



GENERAL
DATA
PROTECTION
REGULATION



FAS
Foundation

DPO
Masterclass

CEP
Practitioner



Foundation Training, Day II Budapest November 2019

All Presentation and Exam 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/2019/11/day1.pdf>
- DPO: <https://www.eugdpr.institute/wp-content/uploads/2019/11/day2.pdf>
- CEP: <https://www.eugdpr.institute/wp-content/uploads/2019/11/day3.pdf>

2019/10 Key Findings/Focus areas

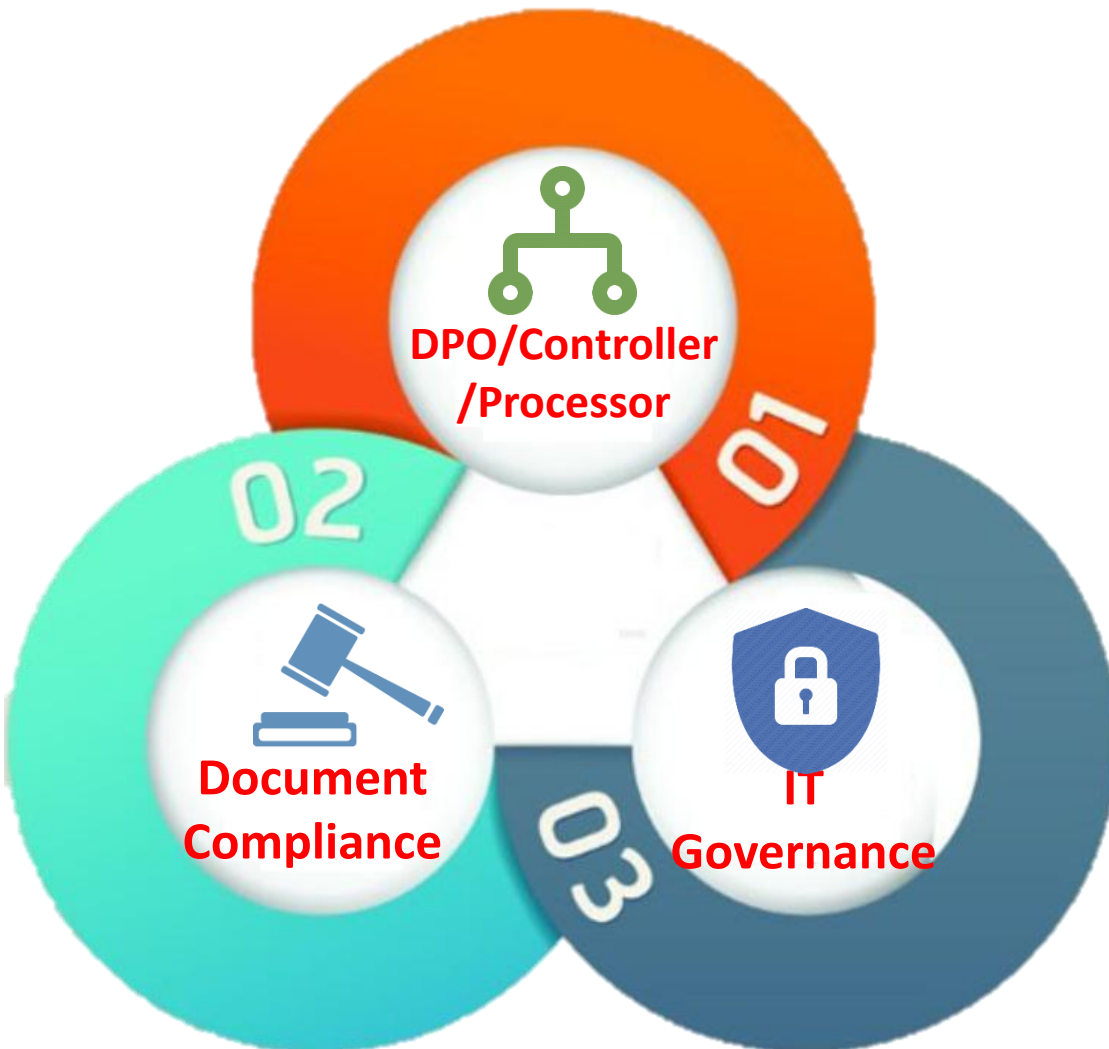
- The adoption of next-generation digitisation/IT transformation include IT governance mechanisms, automation methodologies and enabling technologies that comprise the next-generation IT infrastructure
- Organisations that are digital leaders have made substantially more progress with their IT innovation and data transformation initiatives.

Top 10 Priorities for 2019:

- Enterprise Risk Management
- Cybersecurity Risk/Threat
- Vendor/3rd Party Risk management
- Fraud Risk Management
- COSO Integrated Control Framework
- Agile risk and compliance
- Cloud computing
- Lease Accounting Standard – Accounting Standards Update No. 2016-01, Leases (842)
- AICPA’s Criteria for Management’s Description of an Entity’s Cybersecurity Risk Management Program (Exposure Draft)
- Revenue Recognition Standard (Financial Accounting Standards Board [FASB] Accounting Standards Update No. 2014-09)
- <https://www.businesswire.com/news/home/20160919005649/en/AICPA-Proposes-Criteria-Cybersecurity-Risk-Management>
- <https://www.fasb.org/jsp/FASB/Page/ImageBridgePage&cid=1176169257359>

Preparing for the regulations (GDPR)

1. Gain 'buy in' from key people in your organisation
2. Escalate the impact GDPR is likely to have throughout the organisation
3. Identify primary areas that could cause compliance problems
4. Compliance with the areas that need a review; IT Governance approach
5. New procedures in place to deal with the transparency, rights, ownership
6. Start by looking at your organisation's risk register/databases
7. Review the significant resource implications
8. New elements with significant enhancements, some first, some different
9. Map out which parts of the DPR will have the greatest impact on your business
10. Documentation that data controllers can demonstrate accountability
11. Review all contracts and other schedules where personal data is shared
12. Provisions relating to profiling for children's data
13. Compliance difficult if delayed till the last minute



- ✎ **GDPR Functions**
- ✎ **Controller/Processor /DPO Challenges**
- ✎ **Corporate culture**
- ✎ **Holistic Approach**
- ✎ **IT and Cyber security**
- ✎ **Automate compliance**
- ✎ **Checklists and Templates**
- ✎ **Oversight Authorities**



- ✎ 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 data 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?



Reduced GDPR focus, in 1,5 years



- 48% of decision-makers reported that their business was fully compliant
- 42% rated their organisation as 'mostly compliant'
- 35% said GDPR was less of a priority for their organisation in the last 12 months
- 28% had implementing new processes around the handling of sensitive data
- 18% employed DPO, other compliance staff 18%, and new technology 17%
- 7% said user education and training had been their biggest area of investment
- 35% decision-makers; majority of compliance activity up to the May 2018 deadline
- 6% said that the ICO's high-profile announcements of fine British Airways and Marriott had subsequently shocked the back to greater awareness.
- 70% of decision-makers; organisation felt very positively about GDPR
- 62% said their business had made GDPR a top priority over the past year

+50% not fully GDPR compliant- a perfect storm



- 19 months after 19th May 52% not fully GDPR compliant
- 37% have reported an incident to DPA in the past 12 months
 - mid-sized organisations versus larger enterprises; double the amount
 - 17% having reported more than once
- 39.5% of mid-sized companies reported full GDPR compliance
- 56% of large and 51% of small companies.
- 53% of mid-size companies reported data breaches in the past 12 months
 - compared with 36% of small companies and
 - 23% of enterprise organisations*. Similarly, a notably lower percentage
 - An evident gap in compliance performance among mid-size companies

Source; ICO Egress survey, September 2019

12 steps for compliance

GDPR is here to stay at a global level,. Training and awareness of the principles and values will enhance the GRC processes in the organisation

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;

Data is processed fairly and Lawfully implemented, executed and processed;

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 six lawful purposes, and not be further processed in any manner incompatible with those purposes;

12 steps for compliance

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;

Data is 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.

12 steps for compliance

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).

Evaluate the GRC/GDPR and IT Governance and Security organisation;

Keep logs, documentation, records, and evidence of processes, systems, access, deletion;

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 the country, unless that State or territory ensures an adequate level of protection for the rights/freedoms of data subjects.

Determine the sensitive data, implement controls, policies and monitoring activities;

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.

Brexit Consequences

1 **Continue to comply** and apply same GDPR standards and criteria for both the UK and the Europe.

4 **Evaluate how Brexit will affect** the data protection regimes Review the structure, handling and data flows of EU set-ups.

2 **Data- flows & transfers** to the UK are reviewed & identified. Identify & ensure safeguards as a third country

5 **Review the privacy data** and internal documentation to identify any details that need an update.

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12-infonote-nodeal-brexit_en.pdf

3 **Data- flows & transfers** from the UK are reviewed & identified, with the new transfer/ documentation provisions.

6 **Ensure that key people are aware** of any steps and plans. Update with the latest information & guidance.

Brush up

GDPR
MASTERCLASS



Key Components and Provisions of GDPR

GDPR Overview

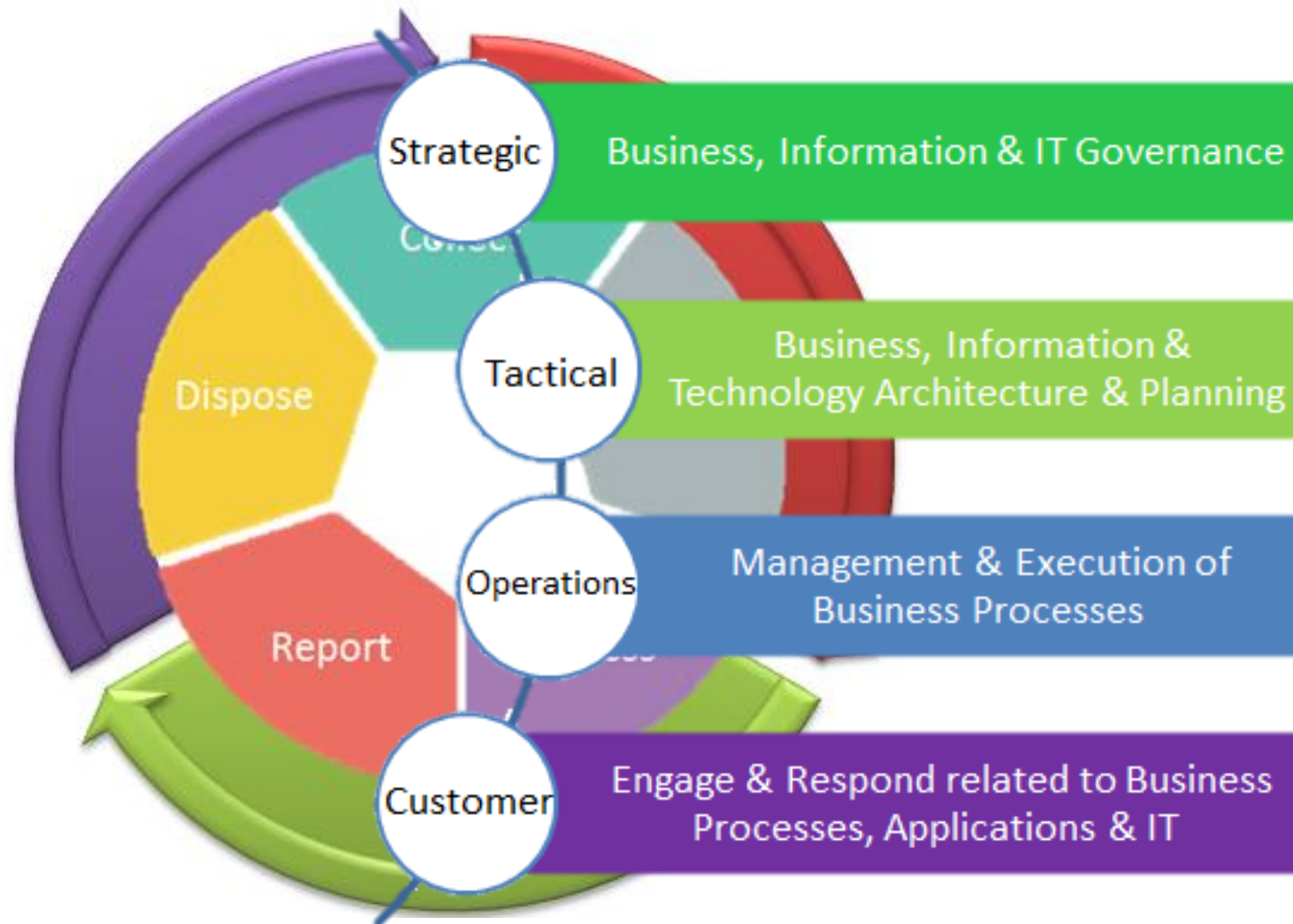
**GDPR
assessment
and
consulting**



**Privacy
engineering**

Privacy Impact Assessment

GDPR Overview



GDPR Overview

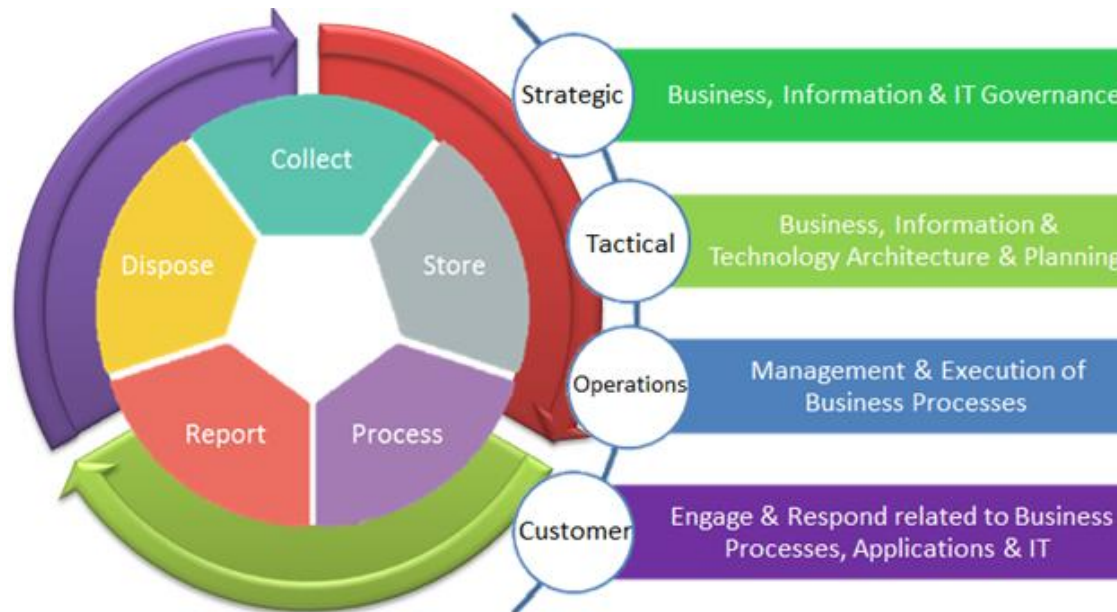
Strategize the approach

Team and budget

Build ops and technical controls

Implement controls

Monitor controls



Core Principles

One Stop Shop

Data Subject Rights

Explicit Consent

Risk Based Approach

DPO Role/ 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

INDUSTRY NEWS > MANUFACTURING

Boeing discloses 36,000-employee data breach after email to spouse for help

Feb 28, 2017, 5:52pm PST Updated Mar 1, 2017, 9:16am PST

Think twice before asking your spouse for help formatting a document, especially if it contains personal information for 36,000 of your co-workers.

Boeing launched an internal security investigation and notified Washington state Attorney General [Bob Ferguson](#) and officials in California, North Carolina and Massachusetts that employee data left control of the company when a worker emailed a spreadsheet to his significant other.

Boeing said the unnamed employee told investigators he sent the document to get his spouse's help on some formatting issues.

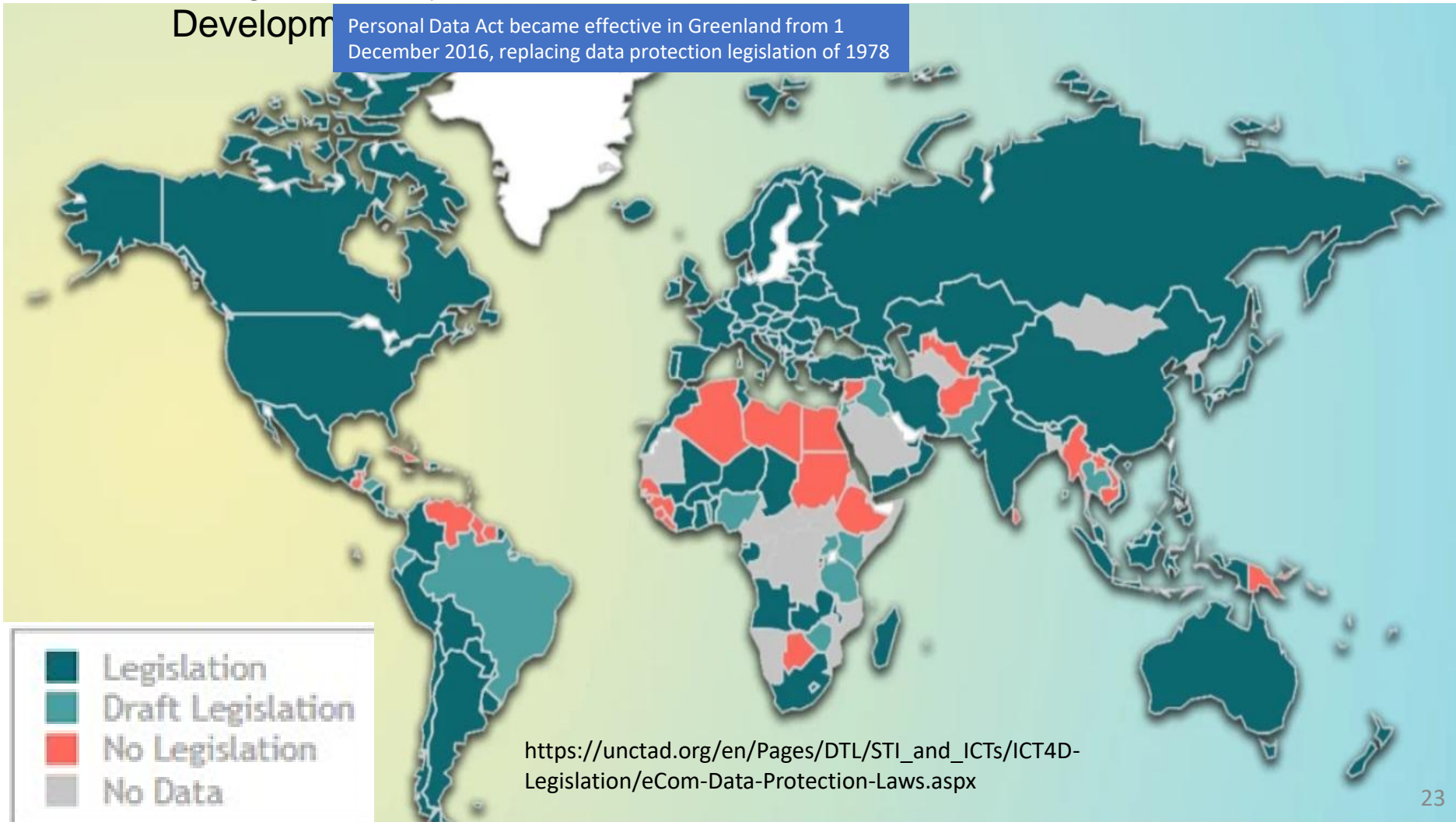


Current trends in the data protection industry

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

- Organisations 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

How to avoid the GDPR scope?

For an Organisation to ensure that GDPR does not apply :

- Avoid giving the impression that you offer goods or services to users in the EU.
- Remove the top-level domain names of EU from the organization`s website, e.g. “de.”
- No services to EU users on websites marketing
- Removing all EU countries from website address fields or drop-down menus.
- Not using EU member state languages.

15:54 Mon, 13 Jun

VPN 35%



Access Denied
www.baskinrobbins.com



Access Denied

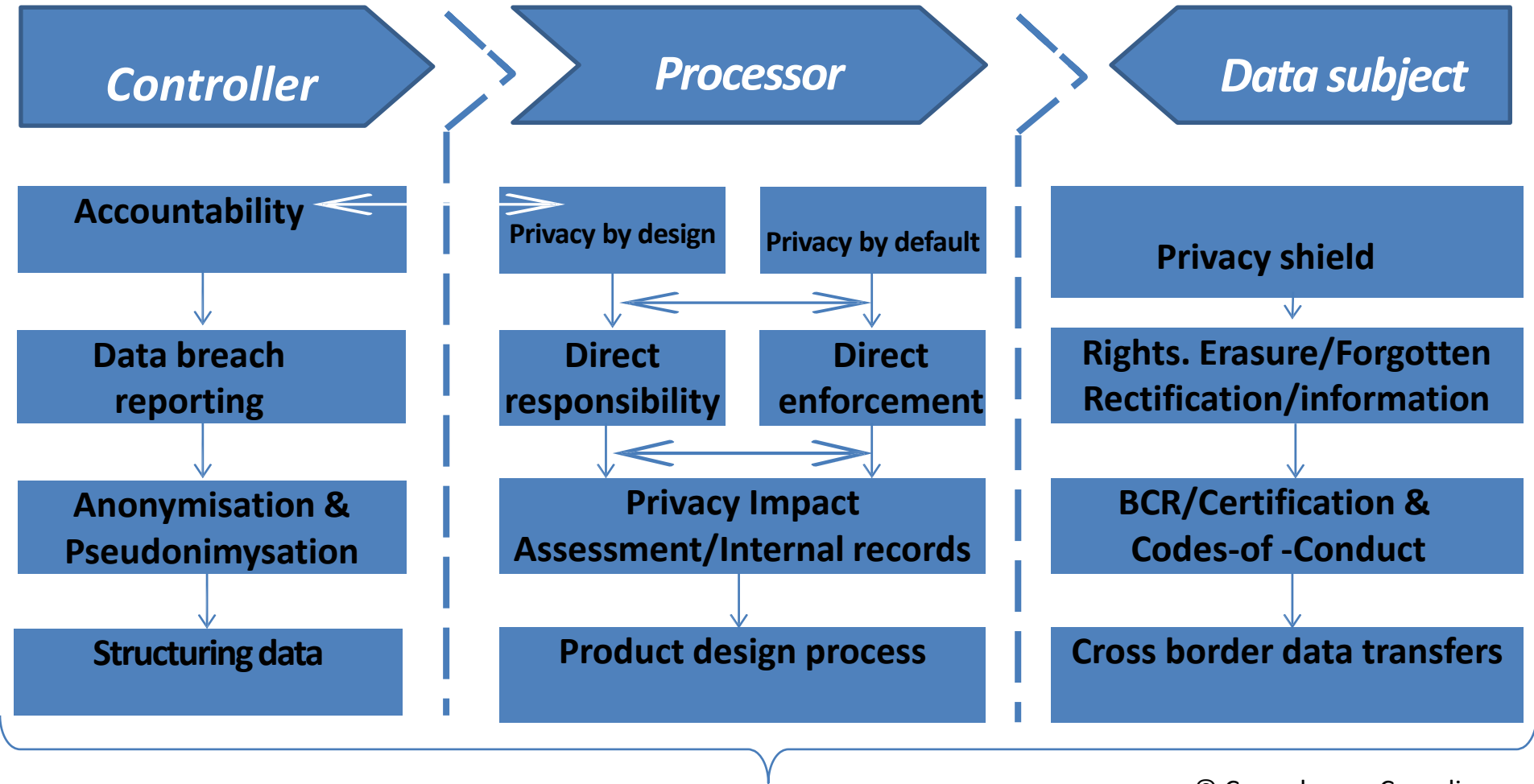
You don't have permission to access "http://www.baskinrobbins.com/content/baskinrobbins/en/products/icecream/flavors.html?" on this server.

Reference #18.6702655f.1563026043.e51e10b

How to avoid the 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

- **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

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



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**

Consent

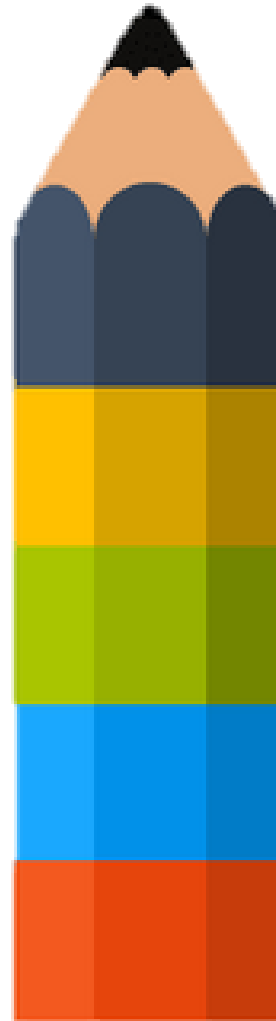
Data subjects understand and explicitly or implicitly agree with the uses of personal information

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

Access and correction

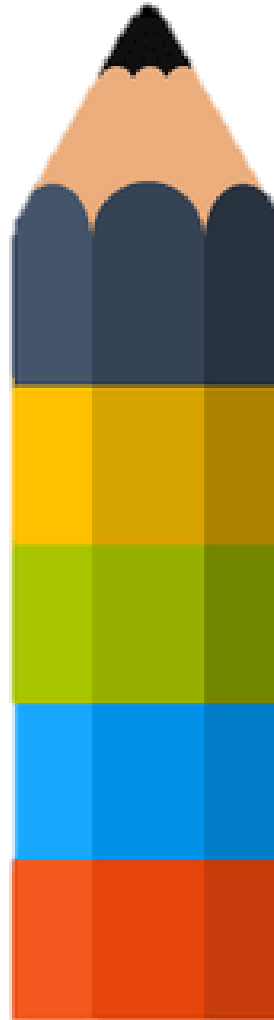
Data subjects access and correct personal information to ensure is accurate, complete and relevant

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

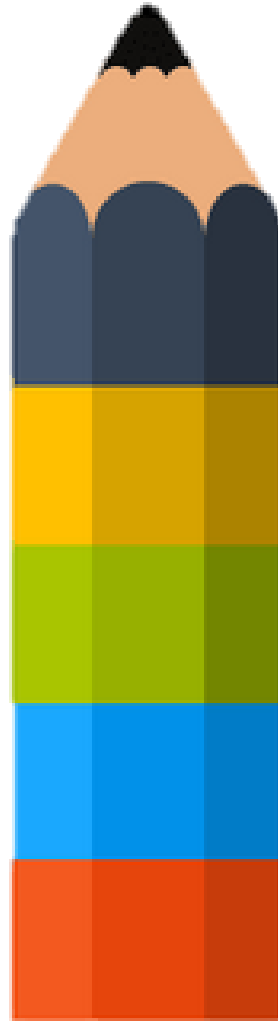
Data controllers consider privacy from the design to the complete development process of new products, processes or services

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

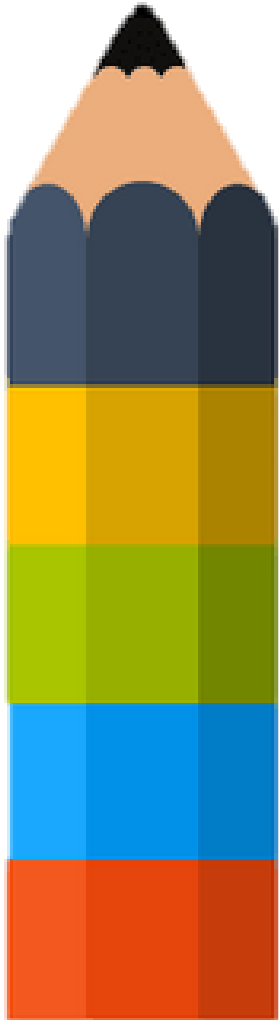


Sensitivity

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



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*

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), behaviour 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

Ideas for “when” to “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 “when” to “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

- ✎ 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 complying

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 Auditor	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 data controller 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 data controller 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.

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

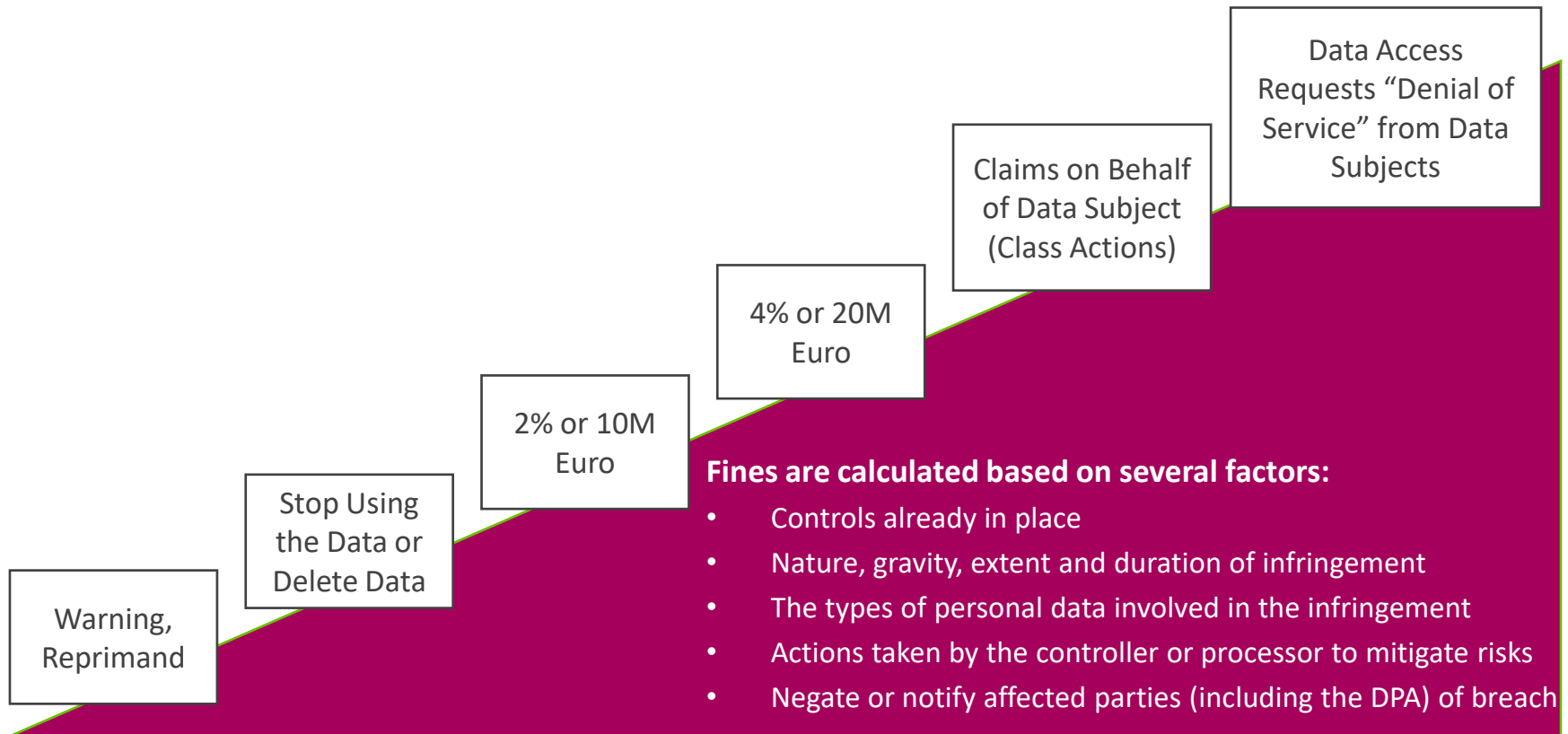
 How do you audit third parties

 How do you write auditing clauses with data processors

 What audit standard is best to use

 What audit tools/templates are available to monitor the transfer, use and processing of personal information

When do the fines stop



Remedies, Liabilities, Penalties

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 must 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.

- ✎ The Social media sites /apps share information that it shouldn't.
- ✎ Therefore must roll out several changes to protect user's data
 - ✎ What are the rules that bans apps from displaying ads that could potentially trick users into downloading unwanted software or share data.
- ✎ What should be the restrictions on how to collect a user's data.
- ✎ Under the new guidance the apps must provide their privacy policy and prompt users to share their data.
 - ✎ List all of the personal data that can be shared with or without consent.
- ✎ Applications which collect/transmit personal data (not required for the app to function) must inform how the data is used.
 - ✎ How can the data subject feel comfortable that the rights are protected

Group Discussion

- ✎ If an app collects and transmits personal data unrelated to the functionality of the app then what must the app do prior to collection and transmission of the data,
 - ✎ the app must prominently highlight how the user data will be used and have the user provide affirmative consent for such use.
- ✎ 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 additional recommendations would you give to ensure GDPR Compliance**
- ✎ **The apps and websites must make sure that primary issues like consent or showing a warning whenever it collects any data without telling the data subject, is taken into consideration.**

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

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	Bidding 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

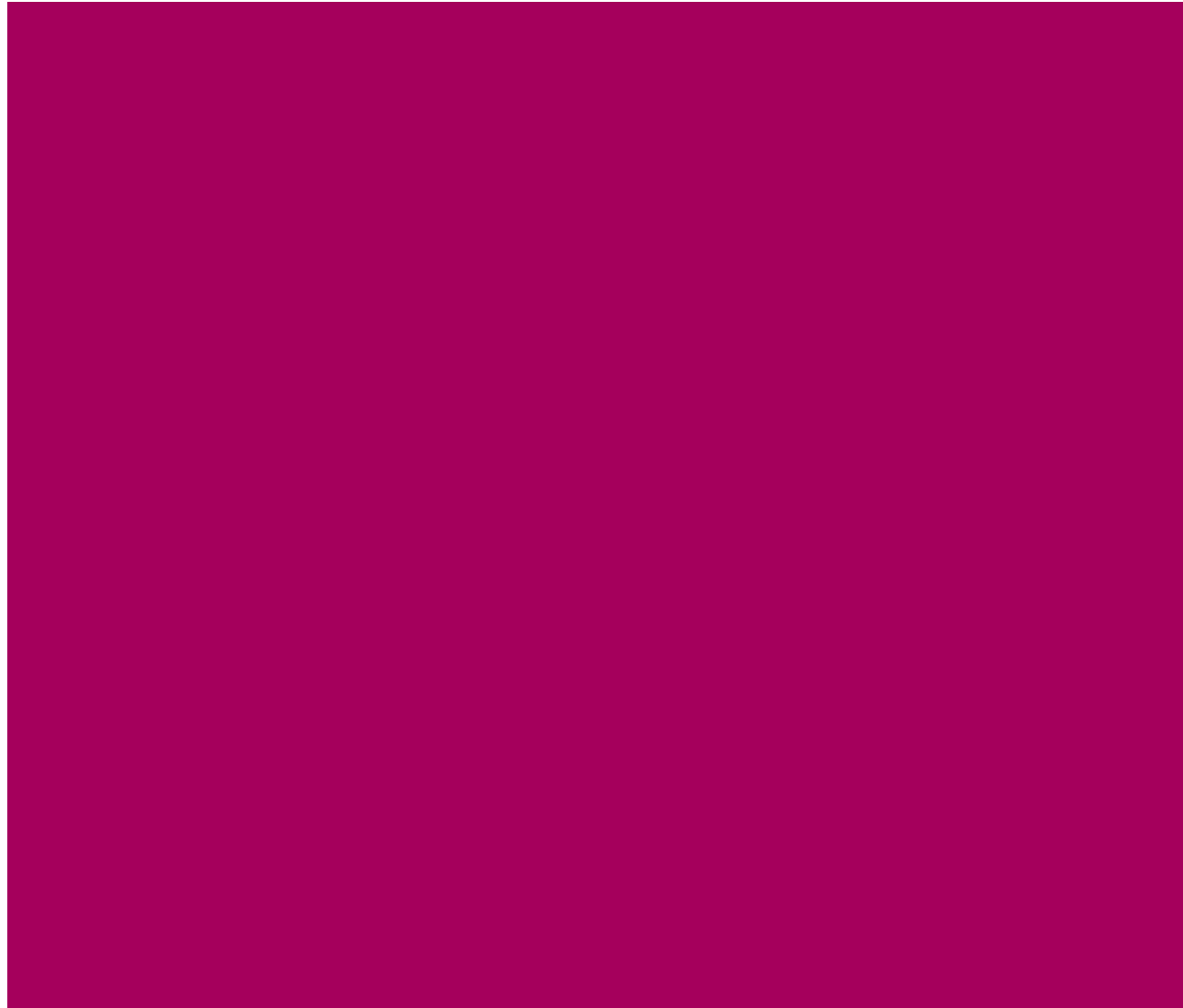
- ✎ **Create & sign off an action plan document by the involved manager depending on the information type**
 - ✎ Follow-up on action plans and document implementation measures (IT and non-IT changes)
 - ✎ Monitoring of risk registry
 - ✎ On-going and past due audits
 - ✎ Involving board members, list 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

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

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 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 GDPR functions



- The Basics;
- A person or the position or responsibility component deals with a matter in which s/he, directly or indirectly, has a *personal* interest that impairs their independence; Governance, Family and Financial interests
- Ensure that ethics and integrity mandates focus on the independence, impartiality, objectivity, accountability and loyalty of the data subject, stakeholders and staff members
- Set up procedures/program such as the management of conflicts of interest to comply with the legal obligations.

- Advance with the following topics:
- Balance transparency in the interests of the data subject
- Data protection rights of individuals to establish trust
- Ensure accountability and demonstrate the independence of the stakeholders
 - high level of impartiality in the performance of their duties (influence decisions, political or sensitive posts)
- Ensure that all potential conflicts are monitored,
 - to ensure that the decisions and actions of key positions are not influenced by their (private) interests.
- Carefully consider what information needs to be made public.

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

- ✎ 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 PR
 - ✎ 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

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

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

- 1 Regulations } GDPR
Local national provisions
- 2 Technical and organizational measures and procedures
- 3 Data security by design and by default
- 4 Industry and sector-specific knowledge
- 5 Experience with the size of the controller or processor
- 6 Awareness of the sensitivity of the data processed
- 7 Experience in inspections, consultation and analysis
- 8 Ability to document processes
- 9 Ability to work with data subjects' and employees' representation organizations
- 10 And get ongoing advanced training!

- ✎ 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

- ✎ DPOs can be voluntary appointed in private organizations
 - ✎ When it is not required by the GDPR
 - ✎ Reason: reduce eventual fines
- ✎ 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

- The Role and function of the DPO is the manifestation of the supervisory authority in an organisation.
- The importance of designating a DPO in achieving compliance with the GDPR must, therefore, be carefully addressed.
- A decision not to appoint a DPO must be signed off on at a senior level and not opting for a DPO where one is required, may attract a substantial fine.

The DPO and the Organisation



- DPOs may be internal (employee) or external (consultant).
- The appointment of DPO is not mandatory, however, advisable for organisations processing personal data to appoint a DPO
- The DPO should report to the highest level of management. Ideally, to the board of directors so that management receives timely advice on matters of data protection.

Compliance

- DPOs are the cornerstone in terms of GDPR compliance.
- The DPO should advise and train employees in compliance

The autonomy of the DPO

- The autonomy of the DPO is not to compromise by putting them in a position that may lead to a conflict of interest. This is more likely in cases where the DPO is internal.
- The DPO is afforded some form of job security. They cannot be dismissed or penalised by the controller or processor as a result of carrying out his or her duties.
- The DPO does not enjoy permanent job status, security or tenure. They can be disciplined or even terminated for other legitimate reasons, such as disciplinary or non-performance issues.
- The controller and the processor must empower and embrace the DPOs and work closely with them, and not view them as Data Police Officer or Snooping Security.

- If significant risks have been identified in some processing operations, they should advise on whether those operations should be abandoned and what safeguards should be put in place to ensure compliance is achieved.
- The DPO must adopt a pragmatic approach by focusing on high-risk processing activities.
 - without neglecting activities that may be deemed to pose lower levels of risks

Discuss the following

GDPR's primary mandates calls for the designation of a DPO

- how will you ensure that the role is played out in the field
 - in terms of actual job responsibilities, compared to what is spelled out in the regulation?
- What are conflicts in job skills and talents required to effectively carry out the role?
- How will you organise the typical reporting lines, and duties of the job, and how to reflect the future changes?
- What are the perspectives and issues when outsourcing DPO functions?
- What are the differences between an internal DPO from a large, multinational company/a SME and the subcontracted DPO

- The DPO is bound by confidentiality obligations in the performance of their tasks
- The DPO is availed with the necessary resources to enable them to perform their duties and to achieve the desired independence.
 - The scale of resources depends on the complexity and sensitivity of the processing activities but would include finances, equipment, budget and staff.
- Due to the critical role, GDPR requires that the DPO is allowed to exercise the functions independently.
- The reason for independence is in recognition of the critical role of the DPO to ensure compliance
- The DPO must be involved in all issues concerning the protection of personal data in an organisation at the earliest opportunity.
- The controller should not direct the DPO regarding how to perform or do their work.
- The DPO cannot be instructed to reach a particular conclusion concerning the investigation of a complaint.

DPO Role & Responsibilities



- The DPO is not personally liable for noncompliance;
- The Data Controller is accountable for overall compliance
- The DPO handles tracking of compliance activities within the organisation
- The DPO function *must* create inventories and registers that detail the personal data processing operations (ROPA) of the various departments of the organisation.
 - These records are not only necessary for the organisation to comply with its overarching accountability obligations but are also needed for the DPO to perform their functions.

- It is acceptable to assign the DPO with other tasks, that does not require them to determine the means and purposes of processing the data,
 - to avoid confusion with the role of the controller.
- The DPO plays a central role in record-keeping concerning data protection in the organisation as the link between the organisation, supervisory authorities and data subjects.
- The DPO exercise its investigative, corrective, authorisation, and advisory powers.
- The DPO collects information that identifies the processing activities that are taking place, ensure that those activities satisfy GDPR principles and advise the controller or processor accordingly.

- The DPO also plays a vital role in advising the controller regarding issues concerning data protection impact assessment.
 - The DPO should advise whether to carry out the DPIA, what methods should be used in carrying out the DPIA,
 - whether it is necessary to engage outside resources to carry out the DPIA.
- In this duty, the DPO should, therefore, advise the controller on the methodology of the DPIA, which activities require data protection audits and which ones should be the focus of management regarding enhanced security measures, regular training of staff and resource allocation.
- Upon completion of the DPIA, the DPO should advise on whether it has been carried out satisfactorily and how to proceed given its findings.

- The DPO is the contact point for data subjects on issues relating to the processing of their data, including enforcing their rights as provided for under the GDPR.
- The DPO can be easily accessed by the data subjects, whether through telephone, mail or otherwise.
- **DPO and the Supervisory Authorities**
- DPO facilitates the access by the supervisory authority to documents and information to enable it to perform the oversight monitoring role
- The DPO seeks advice from the supervisory authorities when necessary.

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.

Step 4: Scenario planning

Before the breach

- ✎ **Address IT risks and vulnerabilities**
 - ✎ all potential threats are identified and defensible (e.g. penetration testing, vulnerability scanning)
 - ✎ multi-layer cyber security defenses
- ✎ **Plan scenarios for responses**
- ✎ **Improve breach detection**
- ✎ **Require patches on DNS servers**

After the breach

- ✎ **Plan actions to contain damage**
 - ✎ business continuity, disaster recovery and reputation management (e.g. company crisis protocols)
- ✎ **Resilience! Plan how to move on from the breach**
 - ✎ Minimize the risk of future occurrence
 - ✎ Feedback from the incident response teams and affected people
 - ✎ Enhance and modify information security policies and training programs

Step 4: Scenario planning

Data breach response procedure

- ✎ **Specific response requirements**
 - ✎ Linked to the privacy risk assessments and data inventory
- ✎ **Incident handling procedure**
 - ✎ Clear accountability, communication, teams, external help
 - ✎ Scenarios
 - internal or external disclosure
 - malicious attack or accidental
- ✎ **IT Security notification requirements**
- ✎ **Training to the response team**
- ✎ **Regular reviews and simulations (“real-life” exercises)**

Monitor data leakage and loss

- ✎ **Intrusion detection systems, firewalls, anti-virus/malware tools**
- ✎ **Threat intelligence**
- ✎ **Tracking of access and movement of personal information within the systems**
- ✎ **Network scanning for policy violations**
- ✎ **Log examination**

Step 4: Scenario planning

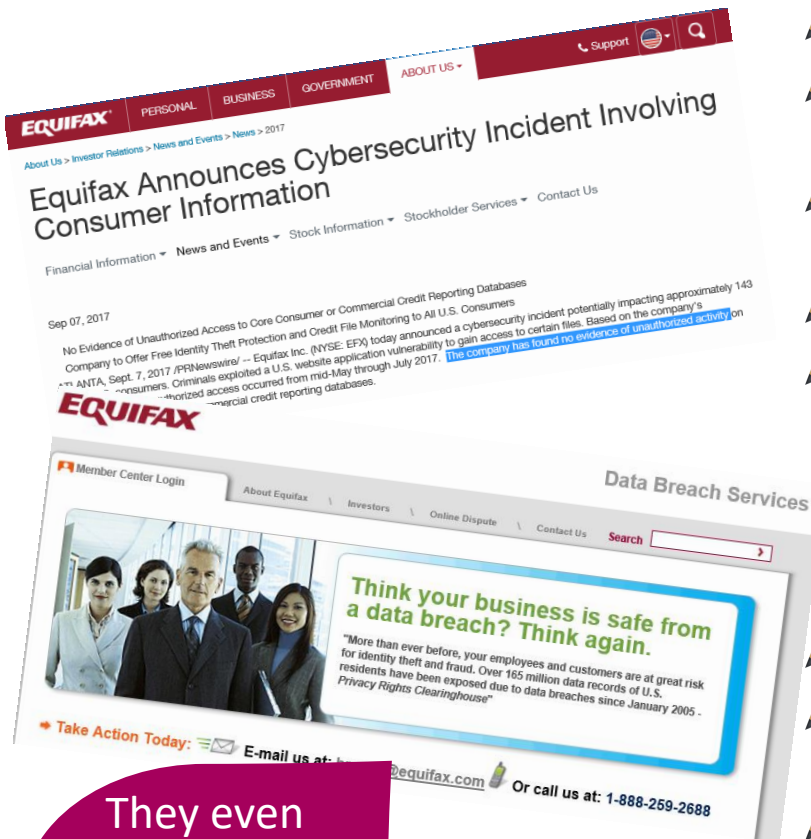
Responding procedure

- ✎ **Validate the breach**
- ✎ **Assign an incident manager (usually CISO) to investigate**
- ✎ **Assemble incident response team (IT, legal, public affairs)**
- ✎ **If the breach is active, block accesses to systems and data**
- ✎ **Identify affected data, machines and devices**
 - ✎ Full extent of the data compromised
- ✎ **Preserve the evidence (logs, backups, images, hardware)**

Monitor data leakage and loss

- ✎ **Notification to data subjects fostering a cooperative help**
 - ✎ If breach likely to result in a high risk to their rights (e.g. fraud, phishing, impersonation for credit application, credit card fraud, loss of reputation, discrimination), no need if breached data is encrypted
 - ✎ Scenarios: customers, employees, vendors
- ✎ **Report to the Supervisory Authority**
 - ✎ DPO role in 72 hours after becoming aware of the breach
 - ✎ Scenarios: inappropriate alteration or data loss
- ✎ **Report to law enforcement in criminal suspicious breaches**

Step 5: Discussion case



- ✎ Equifax, main credit reporting agency
- ✎ Hackers exploited a security vulnerability in a US-based application
- ✎ Exposed names, social security numbers, birth dates, addresses of 143M US consumers and 200K credit card numbers!
- ✎ Required customers to freeze their credit files, offered free credit monitoring and paid new credit cards
- ✎ Equifax had problems with data security before
- ✎ 41 days between discovery and disclosure
- ✎ Significant internal failure to communicate
- ✎ Executives sold 2M in shares just before disclosing
- ✎ Future class action suits

They even offer data breach services

How can we manage the need to investigate a breach within the 72 hours rule, to disclose a breach under IT Security?

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 reputation.*

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 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.

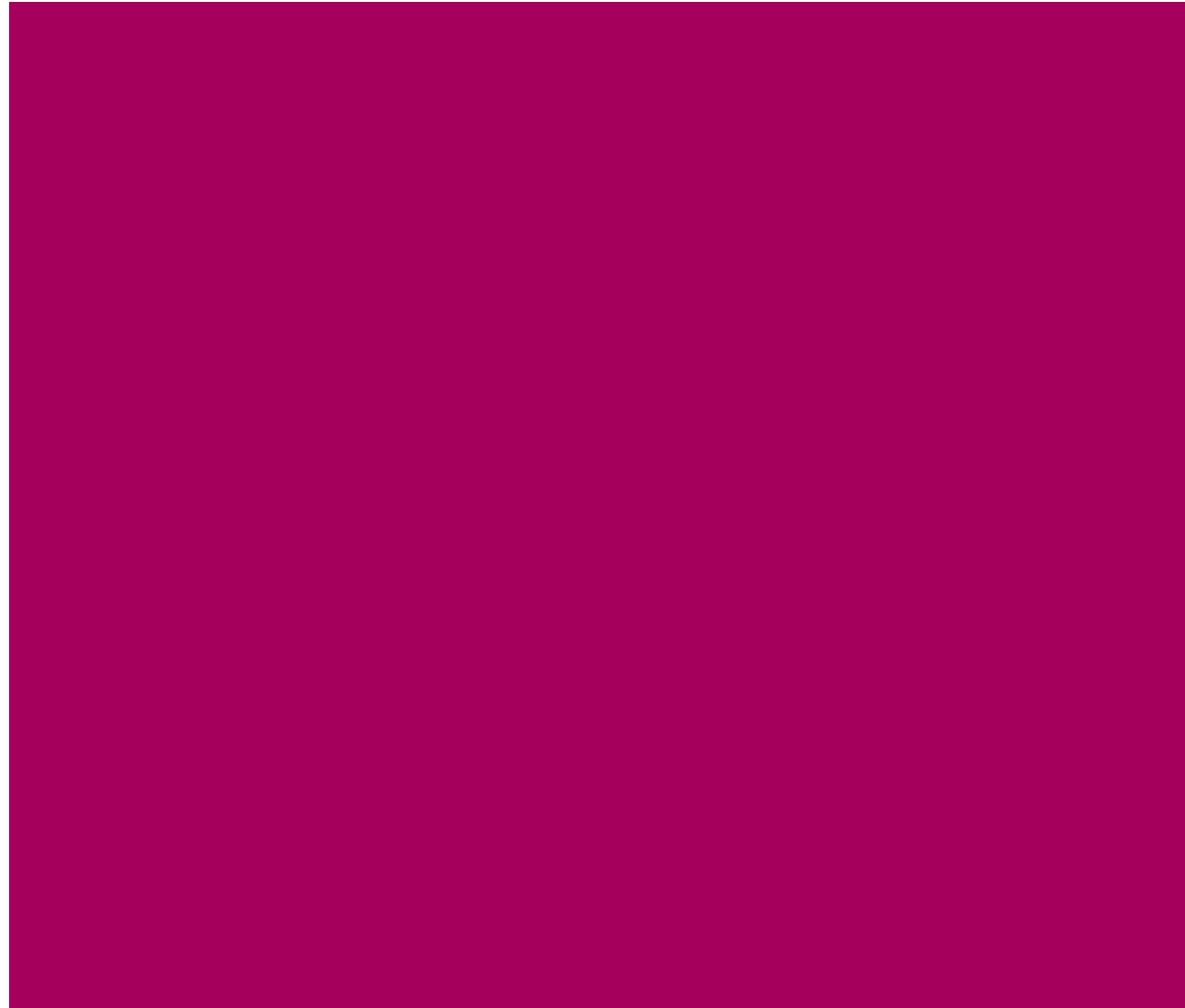
During a raid

- 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



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)

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

- ✎ 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

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

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

- ✎ Policy for collection and use of sensitive 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 data classification policy
 - ✎ Ensure the specific written consent
 - ✎ Contact clauses limiting processed after prior instructions from the controller

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

Consents (arts 7 and 8)

- ✎ Maintaining records of consents
 - ✎ Records of consent are stored in a secure environment (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

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

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?

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!

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 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 agreed to technical measures
- ✎ Controls for subsequent outsourcing

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

- 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.

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

Security of processing (art 32)

- ✎ User management policy
 - ✎ role-based access, segregation of duties
 - ✎ define 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 measures and responses

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

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

Privacy by design and by default (art 25)

- ✎ DPIA policy for
 - ✎ new or
 - ✎ changes to existing } programs, systems, or processes
- ✎ 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)

Controller, Processor and DPO



How to demonstrate compliance?

Data protection officer (arts 37 to 39)

- ✎ Independent oversight role
 - ✎ Evidence of full access to information
 - ✎ Budget
 - ✎ Autonomous, free from 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!

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

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/GDPR desires
 - ✎ Select samples to test how consents are obtained and how contracts are monitored
 - ✎ Reporting to all stakeholders (signature in reports)

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

- Cloud services may transmit data to a third country#
- Controllers will have to meet the usual requirements of the Regulation regarding 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

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 can reduce compliance burden

Binding Corporate Rules

The GDPR expressly recognizes BCRs for controllers and processors as a means of legitimizing intra-group international data transfers

The BCRs must be legally binding and apply to and be enforced by every member of the group of undertakings/enterprises engaged in a joint economic activity, including their employees

BCRs must expressly confer enforceable rights on data subjects. The approach will be more streamlined with a clear list of requirements. This method of compliance is seen by some as the “gold standard” and is likely to become increasingly popular for intra-group transfers

Storage limitation

Deleting individual personal data records in databases, Hadoop, and cloud storage

Fast erasure of individual records

- ✎ BCRs allow companies to transfer personal data outside the bloc from a corporate group or a group of enterprises “engaged in a joint economic activity” operating within the EU to their components outside the EU
- ✎ The mechanism is primarily used by large companies, that have the resources to go through the exhaustive BCR approval process
- ✎ The GDPR after May 2018, recognises BCRs as a legal means of transferring personal data from the EU

Data Processors, Controllers

- ✎ The working party issued separate guidance for data controllers—companies that control the collection and use of personal data—and data processors—companies that process personal data under the instruction of controllers
- ✎ BCRs for processors apply to data received from an EU-based controller that isn't in the same corporate group and then processed by a member of the group
- ✎ BCRs for controllers apply to data transfers from EU-based controllers to non-EU controllers or processors within the same corporate group

Data controllers and processors must now include

- ✎ The scope of the corporate group, including categories of data and types of processing; enforceable rights of individuals, including the right to lodge complaints; and demonstrated accountability

Data Processors must also include

- ✎ Privacy principles related to individual rights; and
- ✎ Service agreements containing all elements required by the GDPR.

Controllers must also include

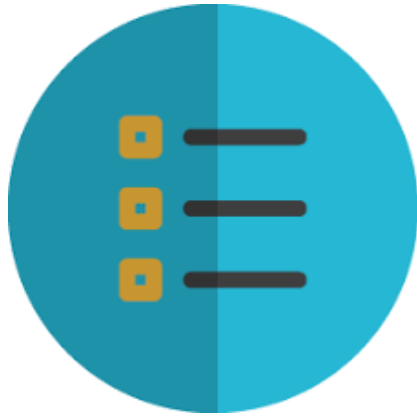
- ✎ Information on individual transparency rights related to processing of their data and the means of exercising those rights
- ✎ An explanation of privacy principles, including lawfulness, data minimization, storage limitation, guarantees of processing sensitive data, and onward transfer requirements to bodies not bound by BCRs;
- ✎ A list of any third-country legal commitments having adverse affect on BCRs will be reported to authorities.

Data Transfer- No adequacy decision, (not within a group where BCR applies). Implementing Standard Contract Clauses (SCCs) is required before the Data Transfer can take place.

- Are the SCCs and the DPA the same?
- Having only the DPA; does the DPA cover both transfer and processing?
- Is a Data Processing Agreement (DPA) is distinct and separate from SCCs and the company needs to have both in place since the SCCs is for transfer of Personal Data while the DPA is for processing of PD?
- Does the DPA only cover the processing part (meaning we have to execute the SCCs and DPA in such case)?
- Transfer of PD processing. Is it allowed by the Regulations to incorporate the essence of the SCCs into a DPA to cover both aspects by a third-party?

- The Standard Contractual Clauses (SCC) is the minimum terms required to comply with article 28 approved by the EU.
- The DPA are the actual terms of the processing between the data controller and processors, setting concrete requirements, roles and responsibilities to each type of requirement. It may be an addendum to an actual contract or a new contract.
- The commission created these models: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

GDPR Compliance



Compliance Checklists



GDPR Templates



GDPR Policies and Procedures

Document and demonstrate GDPR
Compliance



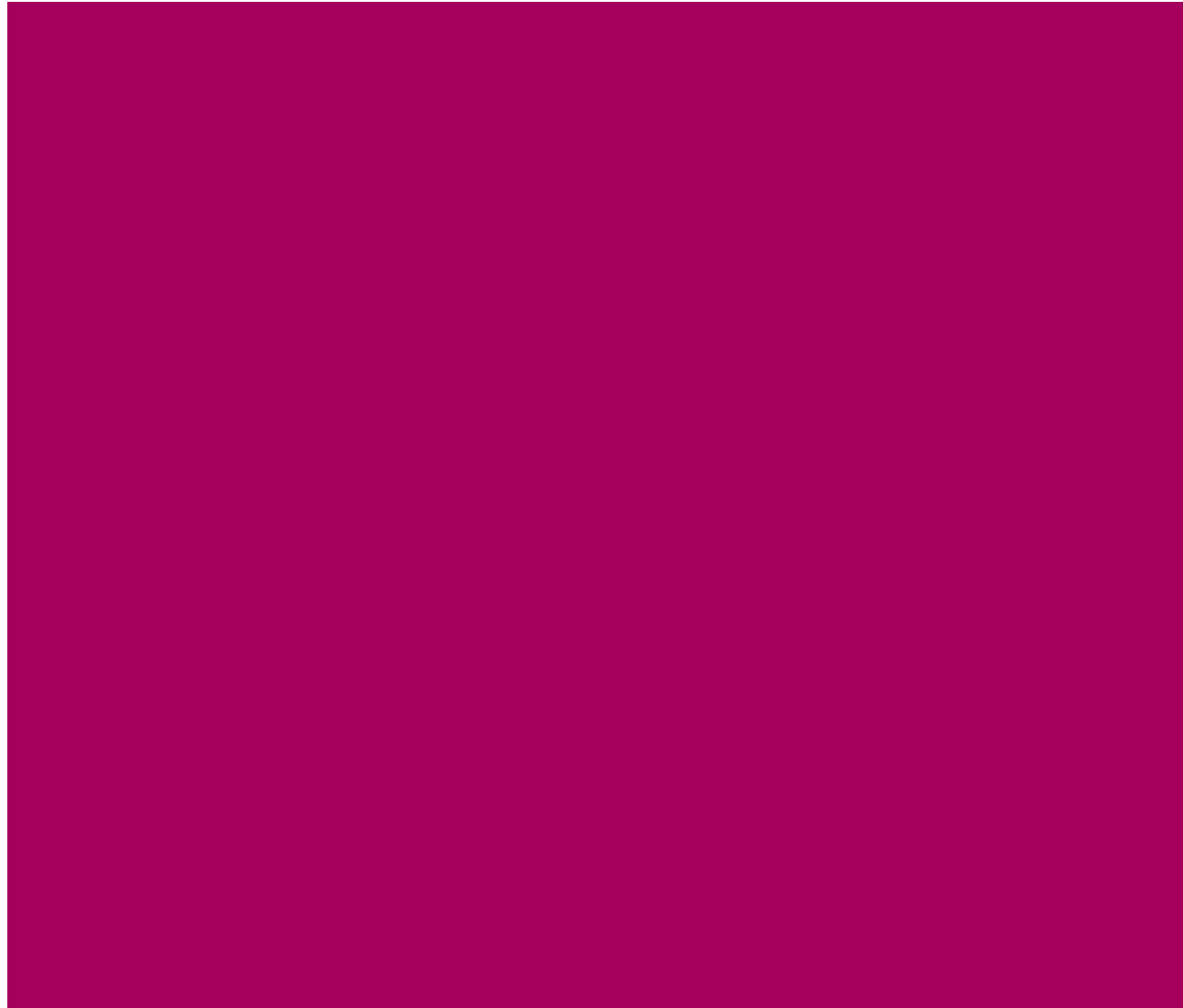
Data transfers



Training and awareness



Privacy and IT 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

Governing privacy & Data Flows



✎ **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				

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

GDPR Implementation Phases



All Presentation and Exam 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/2019/11/day1.pdf>
- DPO: <https://www.eugdpr.institute/wp-content/uploads/2019/11/day2.pdf>
- CEP: <https://www.eugdpr.institute/wp-content/uploads/2019/11/day3.pdf>

Never give up!





Kersi F. Porbunderwalla is the Secretary General of Copenhagen Compliance and President of The EUGDPR Institute and Riskability IT Tools. Kersi is a global consultant, teacher, instructor, researcher, commentator and practitioner on good Governance, Risk Management, Compliance and IT-security (GRC), Bribery, Fraud and anti-Corruption (BFC) and Corporate Social Responsibility (CSR) issues. Kersi lectures at The Govt. Law College (Thrissur, India) Georgetown University (Washington) Cass Business School, (London) and at Fordham University (New York) and Renmin Law School in Beijing. Kersi has conducted several hundred workshops, seminars and international speaking assignments on Regulatory Compliance, GDPR, GRC, CSR, and BFC issues.

Disclaimer: This presentation is prepared for the GDPR Masterclass. The content together with the links to narratives, brochures and information on our websites, is for general informational purposes only. Please refer to Copenhagen Compliance® for specific advice on regulatory compliance and other GRC issues. As always refer to your counsel for legal advice, we are not licensed to provide legal advise.

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



www.copenhagencompliance.com

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

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

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

Email; info@copenhagencompliance.com

Tel. +45 2121 0616



Human Capital Assessment Framework



As ever, always have your legal advisors review and advise on any legal guidance or on any contractual obligation. The Copenhagen Compliance Group is neither a Law Firm nor are we licensed to provide legal advice.

- The examples and scenarios in this presentation are for illustration purposes only, and not based on specific examples to be construed as particular advice on any practical legal issues.
- As always, contact your legal counsel for clarification and recommendations on legal issues. Copenhagen Compliance or The EUGDPR Institute is not licensed to provide legal advice.
- *The copyright of this work belongs to The Information Security Institute® and 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 Information Security Institute®. Carrying out any unauthorized act in relation to this copyright notice may result in both a civil claim for damages and criminal prosecution.*