step 1)

Why GDPR is important?

GDPR MASTERCLASS

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

(A- Plan/Step 1)

Why GDPR is important?

GDPR MASTERCLASS

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 database/ lists**

(A – Plan/Step 1)

It is all about the reputation!

GDPR MASTERCLASS

(A- Plan/Step 2)

Get a team

GDPR MASTERCLASS

One man army?

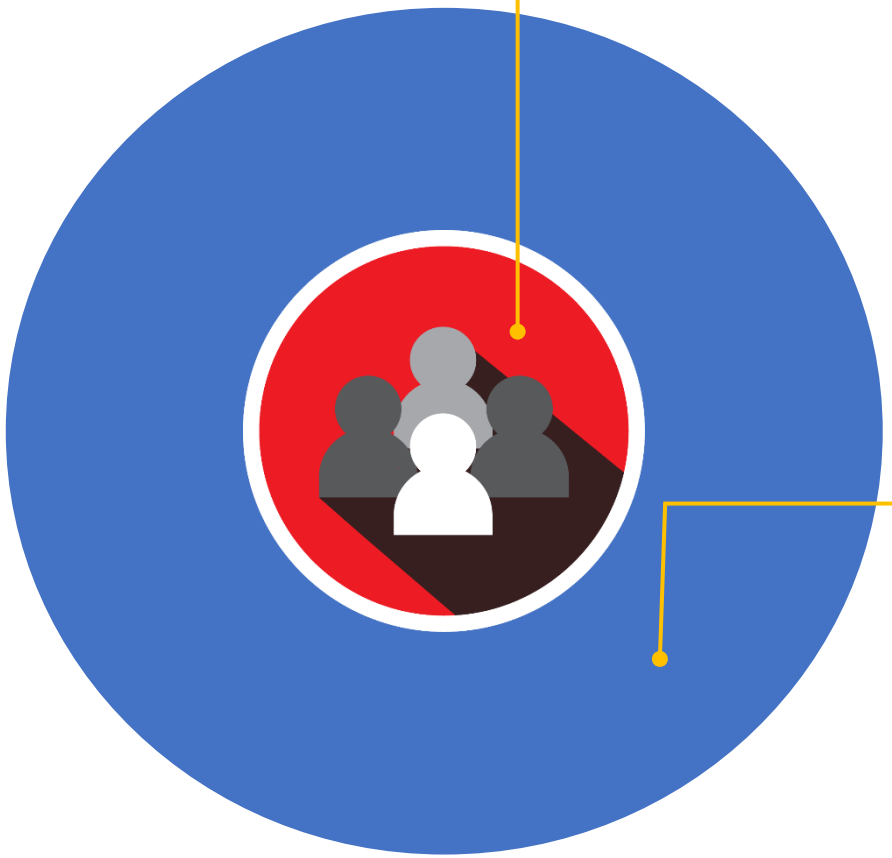
Data Protection Officer

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

(A- Plan/Step 2)

Get the team

GDPR MASTERCLASS



- **Core team**
  - Lead the implementation efforts
  - Knowledge of GDPR compliance, privacy controls, data- and cybersecurity, change management
- **Subject matter experts**
  - IT, compliance, HR, Marketing, Procurement, Accounting and Finance, Customer support

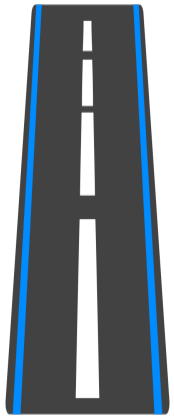
(A- Plan/Step 3)

Identify Relevant processes

GDPR MASTERCLASS

Scope

Business functions



Understand areas dealing with personal information
3rd parties processing personal information
Get priorities
Define deadlines in the roadmap

(A- Plan/Step 3)
Identify Relevant Process Scope example

GDPR MASTERCLASS

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

SAP uAttend SharePoint Peakon

In Scope

(A- Plan/Step 3)

Identify Relevant Process Scope example

GDPR MASTERCLASS

Flow In

Employee

Flow Out

Maintain HR policies

Create employee records

Create health records

Handle employee cases

Handle exits

In Scope

(A- Plan/Step 6)

3rd Party/Vendors;

GDPR MASTERCLASS

- GDPR protects data, not systems. The challenge for a breach relates to the sensitive data was, not where in the data lifecycle. For decades companies have built up massive datasets, copied and stored around the world on various platforms; manage the infrastructure beyond own borders
- The largest data exposures involved third parties (vendor, operating processes, cloud storage, contracted developer, analytics firm, all third-party data handling is a significant business risk
- **Independent Assessment**
  - Reveal how how seriously they take data security, best practices against common threats and breach trajectories, glaring misconfigurations, accessible architecture.
- **Vendor Questionnaires**

  Reveal the vendor's infrastructure, technology and processes. If the vendor utilizes cloud technology can help inform you of the risk of public bucket exposure.
- **Data Breach Audits**

  The most effective way to ensure GDPR exposures do not exist is to audit them independently and staging an attempt to break-in, look for public exposure

(A- Plan/Step 3)

Identify Relevant Process
Repair or Replace

GDPR MASTERCLASS

(A- Plan / Step 3)
What is personal information?

GDPR MASTERCLASS

Any information

… relating to an identified or identifiable …

natural person
the data subject!

How is data identifiable?

GDPR MASTERCLASS

A Hungarian person **10 M**

How is data identifiable?

GDPR MASTERCLASS

A Hungarian woman **5,4 M**

How is data identifiable?

GDPR MASTERCLASS

A Hungarian woman born in 2000

0,950 M

How is data identifiable?

GDPR MASTERCLASS

A Hungarian who lives in Tihany. **1**

(A-Plan / Step 3)

How data is identifiable?

GDPR MASTERCLASS

1 identifier

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

NEW

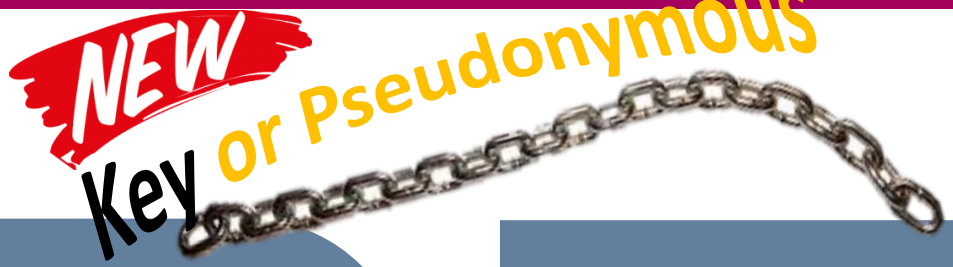
1 or + factors

Physical
Physiological
Economic
Cultural
Social
Mental

(A-Plan / Step 3)

How data is identifiable?

GDPR MASTERCLASS



1 identifier

NEW

Pseudonymous

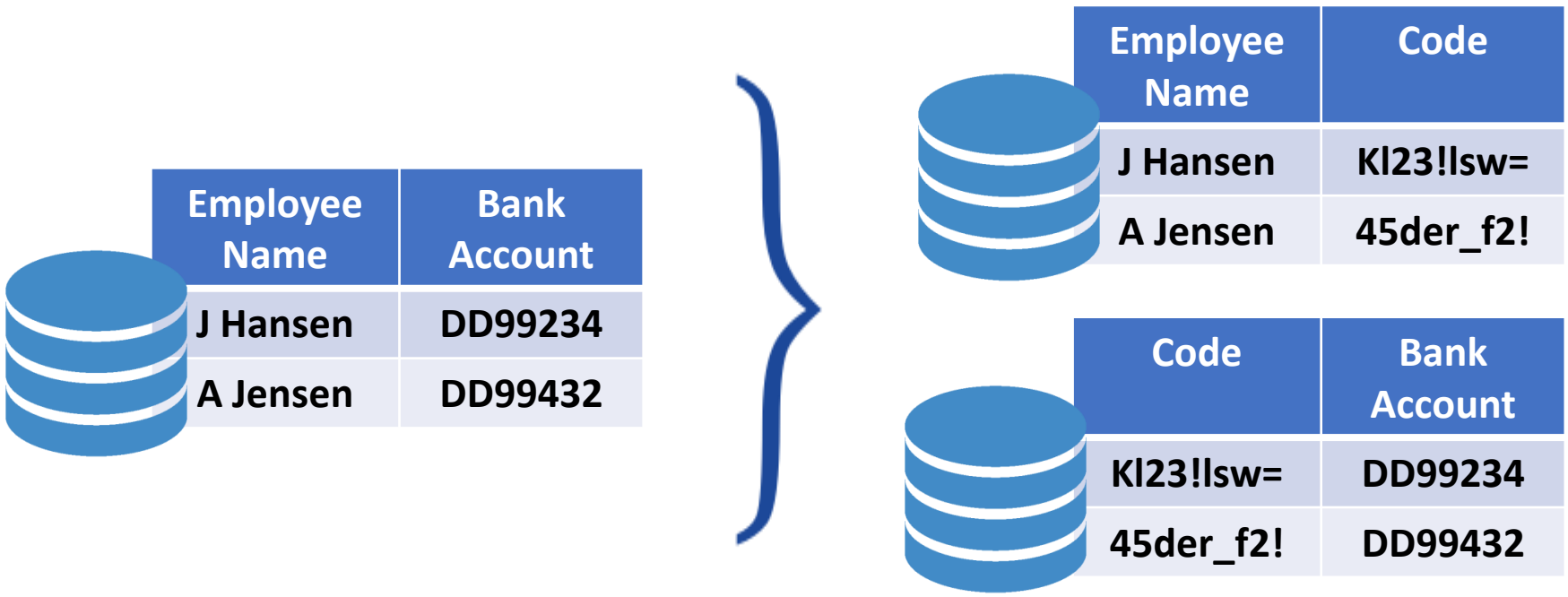
Coded data linked by a secure and separated key to re-identify a data subject

1 or + factors

(A-Plan/Step 3)

What is pseudonymisation?

GDPR MASTERCLASS



- 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

(A-Plan/Step 3)

What is encryption?

GDPR MASTERCLASS

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

(A-Plan/Step 3)

Which data is sensitive?

GDPR MASTERCLASS

Health

Biometric NEW

Genetic NEW

Trade union

Racial

Political

Religion

Sex life

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

(A- Plan/Step 4)

Compile a data inventory

GDPR MASTERCLASS

RoPA: Record of Processing Activities

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

(A- Plan/Step 4)

Compile a data inventory

GDPR MASTERCLASS

Who

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

Where

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

Why

- the personal data is under the organization control?

When

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

What

- safety mechanisms and controls are in place?

(A- Plan/Step 4)

Template & example

GDPR MASTERCLASS

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

(A- Plan/Step 4)
Template & example
Additional Fields

GDPR MASTERCLASS

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**

(A- Plan/Step 4)

Data Inventory lays the Foundation for Compliance

GDPR MASTERCLASS

If you Know your **Data** =

You Know your **Information Assets**

If you Know your **Information Assets** =

You know your **Risks**

If you Know your **Risks** =

You Know your **Controls**

If you Know your **Controls** =

You Know your **Compliance**

(A- Plan/Step 5)
Clean the House : Data Minimization

GDPR MASTERCLASS

The GDPR is an opportunity to improve data practices

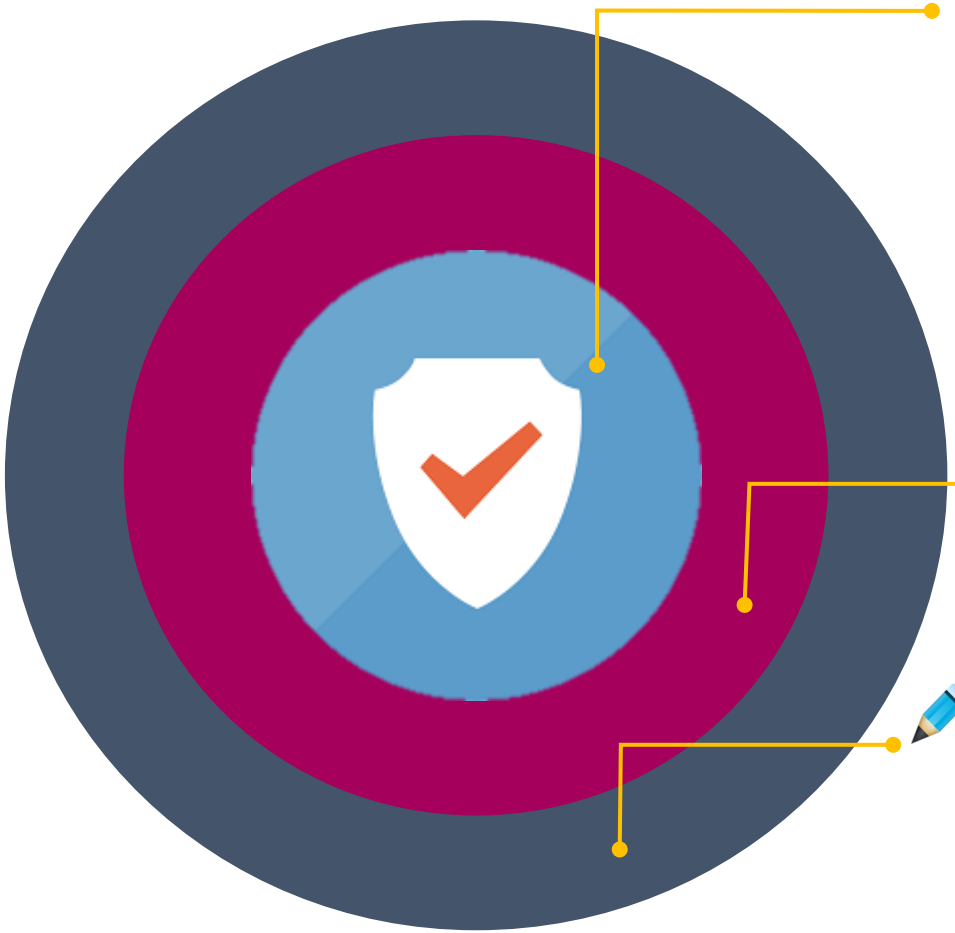
De-risk! Start clean!

- **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**

(A- Plan/Step 6)

Privacy policy

GDPR MASTERCLASS



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

(A- Plan/Step 6)

Documentation requirements

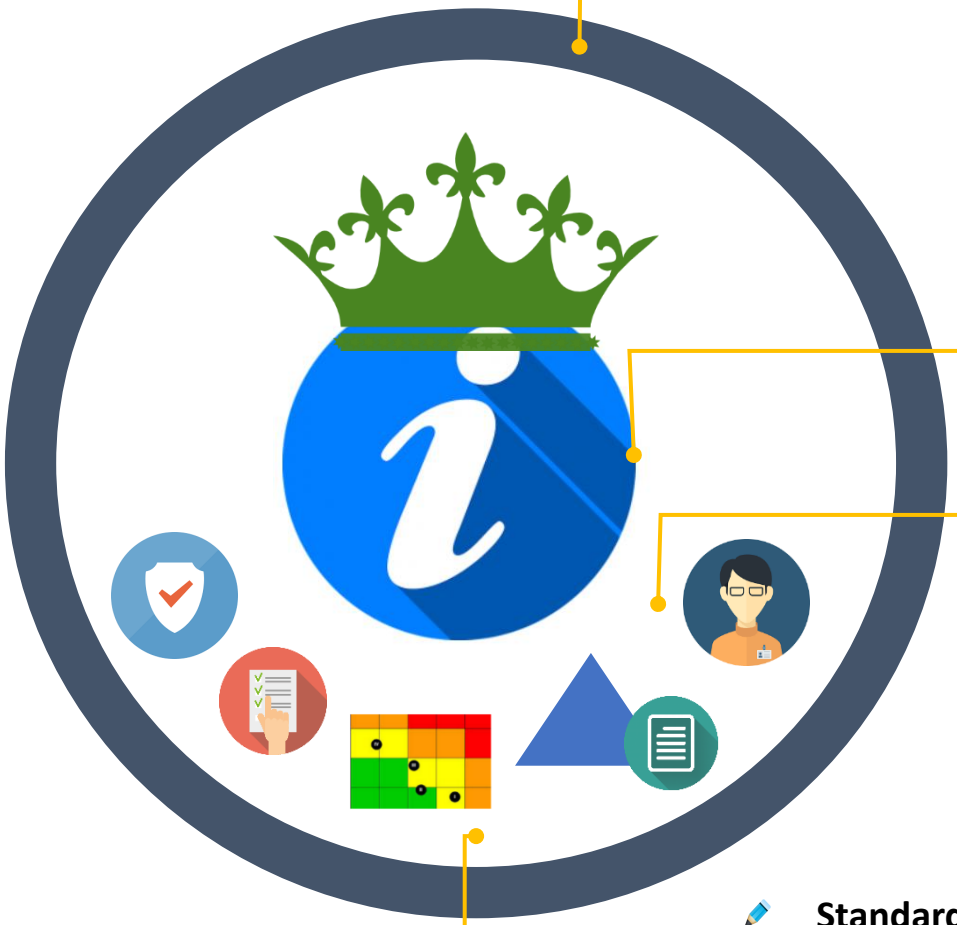
GDPR MASTERCLASS

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

(A-Plan/Step 6)

Data Protection Management System

GDPR MASTERCLASS



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

(A- Plan/Step 6)

Privacy Policy

GDPR MASTERCLASS

Accountability and Transparency

Controller	Processor	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

(A-Plan / Step 6)

Create a privacy policy

GDPR MASTERCLASS

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

(A-Plan / Step 6)

Create a privacy policy

GDPR MASTERCLASS

Tips

- **Focus on the organizational culture**
  - address what is important to the employees
    - doubts, types of data, what employees are not aware or find questionable
  - use active tense and plain language → it is not a legal document!
- **Customize the messages**
  - not a one size fits all → no copy-past from consultants
  - consider to divide the policy for groups of employees
  - the privacy policy requires to previously perform a data inventory
  - cover all the GDPR rights and key privacy risks
- **Consult others**
  - IT department for the data governance requirements
  - Compliance department for guidance about policies
  - RH for communications and training

(A-Plan/Step 6)

Create a privacy policy

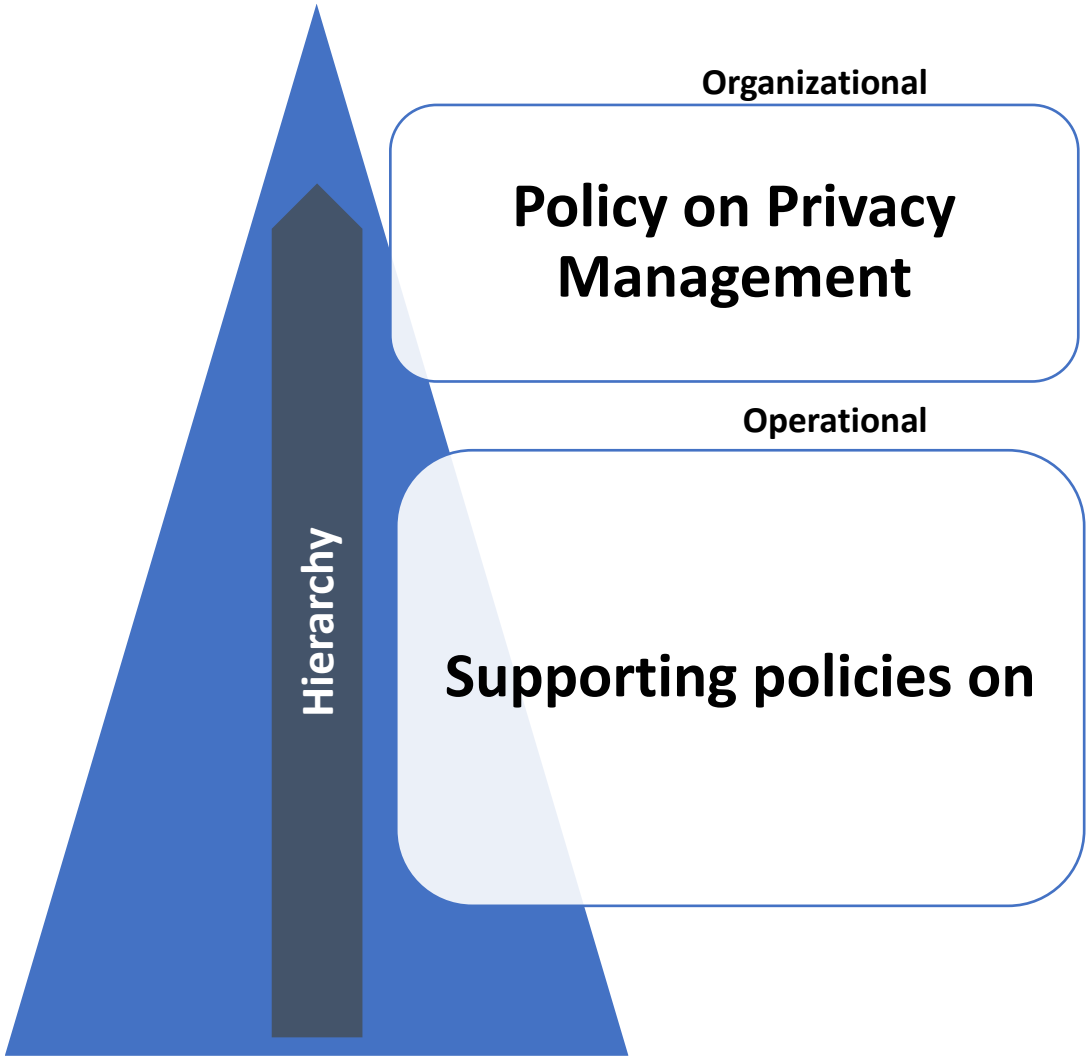
GDPR MASTERCLASS

Recommended chapters

- Organization privacy vision
- Define data categories
- Organization of applicable policies
  - Data retention, information security, recognise GDRP 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

(A-Plan/Step 6)
Create a privacy policy

GDPR MASTERCLASS



- 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

(A-Plan/Step 6)
Create a privacy policy

GDPR MASTERCLASS

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

http://www.eugdpr.institute/wp-content/uploads/2017/10/GDPR_Institute_Privacy_Policy_Model.pdf

(A-Plan/Step 6) Supporting policies

GDPR MASTERCLASS

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

GDPR MASTERCLASS

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

(B - Do / Step 1)

Limit Access

GDPR MASTERCLASS

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

(B - Do / Step 1)

Limit access

GDPR MASTERCLASS

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	

(B - Do / Step 1)

Principles

GDPR MASTERCLASS

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

(B - Do / Step 1)

Principles

GDPR MASTERCLASS

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

(B - Do / Step 1)

Principles

GDPR MASTERCLASS

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

(B - Do / Step 1)

Rights

GDPR MASTERCLASS

To access data

request access to personal data to verify lawfulness of processing

NEW

To data portability

common format, even directly transmitted between controllers

NEW

To rectify and be forgotten

when no longer necessary or consent is withdrawn

To object by controller

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

NEW

To restrict processing

limiting the data use or transfer

To limit profiling

right to not be subjected to automated individual decision making

Study case

GDPR MASTERCLASS

How to react after receiving a data subject request?

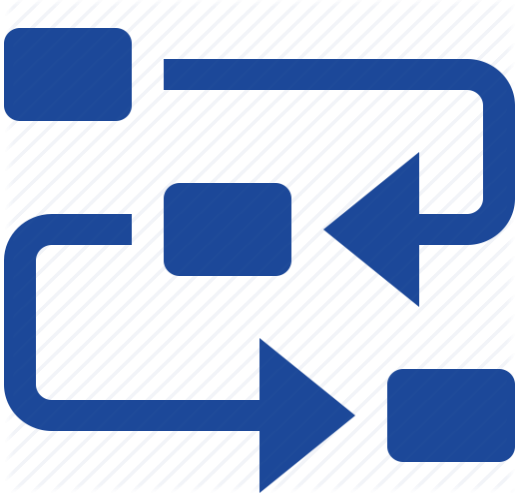
- How and when you got the consent
- What the consent covers
- How to demonstrate the processing according to the consent
- Where the data was stored and how it was accessed

(B - Do / Step 1)

Legal Basis for Processing Personal Data

GDPR MASTERCLASS

- Legitimate Interest
- Compliance with Legal Obligation
- Vital Interest of Individual



- Contract
- Consent
- Public Interest

Difficulties collecting consent = more appropriate legal basis should be used

Consent is not appropriate = may be considered unfair and misleading

(B - Do / Step 2)

Review consents
How consents should be given?

GDPR MASTERCLASS

Plain language

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

Opt-Out

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

Updated

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

Minors

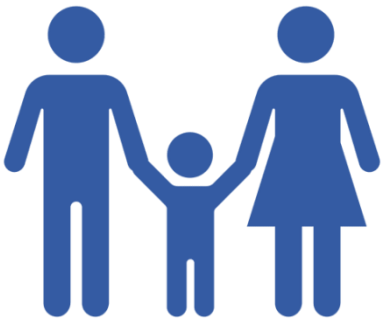
- Parental authorization for children bellow the age of 16
- Reasonable means to verify parental consent

(B - Do / Step 2)

Verify age and parental authorisation

GDPR MASTERCLASS

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

(B - Do / Step 2)

Differences

GDPR MASTERCLASS

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

(B - Do / Step 2)

Consent renewal

GDPR MASTERCLASS

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

Review activities to assess context or purpose changes

Automatically refresh consent at regular intervals

(B - Do / Step 2)

Review consents

GDPR MASTERCLASS

Study case

GDPR MASTERCLASS

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

(B-Do/Step 3)

Prepare to deal with requests

GDPR MASTERCLASS

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

(B - Do / Step 4)

Validate data transfers

GDPR MASTERCLASS

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)

Who needs a DPO?

GDPR MASTERCLASS

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, heath data by a single doctor
- **Processing operations requiring monitoring of sensitive personal data at large scale relating to criminal convictions and offences**

(B - Do / Step 4)

How personal data is processed?

GDPR MASTERCLASS

Collect | **Use** | **Destroy**

Record | ***Transmit*** | ***Restrict***

Change

Display

Electronically | **Manually**

GDPR covers personal information processed <u>wholly</u> or <u>partly</u> by automated means

(B - Do / Step 4)

… but, by who?

GDPR MASTERCLASS

Controller

Who decides why the personal data is needed

Processor

Who processes the data

Service provider, cloud services, outsourcing firms, e-commerce platforms

Natural o legal person including the government

(B - Do / Step 4)

Data controller responsibilities

GDPR MASTERCLASS

- able to 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

(B - Do / Step 4)

Data processor responsibilities

GDPR MASTERCLASS

- 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

(B - Do / Step 4)

The Primary Duties of Data Controllers

GDPR MASTERCLASS

- **The Data Controller/Processor highlights the following:**
- The Controller must ensure that: Data processing agreements or contracts with data processors contain correct Data Privacy & Protection language;
- The Controller must ensure data is not stored for longer than the period necessary for use;
- The Processor must ensure that only processing data specified under the terms of the data processing agreement with the controller are carried out;
  - Maintaining a record of all processing activities;
- The Processor/controller must look into the potential requirement to appoint a Data Protection Officer (“DPO”);
- Determine if an EU representative must be appointed

Group discussion

GDPR MASTERCLASS

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

(B - Do / Step 4)

… but, where?

GDPR MASTERCLASS

in the EU

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

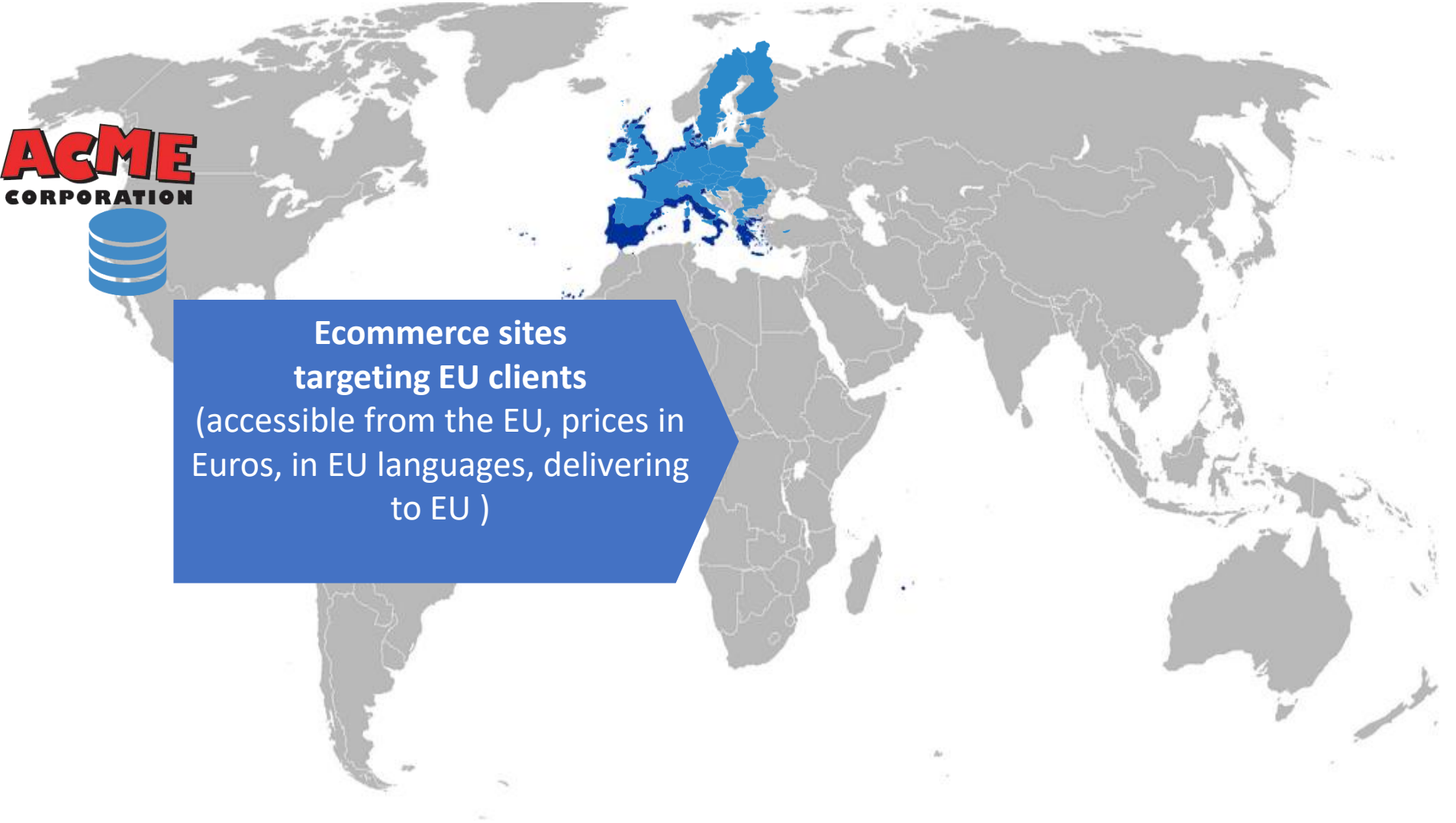
outside the EU

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)

(B - Do / Step 4)

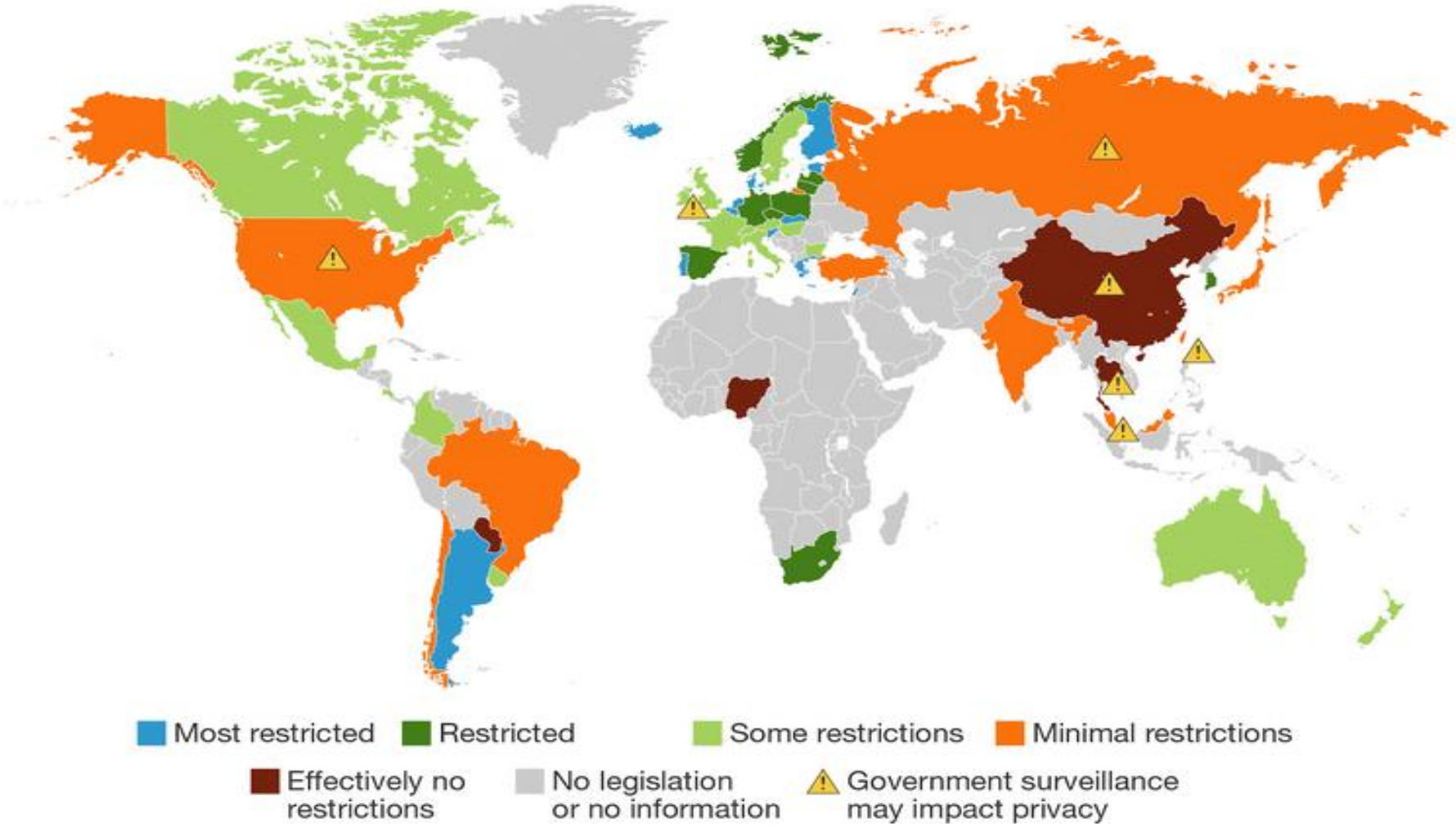
Extra-territorial application

GDPR MASTERCLASS



Views on privacy

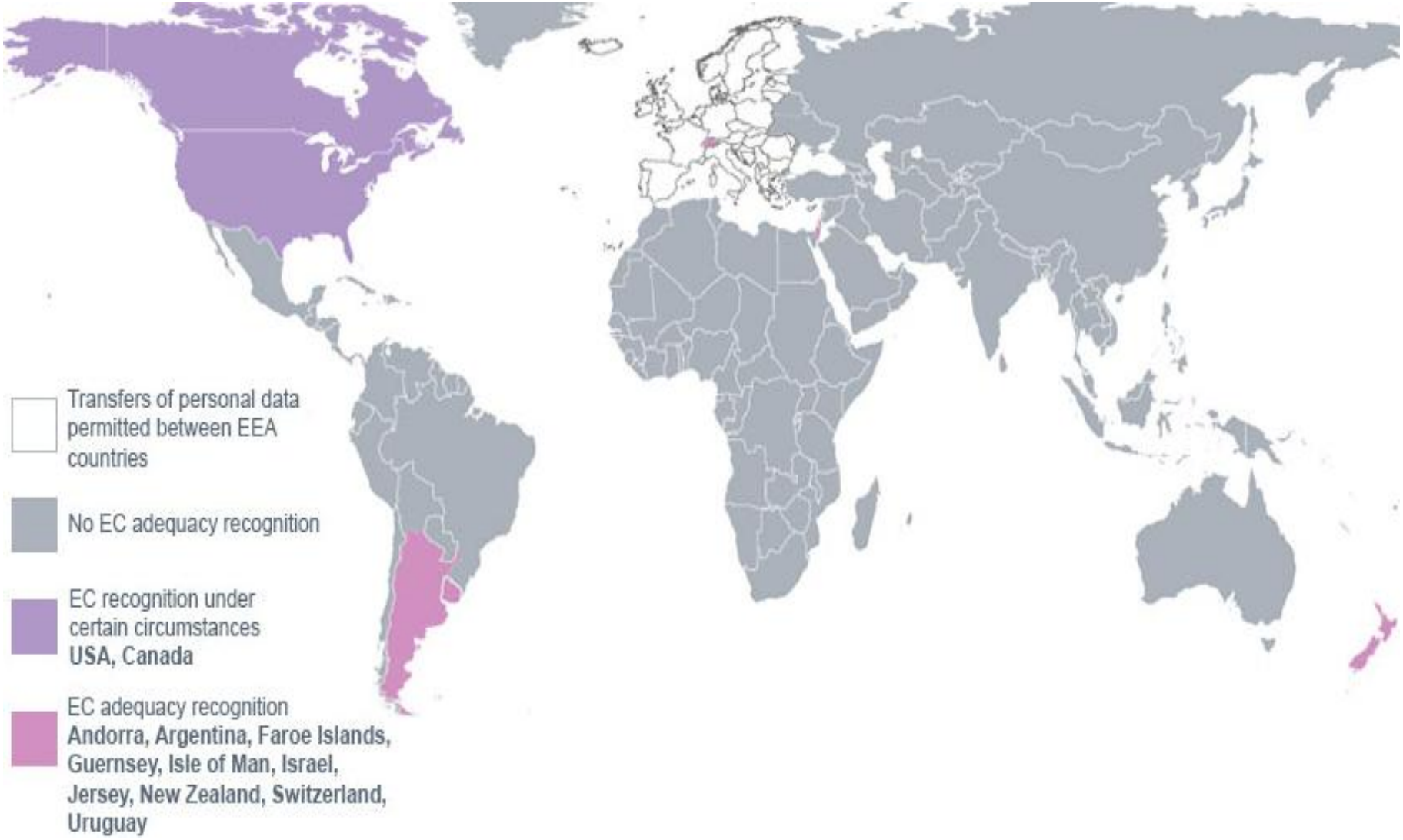
GDPR MASTERCLASS



(B - Do / Step 4)

International transfers

GDPR MASTERCLASS



(B - Do / Step 4)

Adequate safeguards

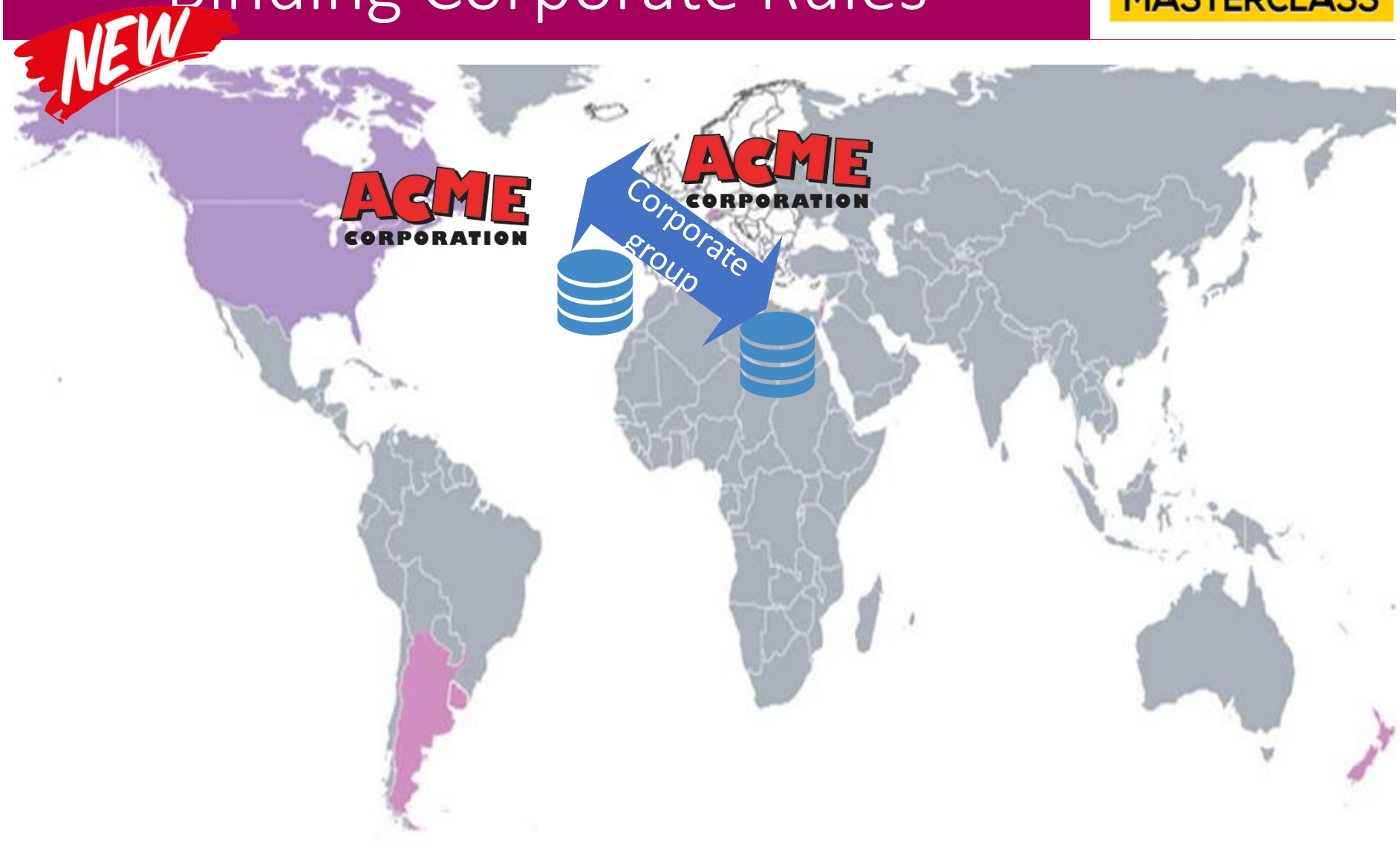
GDPR MASTERCLASS

- 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

(B - Do / Step 4)

Binding Corporate Rules

GDPR MASTERCLASS



(B - Do / Step 4)

Binding corporate rules

GDPR MASTERCLASS

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

(B - Do / Step 4)

Standard data processor clause

GDPR MASTERCLASS

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.

(B - Do / Step 4)

Privacy shield

GDPR MASTERCLASS

- 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

GDPR MASTERCLASS

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

(B - Do / Step 5)

Review contracts

GDPR MASTERCLASS

Controller

Processor

Data exporter when processing is outside de EU

Review <u>data processing agreements:</u> 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

(B - Do / Step 5)

Tips for clauses

GDPR MASTERCLASS

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

- comply with the GDPR 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

(B - Do / Step 6)

How to notify a data breach?

GDPR MASTERCLASS

Data breach

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

When to notify

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

What to notify

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

Whom to notify

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

(B - Do / Step 6)

Data security program

GDPR MASTERCLASS

Encryption of personal data

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

Security measures

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

Resilience

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

Regular security testing

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

C - Improve

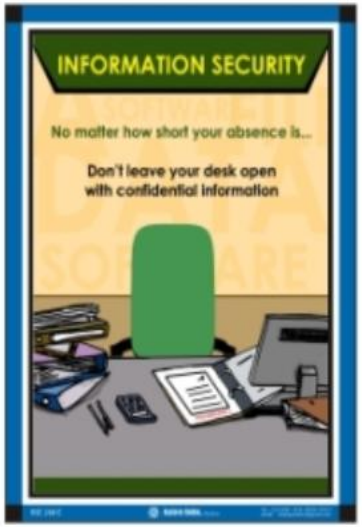
GDPR MASTERCLASS

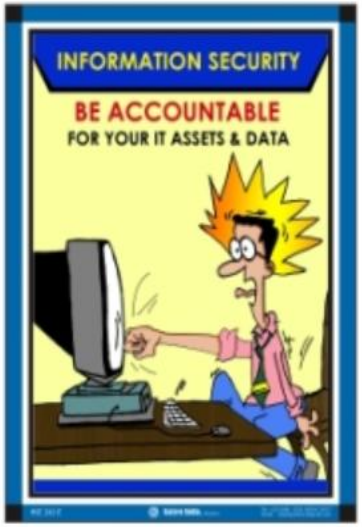
- 1- Train the staff
- 2- DPIAs for business changes
- 3- Audits
- 4- Certifications

(C-Improve/Step 1)

Train your people

GDPR MASTERCLASS





(C-Improve/Step 1)

Train your people

GDPR MASTERCLASS

- 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

(C-Improve/Step 1)

Discussion case

GDPR MASTERCLASS

- **How could you develop training for this risk?**
- **How could you document your training efforts?**

NEW

(C-Improve/Step 1)

Data Protection Impact Assessment (DPIA)

GDPR MASTERCLASS

- 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

(C-Improve/Step 2)

DPIA – Identify the need

GDPR MASTERCLASS

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!

(C-Improve/Step 2)

DPIA – Identify the data flows

GDPR MASTERCLASS

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

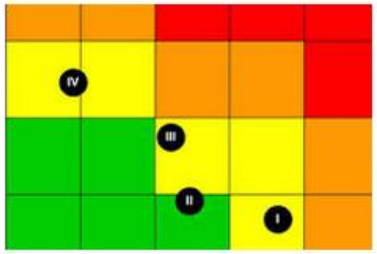
(C-Improve/Step 2)

DPIA- Consult on risks and controls

GDPR MASTERCLASS

Consult all involved parties to have a 360º 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!

(C-Improve/Step 2)

DPIA - Generic risks and controls

GDPR MASTERCLASS

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

(C-Improve/Step 2)

DPIA-Example of risk registry

GDPR MASTERCLASS

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

(C-Improve/Step 2)

What is Privacy

GDPR MASTERCLASS

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

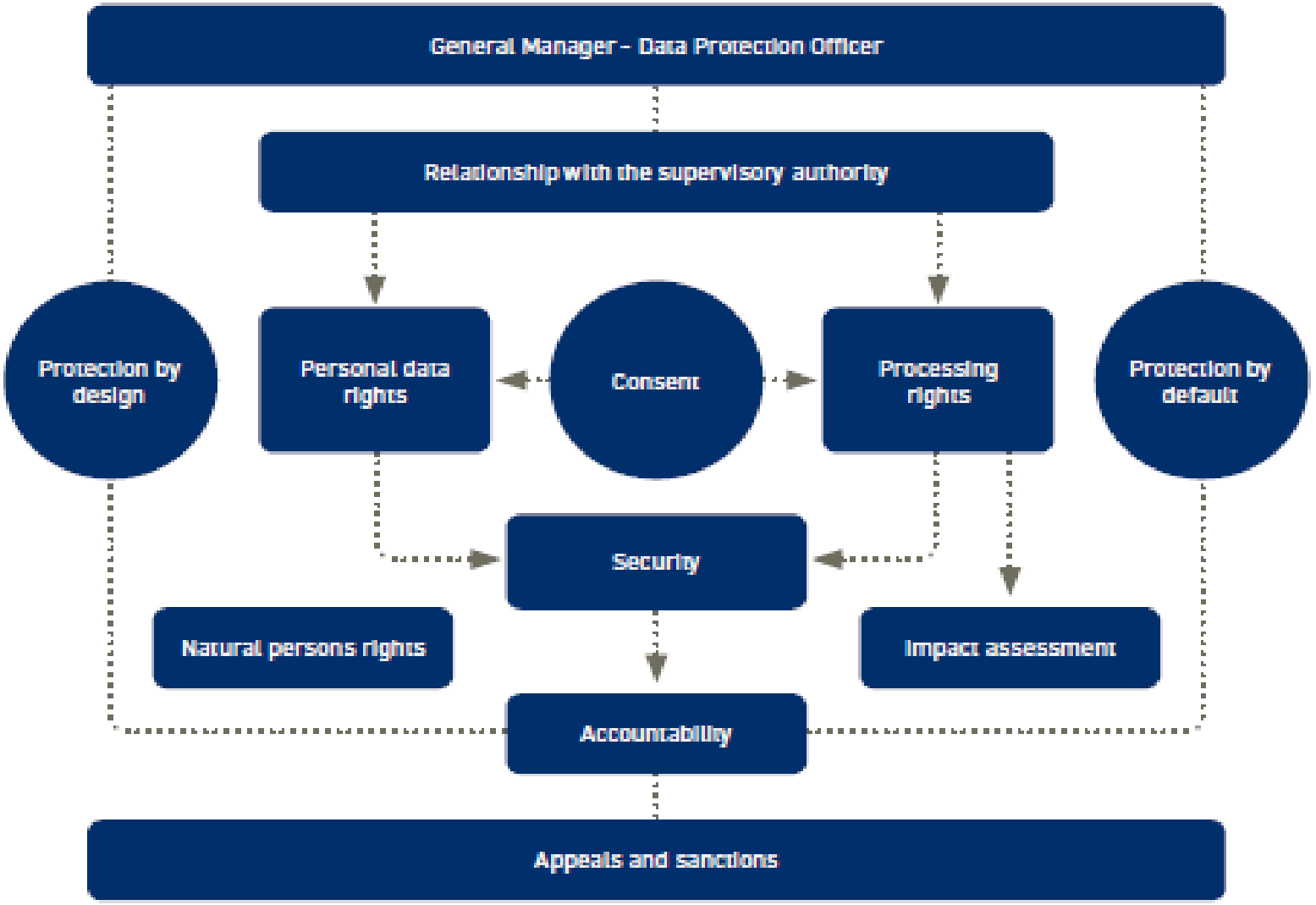
By design

- 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

(C-Improve/Step 2)

Approach to Design and Default

GDPR MASTERCLASS

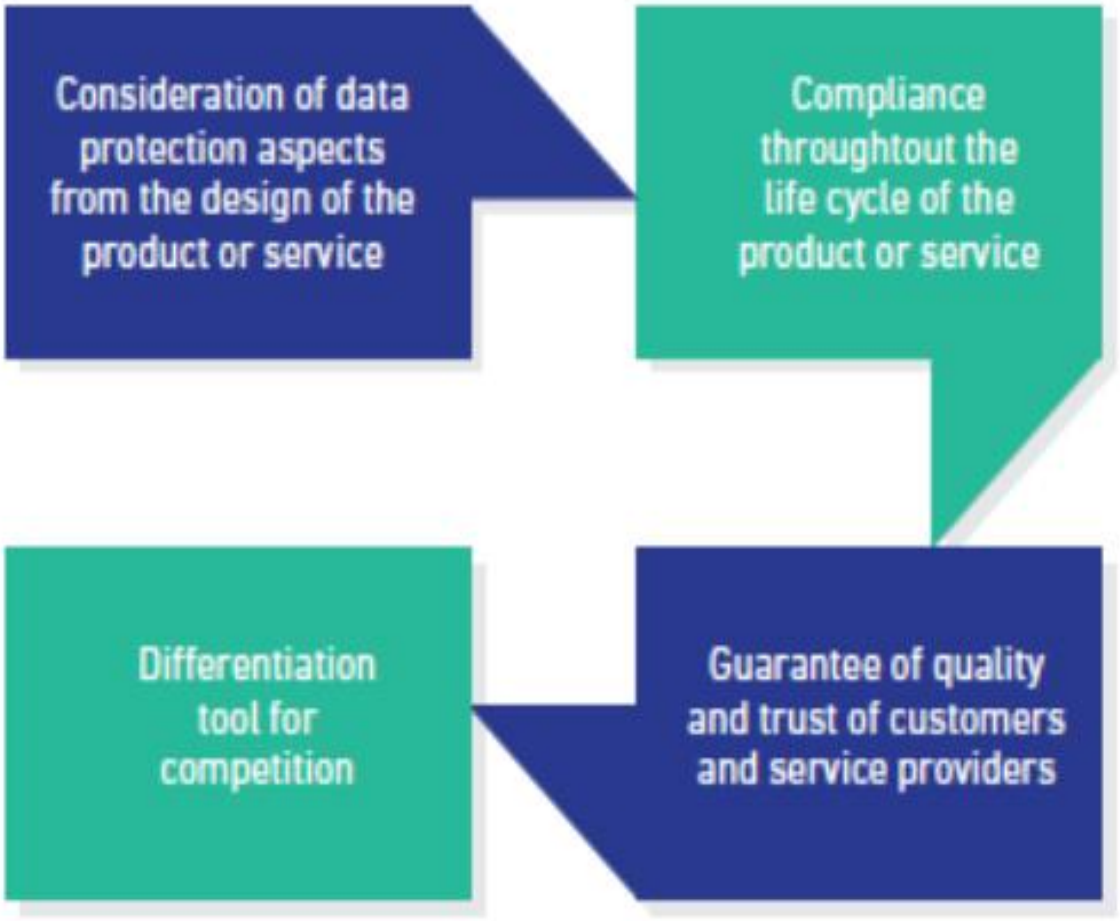


(C-Improve/Step 2)

Data Protection by Design

GDPR MASTERCLASS

The principle of Data Protection by Design requires the organisation to respect DPBD of products, services and systems that use personal data.

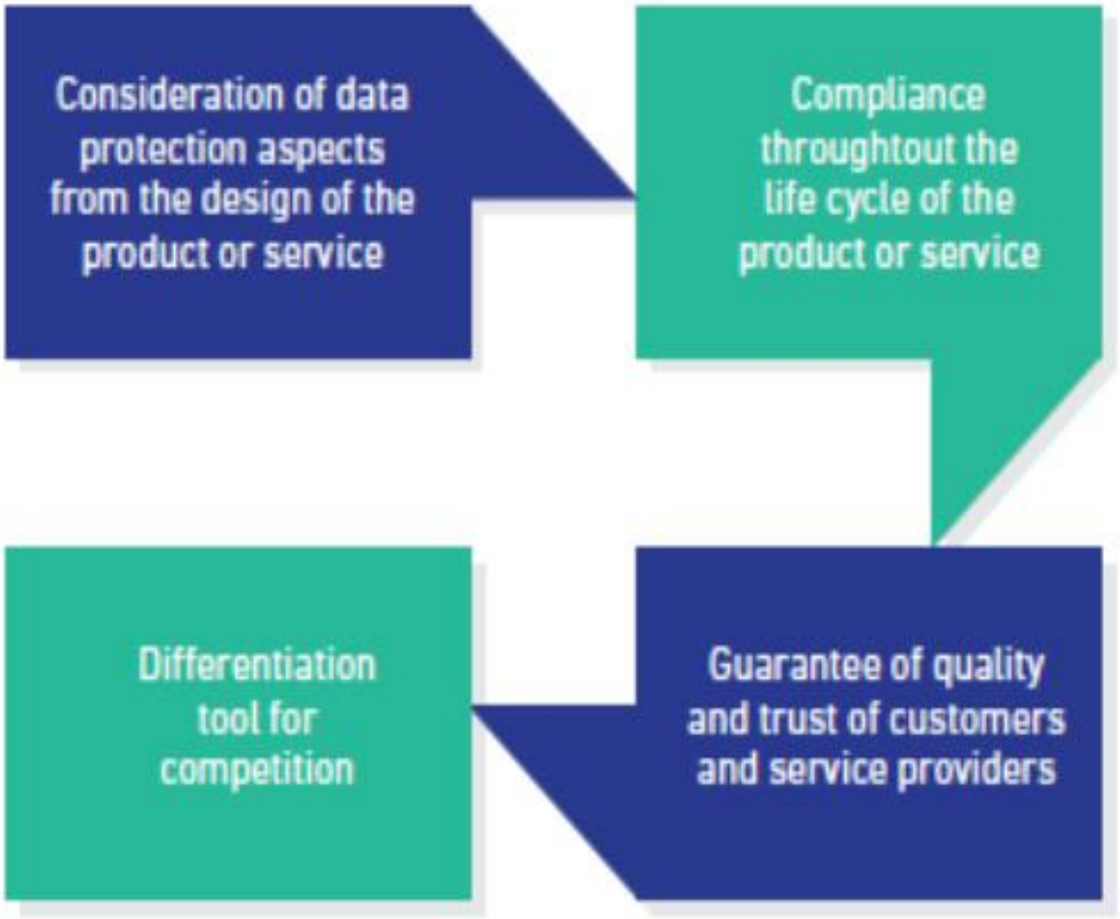


(C-Improve/Step 2)

Data Protection by Default

GDPR MASTERCLASS

The principle of Data Protection by Default requires the organisation to have an information system that guarantees a high level of DP at all stages; registration, operation, administration, integrity and update. The security of the IS must be ensured by its physical or logical elements and monitored according to specifications, vulnerability and updates.



(C-Improve/Step 2)

Group discussion

GDPR MASTERCLASS

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

Clean the house!

GDPR MASTERCLASS

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**

(C-Improve/Step 3)

Audit Compliance

GDPR MASTERCLASS

- 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

(C-Improve/Step 3)

Audit Compliance

GDPR MASTERCLASS

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

(C-Improve/Step 4)

Certification & Code of conduct

GDPR MASTERCLASS

- 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 for earning certification status
- These costs can be offset by reducing audit costs and automation

(C-Improve/Step 4)

Certification & Code of conduct

GDPR MASTERCLASS

- 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

GDPR MASTERCLASS

- 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

GDPR MASTERCLASS

Roadmap

GDPR MASTERCLASS

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 DPIA (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

GDPR MASTERCLASS

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

- Direct obligation
- Meta rule

https://gdpr-info.eu

All Presentation and Exam Links

GDPR MASTERCLASS

- 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/2019/11/day1.pdf
- DPO: https://www.eugdpr.institute/wp-content/uploads/2019/11/day2.pdf
- CEP: https://www.eugdpr.institute/wp-content/uploads/2019/11/day3.pdf

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

GDPR MASTERCLASS

COPENHAGEN COMPLIANCE
Global GRC Solutions

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 in Beijing. Kersi has conducted several hundred workshops, seminars and international speaking assignments on Regulatory Compliance, GDPR, GRC, CSR, and BFC issues.

Copenhagen Compliance UK Ltd®
Info@copenhagencompliance.com
www.eugdpr.institute
21, Cloudseley Street, London N1 OHX, UK.
Kersi Porbunderwalla tel: +45 2121 0616

©Copenhagen Compliance®

GDPR MASTERCLASS

Connecting IT Security to Governance, Risk and Compliance

www.copenhagencompliance.com

HR Riskability

Human Capital Assessment Framework

EU GDPR INSTITUTE

information security institute

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.

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 Copenhagen Compliance Group is neither a Law Firm nor are we licensed to provide legal advice.

Disclaimer/Copyright

GDPR MASTERCLASS

- The examples and scenarios in this presentation are for illustration purposes only, and not based on specific examples to be construed as particular advice on any practical legal issues.
- As always, contact your legal counsel for clarification and recommendations on legal issues. Copenhagen Compliance or The EUGDPR Institute is not licensed to provide legal advice.
-