

Data Protection and You



February 5 2019

The Importance of Data Protection

February 6 2019

The Obligations of Data Processors



by



Venue: The Pegasus Hotel, Windward Suite



Agenda



Day 1. The Importance of Data Protection



7:45 - 8:30	Registration
8:30 – 9:30	Opening Session: Why is data protection important and the ways in which the lack of a mechanism to protect data can negatively impact an organization Presenter: Kersi F. Porbunderwala
9:30 – 10:30	The risk and reward relationship of a prudent data control policy within an organization Presenter: Roeder Jens
10:30 – 10:45	BREAK
10:45 – 11:00	Greetings: Wahkeen Murray (Miss) Permanent Secretary (Acting) Ministry of Science and Technology
11:00 - 12:30	Current trends in the data protection industry Presenter: Roeder Jens
12:30 – 1:30	LUNCH
1:30 – 3:30	Impact of global data protection legislation on a company's operations: <ul style="list-style-type: none">Consider businesses with branches in other Caribbean islands or servers in other Caribbean islands- may also be subject to Data Protection legislation specific to those jurisdictions as a data controller Presenter: Presenter: Roeder Jens
3:30 – 3:45	BREAK
3:45 – 5:00	Extra-Territorial scope: Applicability of the GDPR to organisations: <ul style="list-style-type: none">Processing personal data as a controller or processor in your respective jurisdiction (regardless of whether the processing takes place in the respective jurisdiction);Processing personal data as a processor on behalf of a client data controller (even if based outside the jurisdiction);that are not established in the jurisdiction, but process personal data about data subjects who are in the respective jurisdiction in relation to: Presenter: Kersi F. Porbunderwala



Agenda



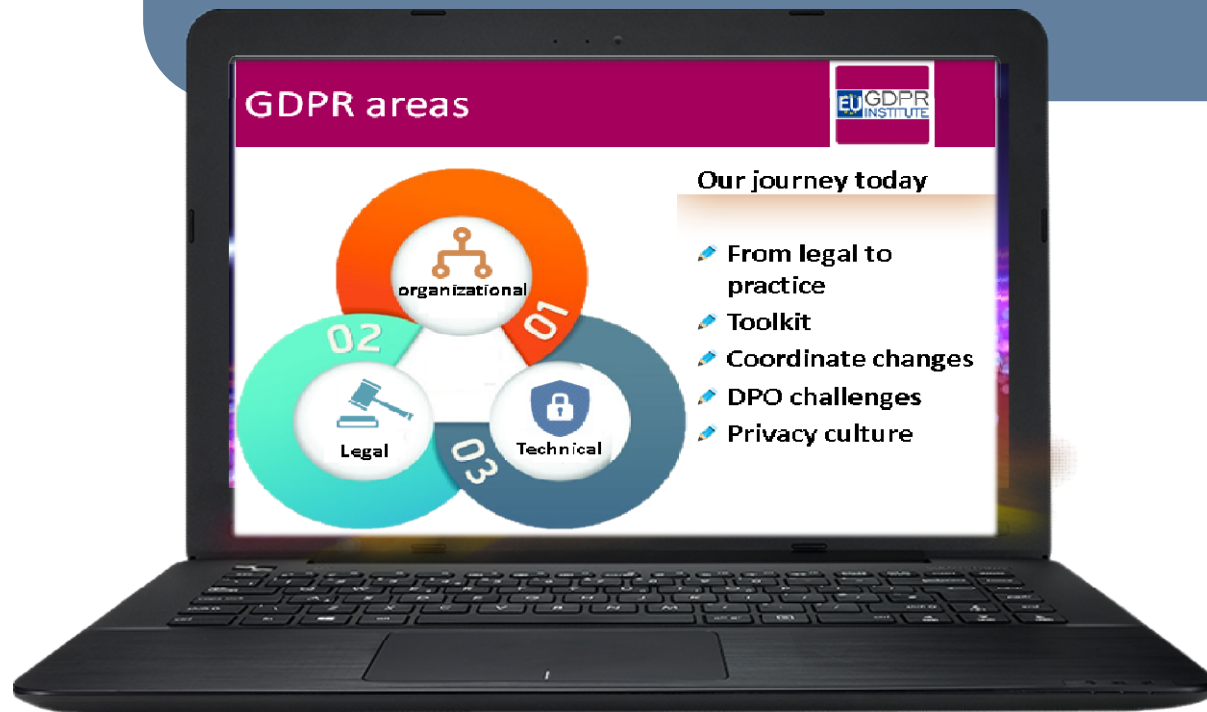
Day II. The Obligations of Data Processors (Stakeholders)

	7:45 - 8:15	Registration	
	8:15 - 9:30	<p>Direct Processor obligations: Data processors have direct obligations under the GDPR when processing on behalf of client data controllers in relation to matters including data security, international data transfers, appointment of sub-processors and security breach notification.</p> <p>Data Controller obligations: Data Controllers must implement appropriate technical and organizational measures to protect the security of data.</p> <p>Presenter: Roeder Jens</p>	
	9:30 - 10:30	<p>International transfers: The GDPR codifies new adequate safeguards for data transfers outside the respective jurisdiction, including:</p> <ul style="list-style-type: none"> • binding corporate rules • standard contractual clauses approved by a local supervisory authority • approved codes of conduct • approved certification mechanisms. <p>Presenter: Kersi F. Porbunderwala</p>	
	10:30 - 10:45	BREAK	
	10:45 - 12:00	<ul style="list-style-type: none"> • Preparing for data protection regulations • Spearheading the move to compliance with the (DPR) • Evaluating the need to carry out a thorough audit of all of an organisation's processing of personal data. • The need for Data Protection Officers (DPO) • Changing the cultural mindset • Embracing the change in cultural mindsets <p>Presenter: Kersi F. Porbunderwala</p>	
	12:00 - 1:00	LUNCH	
	1:00 - 2:30	<ul style="list-style-type: none"> • Conducting an IT Risk Assessment • Deploying & documenting implementation of tools such as Notices to address information security gaps in your own organisation. • Creating & Implementing Data Protection Policies / Initiatives • Setting up procedures and policies to maintain the organisation's full programme management • Establishing efficient procedures for Privacy Impact Assessments, Subject Access Requests and data breaches, etc. <p>Presenter: Marcelle Smart - tTech</p>	
	2:30 - 3:30	<ul style="list-style-type: none"> • The promulgation of the Jamaican Data Protection Act <p>Presenter: Justine Collins HMF</p>	
	3:30 - 3:45	BREAK	
	3:40 - 5:00	<p>Discussion workshop</p> <ul style="list-style-type: none"> • Identify the potential breaches in your current Organisation. • Roles & Responsibilities of the Data Protection Officer & • Conducting a Personal Data Inventory Audit. 	

Access to the presentation



<https://www.eugdpr.institute/feb2019-jamaca/>



What you will receive?



Introductions

Name?

Organization?

Role?

Background?

Expectations?

GDPR areas




- ✎ **Challenges**
- ✎ **Privacy culture**
- ✎ **Compliance journey**
- ✎ **Data Protection**
- ✎ **Organise changes**
- ✎ **Legal to practice**

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.”***



Why is data protection important

The ways in which the lack of a mechanism to protect data can negatively impact an organization

Why is Data Privacy & Protection important?



Privacy is a competitive advantage

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

Evolving information landscape



We are in a rapidly evolving information age

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



Industry is in a digital transformation mode

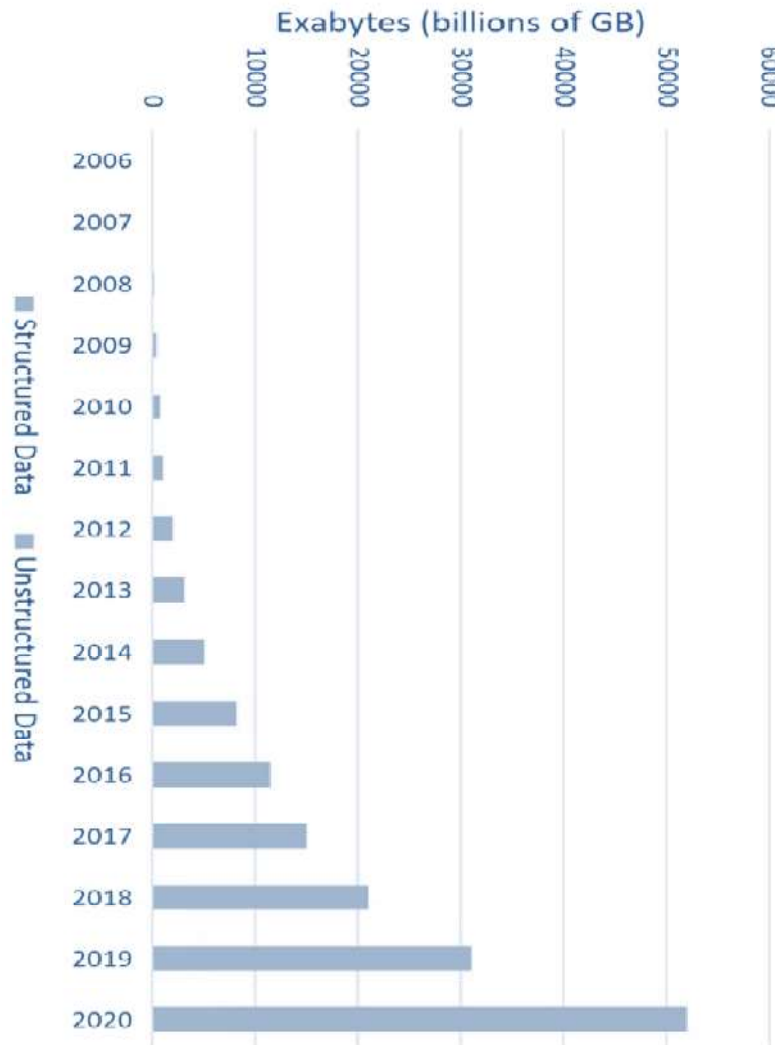
- Mobile finance, digital payments and currency, driverless cars and a host of other rapidly emerging information services are re-shaping traditional business models.



Old laws don't fit; new framework is emerging

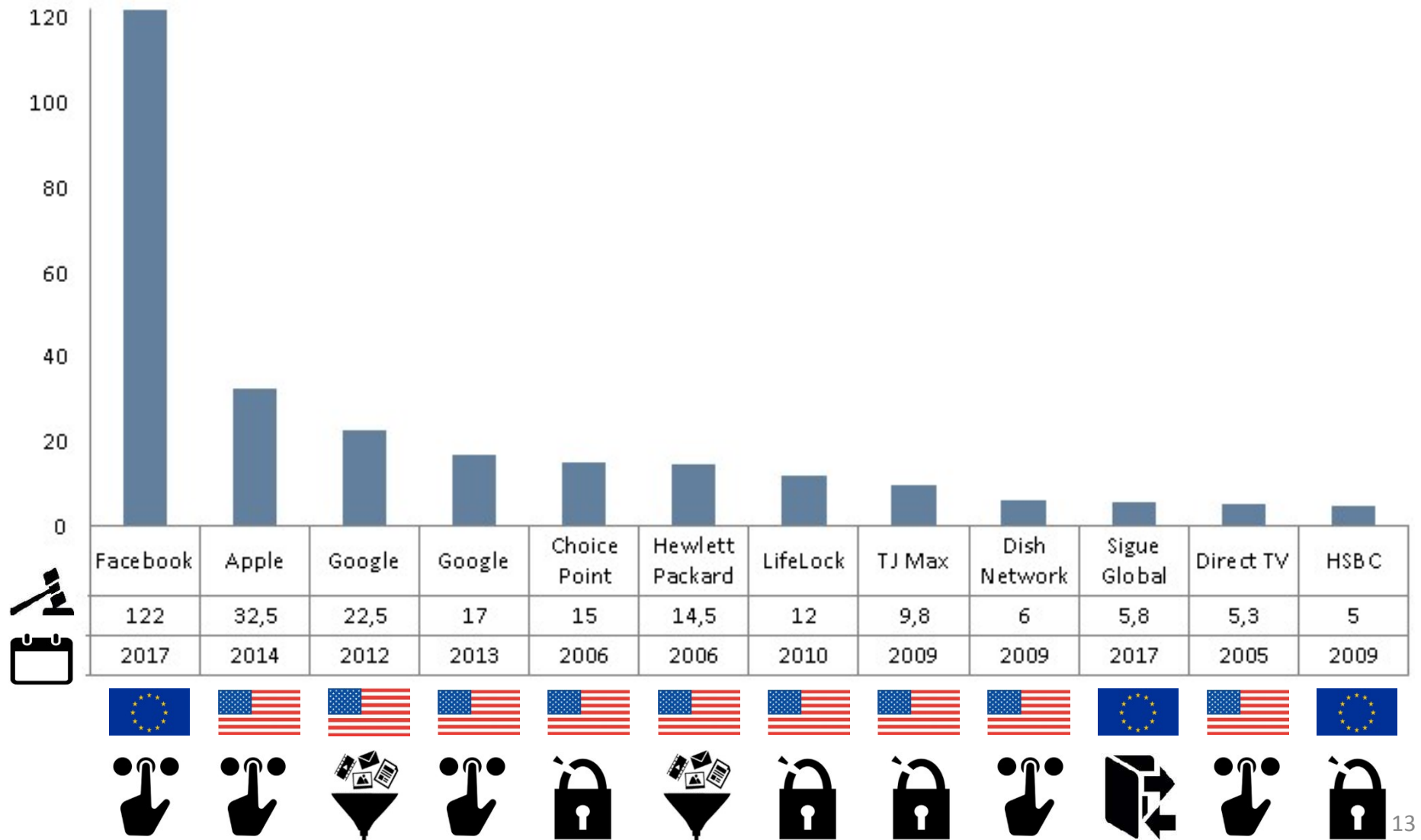
- Information-related global laws and regulations are struggling to adapt to new technologies and new data uses, requiring a new approach to managing information-related global risks.

The explosion of data



- ✎ **90% of world's existing data created in the last 2 years**
- ✎ **1 Billion - pieces of content on Facebook/daily**
- ✎ **2.5 Quintillion - generated by people everyday**
- ✎ **6 Billion - hours of video watched on YouTube every month**
- ✎ **271 Million - Monthly active users on Twitter**
- ✎ **2.7 Zetabytes - Amount of data in the digital universe**

Data privacy fines



What is happening in the world?



There are data breaches everywhere, everyday.



Facebook Security Breach Exposes Accounts of 50 Million Users

CNIL (France)

- From May to Sept.
- 742 data breaches reported – around 6 per day- that referred to 33.7 M citizens
- 65% are due to external malicious acts and 15% by internal human mistakes
- Advised on improving containment measures

CNPD (Lux)

- From May to early Oct.
- 97 data breaches reported
- 36% are due to external malicious acts and 58% by internal human mistakes

FINANCE • EQUIFAX

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



Cambridge Analytica

Cathay Pacific faces probe over massive data breach

Under Armour

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

ICO (UK)

- From March to June
- From almost 500 reports in March to over 1,700 in June. 8 x the average month in 2016/2017
- Currently ICO is receiving 500 reports per week 14

Why we need privacy principles?



📍 Provide a **common language** and **terms** to engage with all stakeholders

📍 Help set **expectations**, stipulate **requirements** and define **obligations**

📍 Harmonize **legal** and **governance** requirements



📍 Create a **structural understanding** of privacy

📍 Make data subjects aware of their **privacy rights**

📍 **Sensitive** entities that deal with transactions involving **personal data**

Drivers to Privacy Laws

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

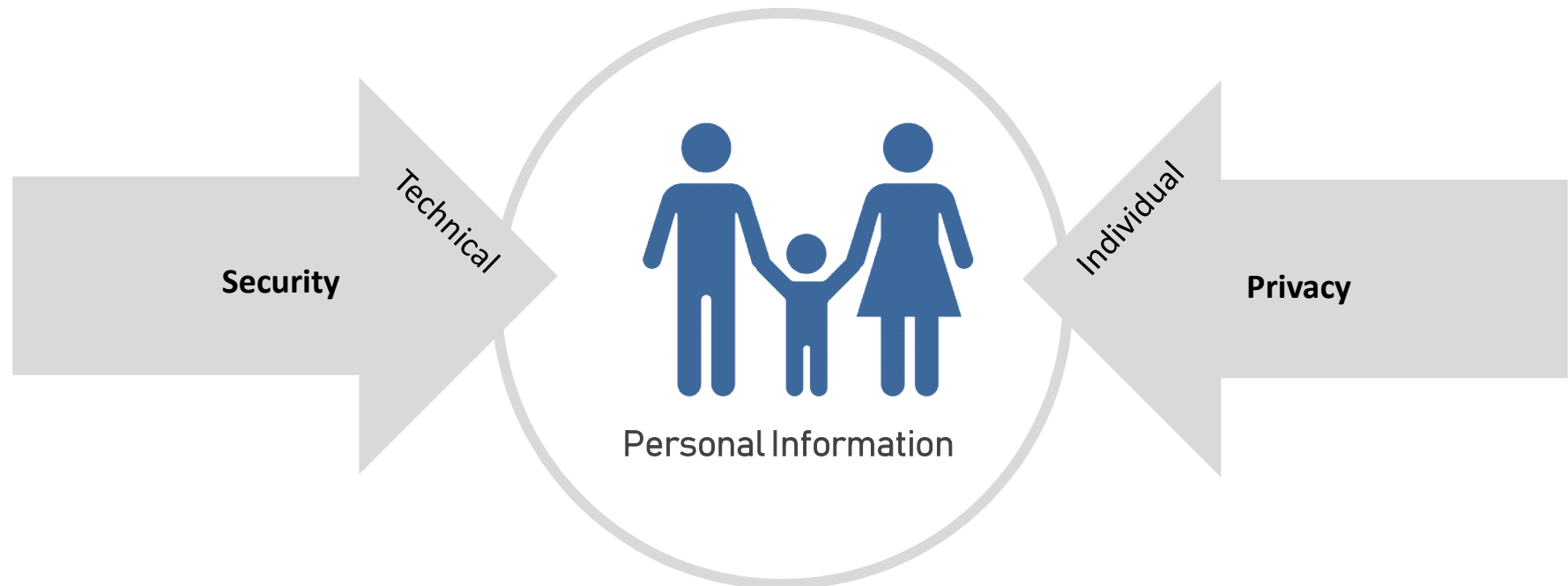
Drivers to Privacy Laws

- ✎ **Products & Services**
 - ✎ **Laws to prevent misuse of information in different contexts**
- ✎ **Analytical Profiling**
 - ✎ **Big data analytics has enabled the collection and structured the scattered bits of PII & production information.**
 - ✎ **Privacy laws a safeguard against misuse of such data and information**
- ✎ **Supply chain, hyper-specialization & global sourcing**
 - ✎ **Businesses are focusing on core competency and outsourcing the rest.**
 - ✎ **Laws can prevent damage from loss of data from such situations**
- ✎ **Transborder data flows & Cloud services**
 - ✎ **Vulnerabilities in data in different geo locations are prevented**

Privacy is a human issue









Data Privacy & Protection requires companies handling residents' data to undertake major operational, privacy and security reforms



Considerably More Than Just a Privacy Policy Update

GDPR so far...



-  drew the attention of boards to privacy issues
-  reached all types of industries
-  secured significant resources
-  increased the collaboration between legal, compliance, HR and IT departments
-  improved contracts with processors
-  responsible, transparent and less invasive use of personal data

GDPR so far...



IT

- ✎ Data breaches
- ✎ 3rd parties and cloud computing

Legal

- ✎ Class actions
- ✎ Fines



HR

- ✎ Pressure from unions and employees
- ✎ Training

Business

- ✎ Limitations for activities
- ✎ Impact on innovation

Board

- ✎ Corporate and personal liabilities
- ✎ Compliance costs

GDPR after May 25th 2018





- ✎ How, when and where the supervisory authorities could start?
- ✎ What companies could be the first target? could they be the American tech firms, the Chinese e-commerce sector or the Russian companies?
- ✎ Would the supervisory authorities be consistent on grounds, accepted evidence and fines?
- ✎ If one investigation is opened in one country, could it lead to investigations in other countries?





Earlier regulations and laws (October 1995)

EU Data Protection Directive

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

Issues

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

Drivers to Privacy Laws

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

Drivers to Privacy Laws

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

Step 1. Approach to governing privacy



- ✎ **Human rights?** Privacy has been accepted as a fundamental right across different countries
- ✎ **Market commodity?** User information has become a product, and therefore, become vulnerable against misuse
 - “Apple, Facebook, Microsoft and Google are not for free, you sell out your own identity”*
- ✎ **Privacy governance?** Challenges in terms of interoperability have resulted in contextual adaptation of different laws. Industries have adopted alternatives to formal regulation like codes of practice, ISO standards and trust seals

Step II. Approach for governing privacy



Comprehensive regulation or sectorial laws?

EU and a number of other countries have adopted comprehensive legislation while other countries regulated different sectors

Governance of cross border data flows

Disparities in national legislations have the potential to actually hamper data flows and raise constraints in trade development so balance must be obtained amidst the cross current of data flows

Strong regulatory infrastructure

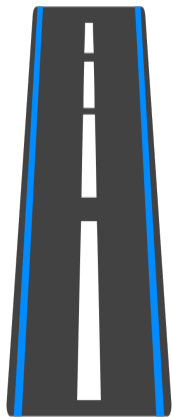
Strong regulation ensures the appointment of a data protection officer to ensure citizen privacy, whilst this might lead to restricting innovation and raising costs

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 4. What is personal information?



Any information



... relating to an
identified or
identifiable ...

natural person
the data subject!



Jamaica's Privacy Protection Bill



- When the Jamaican Data Protection Act is passed, it will mark a shift towards a model similar to EU law, which is cross-sectoral and apply to all industries.
- This is in contrast to Jamaica's current privacy legislation, which is applied at a sectoral level, and more closely resembles the US approach of applying different data protection regimes to different industries.

How data is identifiable?



A Jamaican **2,903,299**



How data is identifiable?



A Jamaican female **1,681,898**



How data is identifiable?



A Jamaica female born in **19,656**



How data is identifiable?



.... lives in Sherwood Content, Trelawny, Jamaica.

1



How data is identifiable?



1 identifier

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

NEW

1 or + factors

Physical
Physiological
Economic
Cultural
Social
Mental

How data is identifiable?



NEW

Key or Pseudonymous

1 identifier

NEW

Pseudonymous

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

**1 or +
factors**



Why is data protection important

The ways in which the lack of a mechanism to protect data can negatively impact an organization

Step 1: Compile a data inventory



Who

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

Where

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

Why

- the personal data is under the organization control?

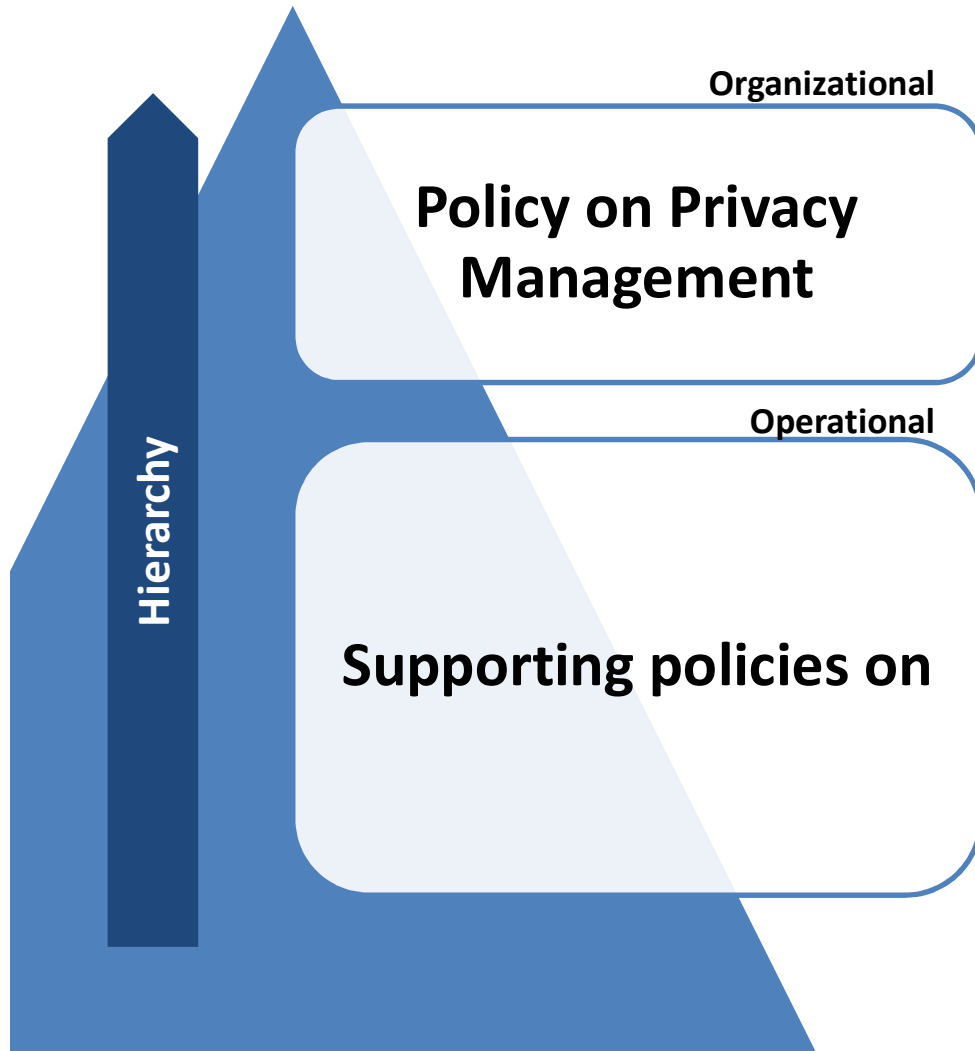
When

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

What

- safety mechanisms and controls are in place?

Step 2 : Create a privacy policy



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

Step 3: 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

NEW

Step: 4



Data Protection Impact Assessment

- ✎ The 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 organization's general risk management framework
- ✎ Mandatory for the data controller for early identification and controls
- ✎ Only for new and high-risk activities or projects to process 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

Step 5: Demonstrate compliance



Principles (art 5)

- ✎ A data privacy policy approved by top management
 - ✎ Integrated with the data security policy
 - ✎ Addressing privacy principles, lawfulness, purpose limitation, transparency, data minimization, accountability, deletion after use quality integrity and confidentiality
 - ✎ Mechanisms to maintain the data quality: data owner
 - ✎ Annually updated
- ✎ Supporting privacy policies
 - ✎ Code of conduct including privacy, staff handbooks, use of IT assets, information classification, document retention, document destruction, marketing
- ✎ DPIAs for new or changing programs, systems, processes

Step 6: Demonstrate compliance



Transparent information (arts 12, 13 and 14)

- ✎ Procedure to obtain valid data privacy notices
 - ✎ Effective communication of how to exercise the rights of the data subject
 - ✎ Notices are gotten before collecting data
 - ✎ Define the mechanisms
 - ✎ statements, icons, pop-up notifications, scripts
 - ✎ Who approves and control the notices (legal knowledge)
 - ✎ Define who is responsible for controlling that processing is consistent with notices and the description of activities is accurate
- ✎ Protocol for a data breach notification
 - ✎ to affected individuals, to regulators, credit agencies, law enforcement

Step 7. Enterprise Risk Requirements



✎ **Data Privacy and Protection is framed within the general risk management framework of the organization. This defines the:**

- ✎ **Scope,**
- ✎ **Policies**
- ✎ **Objectives**
- ✎ **Procedures**
- ✎ **Controls**
- ✎ **Risk assessment methodologies**
- ✎ **Risk treatment plan**

Step 8. Clean the house!



The Data Privacy and Protection is an opportunity to improve data practices

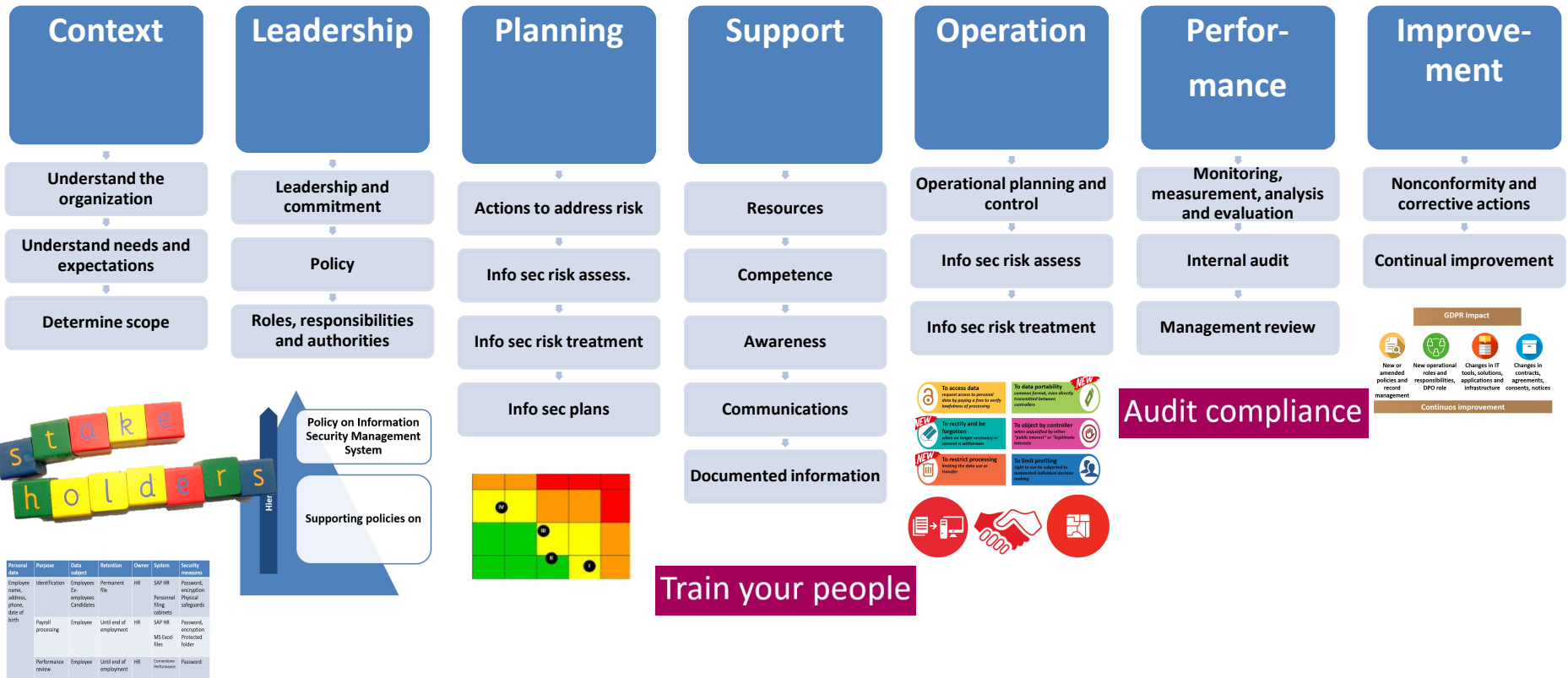
Dismantle risk! Start to clean your data!

- ✎ 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, erase copies and links**
- ✎ Opt out in email lists (ccs are not always necessary)**
- ✎ Remove duplicate, out-of-date and inaccurate records**
- ✎ Be conservative: there are no fines for over-deleting**

Step 9. ISO 27001 Data protection and Data Privacy and Protection



Step 10. ISO 27001 Info Security



Personal Data	Purpose	Data Subject	Retention	Owner	System	Security Measures
Employee names, address, phone, date of birth	Identification	Employees, Ex-employees, Candidates	Permanent file	HR	SAP HR	Password, encryption, Physical safeguards, cabinets
Payroll processing	Employee	Employee	Until end of employment	HR	SAP HR	Password, encryption, Physical folder
Performance review	Employee	Employee	Until end of employment	HR	Compass Performance	Password

Data protection (ISO 27001) is needed for privacy (Data Privacy and Protection)

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



Protests in Berlin against US surveillance, after the Edward Snowden case. Photograph: Lars Dickhoff/Corbis

9:30 – 10:30



The risk and reward relationship

**Prudent data control policy
within an organization**

Step 1. Data Control Policy



**Data privacy
Policy**

**Communication
Policy**

**Information
Policy**



**Ability to limit
access and control
the use of personal
data**

**Ability to
communicate with
others without
being monitored by
other people or
organizations**

**Ability to determine
when and to what
extent personal
information is
collected, used,
stored, processed
transmitted, deleted
and controlled.**

Step 2. Controls for governance policy



- ✎ **GDPR applies** across all member states of the European Union
- ✎ **GDPR applies** to all organizations processing the data of EU data subjects



- ✎ A **complete overhaul** of data protection regulation with extensive updates of what can be considered identifiable information needs numerous Policies
- ✎ **Specific** and significant policies to protect rights for data subjects to seek compensation, rights to erasure and accurate representation
- ✎ **Compensation controls** can be sought against organizations and individuals employed by them
- ✎ **Significant** reduction in fines based on the implementation of technical organizational controls are implemented



Step 3. Control Policies for Data Privacy



1. ASSURANCE

- ✎ Use of certification schemes providing assurance about managing information security risks

2. NOT JUST PERSONAL DATA

- ✎ Protects customer information
- ✎ Protects your information assets
- ✎ Includes electronic information and in hard copy format

3. CONTROLS AND SECURITY FRAMEWORK

- ✎ Selection of technical and organizational controls to mitigate risks

4. PEOPLE, PROCESSES AND TECHNOLOGY

- ✎ Protects from technology-based risks
- ✎ Educates the poorly informed staff
- ✎ Corrects ineffective procedures

5. ACCOUNTABILITY

- ✎ Requires security regimes to be supported by top leadership
- ✎ Requires a senior individual who takes accountability
- ✎ Mandates clear accountability for data protection

Step 3. Control Policies for Data Privacy



6. RISK ASSESSMENTS

- ✎ Conducts regular risk assessments to identify threats and vulnerabilities that can affect your information assets, and to take steps to protect that data

7. CONTINUAL IMPROVEMENT

- ✎ Requires that your ISMS are constantly monitored, updated and reviewed, meaning that it evolves with your business to assure continual improvement, reducing risks

8. TESTING AND AUDITS

- ✎ Requires organizations to carry out regular testing and audits to prove that its security regime is working effectively

9. CERTIFICATION

- ✎ Requires organizations to take the necessary steps to ensure the security controls work as designed. Certification delivers an independent, expert assessment to see if you have implemented adequate measures to protect your data.

10:45-11:30



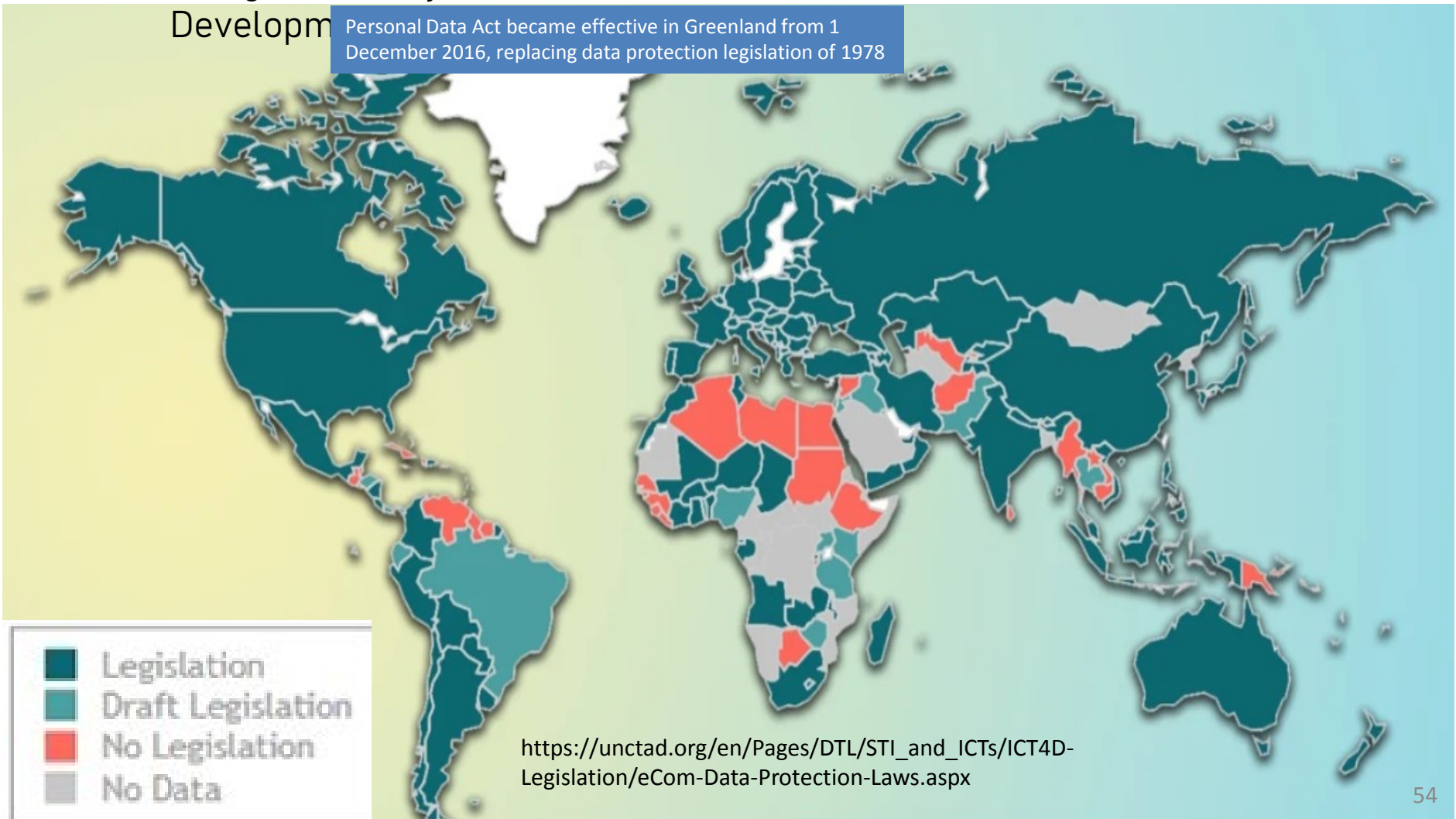
Current trends in the data protection industry

Global Data Protection and Privacy Legislation



[Image: courtesy of United Nations Conference on Trade and Development]

Personal Data Act became effective in Greenland from 1 December 2016, replacing data protection legislation of 1978



https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx

Current trends in the data protection industry



- Data management is continually being challenged—privacy, regulatory violation, legal impact, AI, cloud contracts
- Security vulnerability within the company processing and control infrastructure—authentication, authorization, access control, cryptography, encryption, monitoring
- The threat of “Monoculture” —diversity, resiliency, disaster recovery, business continuity and cyber security
- Data Processor/Service-Level Agreements—vendors and 3rd parties offer flexible, negotiated, customer-specific versions
- Heterogeneous big data and cloud computing environments—the ability to integrate with internal cloud and other (external) cloud vendors

Current trends in the data protection industry



- Technology is becoming smarter & more intuitive
- Legal issues need to be coupled with a people-centric design to engage and integrate processes and controls
- Create designs that help people understand and control the way services use their data and IT
 - ensure that designs build trust, transparency, controls
- Create user-interface design templates that reflect how people actually behave and interact online

Current trends in the data protection industry



- Organizations are looking to contain IT, Privacy and Cyber risks and improve efficiency and scalability of their IT and data infrastructure through the use of hardware-assisted Virtualization Technology to improve flexibility and robustness of their traditional software.
- Place information security initiatives into place, training to address the greatest challenge i.e. the lack of skilled information security resources.
- Cyber security, Privacy and Protection of personal data challenges in new technologies, services, such as social media, networking, virtualization, cloud computing,
- Privacy and data protection gains increased the focus of governments and regulators as they attempt to keep privacy regulations out in front of the potential risks associated with the new technologies.

Current trends in the data protection industry



- Identify data privacy compliance metrics/trends
- Ensure that data protection processes and procedures are being adhered to
- Implement the necessary management reviews
- Simulate incidents (e.g. data breach) to audit data security protocols
- Independent testing and quality assurance via internal or external audit service providers (ISAE 3204)
- Formalize non-compliance and remediation
- Escalate concerns and risks to senior management

1:30 – 3:30



Businesses Impact of global data protection legislation on a company's operations:

Operations, branches and servers in other Caribbean islands- may also be subject to Data Protection legislation

Specific to the jurisdictions as a data controller

The impact of Data Privacy & Protection in Business



- Increasing number of regulations do not render more jobs & growth
- Net neutrality rules could create the next Google or Facebook
 - Google or Facebook rivals are in Russia & China, with no net neutrality rules
- The largest firms benefit at the expense of smaller due to complexities
- Increased government power at the cost of consumer freedom
- The impact on value chain in the upcoming 5G networks in Europe
 - US and China where consumers have adopted pre-5G products and services
- GDPR is the data and IT platform for a “level the playing field”
 - Empowers European consumers
- GDPR’s impact on the advertising market in Europe
- GDPR’s negative impact on venture investment in Europe¹
 - The declines result in projected losses projected between 3,000-30,000 jobs.
- However, the GDPR is now the “global gold standard.”

¹Federal Trade Commission (FTC) and two academics at the Illinois Institute of Technology.

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




Principles

A yellow gavel icon inside a white circle, set against a yellow background.



Processed lawfully, fairly and transparently

Processed in a manner that ensures appropriate security

A green padlock icon inside a white circle, set against a green background.A teal target icon inside a white circle, set against a teal background.

Collected for specified, explicit and legitimate purposes

Accurate and, where necessary, kept up to date

A pink globe icon inside a white circle, set against a pink background.An orange checkmark icon inside a white circle, set against an orange background.

Adequate, relevant and limited to what is necessary

Kept for no longer than is necessary


A blue alarm clock icon inside a white circle, set against a blue background.

Rights



To access data
request access to personal data to verify lawfulness of processing

To data portability
common format, even directly transmitted between controllers



NEW

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




NEW

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




To restrict processing
limiting the data use or transfer

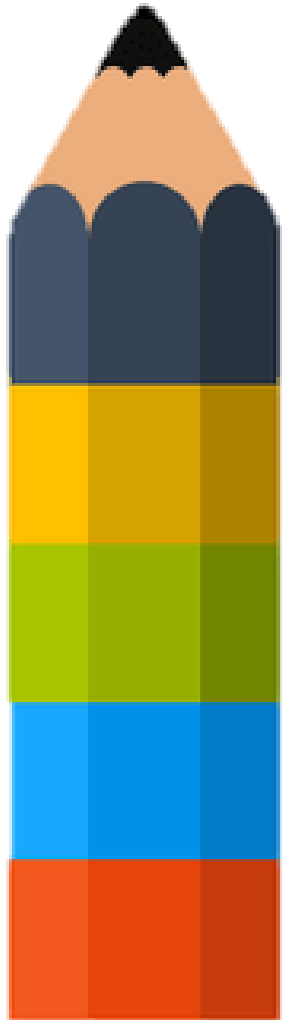


NEW

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



Privacy codes of practice



Organizational codes

Developed by a company or agency (generally public) to apply a privacy law (co-regulatory approach, should be approved by an authority)

i.e. Health Privacy Code of Practice

Sectorial codes

Developed by a trade association

i.e. Privacy code by the Federation of Direct Marketing

Functional codes

Developed to define privacy practices for a particular faction

i.e. direct email and telemarketing

Professional codes

Developed by professional associations

i.e. Research for health

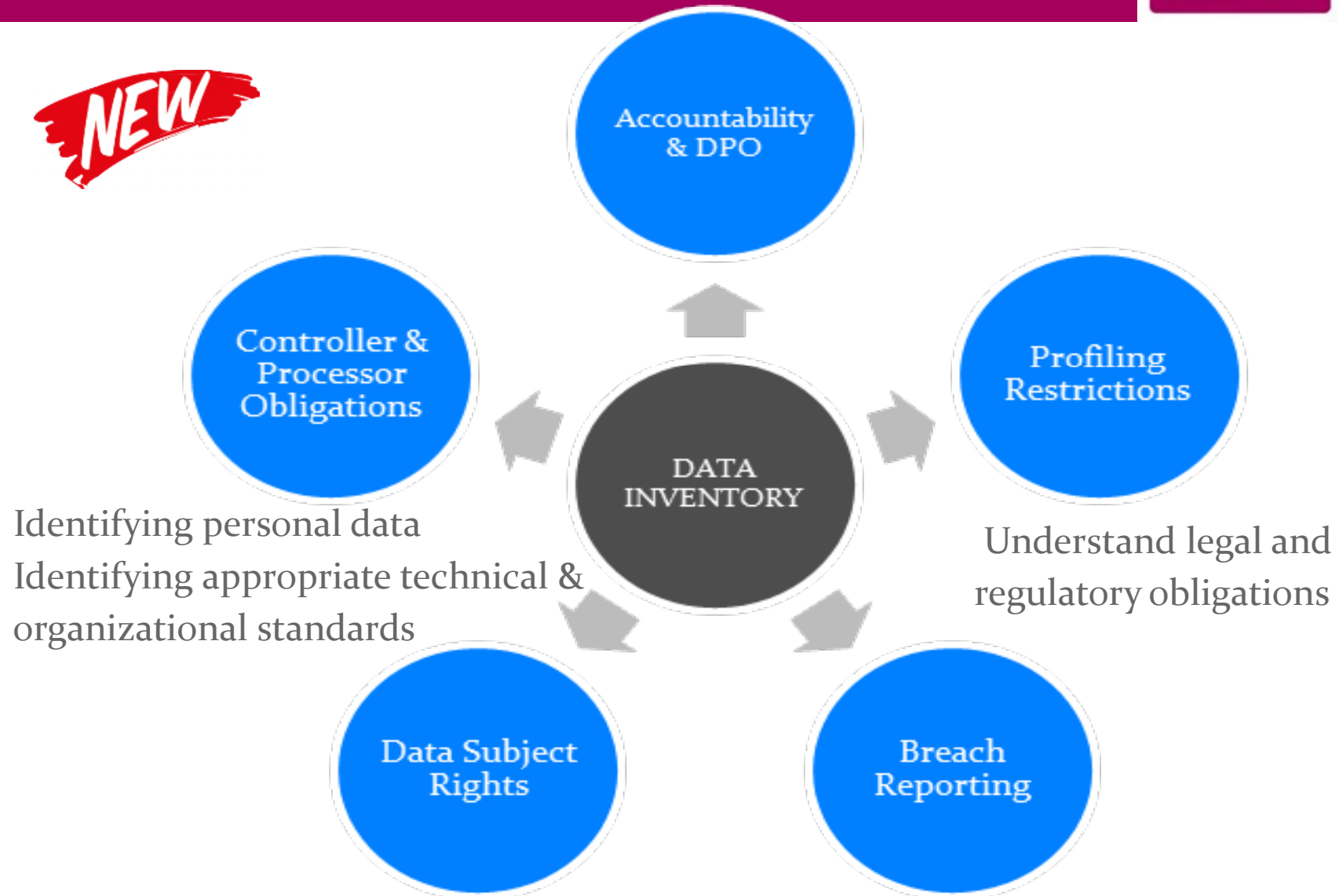
Technological codes

Developed by IT providers when a new technology arises

e.i. Walkie-Talkie privacy code

Data landscape

NEW



California Consumer Privacy Act of 2018



- **Who Is Protected by the CCPA?**
- Protects “consumers,” and natural persons; are California residents
- The rights do not extend to legal persons e.g. corporations (4(1).[1])
- **Who or What Is Regulated by the CCPA?**
- A business that collects “personal information” from consumers
- Does business in California for profit /shareholders financial benefit
- Must meet or surpass one of the following thresholds:
 - \$25 million in annual gross revenue
 - Receive for commercial purposes, sell, or share for commercial purposes, the personal information of 50,000 or more consumers
 - Derive +50% of annual revenue from selling consumers’ personal information
- *Personal information is information that identifies, relates, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.*

California Consumer Privacy Act of 2018 compared to GDPR (1)



- **CCPA** excludes “publicly available information,” (lawfully available via government records).
 - **The GDPR** identifies “special categories of personal data” that are entitled to extra protections,
- CCPA recognizes personal information as a single category that may be composed of different kinds of data. Art. 9.
- **The CCPA** regulates businesses (statutorily defined) under the law.
 - **The GDPR** regulates the “controllers” who determine what personal data is collected and the “processors” who process personal data on behalf of controllers. Art. 4(7)-(8).
- **The CCPA** is limited to the location/residency (California) of the consumer. Focused on protecting the rights of California resident

California Consumer Privacy Act of 2018 compared to GDPR (2)



- **The GDPR** regulates businesses in the EU, Regardless of the personal data collected concerns EU citizens or not.
- **The GDPR** also regulates businesses located outside the EU that offer goods or services in the EU and process the data of EU citizens
- **Like the CCPA, the GDPR** allows data subjects to request information about the personal data that the controller has collected about them, though it distinguishes personal data obtained from the data subject and personal data obtained from outside parties.

California Consumer Privacy Act of 2018 compared to GDPR (3)



- CCPA grants consumers the right to request that businesses delete any personal information that the business has collected from the them.
- The CCPA does not grant consumers the right to request that a business delete personal information obtained from someone other than the consumer
- The CCPA indicates circumstances where a business need not comply with a consumer request to delete personal information.
 - The GDPR contains a provision, the “right to be forgotten allowing data subjects the right to have personal data concerning them deleted by the data. Data subjects enjoy this right regardless of the source from which the data was obtained. Art. 17.
 - The GDPR’s right to be forgotten is also qualified by exceptions

California Consumer Privacy Act of 2018 compared to GDPR (4)



CCPA requires that businesses that sell consumer personal data, or disclose personal information for a business purpose, provide data regarding these practices to the consumer upon request.

The consumer may seek the following information:

- The categories of personal information collected
- The categories of personal information that were sold, and the category/categories of 3rd parties to whom the information was sold
- The categories of personal information that the business disclosed

The CCPA allows consumers to demand that businesses cease and desist from selling their personal information, referring to this as “the right to opt out.” The CCPA adopts an “opt in” when selling a child’s personal information: here affirmative parental consent is required

California Consumer Privacy Act of 2018 compared to GDPR - Summary (5)



Both GDPR and CCPA seek to protect personal privacy, however:

1. The CCPA is a statute about disclosure and transparency applicable to Californian residents only.
2. It requires businesses to proactively disclose to consumers the kinds of personal information that they collect and to tell consumers if they plan to sell consumers' personal data.
3. It gives consumers the right to request the specific personal data that businesses have collected about them, to request that the information be deleted, and to opt out of the sale of their personal information to third parties.
4. The liability portion of the statute subjects covered businesses to lawsuits when their failure to “implement and maintain reasonable security procedures and practices” results in the unauthorized disclosure of personal information

California Consumer Privacy Act of 2018 compared to GDPR - Summary (6)



Both GDPR and CCPA seek to protect personal privacy, however:

1. The CCPA has relatively little to say about what security procedures and practices are “reasonable.”
2. The GDPR is a more comprehensive, “General” regulation. It has wider outreach and goes into greater detail as to how personal data should be protected, particularly:
 1. Data controllers & processors generally must maintain specific records regarding their processing of personal data, use encryption, undertake data protection impact assessments prior to using personal data and must designate a data protection officer where the controller or processor processes personal data on a large scale.
 2. GDPR grants rights to consumers that the CCPA does not. The GDPR gives data subjects the right to request that those who control their personal information rectify any mistakes contained therein, the right to request that restrictions be placed on the use of their data

1:30 – 3:30



Businesses Impact of global data protection legislation on a company's operations:

Operations, branches and servers in other Caribbean islands- may also be subject to Data Protection legislation. Part I/II

Specific to the jurisdictions as a data controller

... but, where?



in the EU

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

outside the EU

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

Worldwide privacy laws



HIPAA Health Insurance Portability and Accountability Act 1996/2009



Personal information

Medical records
Health status
Healthcare payment details

Key provisions

Right to request and correct personal medical information
Limited the conditions to disclose health information
Develop a privacy policy
Appoint a privacy official

Covered entities

Providers of health plans (insurers)
Health care providers (hospitals, dentists)
Subcontractors (claims processing, health analysis)

Penalties

Civil
100 to 50k USD per occurrence
Max 1.5M USD
Criminal
Imprisonment

Worldwide privacy laws



FCRA Fair Credit Reporting Act

1970 / FACTA 2003



Personal information

Personal financial information
Consumer files
Consumer-reporting information

Key provisions

Right to request and correct personal information
Right to opt-out for marketing contact
Limited disclose on reports
Real disposal of information

Covered entities

Credit reporting agencies

Penalties

Civil
1K USD per consumer damage
Max 2.5k USD per violation
Victims of identify theft can file a separated law suit
Criminal

Worldwide privacy laws



US Privacy Act

1974



Personal information

Personal data of US citizen and lawful foreign residents
Social security number usage

Key provisions

No disclosure without Consent rule
Right to receive a notice for voluntary or mandatory collection of personal information

Covered entities

US Federal government agencies
Government contractors

Penalties

Civil
up to 5K USD for willful disclosures
Criminal
for the agency officer

Worldwide privacy laws



Australian Privacy Act

2012



Personal information

Information or opinion about an individual whose identity is apparent or can be reasonable ascertained
Health, employment and credit data

Key provisions

Choice to opt-out of any direct marketing
Allows the use of pseudonyms
Limit international data exports

Covered entities

Most government sectors
Some private organizations

Penalties

Civil
up to 140K EUR for individuals
up to .7M EUR for companies

Worldwide privacy laws



PIPEDA Personal Info Protection and Electronic Doc Act

2012/15/18



Personal information

Any factual or subjective information, recorded or not, about an identifiable individual

Key provisions

10 fair information principles
Document all personal information handling practices
Appoint a privacy officer
Limit international data exports to countries w/same protection

Covered entities

Private organizations, covers personal information in the course of a commercial activity

Penalties

Civil
up to 163K EUR per violation

Worldwide privacy laws



BDSG Federal Data Protection Act

1995



Personal information

Personal relationships: name, address, e-mail, IP address
Factual circumstances: income, taxes, ownership
Sensitive personal data: health, racial, political, lifestyle

Key provisions

Extended the EU directive
Explicit consent in advance
Notify data breaches
Provisions for email marketing as well as online privacy, covering cookies, traffic and location data

Covered entities

Both government and private sectors

Penalties

Civil
up to 300K EUR per violation
Criminal
Imprisonment up to 2 years

Worldwide privacy laws



IT Amendment Act

2008/2016



Personal information

related to a natural person which either directly or indirectly or in combination with other information can lead to identification of an individual

Key provisions

Implemented reasonable security practices and procedures (ie. ISO 27001)

Covered entities

Public and private companies, NGOs, national and foreign

Penalties

Civil
up to 622k EUR

1:30 – 3:30



Businesses Impact of global data protection legislation on a company's operations:

Operations, branches and servers in other Caribbean islands- may also be subject to Data Protection legislation . Part II/II

Specific to the jurisdictions as a data controller

Will GDPR effect Cayman-domiciled funds?



- GDPR applies to EU firms but also to firms established outside of the EU where the processing of personal data involves offering goods or services to EU ‘data subjects’
- Consequences depend on the carried out activities
- if a fund has European investors or is actively marketing to European investors it is in the GDPR scope
- If the Cayman fund is in the scope of the GDPR, it is necessary to appoint a ‘representative’ in the EU to meet its GDPR obligations
- The EU representative will be the point of contact for any queries from the supervisory or oversight authorities or the data subjects about the fund’s activities

Funds in the scope of GDPR?



- Investment funds under any EU Financial Regulator will be considered data controllers about the EU investor data
- Service providers to the Investment funds will be regarded as data processors
- In certain circumstances, the service providers can also be considered as data controllers

What do Cayman-domiciled funds or companies need to do?



- Draft and maintain a Data Protection Policy;
- Complete the data inventory to identify personal data processed by the fund and the lawful/legal basis for processing the data;
- Due diligence of data processors, e.g. the fund administrator;
- Training/awareness- informing and advising the board of their respective obligations under the GDPR;
- Act as the fund's EU representative where necessary.

1:30 – 3:30

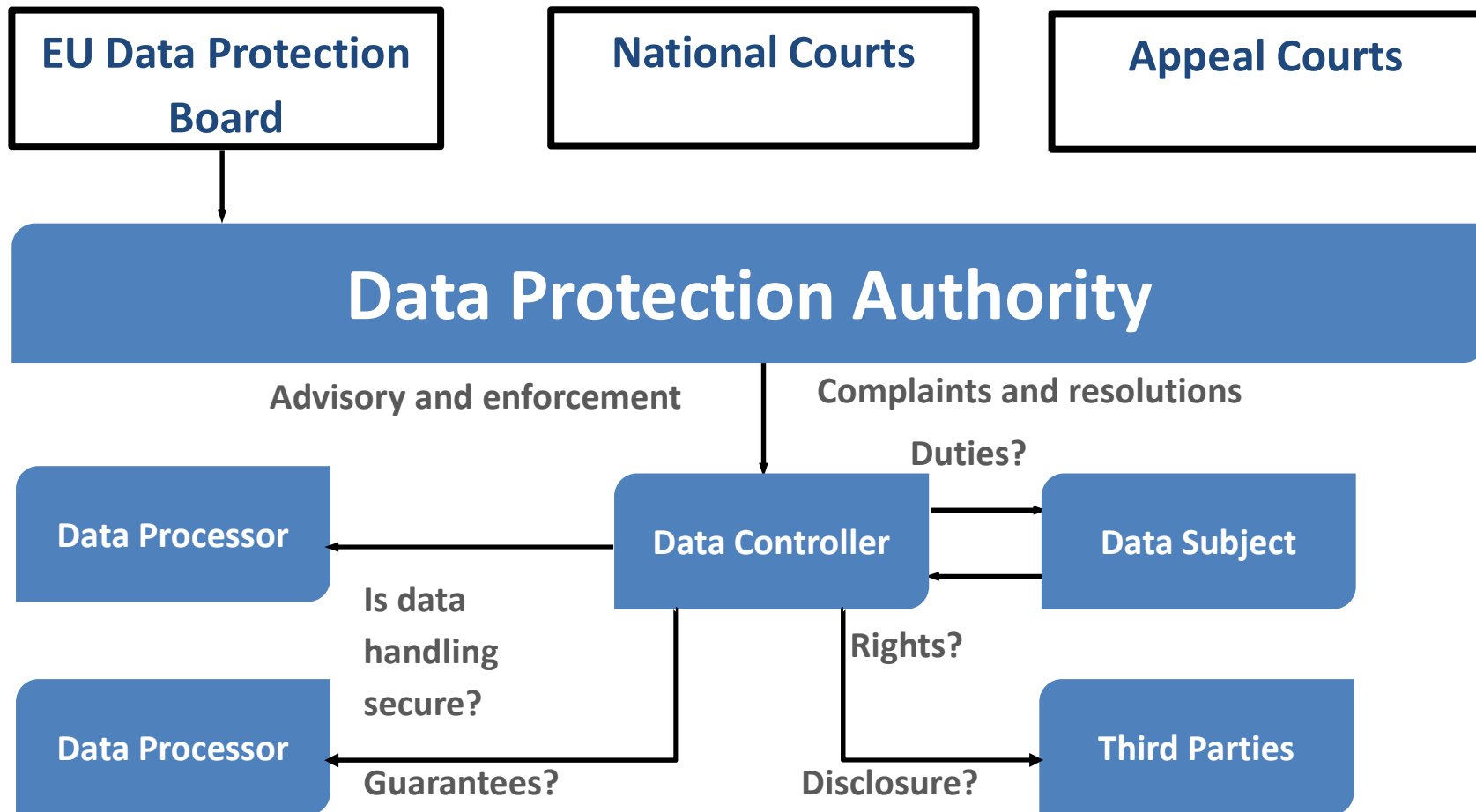


Businesses Impact of global data protection legislation on a company's operations:

Operations, branches and servers in other Caribbean islands- may also be subject to Data Protection legislation

Specific to the jurisdictions as a data controller

Organization



Step 1. The primary duties of data Controllers



- **The same as any other Data Privacy & Protection mandate, the Aata Controller or Processor must highlight the following issues.**
- 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”);
- The Controller must determine if an EU representative must be appointed

Step II. Data controller responsibilities



- **NEW** 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 **NEW**
- exercise overall control
 - Data protection by design and by default
- notify breaches to the oversight authorities

Step 3. Privacy principles (Controller)



Transparency

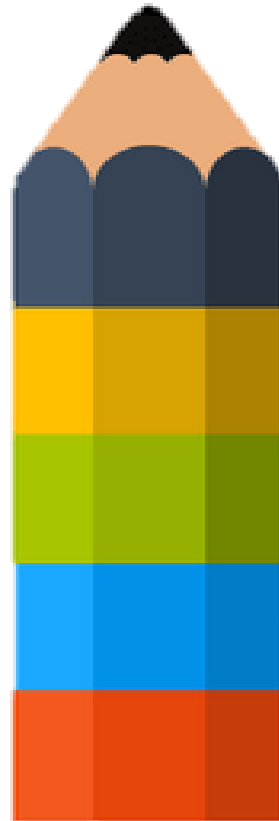
Data controllers have understandable policies for data subjects and third parties

Enforcement

Data controllers should give assurance/certification on privacy policies and regulations

Security

Data controllers must protect the access and modification of personal information



Minimal collection

Data controllers obtain personal data, only for a limited purpose

Minimal use

Data controllers' use of personal information is only for the obtained consent

Accountability

Data controllers are responsible for complying the privacy regulations and principles

Disclosure

Data controllers can transfer and disclose personal information to third parties based on consent

Privacy by design

Data controllers assure privacy by design on the development of new products, processes or services

Privacy principles (data Subject)



Consent

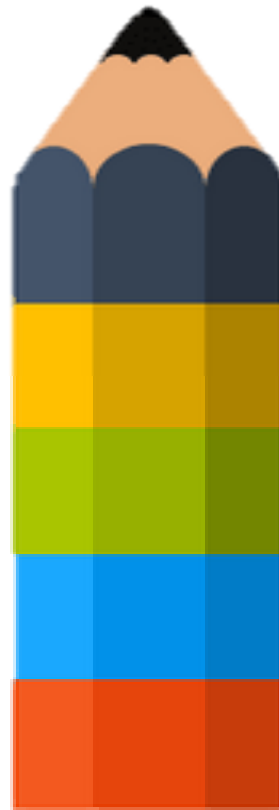
Data subjects understand and explicitly or implicitly agree with the uses of personal information

Notice

Data subjects receive a clear statement on the reason, retention period, access and the rights of personal information

Right to be forgotten

Data subjects are allowed to erase personal information from data controllers and third parties



Anonymity

Data subjects have the option of not identify themselves

Access and correction

Data subjects access and correct personal information to ensure is accurate, complete and relevant

Choice

Data subjects make an informed decision regarding the permits on personal information

Sensitivity

Data subjects are more sensitive to personal data involving health, lifestyle, criminal records..

3:45-17:00



Extra-Territorial scope: GDPR apply to organisations:

- Processing personal data as a controller or processor in your respective jurisdiction
 - regardless of whether the processing takes place in the respective jurisdiction
- Processing personal data as a processor on behalf of a client controller subject to GDPR even if based outside the Jurisdiction,
- Process personal data about data subjects who are in the respective jurisdiction in relation to:
 - offering goods or services to them, irrespective of payment by them,
 - monitoring their behavior taking place within the jurisdiction

Does the GDPR apply to me?

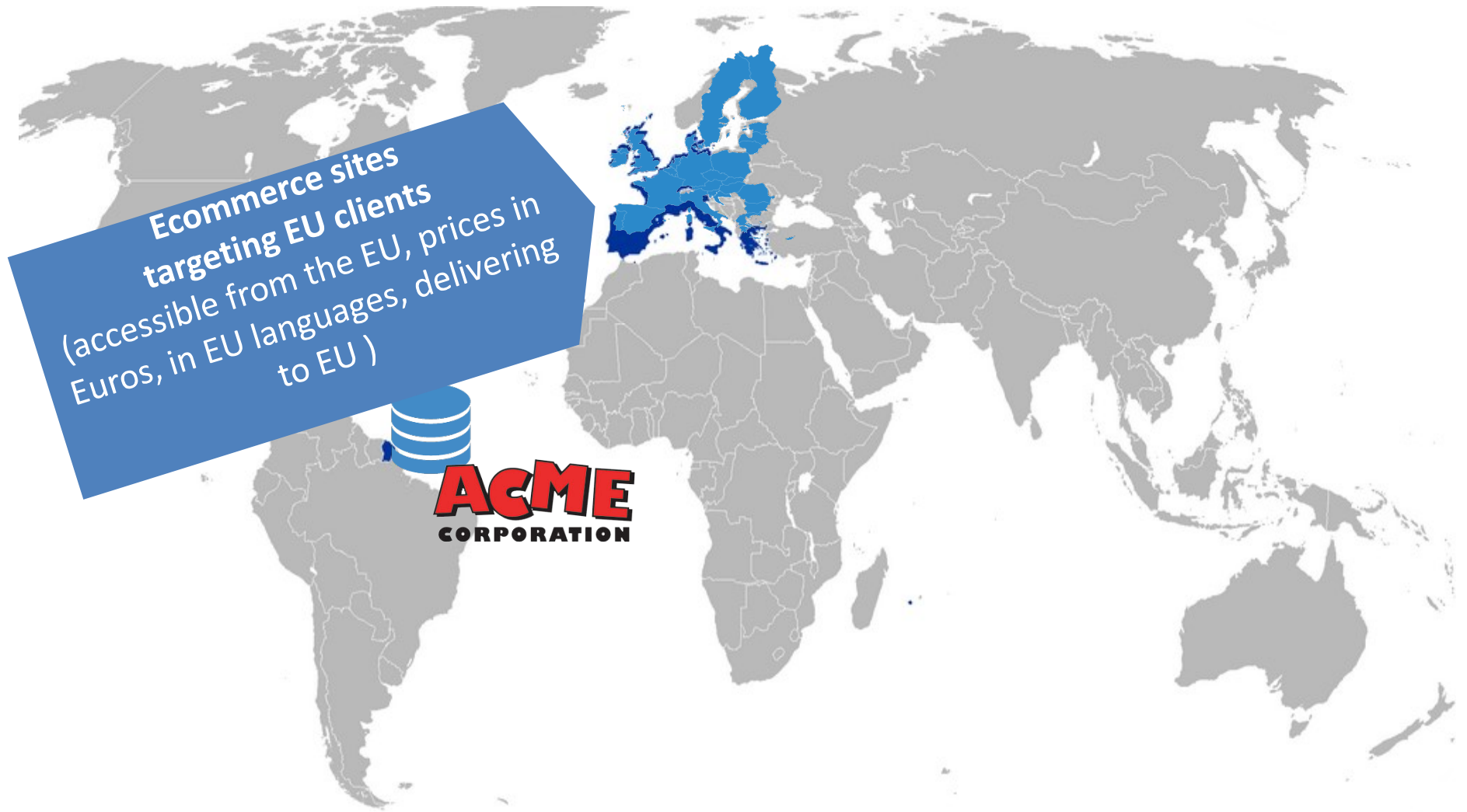


Does my organization offer goods or services to EU residents?

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

Does my organization have employees in the EU?

Extra-territorial application



Cross-border processing



When the controller or processor is established in more than one Member State;

- Processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union or
- Processing of personal data takes place in the context of the activities of a single establishment of a controller or processor in the Union
 - but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

Example I



- What happens if a Jamaican based vendor renders data hosting services on behalf of a corporation located in the U.S., and the data set comprises a large collection of personal data, mostly related to EU data subjects?
- The key issue is around Article 3, Section 2 of the GDPR in relation to the question of whether services are offered to individuals in the EU.
- The scenario described above has nothing to do with targeting EU people from the inception by offering services in order to boost sales.
- Hence, the GDPR does not apply.

Example II



- The Jamaican company (Company A, the processor) offers data hosting services to another company (Company B, the controller).
- At face value, this scenario would not need to be GDPR compliant.
- However, if Company B (the controller) also acts on behalf of other legal entities within a group, and if personal data is transferred from these group legal entities to Company A (the processor),
- The arrangement may be caught by the GDPR.
- If one such group legal entity has an establishment in the EU, the GDPR comes into play via Article 3, Section 1.
- Therefore, all companies should closely review their service contracts from the perspective of group member involvement.
- A Jamaican company can be under GDPR by entering into a service agreement based on this example

How do extra-territorial provisions apply to processors?



- A Jamaican company is offering a consumer cloud service in the EU would clearly be affected by the GDPR (Article 3, Section 2).
- However, the overseas processor is only acting on the instructions of a controller, so would not be dealing with individuals in the EU of its own option.
- This circumstance does not shield it from the GDPR in general.
- The processor might still be caught where it is a sub-processor of a principal processor based in the EU.
- This is because the processor is processing personal data *in the context of the activities of* a controller or processor in the EU.
- Any provision of services to an entity in the EU might bring the overseas processor within the scope of the GDPR and in this instance the overseas processor(s) must be GDPR compliance

Non-GDPR compliance can be accomplished by:



Organization seeks to ensure that the GDPR does not apply to them

- Avoid giving the impression that they offer goods or services to users in the EU.
- Remove the top-level domain names of EU member states from the organization`s website, e.g. “de.”
- Not offering services to EU users on websites or via marketing materials.
- Removing all EU countries from website address fields or drop-down menus.
- Not using EU member state languages.

Non-GDPR compliance can be accomplished by:



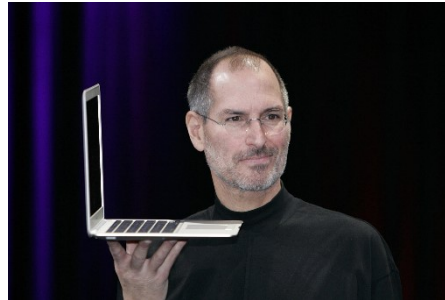
Organizations seeking to ensure that the GDPR does not apply to them:

- Not referring to individuals in a EU member state in order to promote goods and services, e.g. if the organization's website talks about German customers who use the related products.
- Not allowing users hosted in the EU to sign up for services
- Not offering shipments to the EU or payment in euros.
- Including disclaimers on the landing page of the organization`s website stating that neither goods nor services are envisaged as being offered to users in the EU.
- Not entering into direct contractual relationships with EU end users/customers.

Data Privacy and Protection Perceptions



**What the
friends
think**



**What
the mom
thinks**



**What
society
think**



**What
the boss
thinks**



**What the
family
thinks**



**What
we think**

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



Day II

Data Protection and You



February 6 2019

The Obligations of Data Processors



by



Venue: The Jamaica Pegasus Hotel, Windward Suite



Jamaica Stock Exchange
e-Campus

Agenda



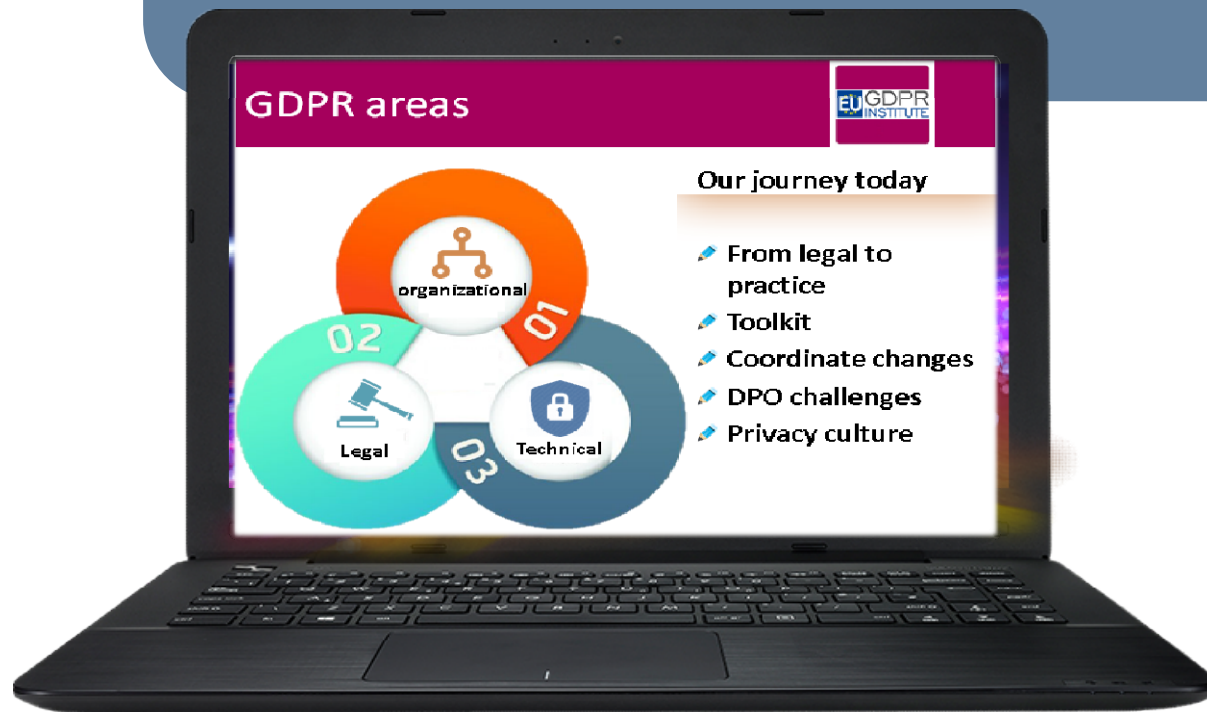
Day II. The Obligations of Data Processors (Stakeholders)

	7:45 - 8:15	Registration	
	8:15 - 9:30	<p>Direct Processor obligations: Data processors have direct obligations under the GDPR when processing on behalf of client data controllers in relation to matters including data security, international data transfers, appointment of sub-processors and security breach notification.</p> <p>Data Controller obligations: Data Controllers must implement appropriate technical and organizational measures to protect the security of data.</p> <p>Presenter: Roeder Jens</p>	
	9:30 - 10:30	<p>International transfers: The GDPR codifies new adequate safeguards for data transfers outside the respective jurisdiction, including:</p> <ul style="list-style-type: none"> • binding corporate rules • standard contractual clauses approved by a local supervisory authority • approved codes of conduct • approved certification mechanisms. <p>Presenter: Kersi F. Porbunderwala</p>	
	10:30 - 10:45	BREAK	
	10:45 - 12:00	<ul style="list-style-type: none"> • Preparing for data protection regulations • Spearheading the move to compliance with the (DPR) • Evaluating the need to carry out a thorough audit of all of an organisation's processing of personal data. • The need for Data Protection Officers (DPO) • Changing the cultural mindset • Embracing the change in cultural mindsets <p>Presenter: Kersi F. Porbunderwala</p>	
	12:00 - 1:00	LUNCH	
	1:00 - 2:30	<ul style="list-style-type: none"> • Conducting an IT Risk Assessment • Deploying & documenting implementation of tools such as Notices to address information security gaps in your own organisation. • Creating & Implementing Data Protection Policies / Initiatives • Setting up procedures and policies to maintain the organisation's full programme management • Establishing efficient procedures for Privacy Impact Assessments, Subject Access Requests and data breaches, etc. <p>Presenter: Marcelle Smart - tTech</p>	
	2:30 - 3:30	<ul style="list-style-type: none"> • The promulgation of the Jamaican Data Protection Act <p>Presenter: Justine Collins HMF</p>	
	3:30 - 3:45	BREAK	
	3:40 - 5:00	<p>Discussion workshop</p> <ul style="list-style-type: none"> • Identify the potential breaches in your current Organisation. • Roles & Responsibilities of the Data Protection Officer & • Conducting a Personal Data Inventory Audit. 	

Access to the presentation



<https://www.eugdpr.institute/feb2019-jamaca/>



What you will receive?



8:30 - 9:30



- **Direct processor obligations:**

- Data processors have direct obligations under the GDPR when processing on behalf of client controllers in relation to matters including
 - data security,
 - international data transfers,
 - appointment of sub-processors and
 - security breach notification.

... but, by who?



Controller

Who decides
why the personal
data is needed

Processor

Who processes
the data

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

Natural or legal person
including the government

Step 1: Review contracts



Controller



Processor

Data exporter when processing is outside de EU

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

Audits and certifications

There are “model clauses” for data exports

Negotiate the cost of GDPR compliance in fees

Foresee dispute resolutions and compensation clauses

Step II. Data processor responsibilities



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

Step 3. The role of the processor in The Main Establishment



- ✎ a controller with central administration in more than EU state
- ✎ The processing of personal data is taken in EU establishments and has the power to decide on the main establishment;
- ✎ a processor with establishments in more than one member State,
 - ✎ the place of its central administration in the Union
 - ✎ if the processor has no central administration in the Union
- ✎ the establishment of the processor where the main processing activities in the context of an establishment, of the processor take place to the extent that the processor is subject to specific obligations under the GDPR mandate

Step 4. Demonstrate compliance



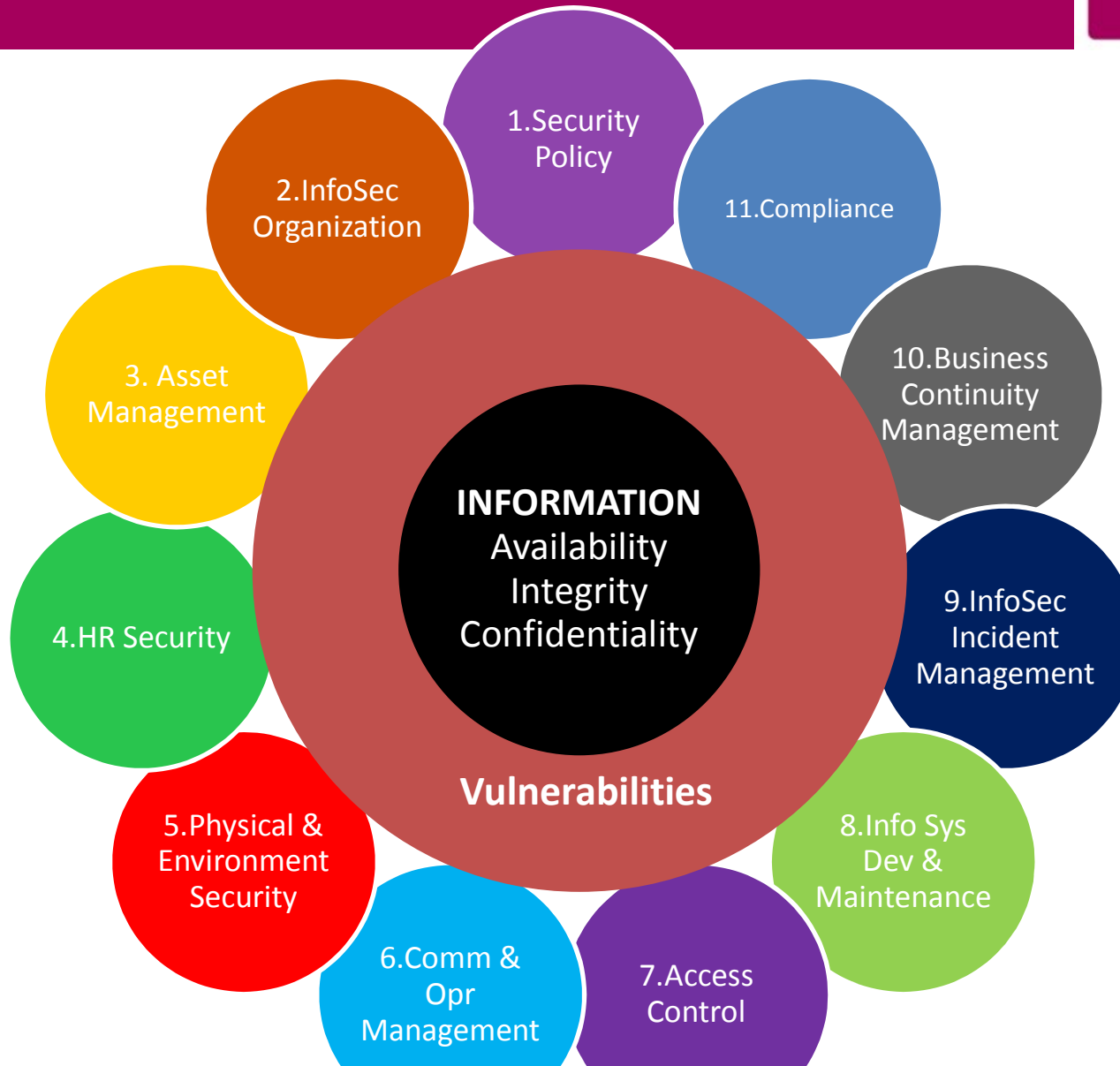
- ✎ For non-EU data controllers/processors, mandate to designate a representative in the EU and external communication in privacy notes and website (art. 27)
- ✎ Privacy Officer, Privacy Counsel, CPO, Representative

8:30 - 9:30



- Direct processor obligations:
- Data processors have direct obligations under the GDPR when processing on behalf of client controllers in relation to matters including
 - data security,
 - international data transfers,
 - appointment of sub-processors and
 - security breach notification.

Domains of ISO 27001



Privacy and security (protection)



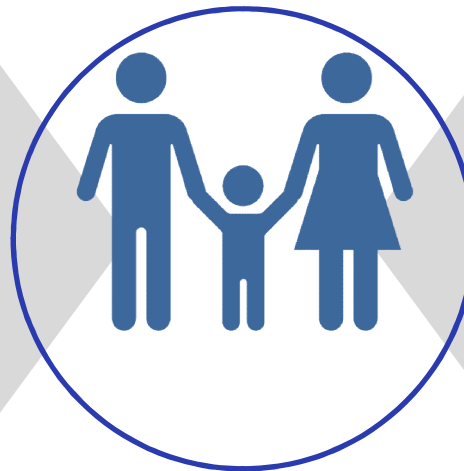
PRIVACY MANAGEMENT

Implement a Privacy Program with Central Compliance Record Keeping

- Accountability
- Consent Management
- Privacy by Design, PIA, DPIA
- Records of Processing / Data Map
- Incident Response Management
- Vendor / Supplier Risk Management
- Cookie Law Compliance
- Subject Rights Management
- Privacy Data Discovery
- Anonymization/Pseudonymization

Individual

Privacy



Data

Security

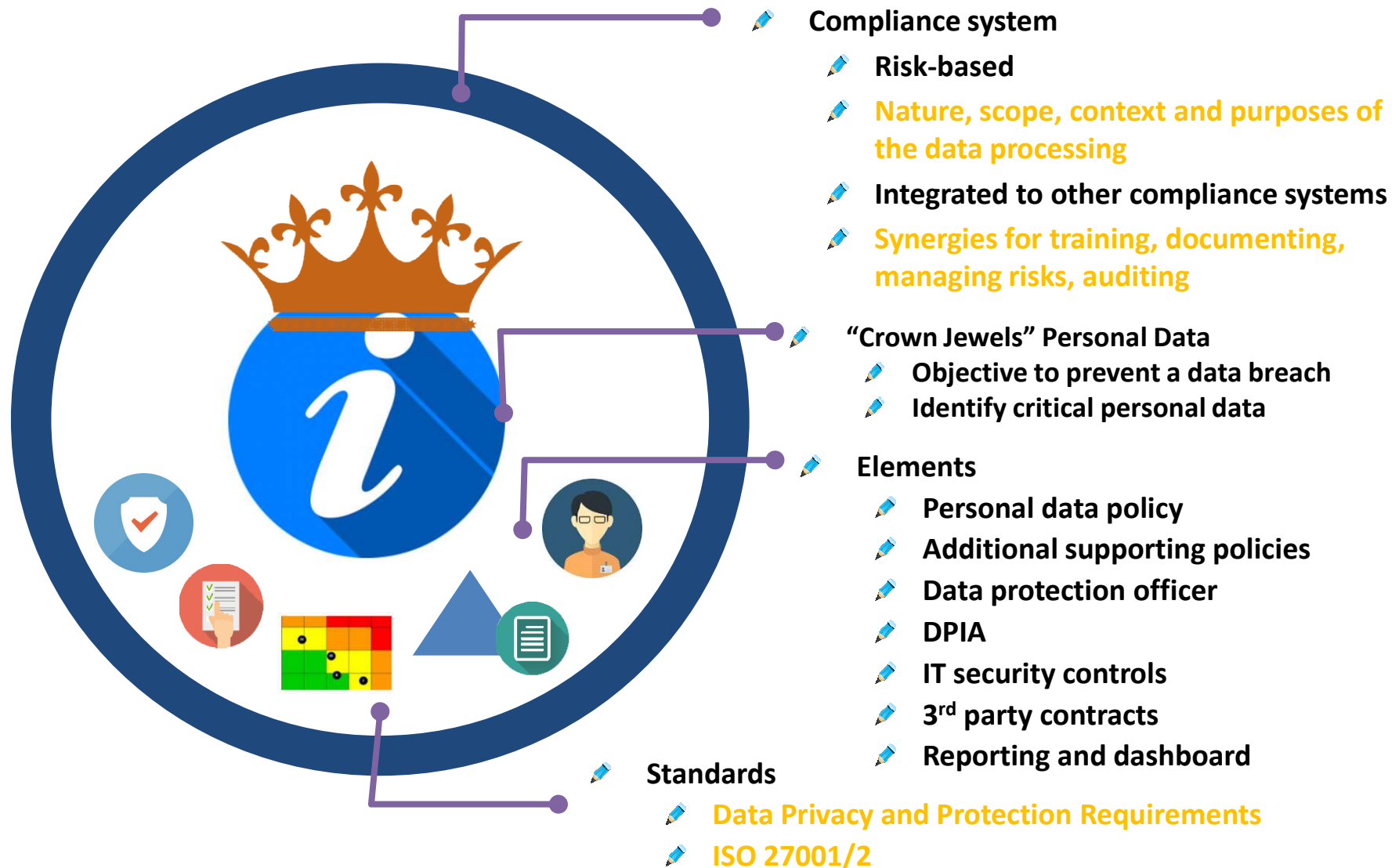
INFORMATION SECURITY

Confidentiality, Integrity, Availability (CIA)

- Data Loss Prevention (DLP)
- Data Centric Audit and Protection (DCAP)
- Governance Risk Compliance (GRC)
- Enterprise Mobile Management (EMM)
- Identity and Access Management (IAM)
- Information Governance (IG)

Data protection is needed for privacy

Data Protection Management System



Step 5: Data security program



Encryption of personal data

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



Security measures

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



Resilience

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



Regular security testing

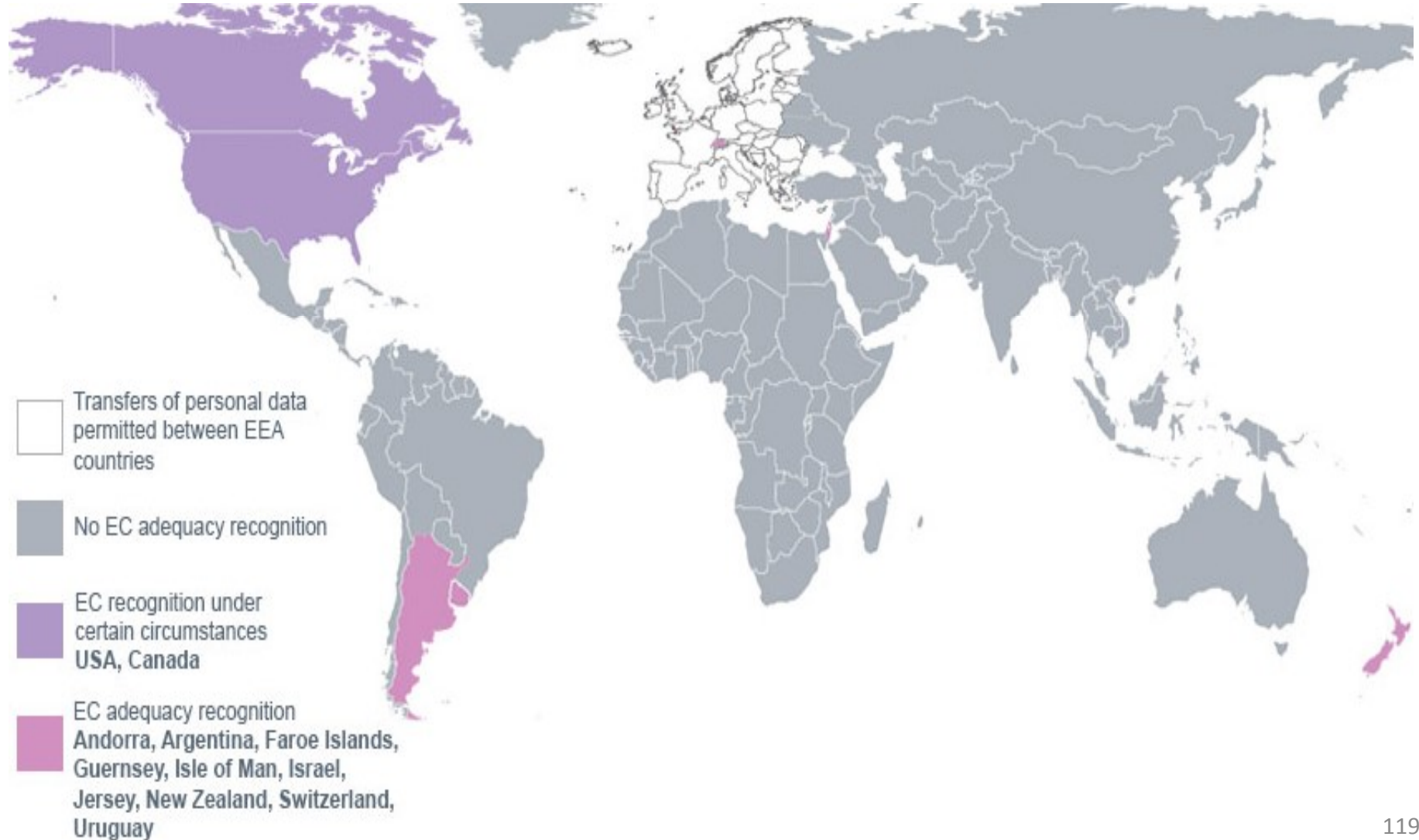
- Assessment of the effectiveness of security practices and solutions
- Penetration, network and application security testing

8:30 - 9:30



- Direct processor obligations:
- Data processors have direct obligations under the GDPR when processing on behalf of client controllers in relation to matters including
- data security
- international data transfers
- appointment of sub-processors and
- security breach notification.

International data transfers



International Data Transfers



- Cloud services may transmit data to a third country#
- Controllers will have to meet the usual requirements of the Regulation with regard to international data transfer.
- This includes having a legitimate reason for the transfer, asserting the data protection principles, applying appropriate controls or measures to protect the personal data (such as model contract clauses¹), and informing the data subject of the transfer of their personal data.

¹https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en

8:30 - 9:30



- Direct processor obligations:
- Data processors have direct obligations under the GDPR when processing on behalf of client controllers in relation to matters including
 - data security
 - international data transfers
 - appointment of sub-processors and
 - security breach notification.

Evaluating sub-processor risks



- A compliance team tasked with reviewing sub-processors under the GDPR could be muddled by the implications of contracting with a Jamaican software vendor.
- Reviewing the answers provided on a vendor questionnaire or the assurances of security commitments regarding encryption
- How does an EU data processor/controller under the GDPR evaluate a Jamaican sub-processor?
- Jamaican law provides clarifications on individual privacy and communications encryption.
- What would happen if the EU's personal data protection regulations ever came into conflict with Jamaican anti-encryption position and antipathy toward data privacy
- European organizations would identify vendors headquartered or operating in Jamaica and watch for any further news about the effects of the local law(s)

8:30 - 9:30



- Direct processor obligations:
- Data processors have direct obligations under the GDPR when processing on behalf of client controllers in relation to matters including
 - data security
 - international data transfers
 - appointment of sub-processors and
 - security breach notification.

Why GDPR is important?



Fines!



NEW

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

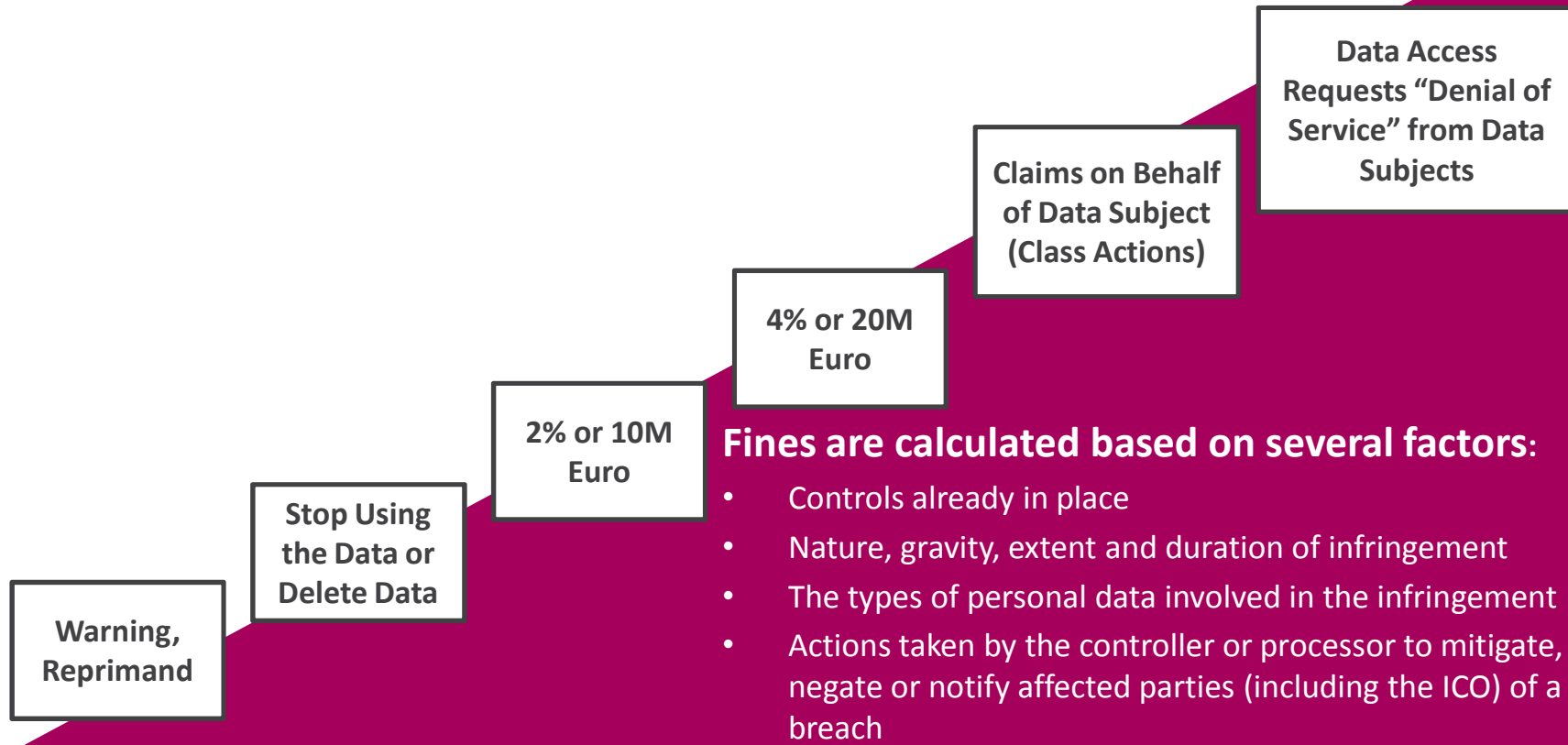
Failure to implement core principles, infringement of personal rights and the transfer of personal data to countries or organizations without adequate protection

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

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

Reduced with appropriate technical and organizational measures

When do the fines stop



Remedies + Liabilities + Penalties

Step 7: How to notify a data breach?



Data breach

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



When to notify

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



What to notify

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



Whom to notify

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

Example of risk registry



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

9:30 – 10:30



- **International transfers:** The GDPR codifies new **adequate safeguards for data transfers** outside the respective jurisdiction, including:
 - binding corporate rules
 - standard contractual clauses approved by a local supervisory authority
 - approved codes of conduct
 - approved certification mechanisms.

Define adequate safeguards



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

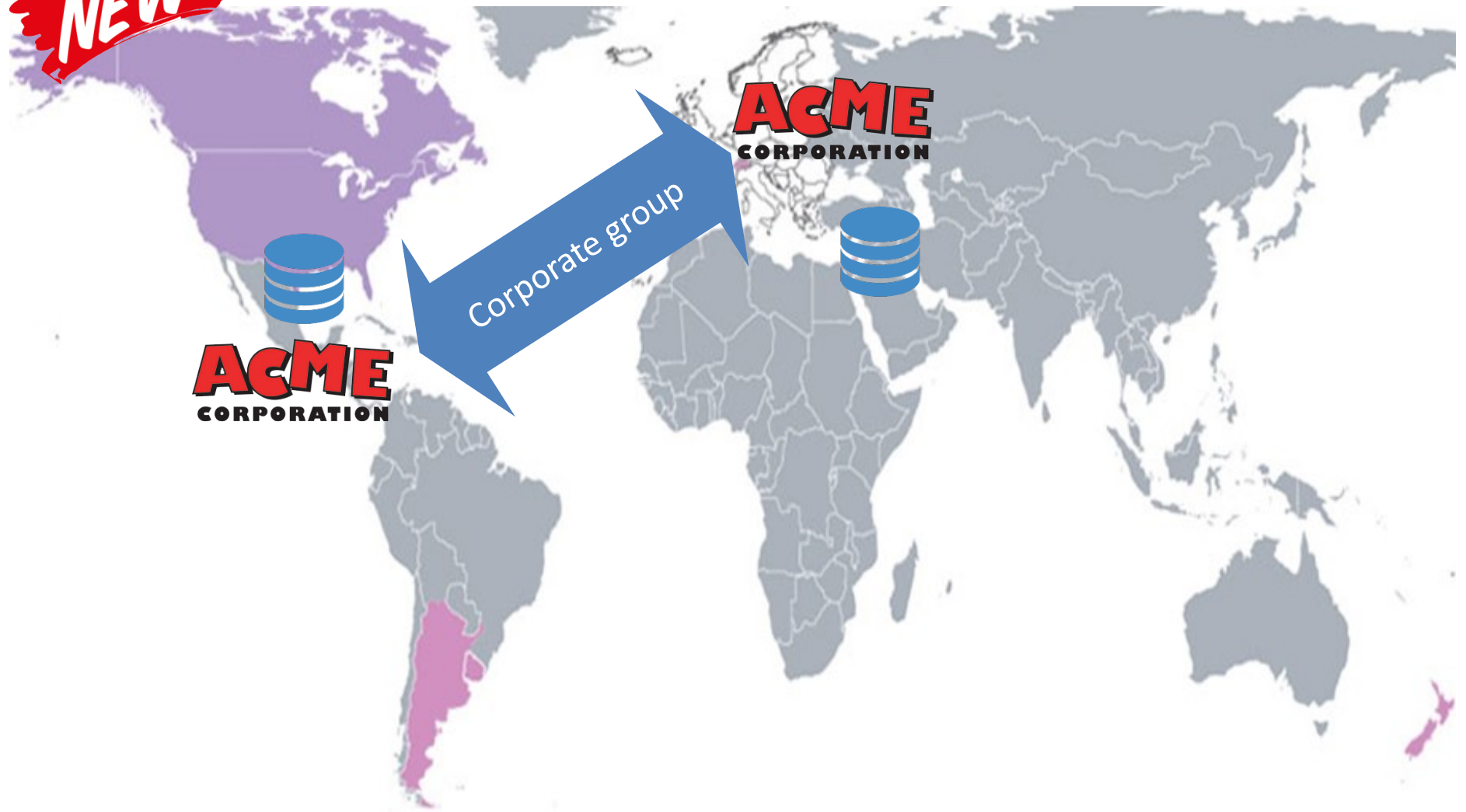
9:30 – 10:30



- **International transfers:** The GDPR codifies new **adequate safeguards for data transfers** outside the respective jurisdiction, including:
 - binding corporate rules
 - standard contractual clauses approved by a local supervisory authority
 - approved codes of conduct
 - approved certification mechanisms.

Binding corporate rules

NEW



Step 4: Binding corporate rules



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

Binding Corporate Rules



- Personal data protection policies which are adhered to by a controller or processor
the policies are related and established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor.
- The data transfers are to one or more third countries within a group of undertakings or group of enterprises engaged in a joint economic activity

9:30 – 10:30



- **International transfers:** The GDPR codifies new **adequate safeguards for data transfers** outside the respective jurisdiction, including:
 - binding corporate rules
 - standard contractual clauses approved by a local supervisory authority
 - approved codes of conduct
 - approved certification mechanisms.

Standard Contractual Clause



- The Article 29 Working Party has released its working draft on standard contractual clauses for the transfer of personal data from an EU data processor to a non-EU data sub-processor.
- Standard contractual clauses for the transfer of personal data to processors in third countries from an EU data processor to a non-EU data sub-processor.
- The working document amends or supplements existing model clauses currently in place under the Data Protection Directive.
- <https://ec.europa.eu/newsroom/article29/news-overview.cfm>

standard model clauses



- The standard model clauses incorporate information security requirements and sub-contracting liability concerns by striking a balance between company concerns and the rights of data subjects.
- if data processors decide to make modifications to previously agreed data processing contracts or decide to sub-contract the processing operations, then the amended contracts will need to comply with the newly issued model clauses
- The clauses require technical and organizational security measures to be applied by the data processors established in third countries.
- These measures should take into account existing data protection laws and balance the costs to companies in order to protect such data with security precautions.

standard model clauses



- The data processor will remain liable for violations by sub-processors.
- The model clauses also cover sub-processing to ensure that if the data processor subcontracts his processing duties, such subcontractors will ensure that the personal data continues to be protected (Clause 11).
- This is complemented by third-party beneficiary rights granted to the data subjects to allow for their individual enforcement of the contract (Clause 3).
- This focus on individual rights is expanded by the data subject's rights to make claims and pursue compensation from the data controller for any breach by the data processor or sub-processors of its obligations in case of bankruptcy or insolvency proceedings concerning the exporter (Clause 6).

Demonstrate compliance



Data transfers (arts 45 to 49)

- ✎ Records of the transfer mechanism used for cross-border data flows
 - ✎ standard contractual clauses, binding corporate rules, EU-US privacy shield, approvals from regulators
 - ✎ authorized transfer (e.g. consent, performance of a contract, public interest)
 - ✎ linked to the data inventory

9:30 – 10:30



- **International transfers:** The GDPR codifies new **adequate safeguards for data transfers** outside the respective jurisdiction, including:
 - binding corporate rules
 - standard contractual clauses approved by a local supervisory authority
 - approved codes of conduct
 - approved certification mechanisms.

Step 7: Code of conduct & certification



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

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



10:45 - 12:00



- Preparing for data protection regulations
- Spearheading the move to compliance with the (DPR)
- evaluate the need to carry out a thorough audit of all the organisation's processing of personal data.
- The need for Data Protection Officers (DPO)
- Changing the cultural mindset
- Embracing the change in cultural mindsets

Preparing for data protection regulations (DPR)



- Appreciate the impact DPR is likely to have
- Identify areas that could cause compliance problems
- Start by looking at your organisation's risk register
- Review the significant resource implications
- New elements with significant enhancements, some first, some different
- Map out which parts of the DPR will have the greatest impact on your business
- Gain 'buy in' from key people in your organisation.
- New procedures in place to deal with the transparency, rights, ownership
- Documentation that data controllers can demonstrate accountability
- Compliance with the areas that need a review Governance approach
- Review all contracts and other schedules where personal data is shared
- Provisions relating to profiling or children's data
- Compliance difficult if delayed till the last minute

12 steps for compliance



1

Awareness

Check if you are a Competent Authority under Schedule 7 of the DP Act 2018 or have statutory functions for any of the law enforcement purposes. If so, you should make sure that key people in your organisation are aware that as of May 2018, the law has changed.

2

Information you hold – mapping

You should document what personal data you hold, where you hold it, where it came from, who you share it with and who is responsible for it. Identify what personal data is being processed under Part 3 (of the DP Act 2018) and what is being processed under other parts of the Act and GDPR. Do you work jointly with other organisations? Do you use data processors? You may need to organise an information audit and review any contracts or agreements.

be adequate, relevant, and not excessive, in relation to the purpose for which it is processed;

be processed fairly and lawfully;

3

Lawful basis for processing personal data

You should identify the lawful basis for your processing activity, document it and update your privacy notices to explain it, using clear and plain language.

4

Consent

If you rely on consent you need to consider whether this is appropriate or whether you should use another lawful basis. If consent is appropriate then you should review how you seek, record and manage consent and whether you need to make any changes. You will need to refresh existing consents if they do not meet the standard required.

be obtained only for one or more specified and lawful purposes, and not be further processed in any manner incompatible with those purposes;

5

Privacy notices

You should review your current privacy notices and ensure that these are in an easily accessible form and up-to-date. You will need to include more detailed information including your lawful basis for processing personal data and retention periods unless an exemption applies.

be accurate and, where necessary, kept up to date;

be processed in accordance with the rights of data subjects;

6

Individuals' rights

You should check your procedures to ensure they cover all the rights individuals may have, including deletion, so that you know how to respond within the specified timescales.

7

Data breaches

You should ensure that you have the right procedures in place to identify, manage and investigate a breach. You will need to have processes in place to determine whether you need to report the breach to the ICO, based on the risks to individuals' rights and freedoms. If you decide that it is necessary to report you will need to do so no later than 72 hours after becoming aware of it. You should be prepared to notify affected individuals in some cases.

be protected using appropriate technical and organizational measures

not be kept for longer than is necessary for that purpose, and be disposed of in accordance with regulation;

8

Data protection by design and DPIAs

Make sure you are familiar with the ICO's code of practice on privacy impact assessments as Data Protection Impact Assessments are now mandatory where any processing is likely to result in a high risk to the rights and freedoms of individuals.

9

Data Protection Officers

Ensure you designate someone to take responsibility for your data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You are now required to have a Data Protection Officer (unless you already have one under the requirements of the GDPR or a specific piece of European law enforcement legislation).

10

Logging

You should ensure that you are able to keep logs of processing operations in automated processing systems. This will include a log of any alterations to records, access to records, erasure and disclosures of records unless an exemption applies.

11

International

You should review procedures for transferring or sharing personal data across borders (either with relevant authorities or others) to ensure that they are compliant.

not be transferred to a State or territory outside of Jamaica, unless that State or territory ensures an adequate level of protection for the rights and freedoms of data subjects.

12

Sensitive processing

If you are undertaking sensitive processing you will need to ensure that you are compliant with the requirements of the legislation including having an appropriate policy in place.

10:45 - 12:00



- Preparing for Data Protection Regulations
- Spearheading the move to compliance with the (DPR)
- evaluate the need to carry out a thorough audit of all the organisation's processing of personal data.
- The need for Data Protection Officers (DPO)
- Changing the cultural mindset
- Embracing the change in cultural mindsets

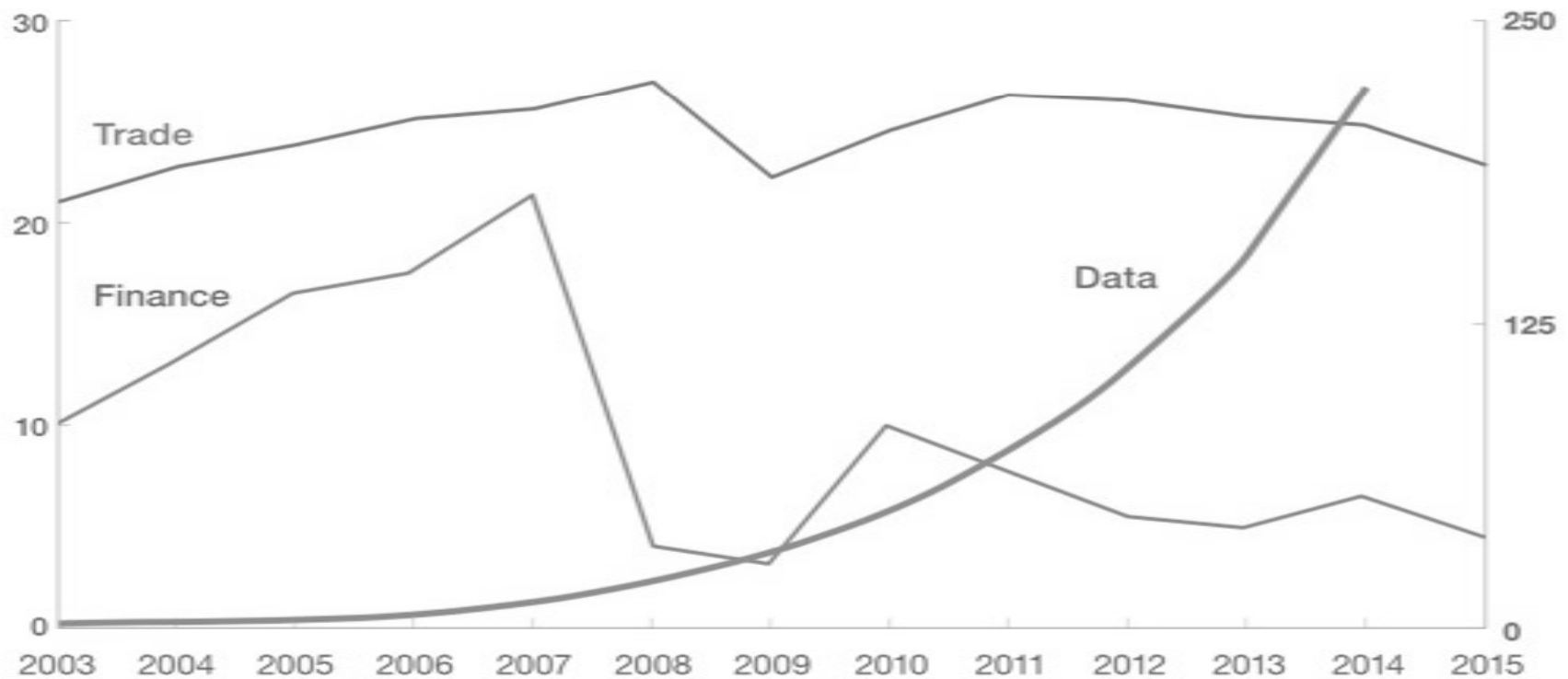
What an opportunity



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

Flows of trade and finance,¹
% of GDP

Flows of data,¹
terabits per second



How does Data Privacy & Protection impact organisations?



The different ways organisation come under DPR?

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 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

How does Data Privacy & Protection impact data transfers



DPR will continue to be in focus for the next decade. Global flow of data in terabytes per second, now exceed the flow of trade and finance as a % of GDP. Therefore, ensure that:

- The third country that processes privacy data, must provide and document that an adequate level of protection for the personal data as determined by the Data Privacy & Protection is in place
- In the absence of that adequate protection the host controller or processor must ensure appropriate safeguards on the condition that enforceable data subject rights and effective legal remedies for individuals are available
- Review other possible mechanisms – that range from Binding Corporate Rules to approved codes of conduct and certification mechanisms, including different types of

Step 3: Repair or replace



It is all about the reputation!



10:45 - 12:00



- Preparing for data protection regulations
- Spearheading the move to compliance with the (DPR)
- Evaluate the need to carry out a thorough audit of all the organisation's processing of personal data.
- The need for Data Protection Officers (DPO)
- Changing the cultural mindset
- Embracing the change in cultural mindsets

Does the auditor have a responsibility to Investigate GDPR compliance



- The auditor must identify/report on material omissions and errors
- The risk of their occurrence, due to a company's failure to comply
- The auditor needs to differentiate between two main categories (*ISA 250, section 6*):
 - a. Laws and regulations that impact directly on the figures and information published in the financial statements and
 - b. Laws and regulations, where compliance (or the lack thereof) can significantly impact on the entity's ability to trade or which threatens its existence (going concern). This includes material fines.
- *Auditor must obtain audit evidence that the entity is in compliance*
- *Regarding b above the auditor should:*
- Make enquiries as to whether the entity is in compliance with relevant laws and regulations
- Inspect correspondence with lawyers, regulators, others
- Material impact of fines of up to 4% of turnover
- Any breach of laws and regulations need to be investigated

Structure of the ISAE3000 report by the independent auditor



Section	Contents
Report by Management	The data controllers report: appropriate IT and organisational data protection & control objectives have been set and monitored. And the entity and the data controller is in compliance with good data practices
Report by reporting accountant	Auditors report on the data controllers report: includes a description of the nature and function of the controls, and control objectives.
Systems description	Description of the procedures and controls used to treat and safeguard personal data related to the service providers and customers The systems description of the controls that have been implemented by the data controller to meet the control objectives.
Control objectives, control activities, testing and results	Control objectives covering the requirements in the relevant articles in the law and description of the specific control activities, performed by the data controller The tests of the control activities and results thereof, performed by the independent auditor are described.
Other information	The service provider has the option (not a requirement) to add further information which has not been provided in the management report and is not part of the auditors report or the systems description.

10:45 - 12:00



- Preparing for data protection regulations
- Spearheading the move to compliance with the (DPR)
- evaluate the need to carry out a thorough audit of all the organisation's processing of personal data.
- The need for Data Protection Officers (DPO)
- Changing the cultural mindset
- Embracing the change in cultural mindsets

Who needs a DPO?



The controller

AND

The processor

1. Processing is carried out by public authority

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

3. Business with a core activity

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

What does a DPO?



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

Independence to ensuring compliance
Employee or external consultant based on a service contract
Expertise in national and European data protection laws
Knowledge of the business sector and of the organization of the controller
Professional ethics and lack of conflict of interests
Groups may designate a single DPO

When the DPO is needed?



If **public authority or body**

(except for courts acting in their capacity)

If **core activities** consists of processing operations...

If required by the **Union or Member State Law**

Possibility of **single DPO for several authorities**

(considering their structure and size)

Requiring regular and systematic monitoring of data subjects on a large scale

Dealing with special categories of data and criminal convictions and offenses

Group of undertaking may appoint a **single DPO**, if accessible

Position of the DPO?



Recruitment base



The DPO shall be designated on the basis of 1) **professional qualities** and 2) **expert knowledge of data protection laws and practice** and the ability to fulfil the tasks

Conjunction



- 1) **Employed** by the data controller or processor
- 2) **Service contract** (independent contractor)

Reporting line



Directly to the highest management level of the data controller or processor

Obligations



- 1) **Keep confidentiality** about the performance of tasks, in accordance with EU and national laws
- 2) Perform duties in an **independent manner**

Tasks of the DPO?



Inform



Advise



Monitor



Contact
point with
the SA



Other tasks

Without creating a
conflict

(DPO as a part time job)

To inform and advise the data controller or processor and the employees processing personal data concerning their obligations under the...

GDPR and EU Laws

National Laws

Advise on impact assessment and monitor its performance

Advise on how to adopt personal data protection policies

Tasks of the DPO?



To do this...

Inform

Advise

Monitor

Contact
point

The data controller or processor shall **support the DPO** in performing their tasks by

Develop internal policies to demonstrate compliance and **audit** their adoption



Resources to carry out the tasks (budget for a privacy program)



Access to personal data and processing operations (political authority)



Maintain the expertise of the DPO (training)

Develop training and awareness campaigns

10:45 - 12:00



- Preparing for data protection regulations
- Spearheading the move to compliance with the (DPR)
- evaluate the need to carry out a thorough audit of all the organisation's processing of personal data.
- The need for Data Protection Officers (DPO)
- Changing the cultural mindset
- Embracing the change in cultural mindsets

Step 1: Tips



- ✎ Educate about GDPR to key stakeholders
 - ✎ Explain the privacy risks for their own career
 - ✎ Invite them to conferences and training
 - ✎ Communicate the link between GDPR and cyber risks
- ✎ Propose a plan adjusted to the Organization culture
 - ✎ Efficient and clear plan
 - ✎ A plan adjusted to available resources
 - ✎ Data Privacy & Protection 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 1: Train your people



- ✎ Employees from the top to the bottom
 - ✎ A clear message: the disciplinary actions for mishandling personal data
 - ✎ 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 Data Privacy & Protection changes privacy practices for each group
 - ✎ Avoid legal terms of the Data Privacy & Protection, 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

10:45 - 12:00



- Preparing for data protection regulations
- Spearheading the move to compliance with (DPR)
- evaluate the need to carry out a thorough audit of all the organisation's processing of personal data.
- The need for Data Protection Officers (DPO)
- Changing the cultural mindset
- Embracing the change in cultural mindsets

Tone-at-the-Top

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**

IT and Data Governance Plan



Build program and team	Identify stakeholders	Allocate resources	Appoint DPO	Define program mission, goals
Assess risks and create awareness	Data inventory and data flow analysis	Conduct risk assessment and identify gaps	Policies, procedures and processes	Communicate views, conduct training
Design and implement operational controls	Obtain and manage consent	Data transfers and 3 rd party management	Individual data protection rights	Technical and administrative safeguards
Manage and enhance controls	Conduct DPAs	Data need, retention, removal	Data integrity and quality	Data breach incident response plan
Demonstrate ongoing compliance	Evaluate and audit control effectiveness	Internal and external reporting	Privacy notice & dispute resolution mechanism	Certification



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

4 - Identify new measures



Prioritize according to tolerance to of privacy risks, link to data classification policy, risks can be accepted

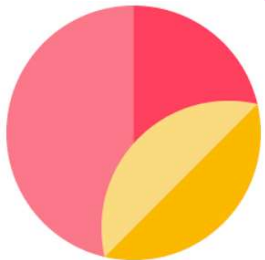


Devise solutions such as new controls and technologies according to the cost/benefit for the risk



Create an action plan and sign off the document by the manager in charge of type of information involved

Data Privacy and Protection compliance. Summary



- ✎ The legal basis of IT and cyber security compliance
- ✎ How is data collected, used, abused or misused?
- ✎ Use of data exactly for the purpose it was collected
- ✎ Consent from data subjects for secondary processing
- ✎ Review change processes in processing personal data
- ✎ Address violations, and remedies for correction
- ✎ Regular reviews of data flow mapping, audits, risk assessments to ensure the legal basis has not changed

- ✎ GDPR is not privacy by choice, follow the privacy data!
- ✎ Does not give the individual full control over the data
- ✎ The reform simplifies and adds compliance complexity
- ✎ The code-of-conduct and certification mechanism ensure structured and efficient means for compliance

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.”

Discussion



- Identify the potential breaches in your current Organisation.
- Roles & Responsibilities of the Data Protection Officer & Conducting a Personal Data Inventory Audit.

Discussion on Data Breach



Identify the components or processes which through knowing how best to respond to threats or incidences will prevent or minimise data breaches?

Discussion on Data Breach



Identify the three prevention strategies to combat, prevent and respond to cyber threats or incidences.

Discussion on Data Breach



Name the three key appropriate action you will undertake when handling data breaches.

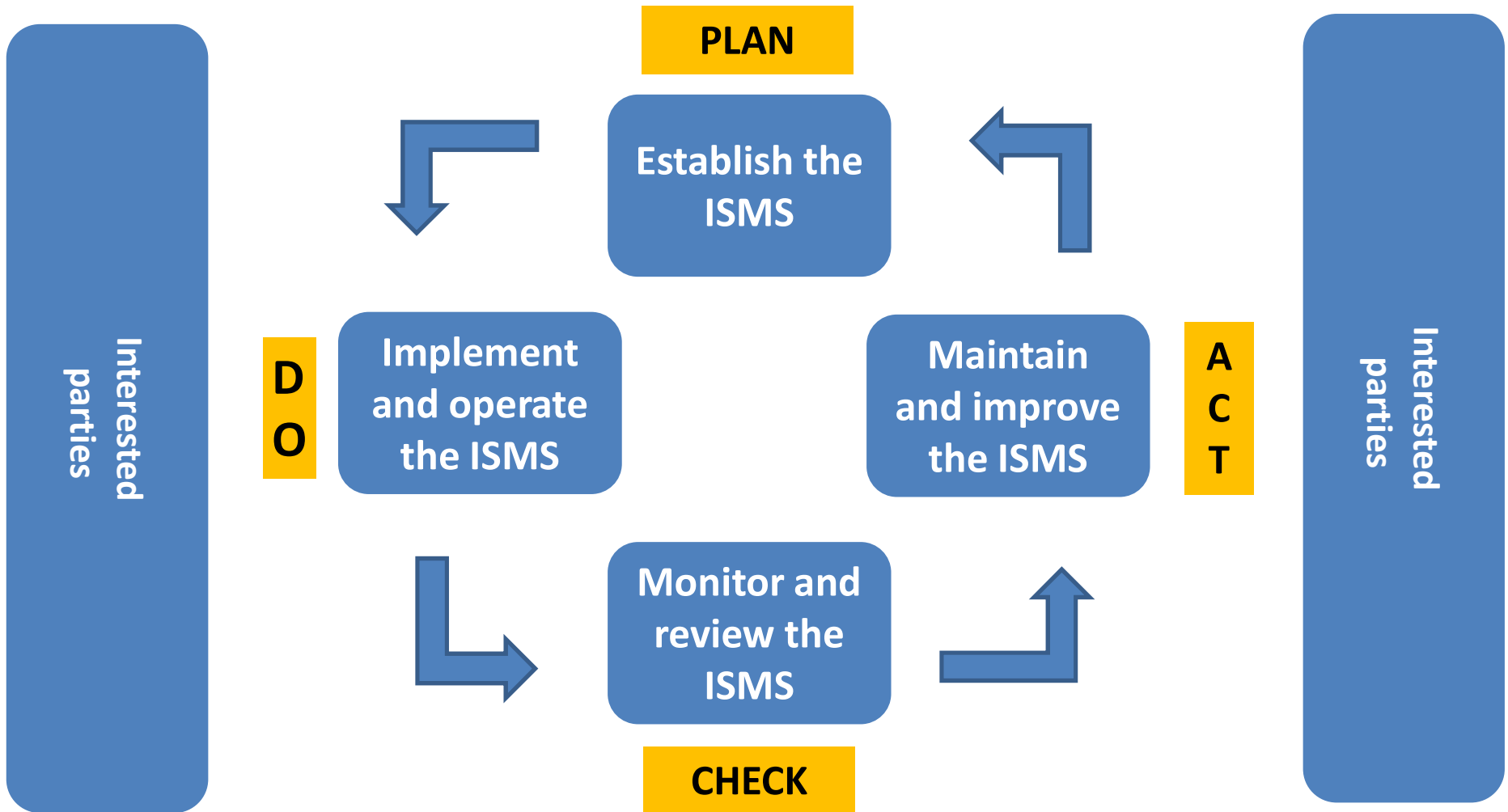
Discussion



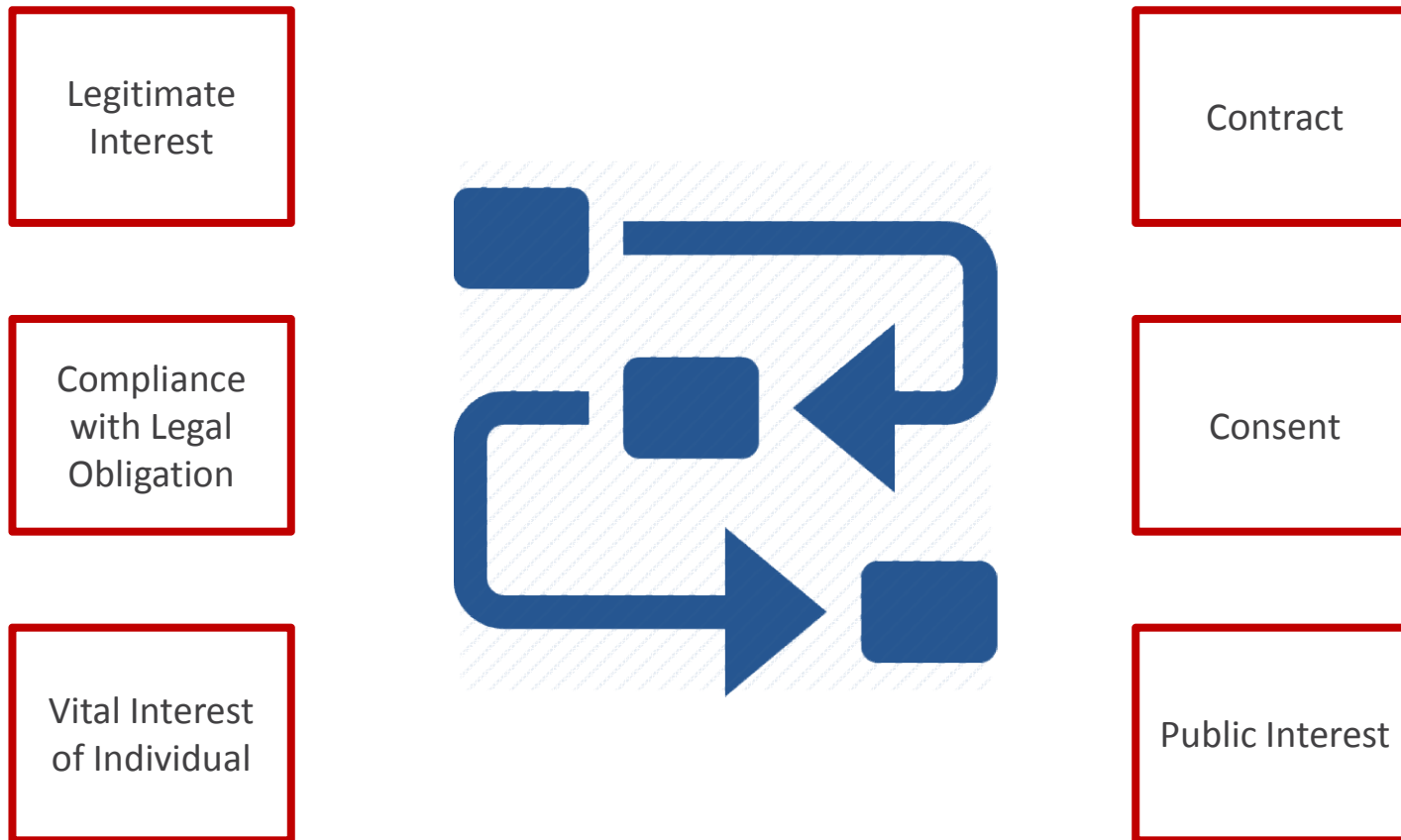
- Identify the potential breaches in your current Organisation.

- Roles & Responsibilities of the Data Protection Officer &
- Conducting a Personal Data Inventory Audit.

ISO 27001 Info Sec



Legal bases for processing



*If it is hard to obtain a valid consent, this probably means that another more appropriate legal basis should be used . Difficulties collecting consent = more appropriate legal basis should be used
Consent is not appropriate = may be considered unfair and misleading*

Data Privacy & Protection Overview



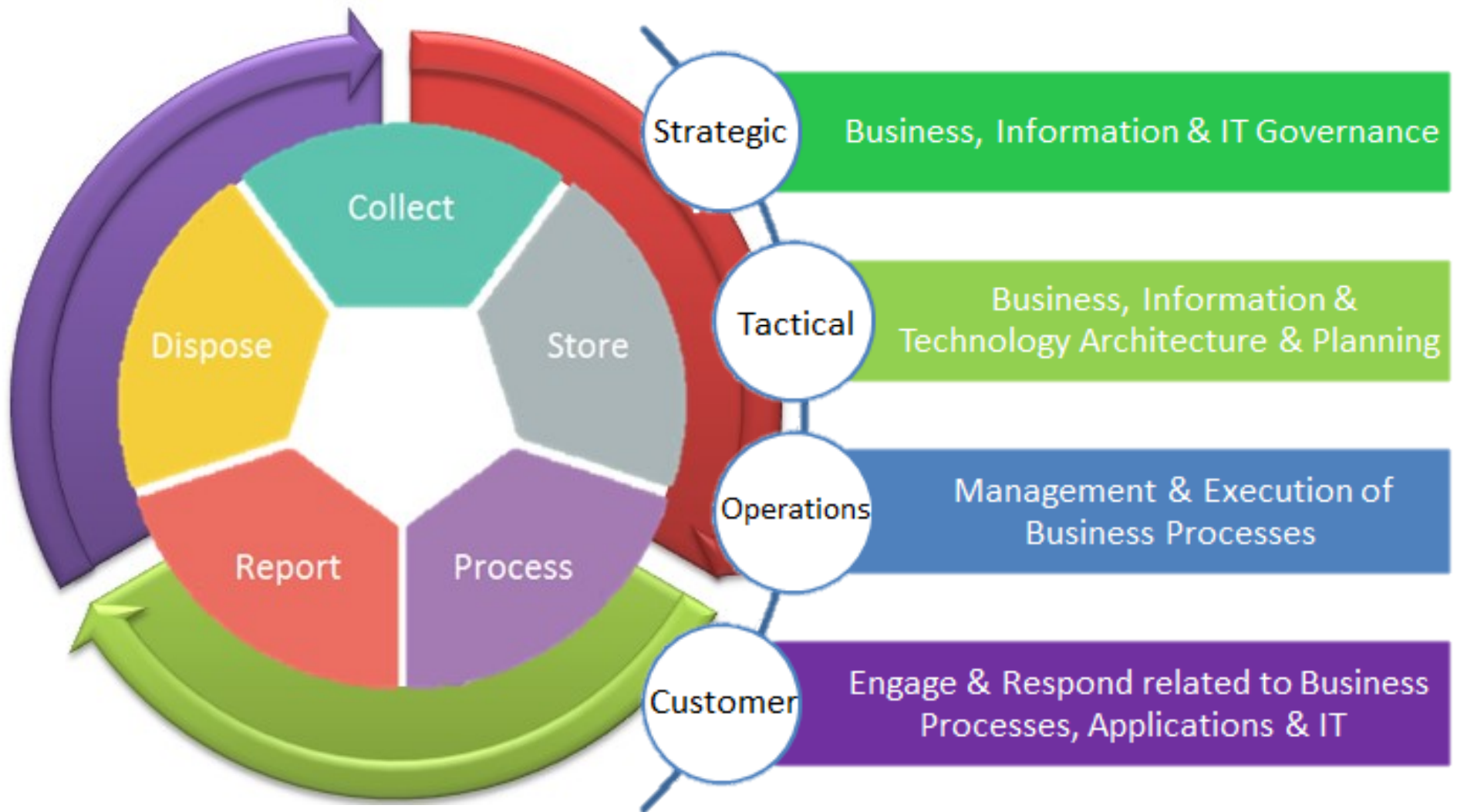
**Data Privacy
& Protection
assessment
and
consulting**



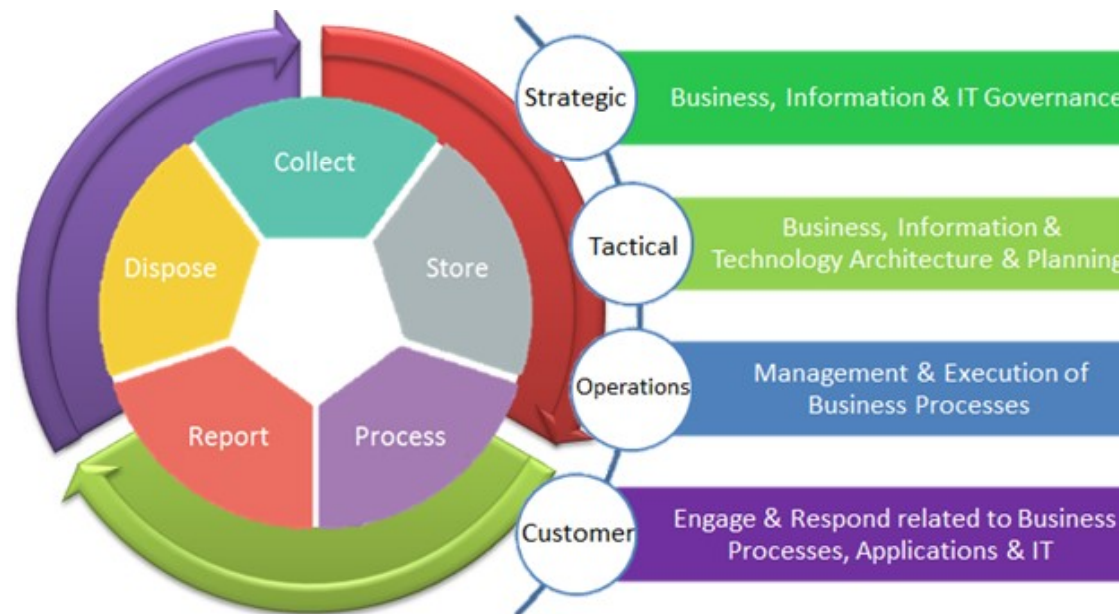
**Privacy
engineering**

Privacy Impact Assessment

Data Privacy & Protection Overview

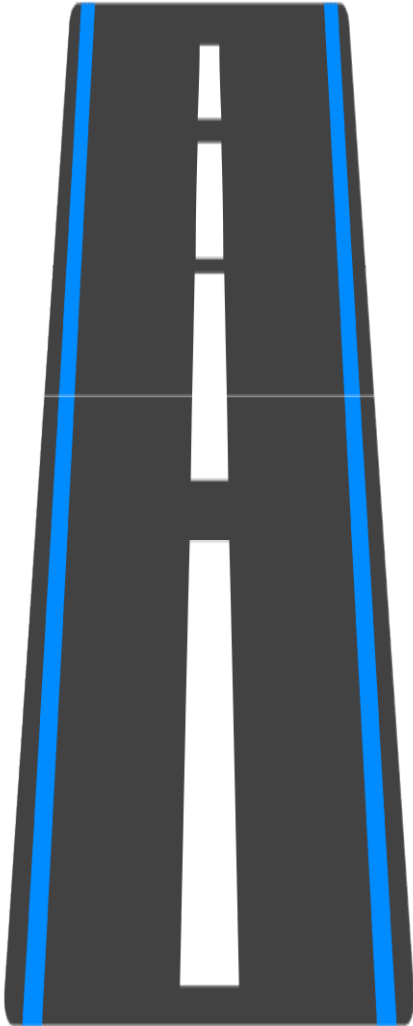


Data Privacy & Protection Overview

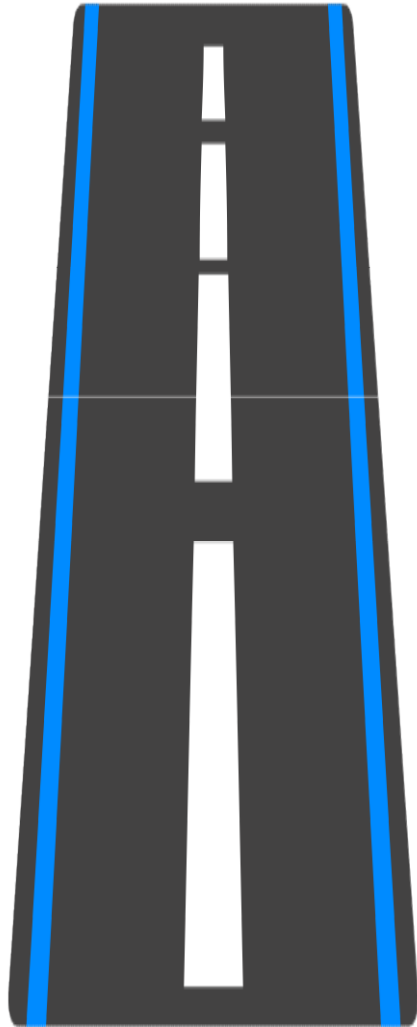









A- Plan

- 
- A large, stylized letter 'A' in a dark grey color. It has a white vertical bar in the center and two blue vertical bars on the left and right sides, creating a road-like appearance.
- ✎ 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







B- Do

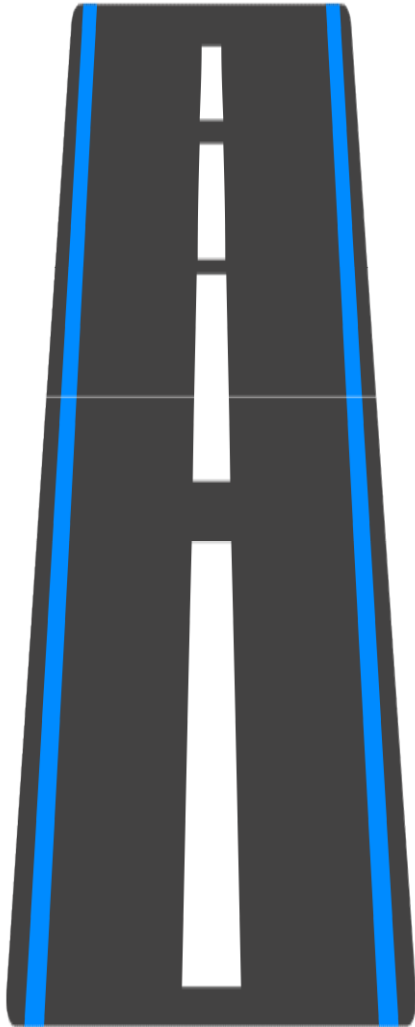
-  **1- Limit accesses**
-  **2- Review consents**
-  **3. Process access requests**
-  **4- Validate data transfers outside the EU**
-  **5- Report data breaches**





C- Improve

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





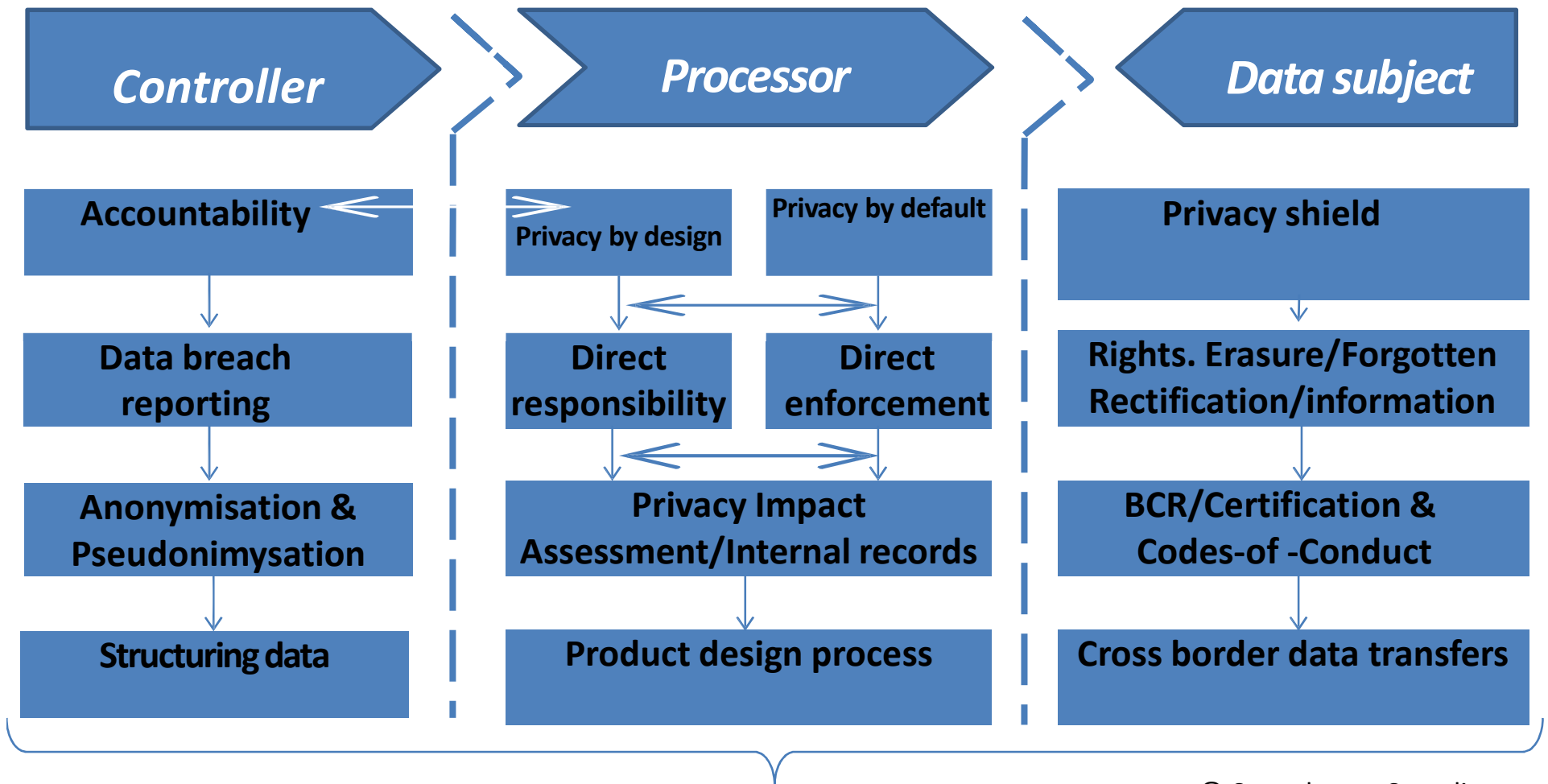
Proportionality

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

Summary

Assemble the Data Privacy & Protection Road Map & Framework



© Copenhagen Compliance

GO TO THE DEVELOPMENT OF YOUR Data Privacy & Protection ROAD MAP & FRAMEWORK

Privacy management platform



Privacy Program Management Tools



Assessment Automation

Conduct PIA, DPIA, PbD and Accountability assessments

GDPR Articles 5, 24, 25, 35 & 36



Data Inventory & Mapping

Keep your record of processing and data flows evergreen

GDPR Articles 6, 30 & 32



Vendor Risk Management

Properly vet any sub-processors to remediate risk

GDPR Articles 24, 28, 29, 32 & 44-49



Incident & Breach Management

Intake analysis and notification workflow for incidents

GDPR Articles 33 & 34

Marketing & Web Compliance Tools



Cookie Consent & Website Scanning

Automate cookie banners, settings and policies

GDPR Articles 4(11), 7, 21, ePrivacy



Universal Consent and Preference Management

Integrate consent across web forms, emails, calls, etc

GDPR Articles 4(11) & 7



Data Subject Access Rights Portal

Handle the lifecycle of deletion, access & other subject requests

GDPR Articles 7 & 12-22



Policy & Notice Management

Manage the privacy policy & notice lifecycle

GDPR Articles 5, 13 & 14

Accountability and Transparency



Privacy Policy

Controllers

Processors

Subjects

Consent

Uses

Transfers

Purpose

Retention



Marketing



HR



Customers



Vendors



Cloud



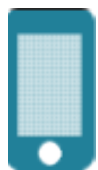
Government



Analytics



Support



R&D



IT



Minors



Employees



M&A



Vendors

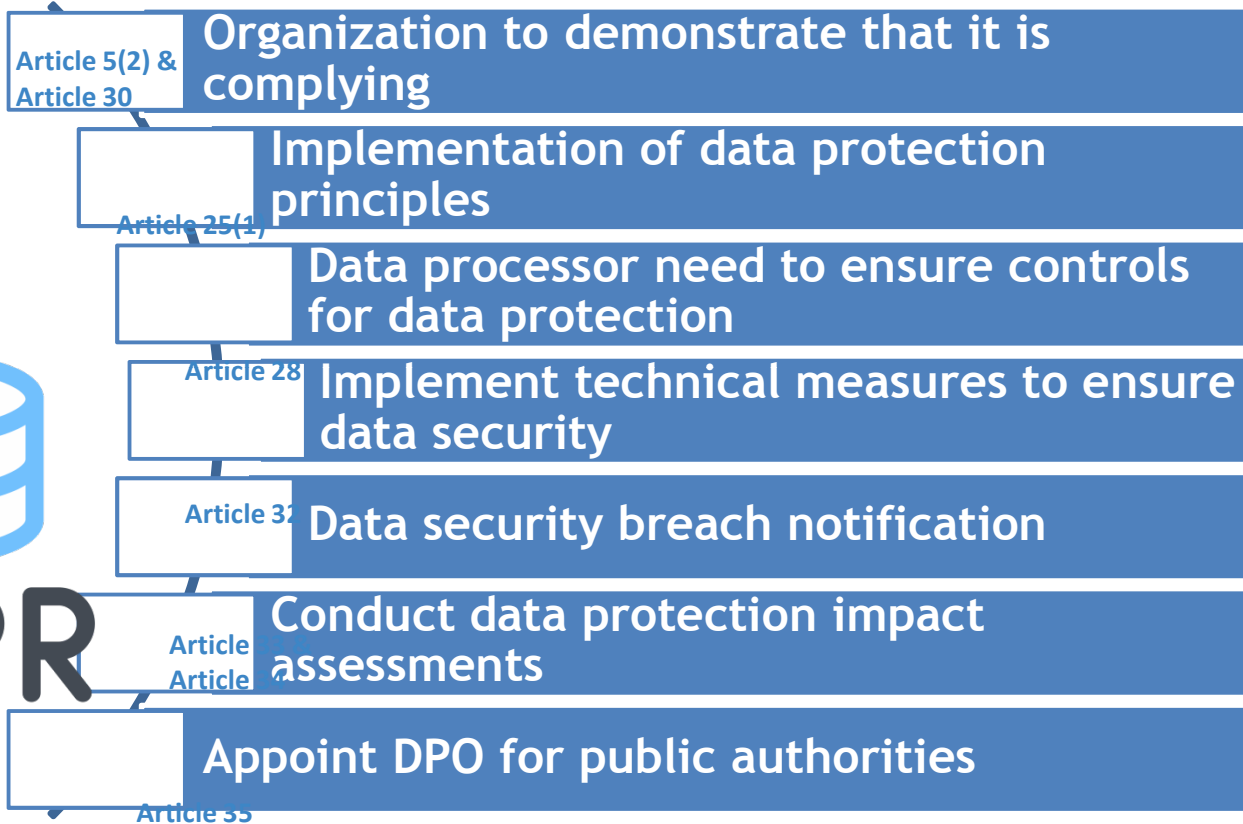


Operations



Backups &
Testing

Summary



Article 37

GDPR Components and Goals



- 1 • Key definitions
- 2 • Bands of penalties and range of awards for breaches
- 3 • Timeline to application of GDPR
- 4 • Six data protection principles, lawfulness and consent
- 5 • Sensitive data
- 6 • Rights of data subjects
- 7 • Controllers and processors
- 8 • Data protection by design

- 9 • Securing personal data
- 10 • Reporting data breaches
- 11 • How to perform a DPIA (data protection impact assessment)
- 12 • Role of the DPO (data protection officer)
- 13 • Role of certifications
- 14 • Transferring personal data outside the EU
- 15 • Powers of supervisory authorities
- 16 • Lead supervisory authority
- 17 • Role of the EDPB (European Data Protection Board)

Roadmap



Key definitions

Clarify the bands of penalties and range of awards for breaches

Review the timeline to reflect the application of GDPR

Role of the DPO (data protection officer)

Six data protection principles, lawfulness and consent

Define sensitive data

Rights of data subjects (a number of national deviations)

Controllers and processors

Data protection by design

Securing personal data

Procedure on reporting data breaches

Transferring personal data outside the EU

How to perform a DDPIA (data protection impact assessment)

Powers of supervisory authorities

Lead supervisory authority

Role of the EDPB (European Data Protection Board)

Importance of certifications

What you have received?



<https://www.eugdpr.institute/wp-content/uploads/2019/02/jamaica.pdf>

Useful GDPR links



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

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



Copyright notice



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

Info@eugdpr.institute

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

The GDPR Institute



www.copenhagencompliance.com



Human Capital Assessment Framework



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

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

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

Disclaimer



- 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 advise.