



GENERAL
DATA
PROTECTION
REGULATION



FAS
Foundation

DPO
Masterclass

CEP
Practitioner



Day 2. Brussels 15th May 2019

All Links



- FAS Presentation - <https://www.eugdpr.institute/fas/>
- FAS Exam - <https://www.eugdpr.institute/gdpr-fas-exam/>
- DPO Presentation - <https://www.eugdpr.institute/dpo/>
- DPO Exam - <https://www.eugdpr.institute/gdpr-dpo-exam/>
- CEP Presentation - <https://www.eugdpr.institute/cep/>
- CEP Exam - <https://www.eugdpr.institute/gdpr-cep-exam/>
- pdf links
 - FAS: <https://www.eugdpr.institute/wp-content/uploads/2019/05/day1.pdf>
 - DPO: <https://www.eugdpr.institute/wp-content/uploads/2019/05/day2.pdf>
 - CEP: <https://www.eugdpr.institute/wp-content/uploads/2019/05/day3.pdf>

Brush up



Key Components and Provisions of GDPR

GDPR Overview



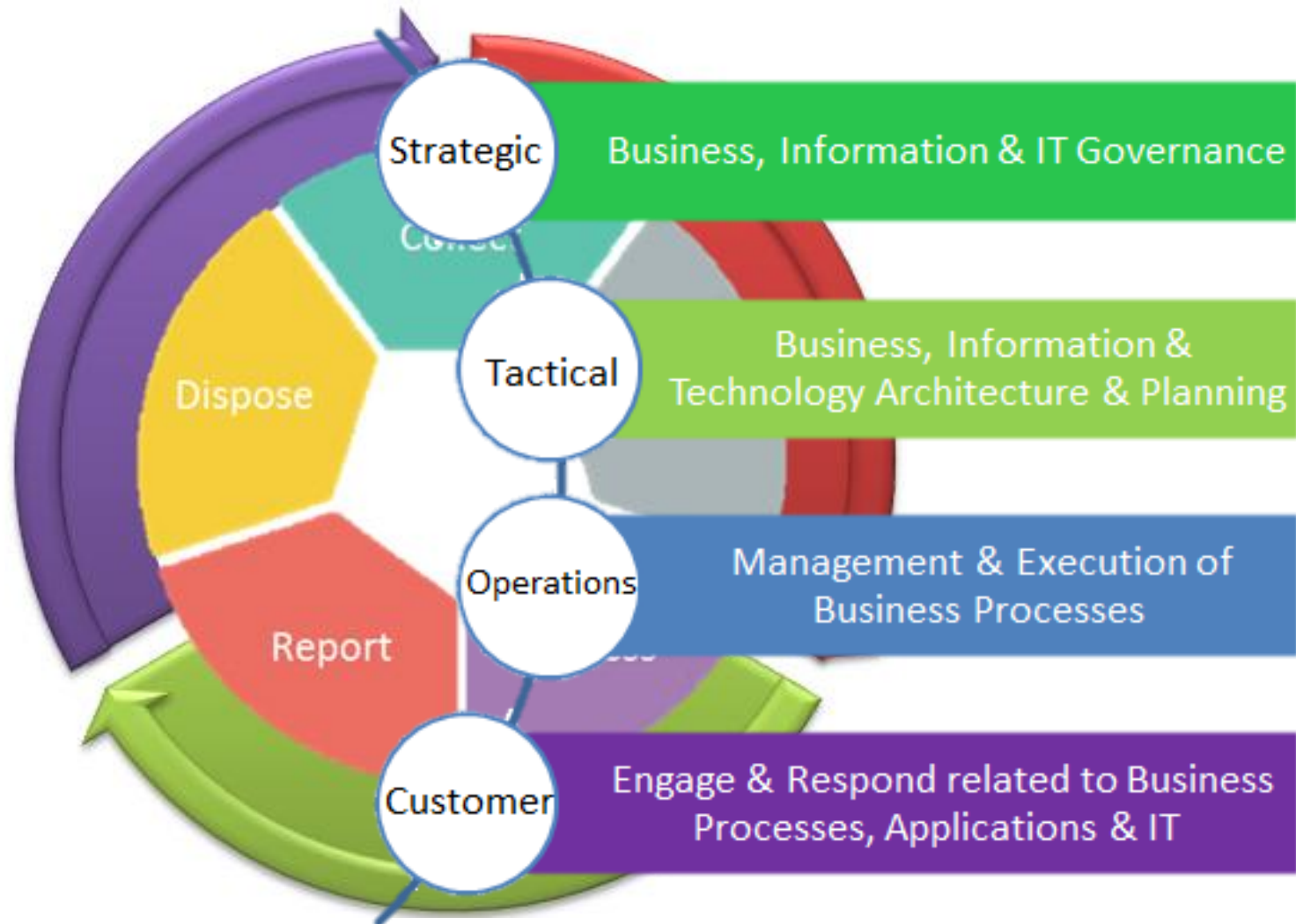
**GDPR
assessment
and
consulting**



**Privacy
engineering**

Privacy Impact Assessment

GDPR Overview



GDPR Overview



Strategize the approach

Team and budget

Build ops and technical controls

Implement controls

Monitor controls



GDPR Compliance

7 Core Principles

One Stop Shop

Data Subject Rights

Explicit Consent

Risk Based Approach

DPO Enforcement

GDPR areas with risk exposure



- ✎ **PIMS** limited documentation from policy downwards, lack of data protection policies and procedures, unclear whether a DPO or DPIAs are mandatory
- ✎ **ISMS** inadequate and unintegrated data security controls, cyber essentials not considered, no penetration testing, limited encryption
- ✎ **Data subject rights** not addressed or absence of transparency
- ✎ **Controller-processor relationships, trans-border data processing** limited information in key GRC and IT security areas
- ✎ **Interaction with the Privacy and Electronic Communications Regulations** confusion over consent and lawfulness of processing

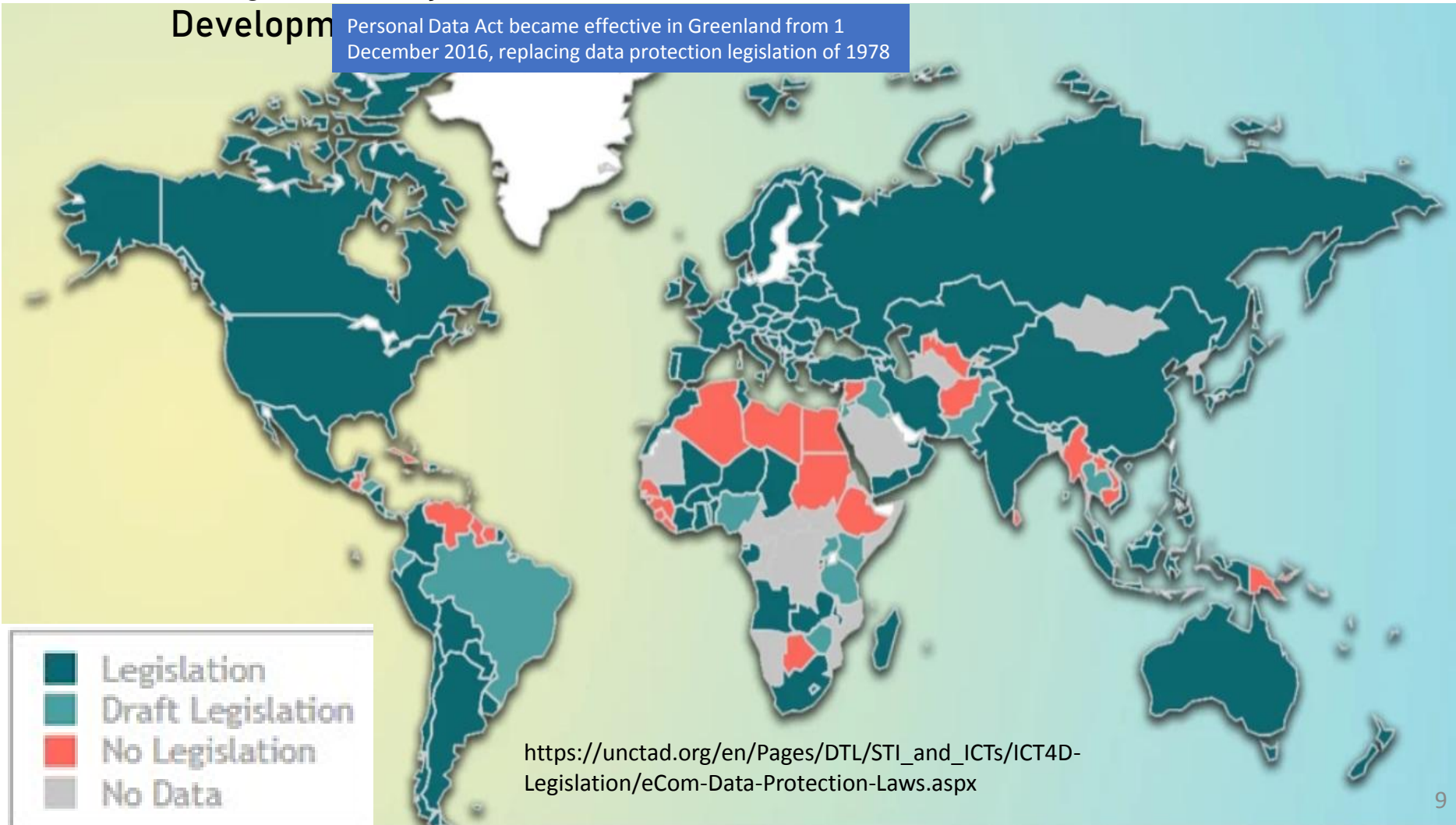


Current trends in the data protection industry

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



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

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

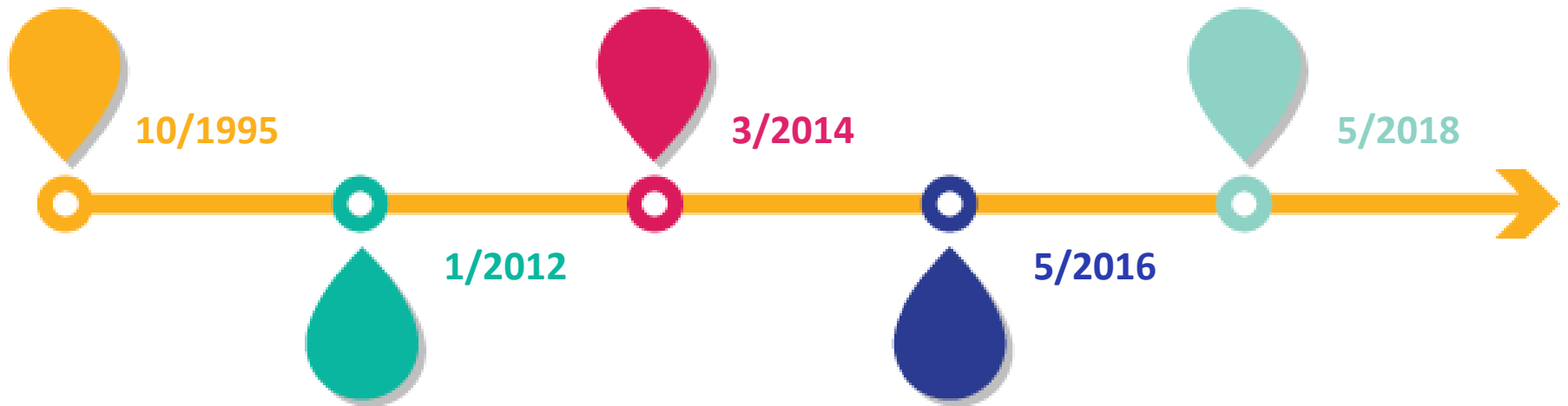
Timeline



Directive 95/46/EC is adopted
Processing of personal data
Free movement of personal data

GDPR draft is adopted
Personal data protection as a
fundamental right
Voted overwhelmingly in favor

GDPR is effective
So now?...



EC proposal reform
Strengthen online privacy rights
and digital economy

GDPR enters into force
Published in the EU Official Journal

How to avoid be GDPR scoped



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

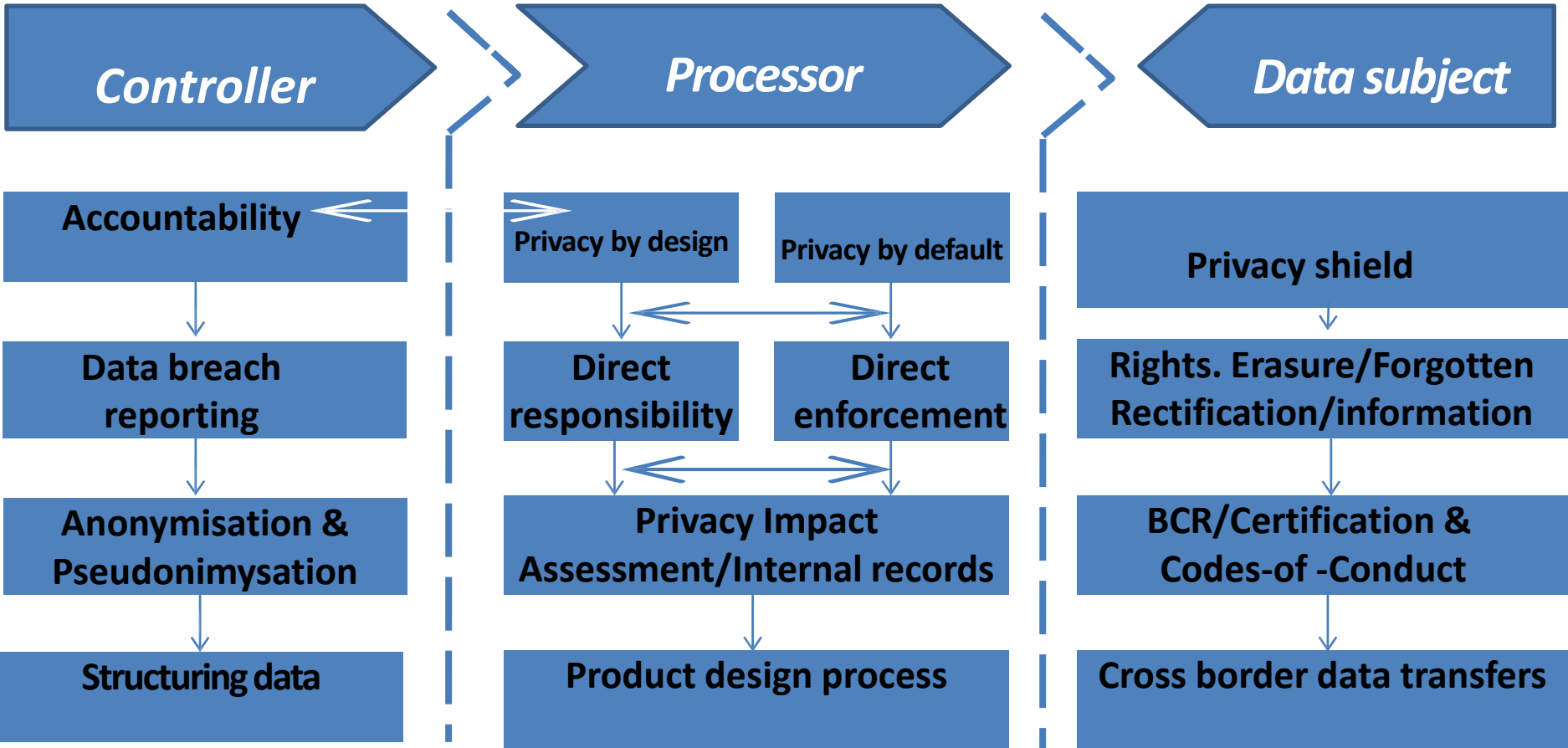
- Avoid giving the impression that they offer goods or services to users in the EU.
- Remove the top-level domain names of EU member states from the organization`s website, e.g. “de.”
- Not offering services to EU users on websites or via marketing materials.
- Removing all EU countries from website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

How to avoid GDPR scope



- 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.

Assemble the Data Privacy & Protection Road Map & Framework



© Copenhagen Compliance

Go To The Development Of Your Data Privacy & Protection Road Map & Framework

Business benefits of data flows



Interconnected machinery. Improve processes and optimise efficiency to reduce downtime or prepare for service replacements

Big data analytics. Collect all operational data and apply advanced statistical analysis for better decisions, for business and customer

Back-office consolidation. Centralise standard business operations for economies of scale (e.g., HR, accounting, payroll, marketing, etc.) to improve buying power and eliminating overlap.

Supply-chain automation. Track inventory levels, process to match supply and demand.

Digital collaboration. Increase communication and collaboration

Cloud scalability Lower capital expenditure and cost structure of information technology (IT) hardware, infrastructure, software, and applications, idle capacity, thus lowering the total cost of ownership and increasing business agility and resilience to failures

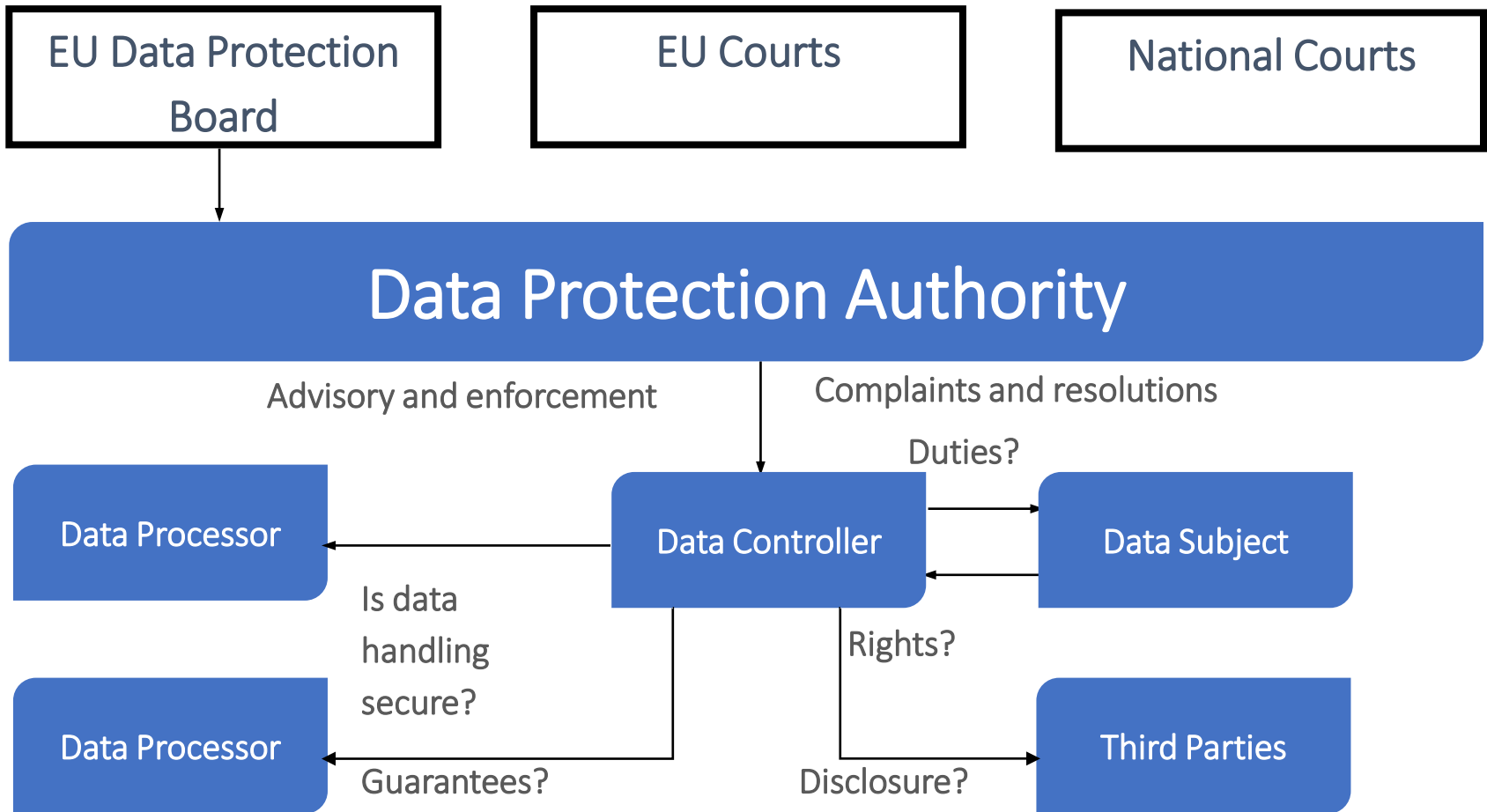
Why is GDPR important?



Privacy as a competitive advantage

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

Organization



Study case



How do you perform the ongoing monitoring of the use of personal information?

- ✎ How do you audit third parties
- ✎ How do you write auditing clauses with data processors
- ✎ What audit standard is best to use
- ✎ What tools are available to monitor the transfer and use of personal information

The GDPR guiding principles



Guiding principles solutions



GDPR Principles	Typical Challenges	Solution and Capabilities
Integrity and confidentiality	Applying industry standard IT security controls to prevent unauthorized access	Strong Encryption, Fine-grained authorization
Accountability	Demonstrating compliance, detecting and analyzing breaches in 72 hours	Comprehensive, inescapable audit trail. Cybersecurity solutions
Lawfulness, fairness and transparency	Implement a way to keep track of personal data	Classifying and tracking lineage of personal data elements
Purpose limitation	Track consent and data usage	DPO can audit precisely how data was used, Keep data governed
Data minimization	Removing or anonymising data where possible Preventing unlawful data transfers outside the EU while still enabling outsourcing	Data can be tagged to indicate allowed purpose, time limit Redacted views
Accuracy	Finding a low overhead way to fix data	Fast updates of individual records

Overview



Privacy Principles
Definition of Privacy
Definition of Private Data

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**

Privacy principles



Consent

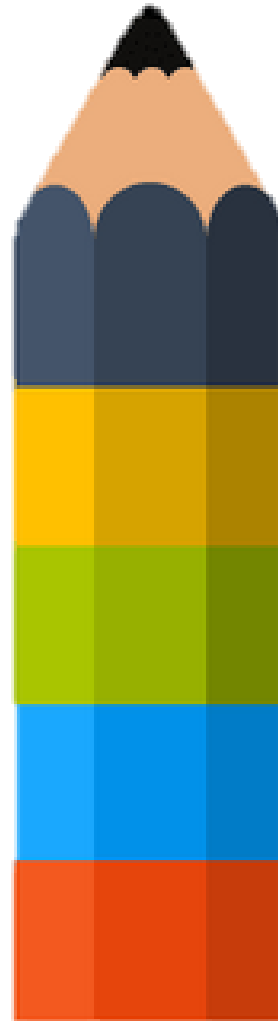
Data subjects understand and explicitly or implicitly agree with the uses of personal information

Notice

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

Minimal use

Data controllers use personal information is only for a obtained consent



Choice

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

Minimal collection

Data controllers obtain personal information is only for a limited purpose

Privacy principles



Access and correction

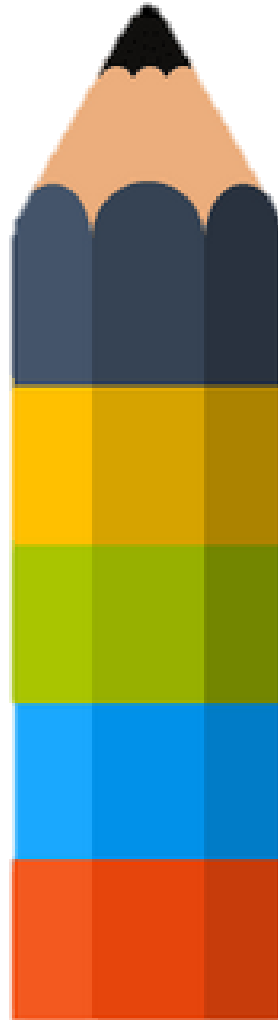
Data subjects access and correct personal information to ensure is accurate, complete and relevant

Security

Data controllers protect the access and modification of personal information

Transparency

Data controllers have understandable policies for data subjects and third parties



Accountability

Data controllers are responsible for complying this privacy regulations and principles

Disclosure

Data controllers can transfer and disclose personal information to third parties for the purposes described by the consents

New privacy principles



Privacy by design

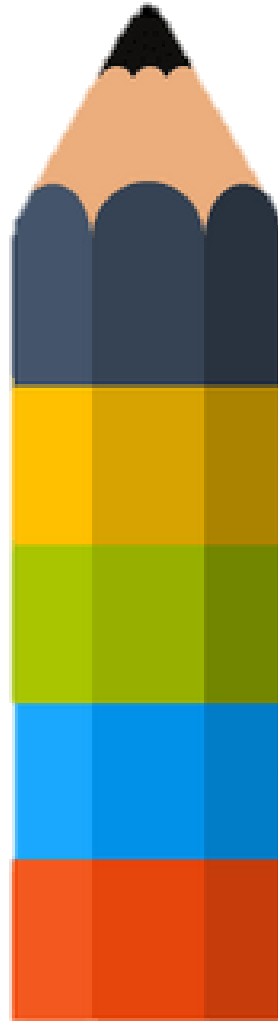
Data controllers consider privacy from the design to the complete development process of new products, processes or services

Anonymity

Data subjects have the option of not identifying themselves

Right to be forgotten

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



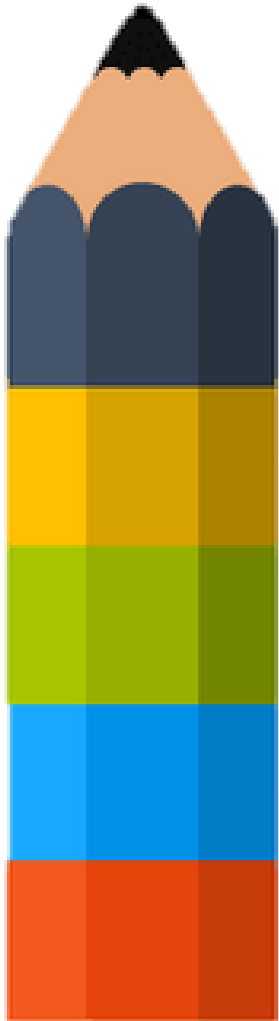
Sensitivity

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

Enforcement

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

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
e.i. 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*

Let's practice



Examples from “when” to “what” of personal info

- ✎ When visitors access to the organization website
 - ✎ IP location, cookies, device information, browser information (e.g. language), behavior information
- ✎ When clients shop from the organization website
 - ✎ name, address, email, bank/credit card details
- ✎ When clients contact the organization by website
 - ✎ name, address, organization, phone number

Let's practice



Ideas for the “what”?

✎ When candidates apply for a job

✎ name, address, email, phone, age, places of employment

✎ When employees are hired

✎ name, date of birth, address, SSN, bank details, salary, vital records, photo, family details, health, tax and retirement number, passport, car license plate

✎ When clients take part in a prize draw

✎ name, phone

Let's practice



Ideas for the “what”?


- ✎ When visitors are video monitored at the lobby
 - ✎ Images, activity
- ✎ When fingers are scanned for door access
 - ✎ fingerprints (biometric)
- ✎ When visitors follow organization social media
 - ✎ data according to Facebook or LinkedIn policies

Let's practice



Ideas for the “what”?

When suppliers are created

-  Names, phones, addresses, emails, executives, transaction records, tax number, financial data

When employee users are created

-  PC IP address, mobile device, activity, password

When visitors get a organization parking permit

-  license plate, name







Auditor's responsibility for GDPR



- ✎ 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.

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

HR

- ✎ Pressure from unions and employees
- ✎ Training

Legal

- ✎ Class actions
- ✎ Fines

Business

- ✎ Limitations for activities
- ✎ Impact on innovation

Board

- ✎ Corporate and personal liabilities
- ✎ Compliance costs

key concerns

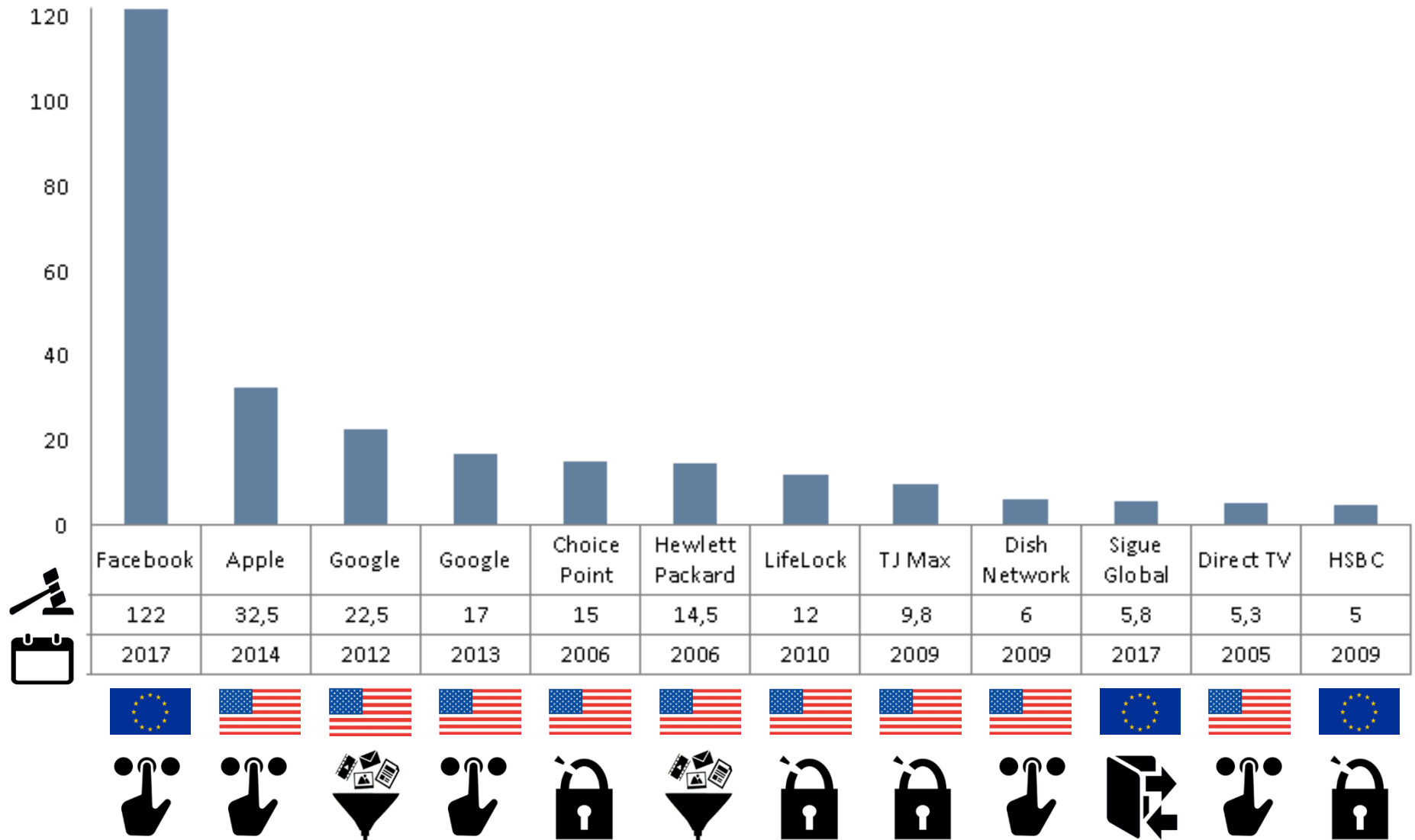
GDPR after May 25th 2018



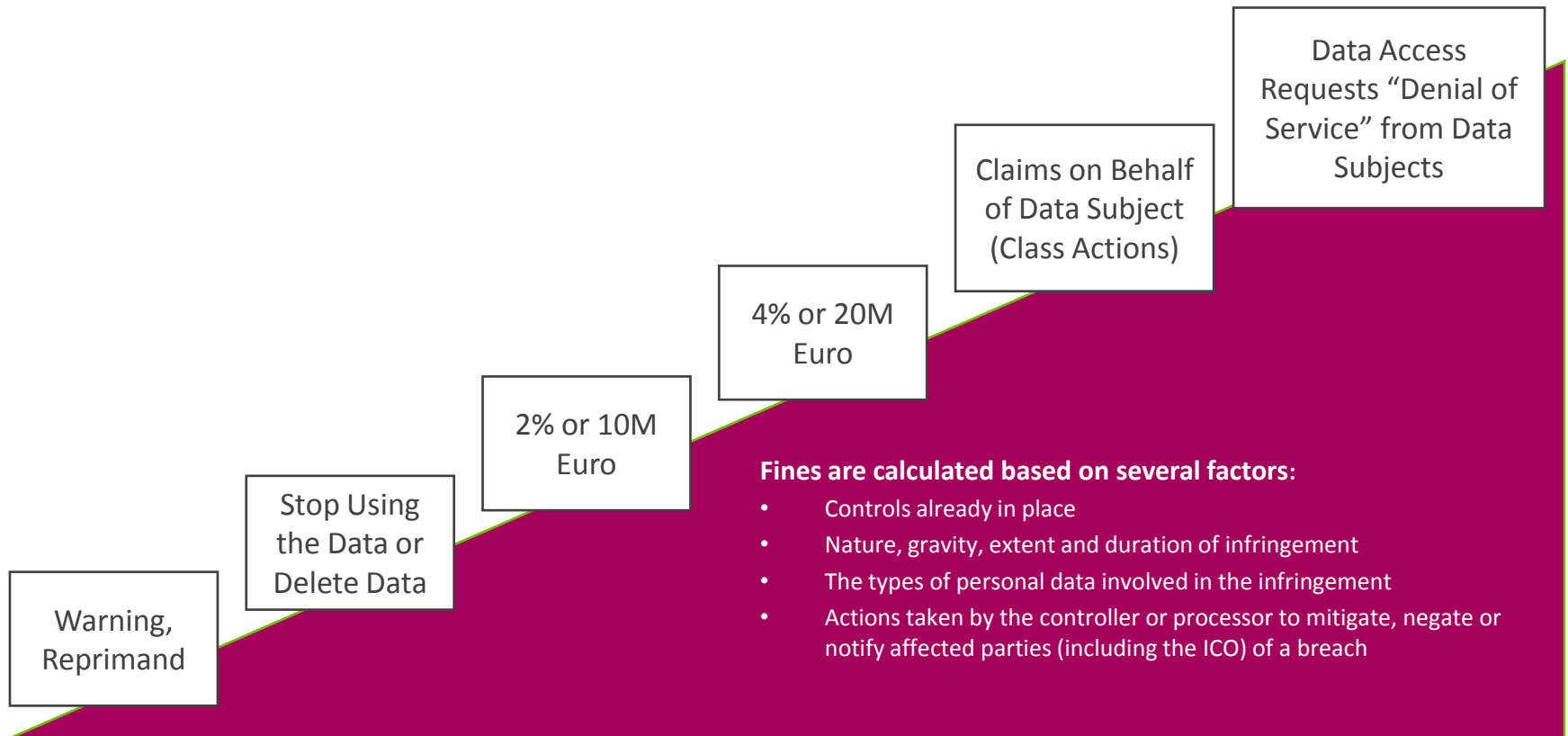
- ✎ **how, when and where the supervisory authorities could start?**
- ✎ **what companies could be the first target? could them be the American tech firms, the Chinese e-commerce sector or the Russian companies?**
- ✎ **would the supervisory authorities be consistent on grounds, accepted evidence and fines?**
- ✎ **if one investigation is opened in one country, could it lead to investigations in other countries?**



Data privacy fines



When do the fines stop



Remedies, Liabilities, Penalties

Discussion on Data Breach



What are the three key steps that you can take as a business to minimize potential damages, of a data breach

GDPR data governance plan



Build program and team	Identify stakeholders	Allocate resources and budget	Appoint DPO	Define program mission and goals
Assess risks and create awareness	Conduct data inventory and data flow analysis	Conduct risk assessment and identify gaps	Develop policies, procedures and processes	Communicate expectations and conduct training
Design and implement operational controls	Obtain and manage consent	Data transfers and 3rd party management	Individual data protection rights	Physical, technical and administrative safeguards
Manage and enhance controls	Conduct DPAs	Data necessity, retention and disposal	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

Discussion case



- You have to choose types of information you want to receive from a supermarket – groceries, holidays, clothing, wine club, third party providers.
- A series of tick boxes at sign up where you can choose which lists you want to be on – men’s fashion, women’s fashion, kid’s fashion is provided.
- Within the same consent request the retailer asks its customers for consent to use their data to send them marketing by email and also to share their details with other companies within their group.
- Is this consent granular?
- Should a specific consent be collected to send the contact details to commercial partners?
- It is not granular because no separate consent for the two separate purposes, therefore the consent will not be valid.
- If you are sending emails about your own business services, which they originally signed up to for generally, then this is still ok.

Breakout session

Discussion in groups



- ✎ **Google, Facebook and Twitter are cracking down on apps that share information it shouldn't.**
- ✎ **Google is planning to roll out several changes designed to protect users on Android, e.g. the new rules that banned apps from displaying ads on your lock screen. These could potentially trick users into downloading unwanted software or sharing data that they don't want to.**
- ✎ **The Safe Browsing team of the EUGDPR Institute is laying out new restrictions on how apps collect a user's data. Under the new policy, apps must provide their privacy policy and prompt users to share their data. This applies to everything from a user's phone number to the list of apps installed on the phone.**
- ✎ **Applications which collect and transmit personal data not required for the app to function must tell users how the data will be used.**
- ✎ **If an app collects and transmits personal data unrelated to the functionality of the app then, prior to collection and transmission, the app must prominently highlight how the user data will be used and have the user provide affirmative consent for such use.**

Breakout session

Discussion in groups



- ✎ The new requirements will apply to all functions of an app. For example, if an application wants to send analytics or crash reports, it cannot transmit the list of installed packages unrelated to the app unless it discloses that and gets permission from the user.**
- ✎ What advise would you give to The Safe Browsing team of The EUGDPR Institute to ensure GDPR Compliance on Google, Facebook and Twitter to make sure that primary issues like consent or showing a warning whenever it tries to collect your data without telling you.is taken into consideration to avoid issues with the DPA.**

Change management



GDPR Impact



New or amended policies and record management



New operational roles and responsibilities, DPO role



Changes in IT tools, solutions, applications and infrastructure



Changes in contracts, agreements, consents, notices

Continuous improvement

Change management



GDPR Impact



Create a protection impact assessment policy
Improve the access management policy
Review processes dealing with personal information



Identify owners of personal data
Assess key staff skills
Create and conduct learning and awareness programs
Communicate the GDPR changes



Determine the need for DPIAs
Follow-up remediation plans for IT solutions
Incident management



Document compliance efforts
Get approvals for changes
Metrics for GDPR compliance

Change management



	Privacy (DPO)	IT InfoSec	Legal	Procurement	Compliance	Business	HR
Data breach notification	■	■	■	■	■	■	■
Data lifecycle mgmt.	■	■	■	■	■	■	■
3 rd -party disclosures	■	■	■	■	■	■	■
Governance	■	■	■	■	■	■	■
DPIA	■	■	■	■	■	■	■
Data transfers	■	■	■	■	■	■	■
Rights for data subjects	■	■	■	■	■	■	■
Privacy by design	■	■	■	■	■	■	■
Data security	■	■	■	■	■	■	■
Monitoring	■	■	■	■	■	■	■

Roadmap schedule



Plan



Do



Improve

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

GDPR Effective

GDPR Action Plan



- ✎ **Create & sign off an action plan document by the involved manager depending on the information type**
 - ✎ Follow-up on action plans and document implementation measures (IT and non-IT changes)
 - ✎ Monitoring of risk registry
 - ✎ On-going and past due audits
 - ✎ Involving board members, list of project stakeholders, budgets, approval
- ✎ **for detected GDPR risks**
 - ✎ Evidence of monitoring on closing issues
 - ✎ Changes to systems and controls are tested as effective
- ✎ **Supervise the data protection impact assessments and monitor the action plans.**

Choose the right GDPR tool



Things to consider

- ✎ Level of integration with your various privacy workflows and legacy systems
- ✎ Stand-alone consent management vs. comprehensive privacy management platform
- ✎ Ease of implementation and user experience
- ✎ Scalability across legal entities, departments, regions

Data Protection Officer



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



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

Develop training and awareness campaigns

Obligation to display contact information



In connection with?	Who?
Personal data collection	DC
Records of processing activities	DC
	DP
Personal data breaches	DP
Prior consultation. High risk	DC
DPO accession	DC/DP

Obligation of other to display DPO



Where?	To whom?	Article?
Information i.c.w. proactive disclosure duty	Data Subject	13/14, § (1), point b
Record of processing activities under Art. 30	SA	30, § (1), point a
		30, § (2), point a
Reporting	DC	33, (3), point b
Consultation	SA	36, § (3), point d
Notifications	SA	37, § (7)
In the publication (Web)	Public	

DPO functions



Independence



Key for assuming the monitoring obligations resting with the Data Protection Authority

✦ Through separation of duties (art 38)

- ✦ Avoid conflicts of interest (no self-monitoring, impartiality, no relatives)
 - ✦ Forbidden to manage IT systems (CISO/CIO) and privacy risks (generally involving board members and HR, compliance, legal and marketing functions)
 - ✦ Lead to a dedicated full time position
- ✦ It may justify to outsource the role in an independent contractor

✦ Direct report to the CEO or highest management level

- ✦ Privacy is an integral part of a governance structure and culture
- ✦ Active support to/from senior management
 - ✦ Real reporting lines to the board (effective access, frequent reporting)
 - ✦ Avoid reporting into IT, legal or compliance functions

✦ Autonomous

- ✦ Nobody instructs the DPO on how to approach tasks
- ✦ Tip: disagreements with top management should be documented

Independence



✦ Protected employment status

- ✦ Freedom from unfair dismissal (e.g. for performing delegated tasks)
- ✦ Appointed for a 2 to 5-years term (reappointed up to 10 years in total)
- ✦ No penalized in disagreeing with the business
- ✦ Can be dismissed for performance and ethical issues

✦ Separated budget

- ✦ Incl. training, staff, travel, IT solutions, external advise and equipment

✦ Professional qualities of an experienced manager

- ✦ Access to independent legal counsel for non-lawyer DPOs

Requirements










- ✎ Expert knowledge of data protection law (art 37)
 - ✎ Privacy lawyer (but not single skilled)
 - ✎ You do not need to be a lawyer to understand just one regulation with 99 arts
 - ✎ Also: auditor, compliance specialist, IT specialist, non-technical manager
- ✎ Many non-legal skillset
 - ✎ Info security, risk assessment, compliance, business strategy, data governance, change management and handling public relations
 - ✎ High seniority to be a trusted business advisor and leader
- ✎ Formal certifications (by country)
- ✎ Maintain confidentiality
- ✎ Physical location is not relevant, but should be reachable

Tasks (art. 39)



Tips:

-  Really understand the organization-specific privacy and security risks
-  Link the risks to the nature, scope, context, and purposes of processing
-  Clearly agree on the title, status, position and tasks
-  No individual liability of the DPO for non-compliance by the business
-  Contact point: consult and co-operate with supervisory authorities
 -  Notification of breaches
 -  Not a whistleblower role! Not a Data Police Officer!

Independently, monitor compliance with the GDPR

- ✎ Audits against GDPR, internal policies and contracts
- ✎ Keep the inventory of processing operations
- ✎ Prioritize controls in a privacy program and monitor compliance
 - ✎ data protection policies, training, data security practices, maintain documentation
 - ✎ Ensure that responsibilities on privacy controls are clear
- ✎ Supervise the data protection impact assessments and monitor the action plans
- ✎ Coordinate how subject access requests are responded

Strategically, inform and advise on data protection issues

- ✎ Attend relevant meetings about data processing (before decisions are made)
- ✎ Train and raise awareness to staff managing personal information
- ✎ Suggest potential solutions, legal interpretational and implementation changes
- ✎ Involved in any security breach
- ✎ Business is not required to follow the DPO's advice

Obligation to display contact information



In connection with?	Who?
Personal data collection	DC
Records of processing activities	DC
	DP
Personal data breaches	DP
Prior consultation. High risk	DC
DPO accession	DC/DP





Obligation of other to display DPO



Where?	To whom?	Article?
Information i.c.w. proactive disclosure duty	Data Subject	13/14, § (1), point b
Record of processing activities under Art. 30	SA	30, § (1), point a
		30, § (2), point a
Reporting	DC	33, (3), point b
Consultation	SA	36, § (3), point d
Notifications	SA	37, § (7)
In the publication (Web)	Public	

Supporting role



	DPO	Board	Managers
Privacy policy 	Drafting Monitoring compliance Conducting audits	Approving	Implementing Complying
Privacy risks 	Facilitating management Advising how to control risks	Owning	Identifying Performing DPIAs Managing risks
Training 	Developing contents Ensuring training	Endorsing awareness campaigns	HR: Provide training
External communications 	Liaising with the Supervisory Managing complains	Responding to a data breach	Handling subject data requests

Skills



1 Regulations } GDPR
Local national provisions

Technical and organizational
measures and procedures

2

3 Data security by design and
by default

Industry and sector-
specific knowledge

4

5

Experience with the size of the
controller or processor

Experience in
inspections,
consultation and
analysis

7

6
8

Awareness of the sensitivity of
the data processed

Ability to document processes

9

Ability to work with data subjects'
and employees' representation
organizations

And get ongoing advanced
training!

10

Communication



- ✎ Communicate the contact details of the DPO to
 - ✎ the supervisory authority
 - ✎ the public for complaints and disputes
- ✎ External-facing role
 - ✎ Independent monitor of data protection compliance
 - ✎ Keep the inventory of processing operations

Voluntary



- ✍ DPOs can be voluntary appointed in private organizations
 - ✍ When it is not required by the GDPR
 - ✍ Reason: reduce eventual fines
- ✍ They can be officially communicated to the Supervising Authority
 - ✍ Once registered, the DPO must follow the same requirements as obligated
- ✍ Alternative, informally allocate responsibility for data privacy compliance other employee
 - ✍ Tip: do not name the position/role as DPO, but as Data Privacy Officer
 - ✍ Chief of Internal Audit? IT audit/compliance experts?

Relationship with the Board



- ✎ The DPO should directly report to the highest mgmt level (art. 36.2)
- ✎ Reporting line to top management, e.g. CEO, board president
- ✎ Sell data protection as a competitive advantage to the Board
- ✎ Understand issues discussed by the Board
 - ✎ new products, technologies, industry-specific, stakeholders' needs
- ✎ Independence requires a channel to escalate issues to the Board
- ✎ Approval to update policies to add privacy controls
- ✎ Usual reports from the DPO to the Board
 - ✎ operation of the privacy program: key performance indicators, training
 - ✎ risk map: new risks, changes in regulations, ignored recommendations
 - ✎ data breaches: past events, consequences, prevention plans
 - ✎ investments: cost of compliance, future budget, plans

Relationship with the CIO



- ✎ Historically, the CIO took personal data protection responsibilities
- ✎ The CIO is a partner for improving the privacy culture
 - ✎ Key: educate the CIO on the new GDPR requirements and best practices to comply with them (what and how)
- ✎ A good working relationship, but separated
 - ✎ Clearly identify personal data protection issues to involve the DPO from other IT tasks
 - ✎ Many shared concerns: confidentiality, security, tools, access controls,...
- ✎ Many remediation actions for GDPR compliance are owned by the CIO
- ✎ The DPO has a consultation (and approving) role
 - ✎ DPIA, privacy by design/default, approve the go-live of apps dealing with personal data

Discussion case

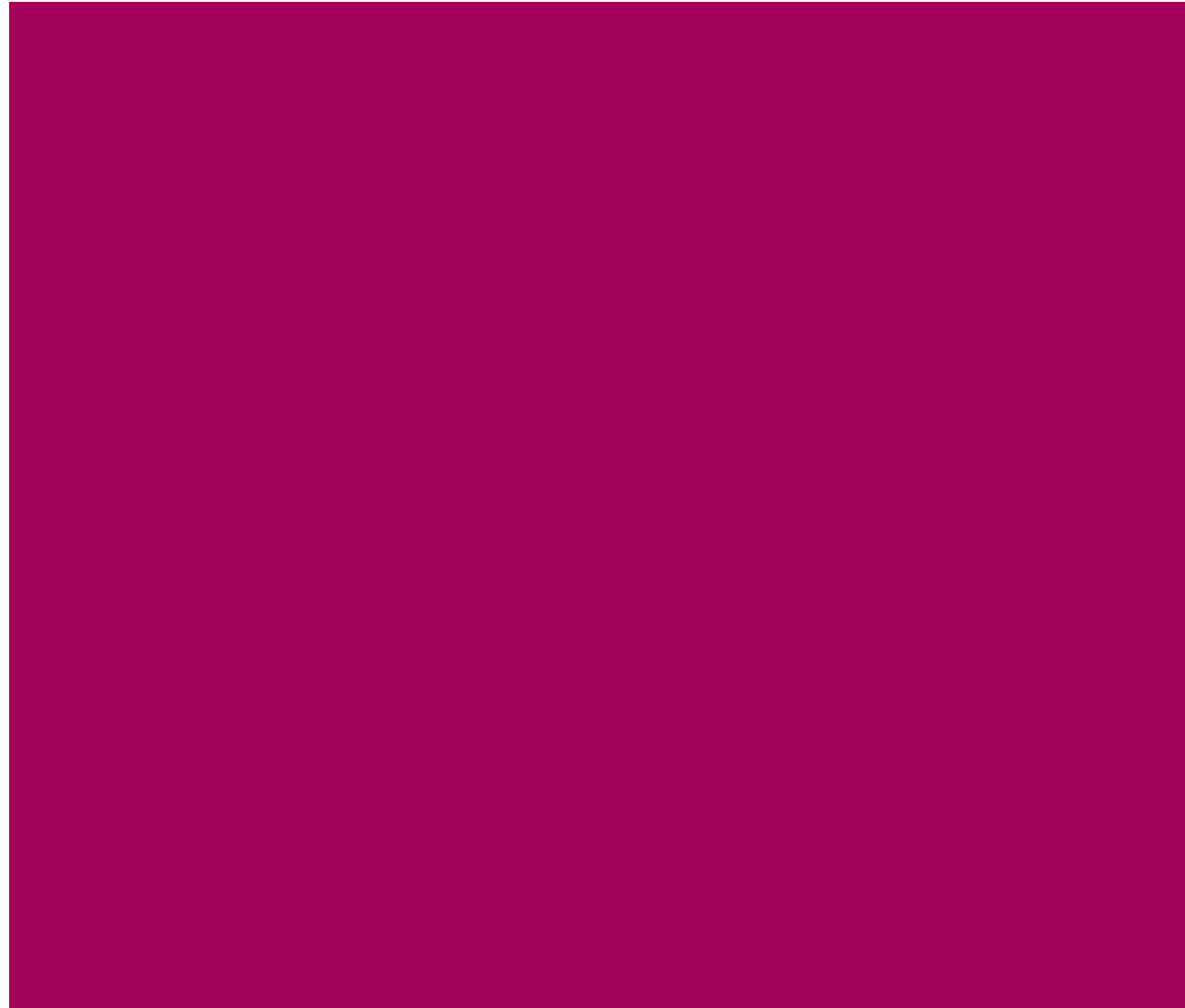


You are the DPO of a large advertising company which monitors behaviours of individuals by collecting registration information, search activities, browsing history, visited pages, time spent in a website, purchasing habits, location, hobbies, age, sex and to make customised ad.

The company regularly posts the customised ad

What should be your approach and action plan to ensure GDPR compliance.

How to demonstrate compliance?



Why documentation?



“If something is not documented, it is not done”

- My auditor

Extensive documentation efforts for GDPR

Discussions about the right level of documentation

Formalizing operational procedures

Need to integrate privacy practices in policies

Controllers must be able to prove their compliance with the GDPR under the accountability principle and upon request of Supervisory Authority

Objectives



Management

- ✦ Privacy is part of the general management system
 - ✦ Documentation is the evidence of accountability and good governance
- ✦ Privacy policy
 - ✦ Supported by: document retention and destruction, info classification, breach management,...
 - ✦ Assess and manage the impact of changes in policies
 - ✦ Available to all the staff (training)

Corporate defense

- ✦ Demonstrate compliance efforts (implementation measures, control improvement)
 - ✦ Records of processing activities under your responsibility (art. 30)
 - ✦ When needed, data protection impact assessment (art. 35)
 - ✦ Records of consent from data subjects and guardians (arts. 7 and 8)
 - ✦ Actions taken during a data breach (arts. 33 and 34)
 - ✦ Purposes for collecting information (art. 13)
- ✦ Document legal basis for the processing (art. 5)
- ✦ Privacy clauses in contracts, bidding corporate rules,...

Audits

- ✦ Outsourcer/data processor must prove technical and organizational controls (art. 28, ISAE 3000 type 1, data protection seals and certifications)

Auditor's responsibility for GDPR



Auditor must obtain audit evidence that the entity is in compliance

So, the auditor should

- ✎ Make enquiries as to whether the entity is in compliance with relevant laws and regulations
- ✎ Inspect correspondence with lawyers and regulators
- ✎ Consider material impact of fines of up to 4% of turnover
- ✎ Investigate any breach GDPR breach

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.

Operational privacy



How to demonstrate compliance?

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

Demonstrate compliance



- ✎ Evidence of board engagement in privacy (art. 5)
 - ✎ Unclear evidence: approving a privacy program, board agendas and minutes covering GDPR issues, evaluation of privacy reports, action plans involving board members, list of project stakeholders, budgets, approval
 - ✎ Nice to have: job roles assigning privacy responsibilities, privacy core team and experts, meetings and guidance with other internal functions dealing with personal data
 - ✎ General: ISO/IEC 27001 compliance certificate

Demonstrate compliance



- ✎ If required, board minute designating a DPO (art. 37, 38)
 - ✎ including evidence of independent reporting (org. chart, reports to the board), delegated tasks (contract, job description), proper budget, qualifications and certifications (CV, identity and background checks) and communication to supervisory authority
- ✎ 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

Demonstrate compliance



Lawfulness of processing (art 6)

- ✎ DPIAs for new or changing programs, systems, processes
- ✎ Contracts and data processing agreements with 3rd parties details the legal reasons for processing
- ✎ Procedure for secondary uses of personal data
 - ✎ How to manage personal information for other purposes other than it was originally collected
 - ✎ Mechanism for de-identifying data (art 89) for archiving purposes in the public interest, or scientific and historical research purposes, or statistical purposes

Demonstrate compliance



Processing of special categories of personal data (art 9) and criminal convictions and offences (art 10)

- ✎ Policy for collection and use of sensitive personal data
 - ✎ How to document legal basis for processing sensitive data contract, vital interests
 - ✎ How to identify racial or ethnic origin, political opinions, biometric data
 - ✎ Controls linked to the data classification policy
 - ✎ Ensure the specific written consent
 - ✎ Contact clauses limiting processed after prior instructions from the controller

Demonstrate compliance



Consents (arts 7 and 8)

- ✎ Procedure to obtain valid consents
 - ✎ Consents are gotten before processing data
 - ✎ Relevance, clear and plain language, simplicity and accessibility
 - ✎ Define who is responsible for controlling that processing is consistent with consents
- ✎ Procedures to respond to requests to opt-out of, restrict or object to processing
 - ✎ Effectively stop processing, responsible person, response actions
- ✎ Procedure for children's consents
 - ✎ How to verify parents/guardians

Demonstrate compliance



Consents (arts 7 and 8)

✎ Maintaining records of consents

- ✎ Records of consent are stored in a secure environment (including how and when consent was provided)
- ✎ The purpose of the processing and the consent language the user has agreed to is stored at the time consent is provided
- ✎ Relevant metadata associated to consent (IP address, geolocation, browser type and device type) is recorded along with consent
- ✎ Terms of service acceptance and its version are recorded at the point of registration, including whether a social identity is used to register

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

Demonstrate compliance



Right of access (art 15)

Also managed for: rectification (art 16) erasure (art 17) restrict processing (art 18) update (art 19) portability (art 20) object (art 21) limit profiling (art 22)

✦ Subject Access Request procedure and similar

✦ Define the channels

- ✦ email, online form, in writing

✦ Formalize who is responsible for responding (on time)

- ✦ who is authorized to access data to respond
- ✦ coordinating with other operative units
- ✦ cover internal data and external data used by other processors and third parties
- ✦ KPI reports (number of request, complains, explanations of root causes)

✦ Define who controls/approves the final action

- ✦ copy, modification, deletion, restriction
- ✦ confirm that the required action is correct (on the event and periodic monitoring)
- ✦ minutes of management meetings justifying any refusal

Manage privacy risks



How to demonstrate compliance?

Demonstrate compliance



Responsibility of the controller (art 24)

- ✎ Formal privacy program
 - ✎ Evidence of accountability in GDPR compliance
 - ✎ Evidence of activities in managing privacy
 - ✎ implementing effective privacy measures and controls
 - ✎ safeguarding the rights of data subjects
 - ✎ Privacy risk assessment across the organization
- ✎ Link to the data privacy policy
- ✎ Contingency plans
 - ✎ Scenario planning, documented actions for breaches
 - ✎ Documented and tested!

Demonstrate compliance



Responsibility of the controller in outsourcing (art 28)

- ✍ Clear instructions from the controller to the processor
 - ✍ Document how they are given and how they are accepted
- ✍ Annual review contracts with third party data processors
 - ✍ Approval of a privacy expert (or DPO)
 - ✍ Use of an approved contract template or approve exceptions
 - ✍ Tip: document the meetings with vendors when discussing privacy issues
- ✍ Maintain data privacy requirements for third parties
 - ✍ clients, vendors, processors, affiliates
- ✍ Due diligence and audits for data privacy and security
 - ✍ posture of potential vendors and current processors
 - ✍ evidence that the controller adopted/will adopt effective technical measures
- ✍ Controls for subsequent outsourcing

Demonstrate compliance



Records of processing activities (art 30)

- ✎ Can be linked to the data inventory
- ✎ List of all processing activities
 - ✎ Where, type of data, type of processing by third parties, cross border data transfers
- ✎ Evidence of updates
- ✎ Approve the inventory of data managed by controllers

Document granularity



- Granularity – the scale or level of detail in a set of data. In GDPR it means the requirement to maintain a record of each processing activity.
- Adopt the following approach to the register the activity:
 - Where a processing activity has multiple purposes, adopt a granularity of one entry for each
 - Processing activity with a distinct purpose – if a processing activity has multiple purposes, multiple entries should be used.
 - Where multiple entities (separate data controllers) perform processing activities, a separate entry is used for each entity.
- Granularity of consent; clear to the data subject what they are giving consenting to
- If a DPA asks to see a register of all processing activities of a given entity, documentation means to be able to provide those processing activities that are relevant to each entity.

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

Demonstrate compliance



Security of processing (art 32)

- ✎ User management policy
 - ✎ role-based access, segregation of duties
 - ✎ defined responsible for approving access rights
- ✎ Technical security measures
 - ✎ intrusion detection, firewalls, monitoring, encrypt personal data
- ✎ Review of user accesses and security measures
- ✎ Confidentiality and privacy provisions in employment/vendor contracts
- ✎ Internal security audits and mitigation responses

Demonstrate compliance



Data protection impact assessment (arts 35 and 36)

- ✎ DPIA guidelines and templates
- ✎ Consultation to all stakeholders
- ✎ Follow-up of action plans for detected risks
 - ✎ Evidence of monitoring for closing issues
 - ✎ Changes to systems and controls are tested as effective
- ✎ Eventual consultation to the supervisory authority

Demonstrate compliance



Data breach notification (arts 33 and 34)

- ✎ Data privacy incident or breach response plan
- ✎ Monitoring of abnormal data activity (e.g. downloads)
- ✎ Escalation procedures involving the privacy expert
- ✎ Protocols for
 - ✎ Breach notification to affected individuals
 - ✎ Breach reporting to regulators, credit agencies, law enforcement
- ✎ Log of incidents with forensic analysis
- ✎ Periodic testing / simulation
- ✎ Insurance

Demonstrate compliance



Privacy by design and by default (art 25)

- ✎ PIA policy for
 - ✎ new or
 - ✎ changes to existing
- ✎ Integrated into system development and business processes
- ✎ Access controls to least privilege
- ✎ Involvement of a privacy expert (or DPO)
- ✎ Assess the risk of affecting data subject rights
- ✎ Assess technical measures (pseudonymisation)

Data Protection Officer



How to demonstrate compliance?

Demonstrate compliance



Data protection officer (arts 37 to 39)

- ✎ Independent oversight role
 - ✎ Evidence of full access to information and staff
 - ✎ Budget
 - ✎ Autonomous, free from other incompatible tasks
- ✎ Documented tasks for a privacy program
 - ✎ Advising on privacy risks
 - ✎ Facilitate changes to embed privacy controls in all policies and updating them annually!

Demonstrate compliance



Data protection officer (arts 37 to 39)

- ✎ Training and awareness campaigns
 - ✎ Materials: training course notes, posters, presentations, leaflets, briefings, web pages, emails, quizzes, competitions
 - ✎ Metrics: attendance, test results,
- ✎ Conducting an enterprise privacy risk assessment
- ✎ Cooperating as point of contact for the supervisory authority

Demonstrate compliance



Data protection officer (arts 37 to 39)

✎ Monitoring compliance with the GDPR

- ✎ Requirements identification
- ✎ Periodic risk-based audits
 - ✎ Start from the data inventory
 - ✎ Focus on processes with complains or incidents, sensitive information, low security and international transfers
 - ✎ Tip: liaise with internal audit and compliance
- ✎ Internal and third party audits
- ✎ Walk-throughs documents
 - ✎ Compare practices against policies and GDPR requirements
 - ✎ Select samples to test how consents are obtained and how contracts are monitored
- ✎ Reporting to all stakeholders (signature in reports)

Demonstrate compliance



Data protection officer (arts 37 to 39)

✎ Reporting to the upper management

- ✎ Advances in the privacy program (reports, schedules)
- ✎ Involving key stakeholders (meeting)
- ✎ Tip: Document all the evidence of the rationality to tolerate risks

✎ Tracking of risks and regulations

- ✎ Evidence of monitoring changes in GDPR requirements
- ✎ Participation in training and conferences, subscription to legal services to receive updates, meetings with the legal counsel

Dawn Raids



- Dawn raids are relevant in several oversight compliance perspectives
- The oversight authorities *can suddenly and without warning*, sometimes even together with other oversight authorities, e.g. antitrust authorities, and police and armed with a search warrant, barge into the company's premises looking to seize, as much as possible.
- A control visit scenarios like the one described above, are a new reality in their crackdown on cyber, data privacy, data protection, competition law and antitrust and other suspected violations.
- Conducting a scenario planning exercise can help all stakeholders to understand what to expect in the event of a surprise dawn raid.
 - How to respond to ensure that employees cooperate during an investigation
 - Protect the legal rights of the company and employees
 - *Just one misstep has the potential to throw any company into a tailspin disrupting the company's day-to-day operations, not to mention damaging its*

Preparing for Dawn Raids



- Robust data privacy, protection or antitrust compliance programs should include employee training on how to respond to a raid, especially about security guards and receptionists
- Employees need to know who to alert when the investigators arrive because time and speed are of the essence.
- Consider a laminated, one-page raid manual for front-desk staff and the security team to refer to, particularly in the absence of legal counsel

Preparing for Dawn Raids



- Check the validity of the warrant correctly
- make sure it covers the company and premises;
- understand the scope and subject matter of the investigation (alleged violations, relevant products and services, departments, geographical range)
- Identify the date when the warrant ceases to affect.
 - In the European Union and the United Kingdom—oversight authorities have no obligation to wait for legal counsel to arrive before starting their inspection. This situation is especially the case when the alleged non-compliance or breach constitutes a potential criminal investigation, resulting in the arrests of individuals.

Dawn Raids



DAWN RAID CHECKLIST

Below is a 10 point checklist of how to prepare customised procedure and respond to a compliance dawn raid.

Pre-raid measures

- Ensure that employees, especially receptionists and security teams, are familiar with their role in the event of a dawn raid.
- Develop a rapid response team with the appropriate skills, knowledge and discipline, including senior management, an IT expert, in-house legal or compliance representatives, and external counsel.
- Provide employees with a laminated, one-page raid manual for front-desk staff and security teams to remind them what to do, and who to call immediately, during a raid.

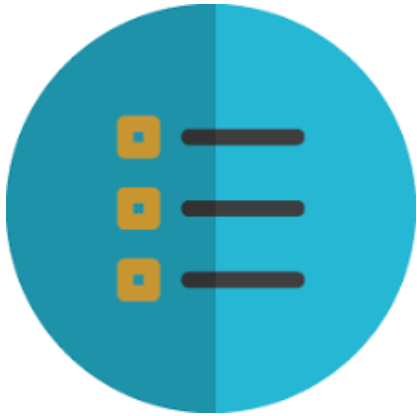
During a raid

- Reception staff should find an empty conference room that can be allocated to investigators, and a high-performance photocopier should be made available.
- Ask the investigators if they will wait until external counsel arrive (investigators may agree to do so for a short time).
- Ask to see the subpoena: Check that it applies to the company's premises. Check to see if it is for a civil or criminal investigation. Check to see if the date of the subpoena is valid.
- Check the identity of all the investigators.
- Make copies of the summons and investigators' IDs.
- Warn staff not to destroy or conceal any documents, and not to disclose to anyone outside the company about the ongoing investigation.
- Remind employees to act cooperative and not to break any seals.
- Inform the PR team and consider the communication response that needs to be given to the public if the investigation is leaked to the media.

 Dawn Raid template in the toolkit



GDPR



Compliance Checklist

Summary




GDPR Compliance Checklist



Territorial scope

-  identify non-EU group companies that monitor, track or target EU data subjects

Supervisory authority to determine and assert jurisdiction

-  determine the organisation's main establishment/central administration is,
-  where decisions on processing personal data are taken
-  where the main processing activities take place



Data governance and accountability

-  DPO, Design and default, Privacy impact assessments (DPIA), Training
-  identify key stakeholders, demonstrate compliance, consent, reporting lines

Export of personal data

-  identify where personal data is processed within organisation, & third party



Controllers and Processors

-  intra-group, customer or service provider arrangements where a group company is a joint controller
-  intra-group processor agreements, requirements to maintain group liability


GDPR Compliance Checklist




Lawful grounds to process and consent

-  For each type or category of processing, identify and document the grounds for lawful processing & legitimate interests
-  The storage period for the data (required for the fair processing notice)

Fair processing information/notices

-  Best process for fair processing in a clear and intelligible and information machine readable form


Data subject rights

-  Assess how the rights trigger and how they will be exercised in both customer and employee contexts

Big Data, research and automated decision making

-  Link between original and secondary purposes, assess the context and relationship between the data subject and controller

Personal data breach

-  Data breach response and notification procedures to meet 72 hour notification deadline to Supervisory Authority

Privacy governance



Approach for governing privacy



- ✎ **Human right?** 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 has resulted in contextual adaptation of different laws. Industries have adopted alternatives to formal regulation like codes of practice, ISO standards and trust seals

Approach for governing privacy



✎ **Comprehensive regulation or sectorial laws?**

EU and Singapore 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

Directives

- ✍ Require individual implementation in each Member State
- ✍ Each state can implement rules in their own way
- ✍ Are implemented by the creation of national laws approved by the parliaments
- ✍ Set out a goal that a member state must achieve, room for tailoring
- ✍ The EU Data Protection Directive 95/46/EC is a Directive
- ✍ UK Data Protection Act 1998



Regulations

- ✦ Immediately applicable in each Member State in a uniform manner
- ✦ Binding legislative Act
- ✦ Require no local implementing legislation – no tailoring
- ✦ EU GDPR is a Regulation
- ✦ Regulations are not negotiable by member states
- ✦ Regulations may apply to countries outside the EU if they affect EU subjects



Approaches for governing privacy



- ✎ A **complete overhaul** of data protection regulation with extensive updates of what can be considered identifiable information



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

- ✎ **Specific** and significant rights for data subjects to seek compensation, rights to erasure and accurate representation
- ✎ **Compensation** can be sought against organizations and individuals employed by them



- ✎ **Significant** reduction in that amount based on the implementation of technical, or organizational controls implemented



Privacy program



Area	Planned tasks	Owner	End date	Status and comments
Consent practices	<ul style="list-style-type: none">- Identify activities requiring consents- Review the writing to ensure GDPR compliance (e.g. unambiguous, unbundled, up to date)- Ensure processes are in compliance (e.g. withdrawals, other rights)- Test how they are being collected and retained <p><i>Scope: Mkt, sales, HR, procurement systems</i></p>	Jan Hansen (DPO)	30 Oct	Done
Security Plan
Third Parties List				
Training Plan				

All Links



- FAS Presentation - <https://www.eugdpr.institute/fas/>
- FAS Exam - <https://www.eugdpr.institute/gdpr-fas-exam/>
- DPO Presentation - <https://www.eugdpr.institute/dpo/>
- DPO Exam - <https://www.eugdpr.institute/gdpr-dpo-exam/>
- CEP Presentation - <https://www.eugdpr.institute/cep/>
- CEP Exam - <https://www.eugdpr.institute/gdpr-cep-exam/>
- pdf links
 - FAS: <https://www.eugdpr.institute/wp-content/uploads/2019/05/day1.pdf>
 - DPO: <https://www.eugdpr.institute/wp-content/uploads/2019/05/day2.pdf>
 - CEP: <https://www.eugdpr.institute/wp-content/uploads/2019/05/day3.pdf>