How to ensure GDPR compliance

EU GDPR INSTITUTE

by

COPENHAGEN COMPLIANCE

GDPR
Executive Workshop

Overview/Agenda

- GDPR background and terminology.
- The differences between Data subjects, Data Controllers, Data Processors, and their rights.
- International data transfers

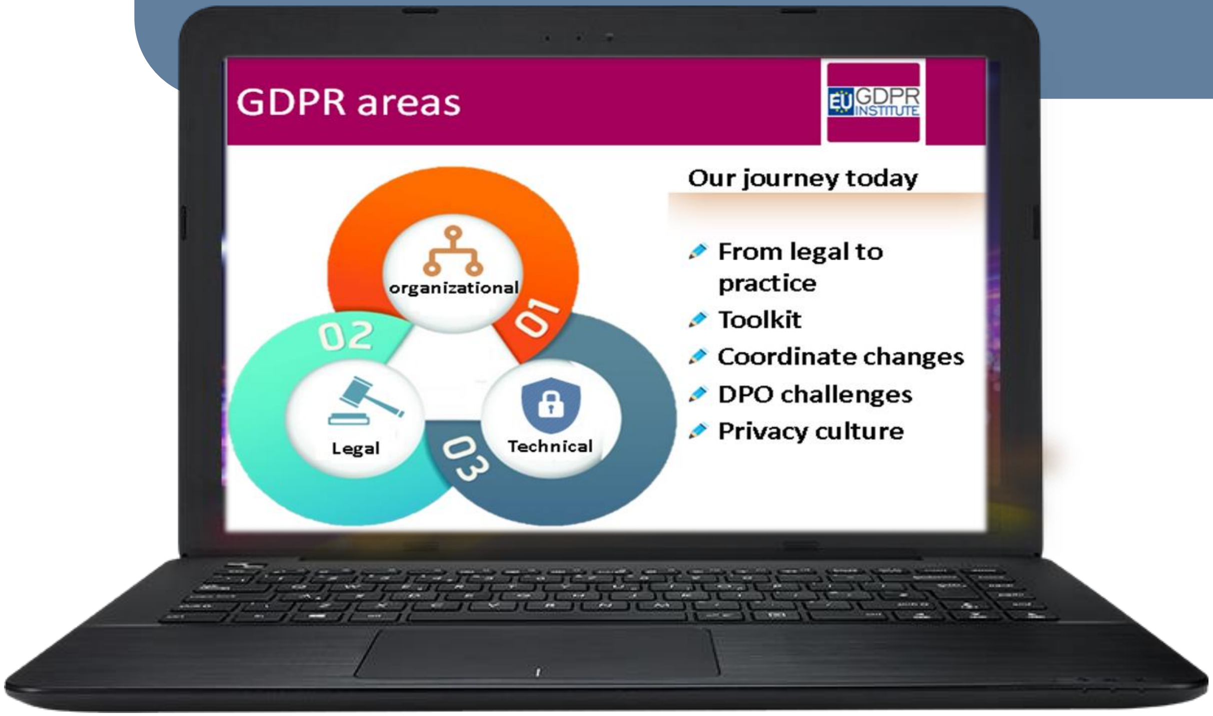
- Policies and disclosures – transparency and consent
- How to perform a data protection impact assessment (DPIAs)
- Key Privacy by Design principles (PbD)

- DPO, Controller, Processor rules, responsibilities and functions
- Binding corporate rules
- ISO 27001

- Incident response and breach reporting
- How to process subject access request
- Business Impacts: Security, Cloud, out-sourcing / Data Processors, IoT, Big Data

Access to the presentation

https://www.eugdpr.institute/fas/



GDPR areas

Our journey today

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

We will focus on issues

… not organizations

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

Does the GDPR applies to me?

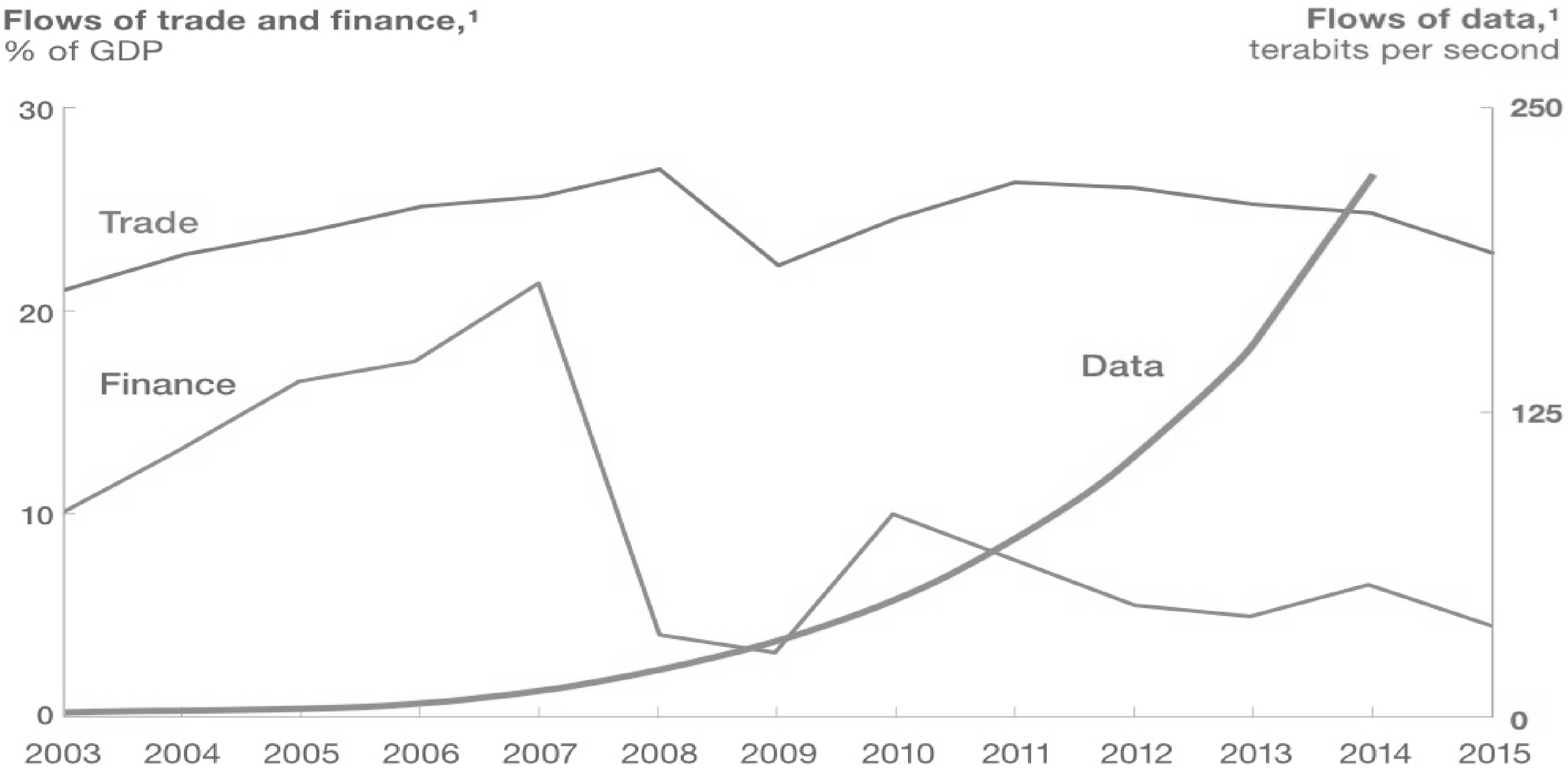
□ Does my organization offer goods or services to EU residents?

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

□ Does my organization have employees in the EU?

What an opportunity

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



How does GDPR impact?

The different ways organisation come under GDPR?
Various ways like offerings goods, services, storing, hosting, accessing, monitoring EU customers, residents and citizens.

Are organizations are not handling the personal data?

1. EU organisation or customers and citizens do not want to take or share the risk of accidental data breach.
2. Often companies outside the EU companies are not sure or unaware of handling of personal data for their business purposes

Companies can transfer penalty risks to insurance?

1. Companies have ensured the due diligence and due care.
2. EU organization will ask how personal data is protected
3. Reputational loss and a risk of losing a future customer

Effects on Mauritius

- With the expanded territorial reach of the GDPR, the new data protection regime help to provide incentives and growth in the Mauritian ICT/business process outsourcing sector,
- Facilitate the transfer of personal data from EU-based companies to Mauritian companies.
- Attract more business opportunities from EU-based companies in emerging areas such as analytics, Big Data and FinTech.
- Companies must provide a level of data protection equivalent to that ensured within the EU
- *How can Mauritius, in principle, be recognised by the European Commission as a third country that provides an adequate level of protection for the purposes of the GDPR.*

The principles of GDPR

The data processor must comply and make sure that personal information is

- **fairly and lawfully processed;**
- **processed for limited purposes;**
- **adequate, relevant and not excessive;**
- **accurate and up to date;**
- **not kept for longer than is necessary;**
- **processed in line with your rights;**
- **it is secure; and**
- **not transferred to other countries without adequate protection.**

Why GDPR is important?

EU GDPR INSTITUTE

Fines!

Fines of MUR 200,000 and prison sentences of up to five years.

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

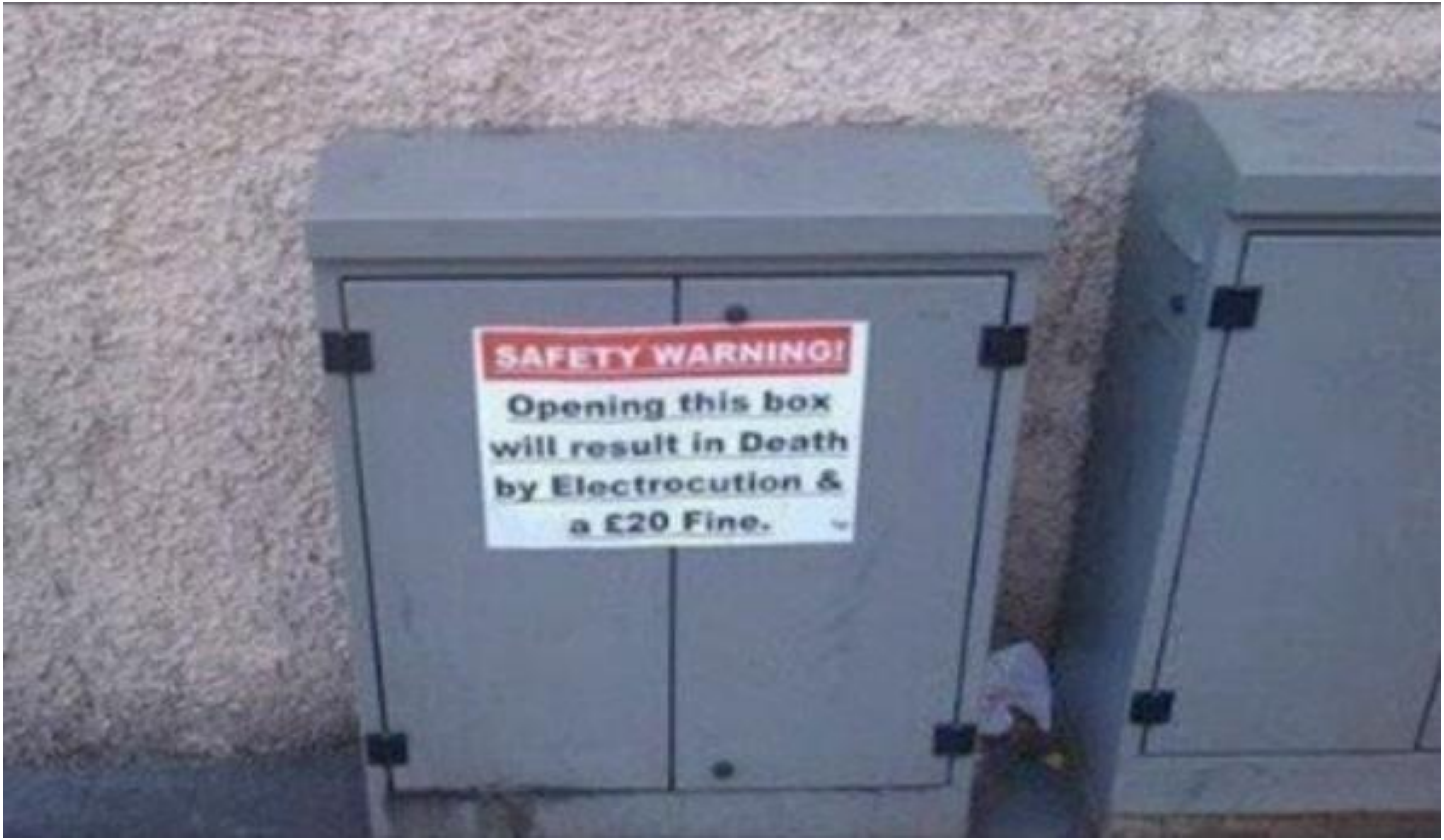
Reduced with appropriate technical and organizational measures

Why GDPR is important?

Privacy is a competitive advantage

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

It is all about the reputation!

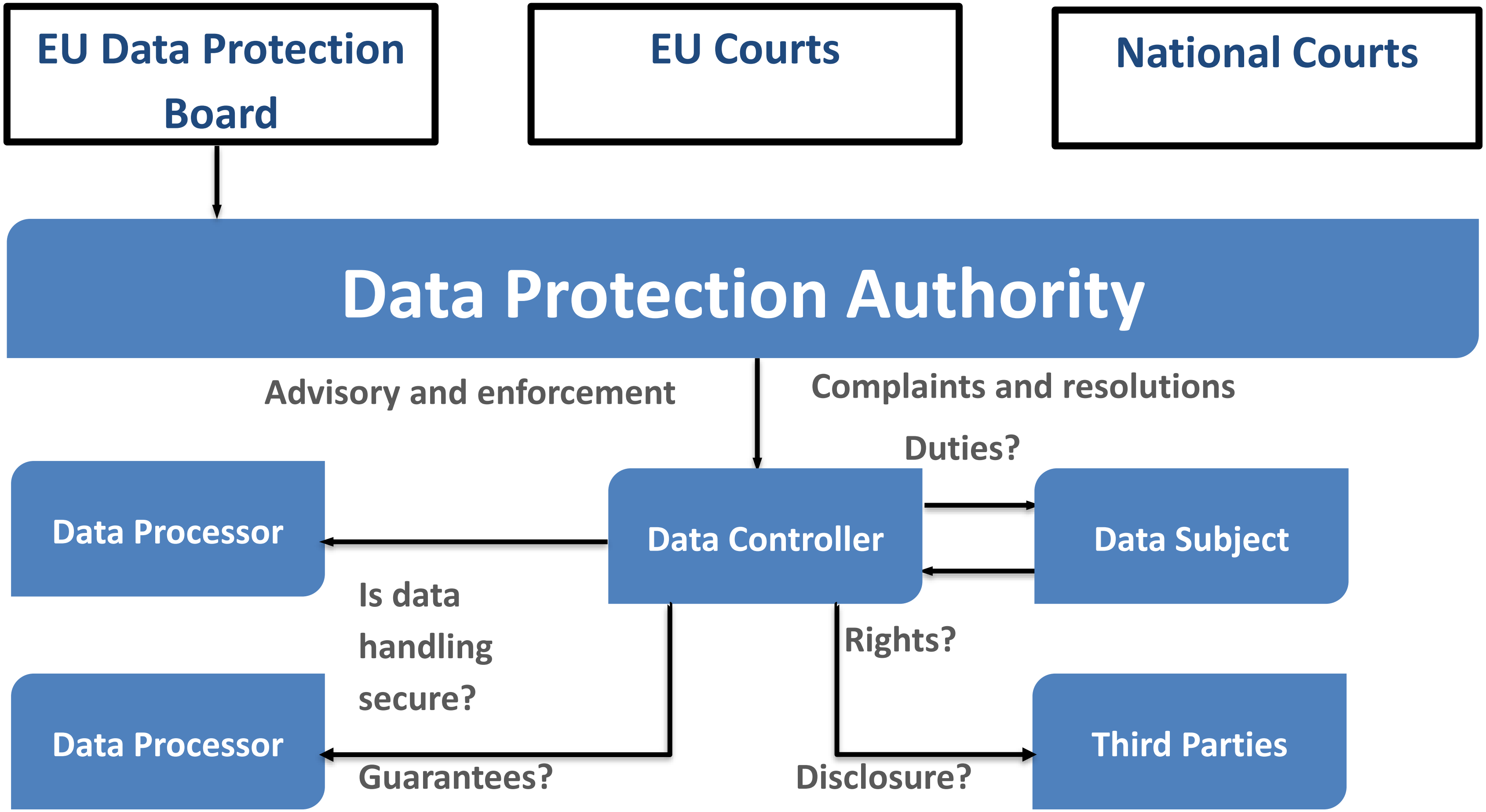

SAFETY WARNING!
Opening this box will result in Death by Electrocution & a £20 Fine.

Info Security and boards

2017 Security and Privacy Survey by Protiviti

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

Organisation



EU Data Protection Board

EU Courts

National Courts

Data Protection Authority

Advisory and enforcement

Complaints and resolutions

Duties?

Data Processor

Data Controller

Data Subject

Is data handling secure?

Rights?

Data Processor

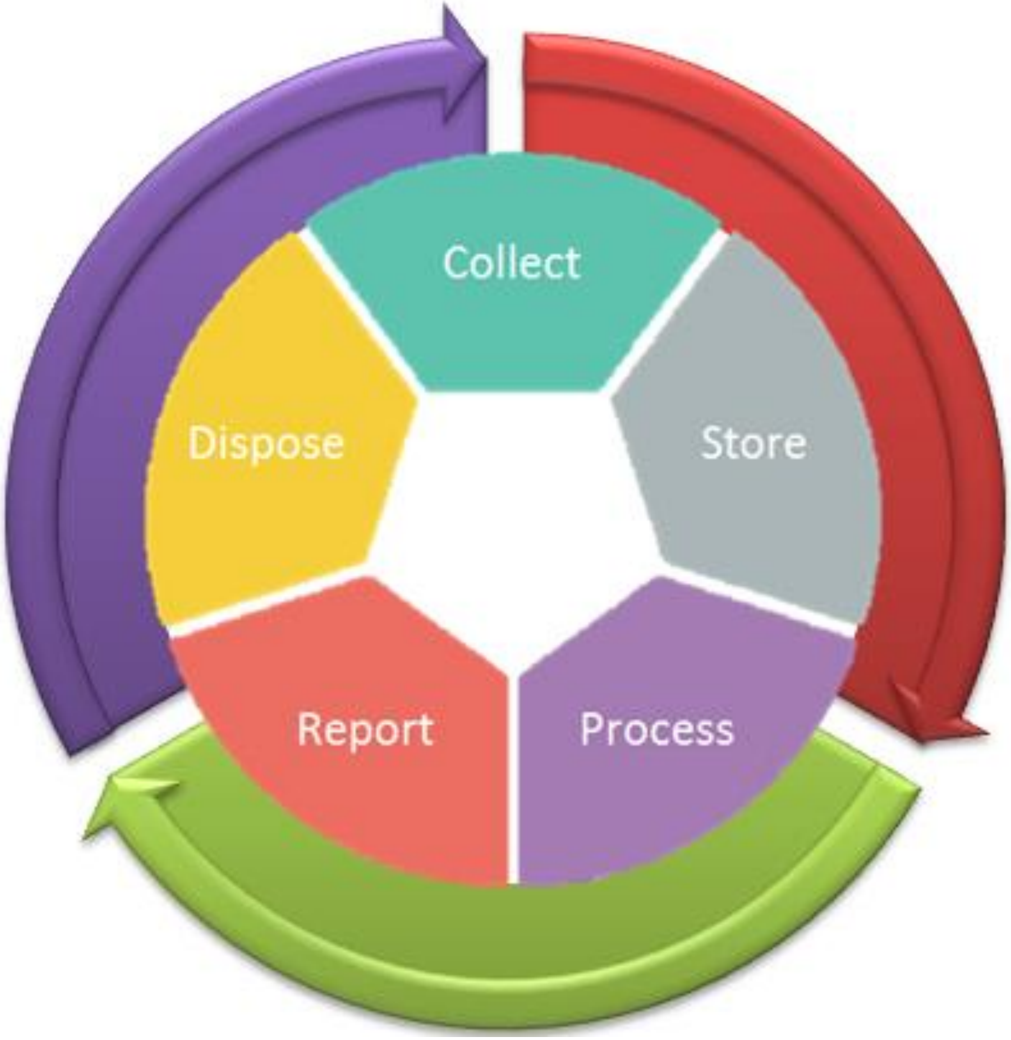
Third Parties

Guarantees?

Disclosure?

GDPR Overview

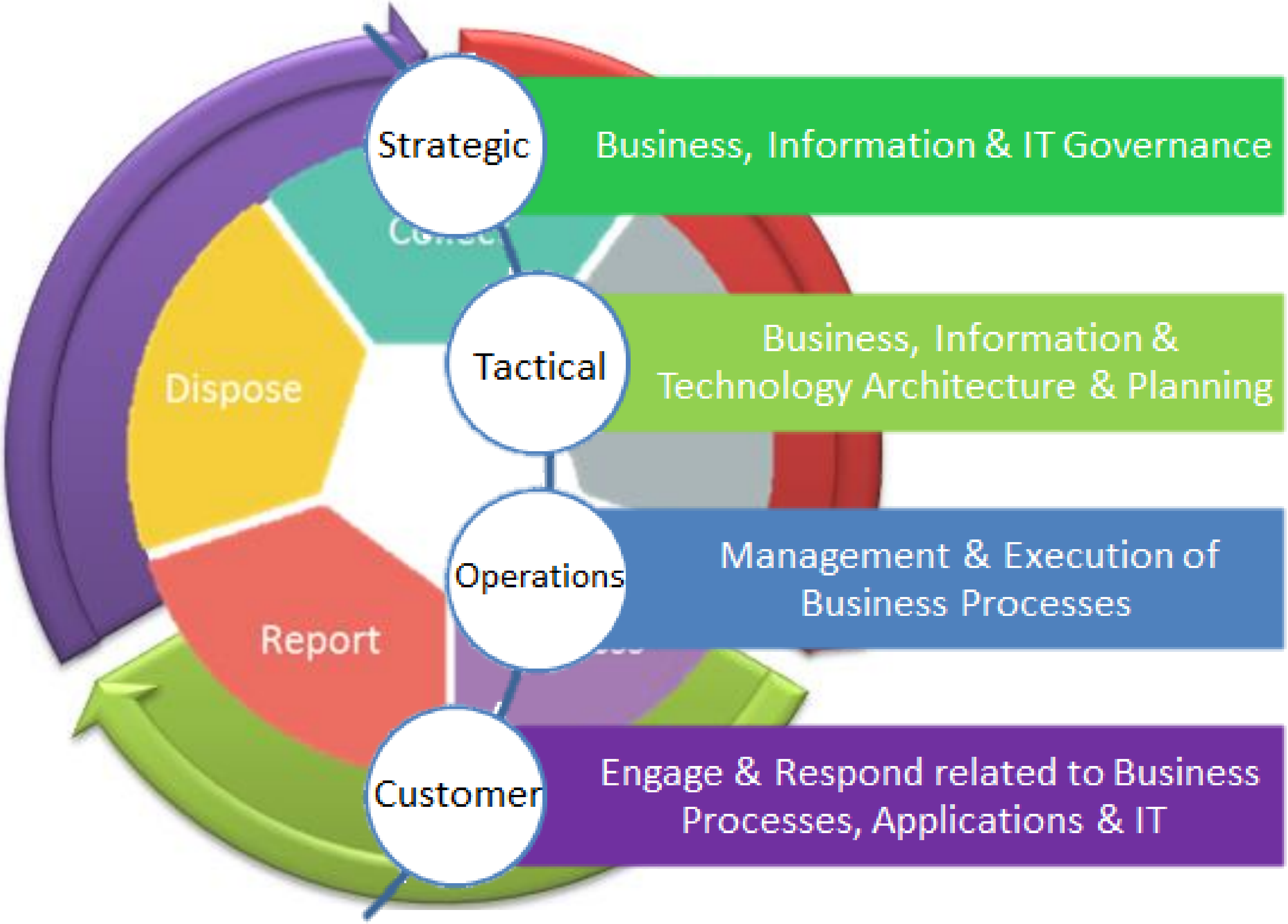
GDPR assessment and consulting



Privacy Re-Engineering?

Privacy Impact Assessment

GDPR Overview



Strategic – Business, Information & IT Governance

Tactical – Business, Information & Technology Architecture & Planning

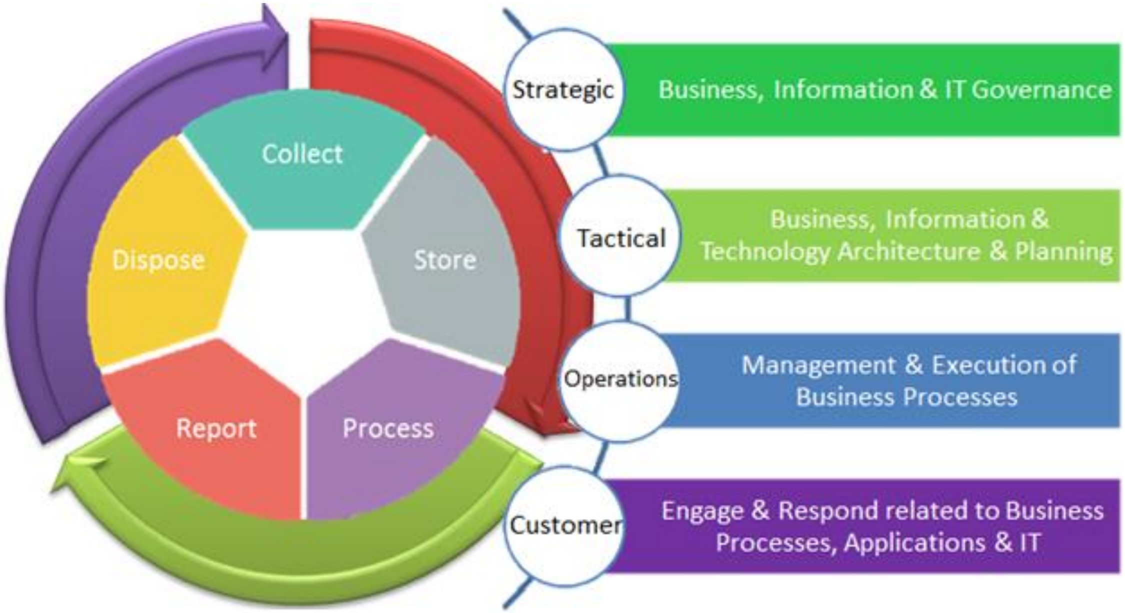
Operations – Management & Execution of Business Processes

Customer – Engage & Respond related to Business Processes, Applications & IT

GDPR Overview

EU GDPR INSTITUTE

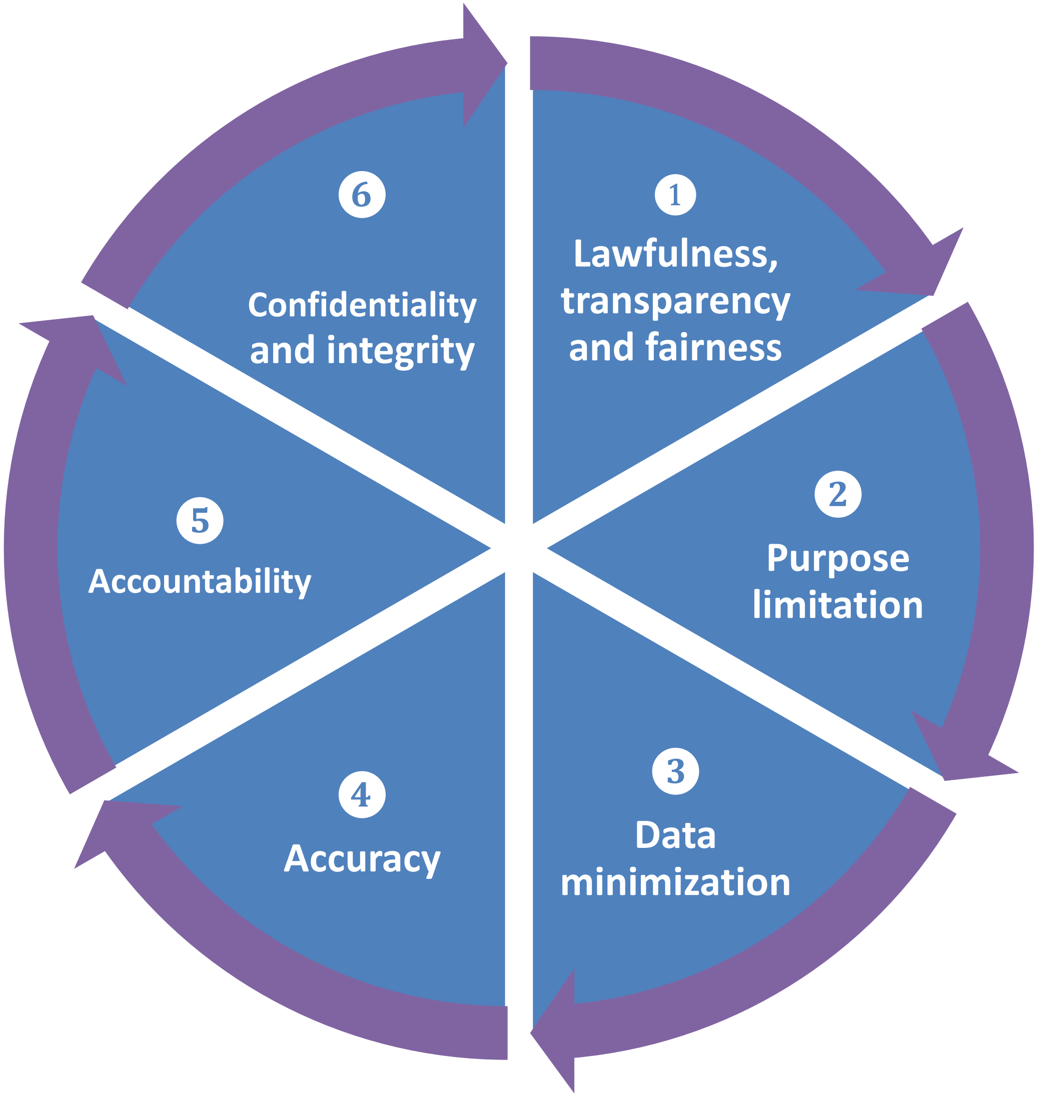
Strategize the approach → Team and budget → Build ops and technical controls → Implement controls → Monitor controls


Collect
Store
Process
Report
Dispose
Strategic
Business, Information & IT Governance
Tactical
Business, Information & Technology Architecture & Planning
Operations
Management & Execution of Business Processes
Customer
Engage & Respond related to Business Processes, Applications & IT

GDPR Compliance

Core Principles → One Stop Shop → Data Subject Rights → Explicit Consent → Risk Based Approach → DPO Enforcement

The GDPR guiding principles


1
Lawfulness, transparency and fairness
2
Purpose limitation
3
Data minimization
4
Accuracy
5
Accountability
6
Confidentiality and integrity

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

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
HR
Logistics
Sales and Marketing
CTO

Step 1: Tips for GDPR Compliance

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

Step 2: Get a team

The image part with relationship ID rId3 was not found in the file.

One man army?

Core Team/Subject Matter Experts

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 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

The image part with relationship ID rId4 was not found in the file.

What is personal information?

Any information

… relating to an identified or identifiable …

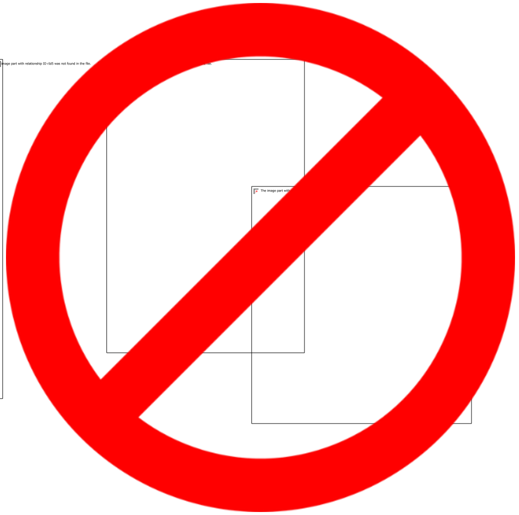
natural person

the data subject!

The image part with relationship ID rId3 was not found in the file.

The image part with relationship ID rId4 was not found in the file.

The image part with relationship ID rId5 was not found in the file.



The image part with

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 is data identifiable?

A Mauritian **+1,3 m**

How is data identifiable?

An Mauritian female **750.000**

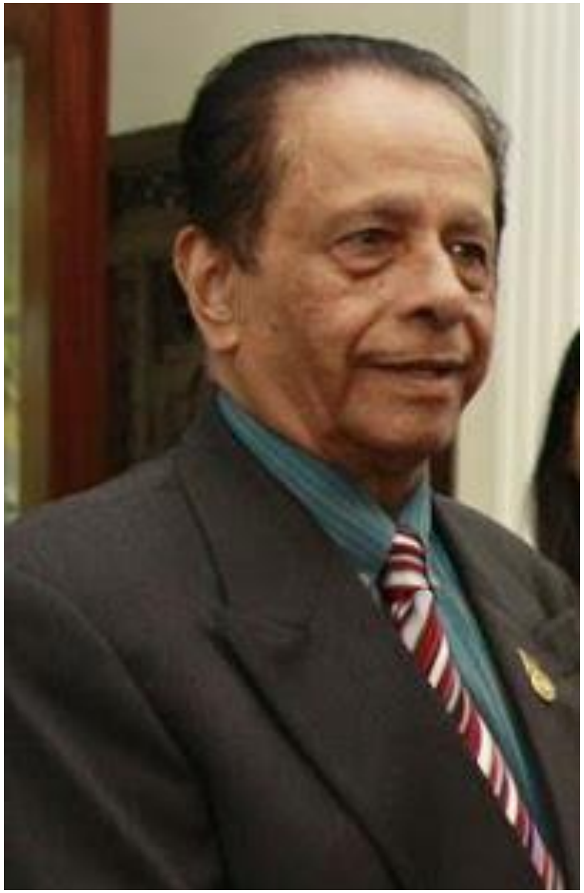
How is data identifiable?

An Mauritian female born in 1995 **45 800**

How is data identifiable?

…. Living in Clarisse House

1



Which data is sensitive?

Health

Biometric

NEW

Genetic

NEW

Trade union

Racial

Political

Religion

Sex life

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

Other personal data stored?

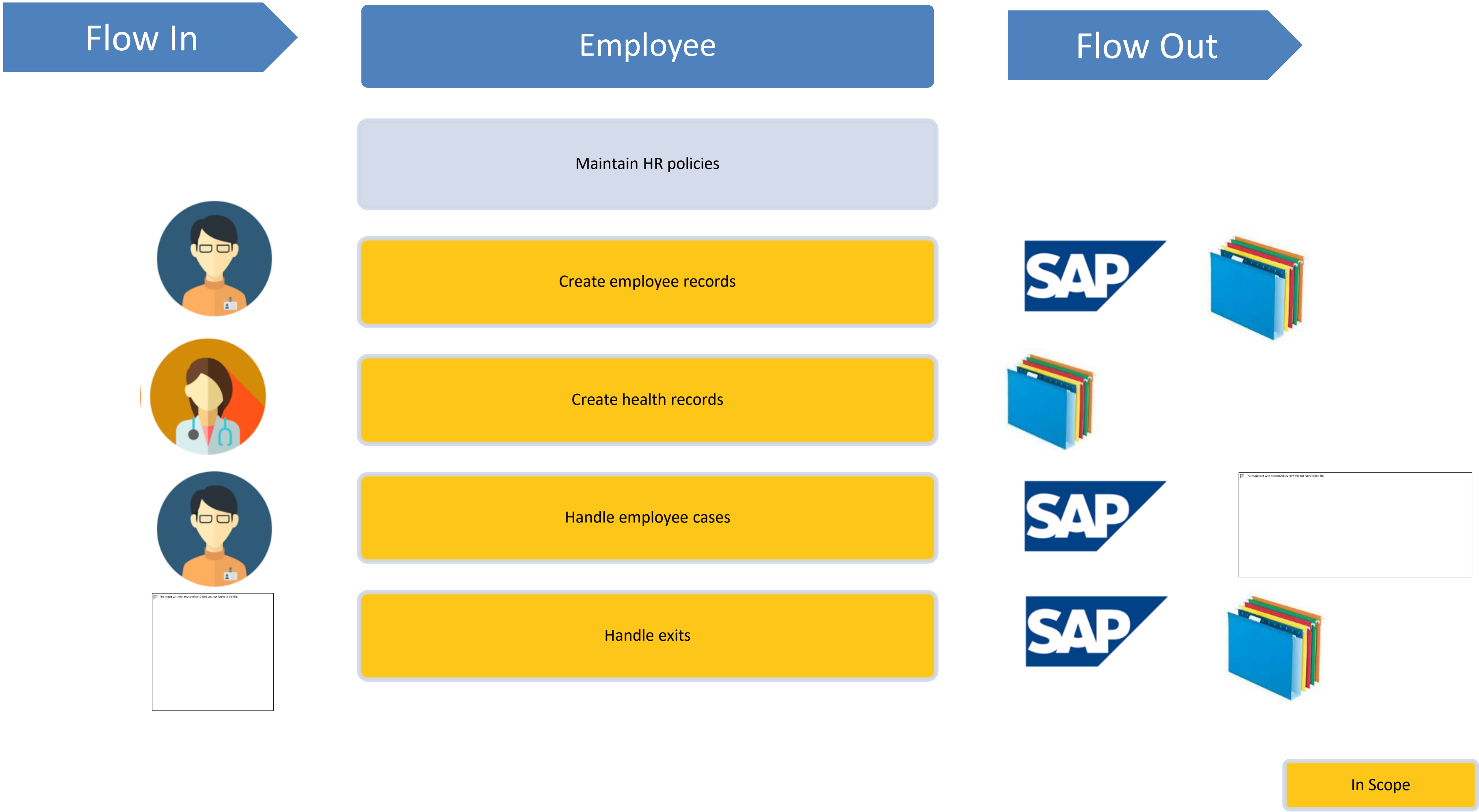
- **Website visitors**
- **Email servers**
- **Marketing databases (call centres), client complains**
- **Customer loyalty programs**
- **Patient/client databases**
- **Personnel files and performance reviews, IQ tests, diplomas, training**
- **Legal documents, contract management and due diligence checks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

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

How do I identify personal data?

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

Step 3: Scope example



Flow In

Employee

Flow Out

Maintain HR policies

Create employee records

Create health records

Handle employee cases

Handle exits

In Scope

SAP
SAP
The image part with relationship ID rId9 was not found in the file.
The image part with relationship ID rId8 was not found in the file.
SAP

Group discussion

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

The image part with relationship ID rId3 was not found in the file.

Step 4: Compile a data inventory

The image part with relationship ID rId4 was not found in the file.

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

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

Step 4: Compile a data inventory

EU GDPR INSTITUTE

Who

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

Where

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

Why

- the personal data is under the Organization control?

When

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

What

- safety mechanisms and controls are is place?

Data landscape

The image part with relationship ID rId3 was not found in the file.

The image part with relationship ID rId4 was not found in the file.

Identifying personal data
Identifying appropriate technical &
organizational standards

Understand legal and
regulatory obligations

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

The image part with relationship ID rId3 was not found in the file.

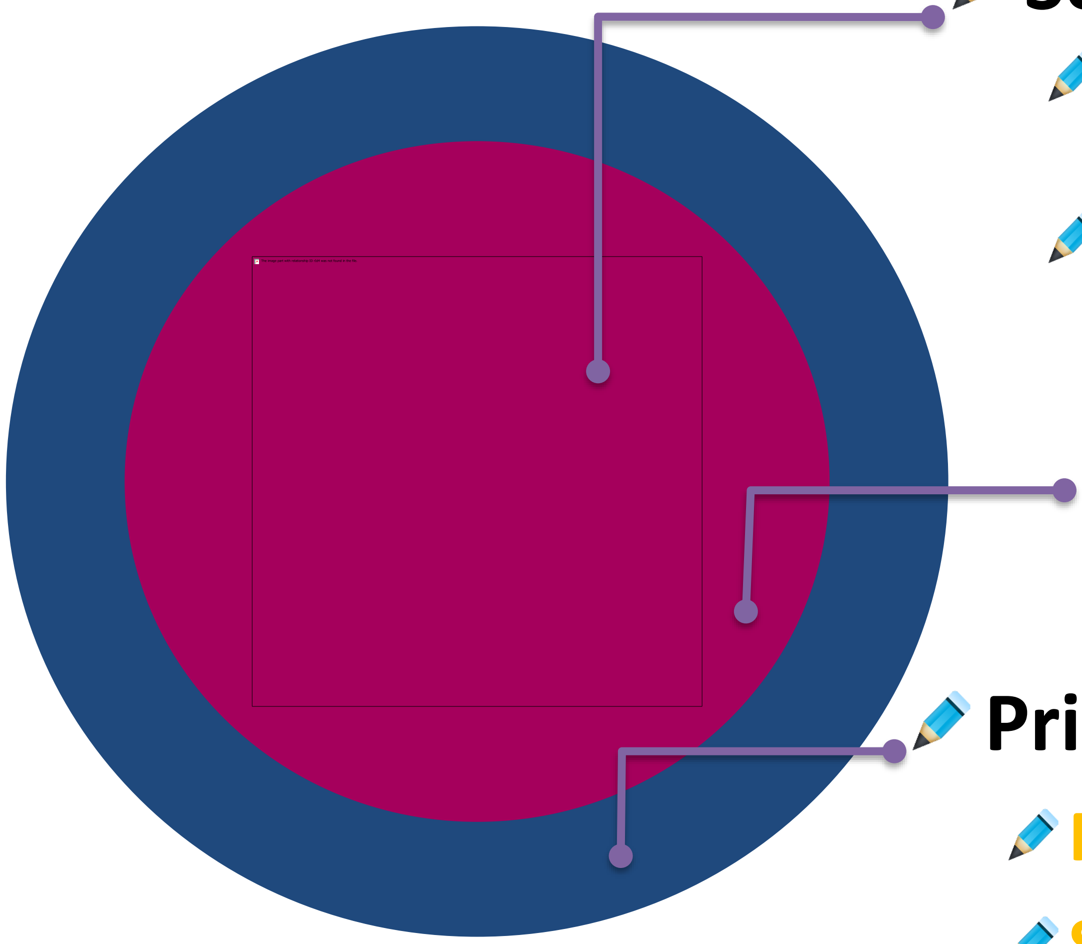
Step 5: Clean the house!

The GDPR is an opportunity to improve data practices

De-risk! Start clean!

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

Step 6: Privacy policy


The image part with relationship ID rId4 was not found in the file.

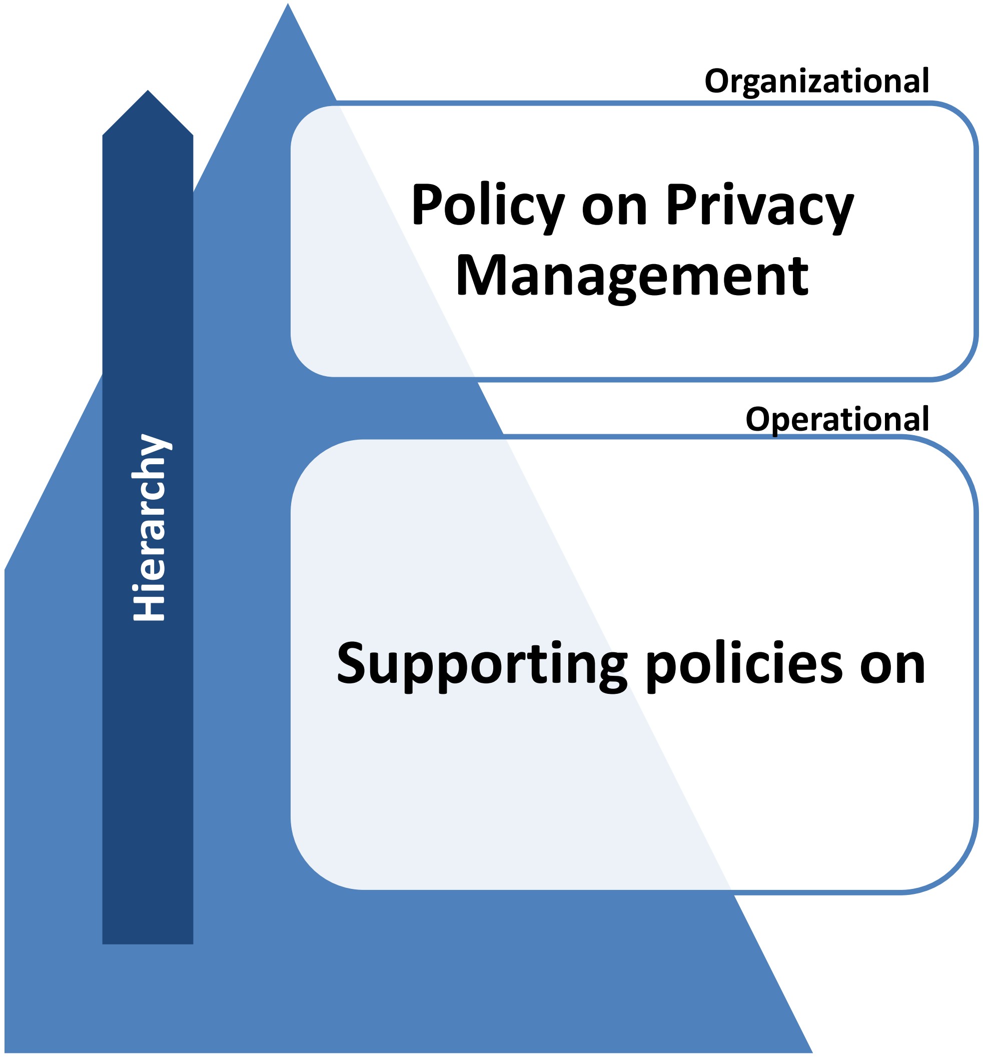
- Security strategy
  - Part of the business ethics
  - Risk tolerance based on the customer trust
- Data security policy
  - Objectives
- Privacy policy
  - Privacy program
  - Supporting policies

Step 6: Create a privacy policy

Best practices based on the ISO 27001

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

Step 6 : Create a privacy policy



Organizational

Policy on Privacy Management

Operational

Supporting policies on

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

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

Step 6: Removable media

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

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

B - Do

The image part with relationship ID rId4 was not found in the file.

Step 1: Limit access

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

Step 2: Review consents
How consents should be given?

The image part with relationship ID rId11 was not found in the file.

Plain language

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

The image part with relationship ID rId12 was not found in the file.

Opt-Out

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

The image part with relationship ID rId9 was not found in the file.

Updated

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

The image part with relationship ID rId10 was not found in the file.

Minors

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

Step 2: Review consents

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

Step 3: Prepare to deal with requests

NEW

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

Step 4: Validate data transfers

Flows-in the organization

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

Flows-out (data transfer or display)

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

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

Principles

Processed lawfully, fairly and transparently

Processed in a manner that ensures appropriate security

Collected for specified, explicit and legitimate purposes

Accurate and, where necessary, kept up to date

Adequate, relevant and limited to what is necessary

Kept for no longer than is necessary

Rights

EU GDPR INSTITUTE

To access data

request access to personal data to verify lawfulness of processing

NEW

To data portability

common format, even directly transmitted between controllers

NEW

To rectify and be forgotten

when no longer necessary or consent is withdrawn

To object by controller

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

NEW

To restrict processing

limiting the data use or transfer

To limit profiling

right to not be subjected to automated individual decision making

Difference

Privacy notices

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

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

Consents

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

Step 6: Review consents
How should consents be given?

EU GDPR INSTITUTE

The image part with relationship ID rId11 was not found in the file.

Plain language

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

The image part with relationship ID rId12 was not found in the file.

Opt-Out

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

The image part with relationship ID rId9 was not found in the file.

Updated

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

The image part with relationship ID rId10 was not found in the file.

Minors

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

Step 7: Notify a data breach

EU GDPR INSTITUTE

Data breach

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

When to notify

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

What to notify

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

Whom to notify

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

Step 8: Data security program

Encryption of personal data

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

Security measures

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

Resilience

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

Regular security testing

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

C – Improve and Maintain

Step 1: Train your people

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

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

Follow-up

Communicate to stakeholders, bottom-up and top-down

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

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

Privacy…

By default

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

By design

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

Step 3: Audit compliance

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

Step 4: Code of conduct & certification

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

Step 4: Code of conduct & certification

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

Data Transfer to Third Countries

Data Transfers

Data Transfer Restrictions

- See map that indicates a general restriction in force regarding the cross-border transfer of data
- Identify general or relevant sector-specific data localisation requirements for data protection compliance.

Adequacy[I]

- EU Commission determines if a third country ensures adequate protection level
- Personal data can flow from the 28 EU countries and 3 EEA member countries

Model Contracts

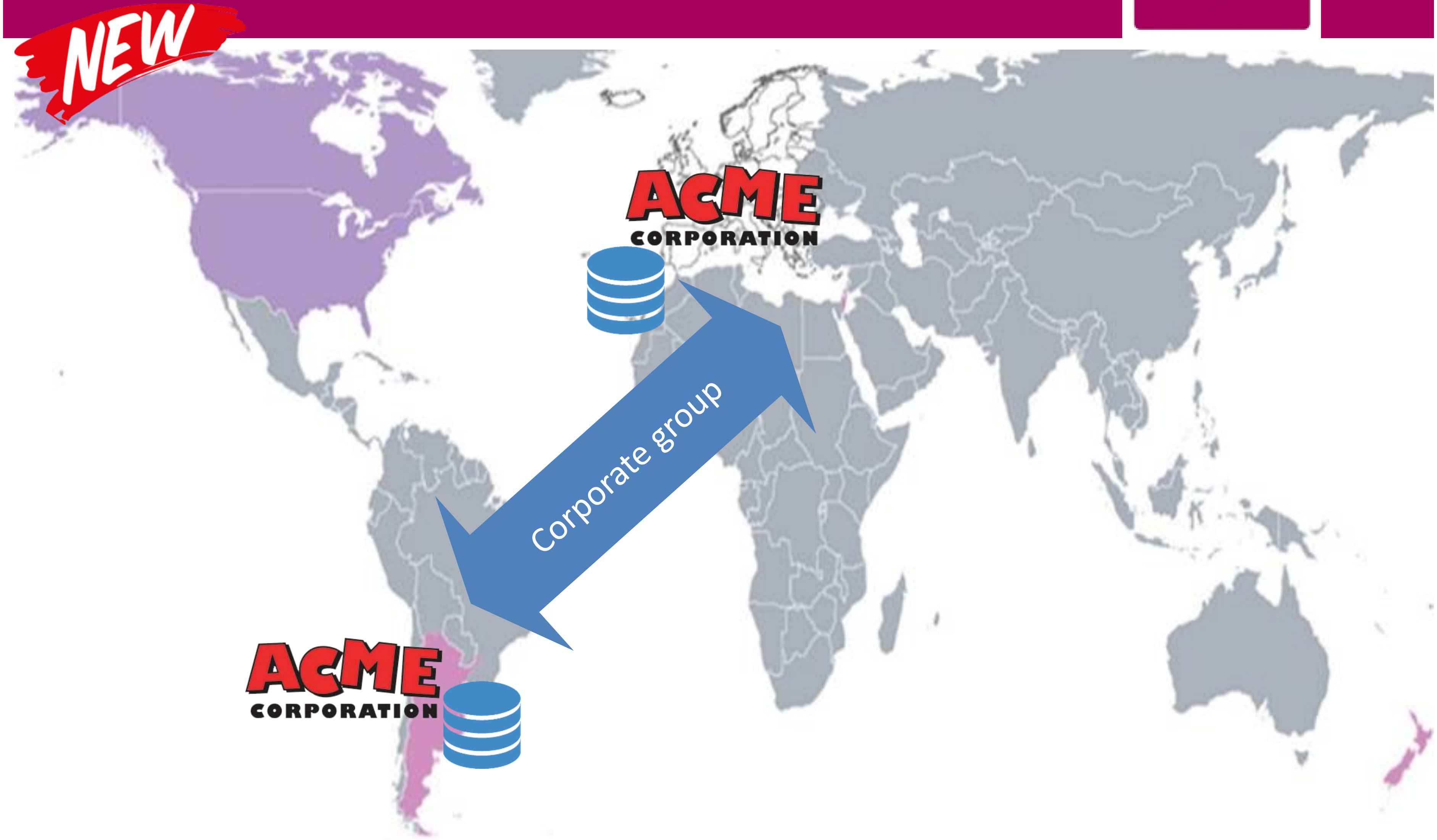
- The Model Contracts Cross-Border Chart provides guidance to data controllers on filing and authorization
- Use of model clause contracts for formalities, timelines, and sanctions listed.

Binding Corporate Rules

- Provides multinational companies with a legal solution meeting their needs and structure.
- Mutual Recognition Cross-Border Chart, Case Studies, Action Plan, Filing needs

[I] The Data Protection Directive (95/46/EU)

Binding corporate rules



National Supervisory Authorities

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

Roadmap schedule

EU GDPR INSTITUTE

Plan · Do · Improve

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

🟦 Process	🟥 Information Documents	🟩 Organization	🟧 Technology

Steering committee meetings

The GDPR Law

- ✎ **General provisions**
  - ✎ **Chapter 1 (Art. 1 – 4)**
- ✎ **Principles**
  - ✎ **Chapter 2 (Art. 5 – 11)**
- ✎ **Data subject rights**
  - ✎ **Chapter 3 (Art. 12 – 23)**
- 🌐 **Controller and processor**
  - 🌐 **Chapter 4 (Art. 24 – 43)**
- ✎ **Transfers**
  - ✎ **Chapter 5 (Art. 44 – 50)**

- 🌐 **Supervisory authorities**
  - 🌐 **Chapter 6 (Art. 51 – 59)**
- ✎ **Cooperation and consistency**
  - ✎ **Chapter 7 (Art. 60 – 76)**
- 🌐 **Remedies, liability & penalties**
  - 🌐 **Chapter 8 (Art. 77 – 84)**
- ✎ **Specific processing situations**
  - ✎ **Chapter 9 (Art. 85 – 91)**
- ✎ **Other rules**
  - ✎ **Chapters 10/12 (Art. 92 – 99)**

✎ **Direct obligation**

🌐 **Meta rule**

🔗 **https://gdpr-info.eu**

The Data Protection Bill

- Data Protection Bill in Mauritius should “in principle” lead to EU adequacy
- The Bill will bring Mauritius’ data protection framework into line with international standards
- Additionally, the Bill aims to simplify the regulatory environment for business in the digital economy
- Promote the safe transfer of personal data to and from foreign jurisdictions.

Mauritius' Data Protection Bill

- The Bill makes personal data breach notification mandatory.
  - A personal data breach must, without undue delay and, where feasible, not later than 72 hours after controller is aware of the breach, be notified to the Data Protection Commissioner.
  - If the data breach is likely to result in a high risks (rights and freedoms of data subjects), the data controller must notify them
- Additionally accountability obligations are imposed on data controllers
  - These include to conduct an assessment of the impact of high risk processing operations, and to keep records of processing operations.
  - The Data Protection Office will encourage compliance with the new law by laying standards for certification mechanisms, seals and marks and certification.

Conclusion

- The GDPR will usher in a new era of data protection mandates on a larger global stage for organisations that may be caught by its broad extra-territorial provisions.
- A Non-EU Entity in non-compliance will be potentially be caught by the GDPR is possible
- Take steps toward compliance or avoidance depends entirely on the unique facts and circumstances of the organisation and its operations.
- The EUGDPR Institute provides training and certification and insights to take certain actions in order to help mitigate against the risk of the GDPR and applying to them under the offering goods or services to soften the ultimate blow of the extra-territorial tests.

Useful Data Protection/Privacy/GDPR links

EU GDPR INSTITUTE

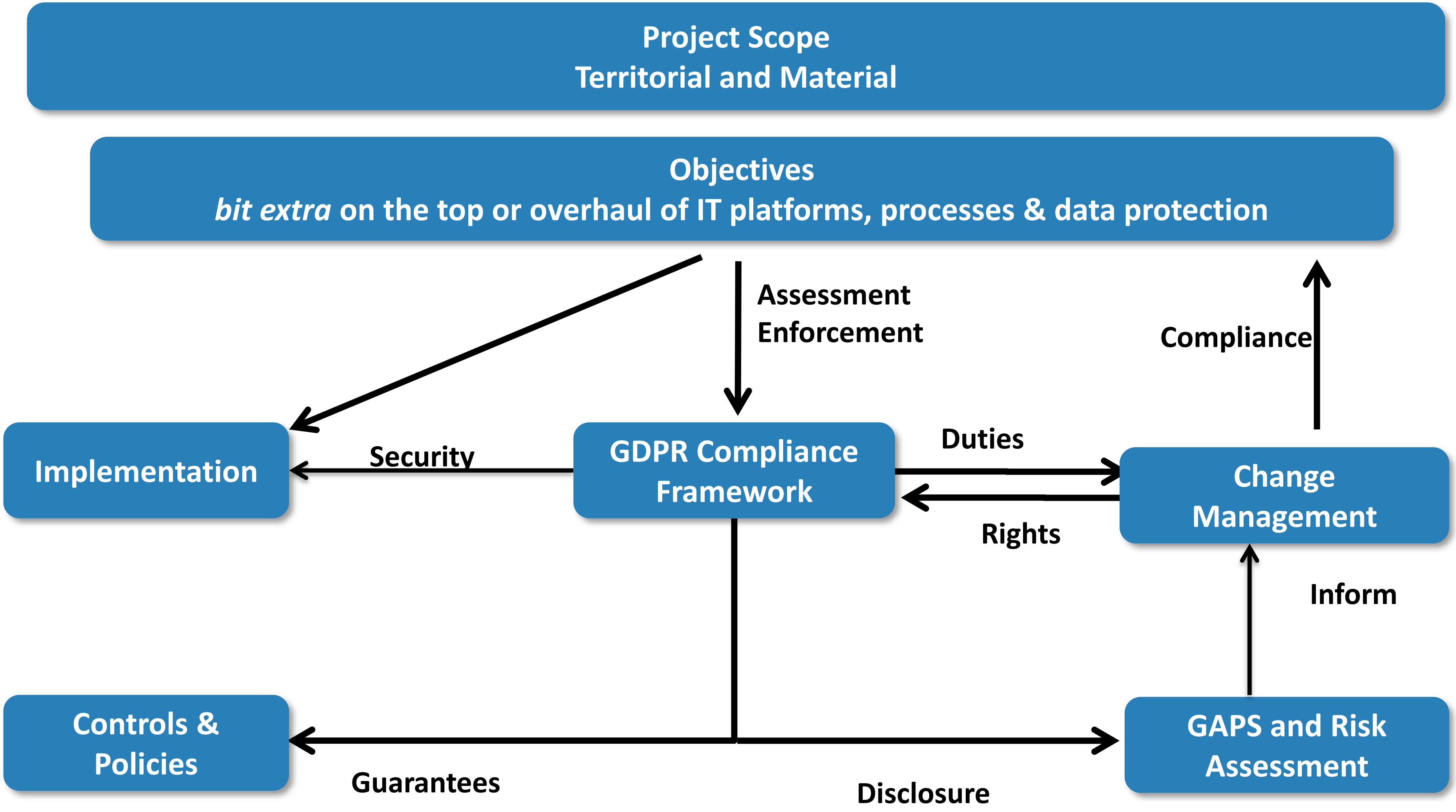
Privacy Shield Framework

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

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

What you have received?

Summary



Project Scope
Territorial and Material

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

Assessment
Enforcement

Compliance

Implementation

Security

GDPR Compliance Framework

Duties

Rights

Change Management

Inform

Controls & Policies

Guarantees

Disclosure

GAPS and Risk Assessment

The GDPR Institute

EU GDPR INSTITUTE

Connecting IT Security to Governance, Risk and Compliance

www.copenhagencompliance.com

HR Riskability

Human Capital Assessment Framework

CERTIFICATION ★ EXERCISES ★ RESEARCH ★ TRAINING
IMPROVE ★ ORGANIZATION ★ NEEDS
IN CONTROL ★ FACILITATION
COPENHAGEN COMPLIANCE
Global GRC Solutions
Corporate Governance
Risk Management
& Compliance
Certification
INSTRUCTION ★ COURSES ★ AUTHORITY ★ TRACKING

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

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

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

e-mail: info@eugdpr.institute

Copyright notice

As usual when in doubt always contact your legal advisers. The EUGDPR Institute and Copenhagen Compliance are not licensed to provide legal advice.