

GDPR compliance



DPO Certification
Day III

Agenda



Time	Topic
09:00 - 09:25	Recap: Values of Data Protection & Privacy
09:25 - 10:30	Plan – DPO’s Role, Responsibility & Tasks
10:30 - 10:45	
10:45 - 11:05	Plan – Governance Plan
11:05 - 12:00	Plan – Binding Corporate Rules
12:00 - 12:30	
12:30 - 13:30	Do – DPO: Scenario Planning
13:30 - 14:20	Do – DPO: The six concluding steps
14:20 - 14:35	
14:35 - 15:35	Perform – Execute The DPO Role
15:35 - 16:00	Perform – DPO Exam

Link for day III presentation



<https://www.eugdpr.institute/dpo-gdpr-day-iii/>

The role & tasks of the DPO



(The data controller is responsible for GDPR compliance)

- involvement in all issues relating to the protection of personal data of the data subject
- consult with controllers on DPIAs;
- instruct controllers and processors on their obligations under the GDPR;
- receive communications from data subjects regarding their rights and processing of their data;
- monitor compliance with the GDPR and related laws and the controller's policies;
- facilitate or carry out audits; attend DP meetings, and cooperate and consult with supervisory authorities.

The DPOs is independent



- DPO mandatory in organisations processing substantial volumes of personal data (article 37)
- A protected position, reporting directly to senior management
 - Appropriately qualified
 - Consulted in respect of all data processing activities
- Will be a 'good practice' appointment outside the mandatory appointments
- Most staff dealing with personal data (eg HR, marketing, etc) will need at least basic training
- Staff awareness training also critical (accidental release of personal data could have financially damaging consequences)

The DPOs is independent



- The DPO's independence as a center tent pole is holding up the whole canvas, and cannot lean in any direction.
- DPOs have parallel responsibilities to the controller's operational teams, to the board of directors, to data subjects, and to the local oversight supervisory authority
- Controllers cannot instruct DPOs in the operation of their responsibilities but can provide the DPO with the necessary resources to carry out their duties.
- Voluntarily appointing a DPO is encouraged by the EU's data protection authorities

The DPOs is independent



- The DPO is the “cornerstones of accountability,” facilitating GDPR compliance to create a potential competitive advantage for the business.
- The DPOs cannot be penalised or dismissed by controllers or processors for performing their tasks
 - including termination of DPOs working under a services contract.
- Data subjects can initiate litigation against both controllers and processors for compliance breaches however data subjects cannot bring a claim against a DPO.

Step 4: Compile a data inventory



NEW



What personal data do we hold?



Where is it?



What is it being used for?



How secure is it?

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

Step 5: Discussion case



WIRED

Privacy

Wetherspoons just deleted its entire customer email database on purpose

-  **UK pub chain deleted their customer emails from marketing database in Jun 2017**
-  **Contacts are now by Twitter and Facebook**
-  **They suffered a breach of 665k emails in 2015**

Step 5: Discussion case



Dear Customer

I'm writing to inform you that we will no longer be sending our monthly customer newsletters by e-mail.

Many companies use e-mail to promote themselves, but we don't want to take this approach – which many consider intrusive.

Our database of customers' e-mail addresses, including yours, will be securely deleted.

In future, rather than e-mailing our newsletters, we will continue to release news stories on our website: jdawetherspoon.com

You can also keep up to date by following our Facebook and Twitter pages, using the links below.

Thank you for your custom – and we hope to see you soon in a Wetherspoon pub.

Many thanks

John Hutson

Chief Executive

Follow us




Like us



Pros

 Less intrusive?

 No need to keep track of consents?

Cons

 Communication of offers

... but, by who?



Controller

**Who decides
why the personal
data is needed**

Processor

**Who processes
the data**

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

**Natural | legal person
including the government**

... but, where?



in the EU

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

outside the EU

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

Exercise



Case:

Imagine that a ridesharing company (*i.e.* URBAN GO) based on a mobile app offers a platform where people (both drivers and riders) can register to use its service. The ridesharing company collects personal data of drivers and riders (name, address, driving license, bank account detail and location data etc.). The company has appointed a fintech solutions provider to process the payment (fare, driver's salary) and transferred all personal data to fintech company.

1. Identify the role – who is a data controller/data processor/data subject.
2. Based on your role, develop an outline of strategy to ensure data protection.



How personal data is processed?



Collect

Use

Destroy

Record

Transmit

Restrict



Change

Display



Electronically

Manually

GDPR covers personal information processed wholly or partly by automated means

Rights/Obligations under GDPR



1. Controller Obligations	1. Individual Rights
Clear Consent	Access to Data
Privacy by design & other considerations <ul style="list-style-type: none">– Lawful basis, fair processing, and specify purposes– Adequate, relevant, not excessive– Data accuracy, retention, and appropriate security	Remedy from supervisory body or court <ul style="list-style-type: none">– Compensation for damage– Compensation for distress Rectification
Clear, detailed Privacy notices	Objectification for direct marketing
Breach Notification	Erasure (Right to be forgotten)
Appointment of Data Protection Officer (high-risk processing)	Data Portability
International transfer adequacy	Restrict Data Processing (Put on Hold)
	Automated decisions and profiling

Extra-territorial application

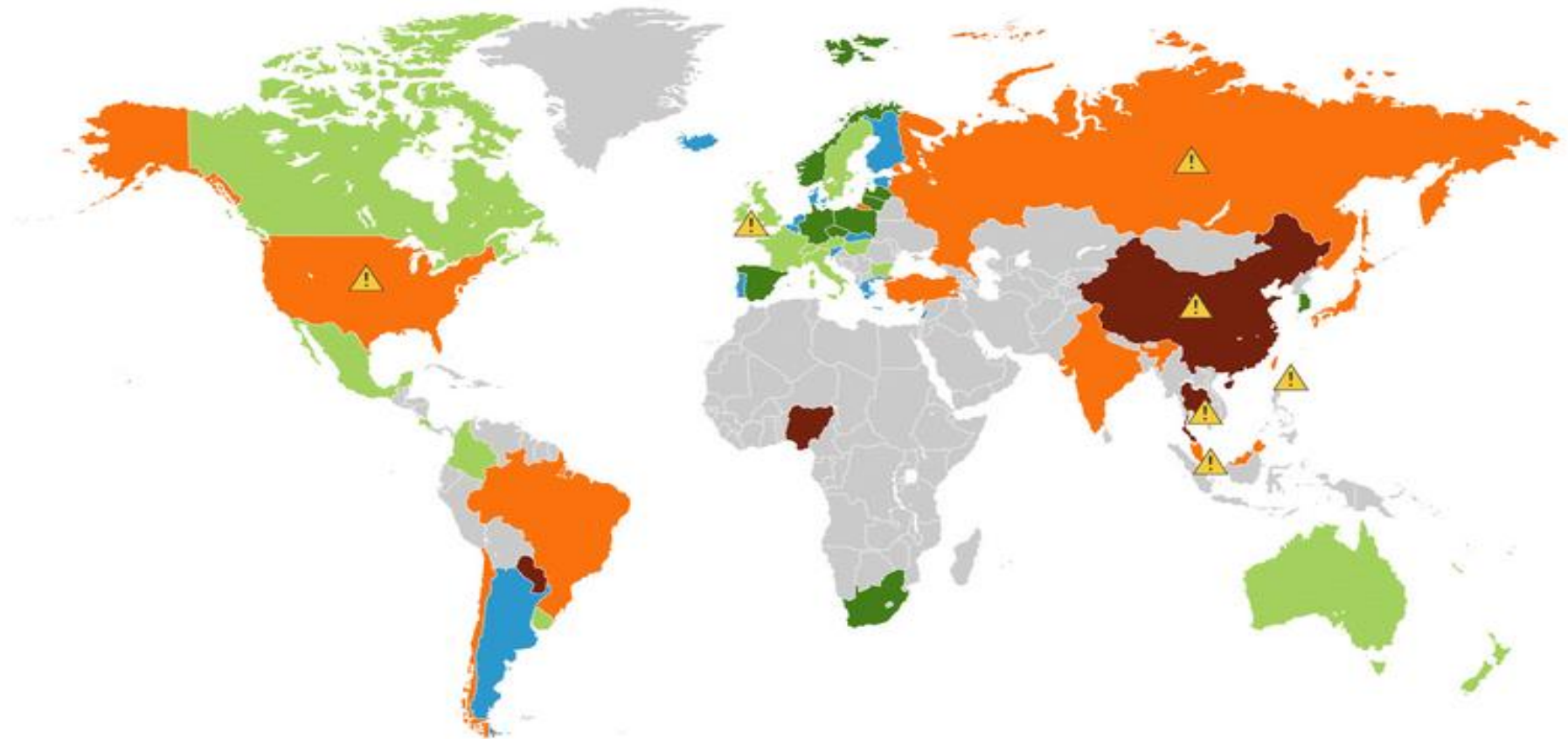


ACME
CORPORATION

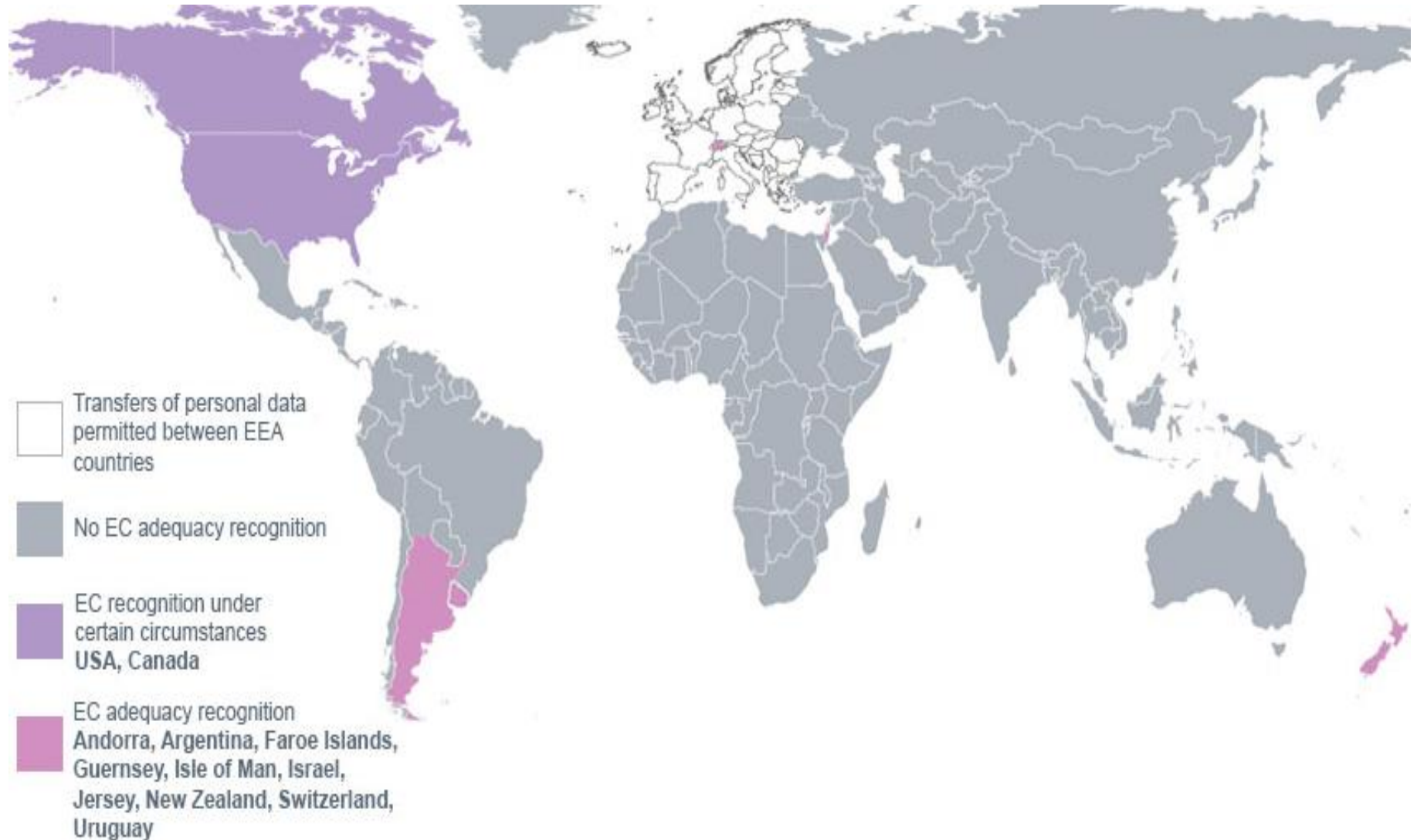


Ecommerce sites
targeting EU clients
(accessible from the EU, prices in
Euros, in EU languages, delivering
to EU)

Views on privacy



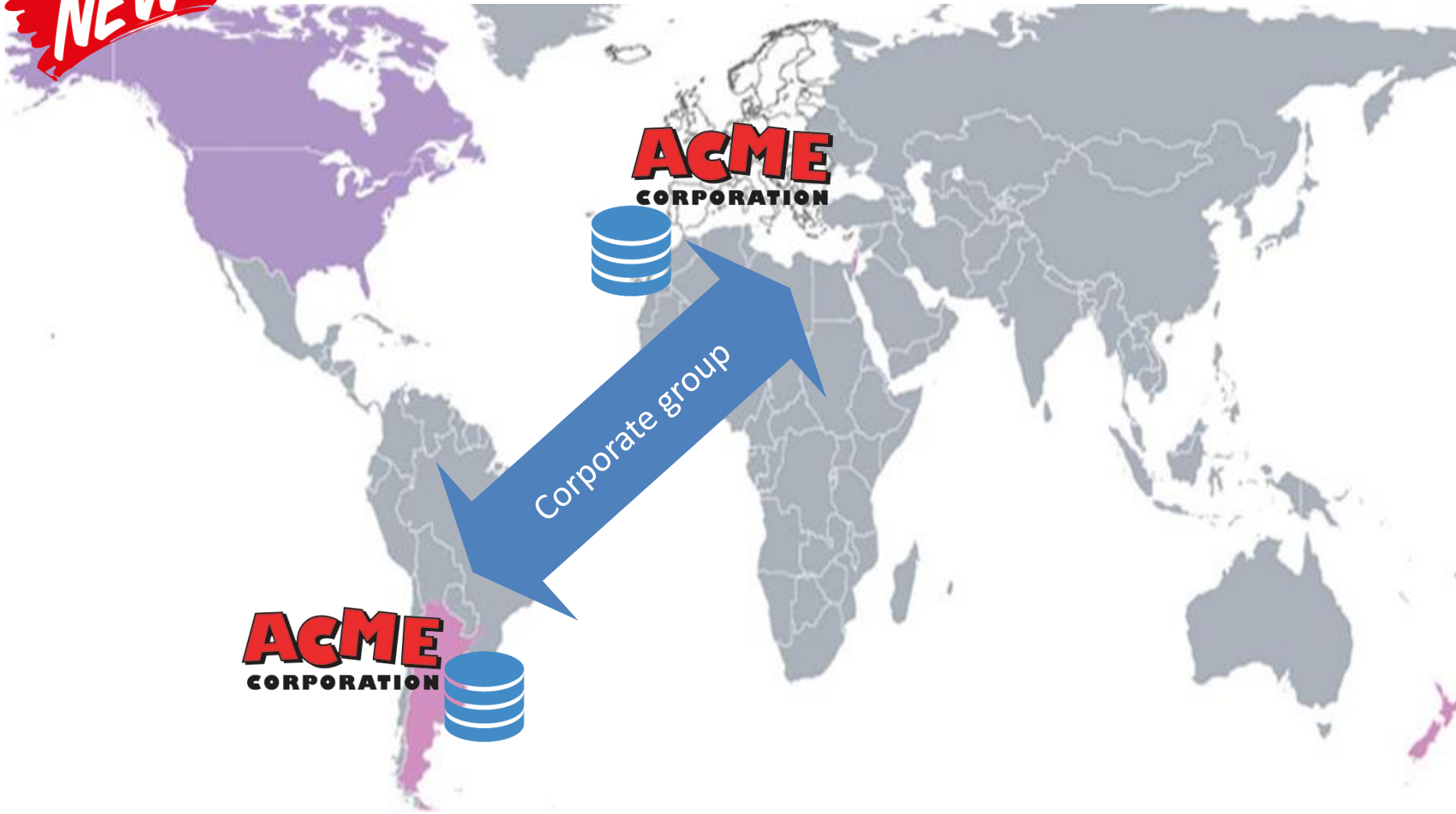
International transfers



Binding corporate rules



NEW



Binding corporate rules



Contract between group companies to transfer information, covering:

- ✎ specify the purposes of the transfer and affected categories of data
- ✎ reflect the requirements of the GDPR
- ✎ confirm that the EU-based data exporters accept liability on behalf of the entire group
- ✎ explain complaint procedures
- ✎ provide mechanisms for ensuring compliance (e.g., audits)

Model pre-approved clauses to reduce compliance burden

Binding corporate rules



- 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, which takes effect in May 2018, recognizes BCRs as a legal means of transferring personal data from the EU.

Binding corporate rules



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.

Binding corporate rules



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.

Binding corporate rules



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.

Binding Corporate Rules



The GDPR expressly recognises BCRs for controllers and processors as a means of legitimising intra-group international data transfers. o

- 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, Cloud storage	Fast erasure of individual records
--------------------	---	------------------------------------

Step 5: How detect a data breach?



Indication of compromise

- ✎ notification from public authorities
 - ✎ FBI knocks at the door
- ✎ from users
 - ✎ oops, I opened a “funny attached file”
- ✎ alerts from 3rd parties
 - ✎ hosting vendor informed they had a malware
- ✎ continuous monitoring solutions
 - ✎ this server is transferring out a lot of amount of data

Incident response protocol

- ✎ Investigate “when” the breach was done
- ✎ Get the investigation team
- ✎ Investigate the level of compromise

Step 5: Scenario planning



Before the breach

- ✎ Address IT risks and vulnerabilities
 - ✎ all potential threats are identified and defendable (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 the 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 5: 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
- ✎ GDPR 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 5: Scenario planning



Responding procedure

- ✎ **Validate the breach**
- ✎ **Assign an incident manager (usually CISO) to investigate**
- ✎ **Assemble incident response team (IT, legal, public affairs)**
- ✎ **If 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



They even
sell data
breach
services

- ✎ 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

How can we manage the need to investigate a breach with the 72 hours rules to disclose a breach under GDPR?

Step 5: Discussion case



Popular restaurant app Zomato says the records of about 17 million users have been stolen in a security breach.

The Indian startup, which covers more than one million eateries across 24 countries, [said Thursday](#) that names, email addresses and encrypted passwords were taken from its database.

The company, which competes with Yelp ([YELP](#)), reassured affected customers that no payment information or credit card details were stolen.

Zomato said the security measures it uses ensure the stolen passwords can't be converted back into normal text, but it still urged users who use the same password on other services to change them. It also logged the affected users out of the app and reset their passwords.

"So far, it looks like an internal (human) security breach - some employee's development account got compromised," the company said in [a blog post](#), without providing further details. It didn't immediately respond to a request for more information.


Step 1: Train your people



Step 1: Discussion case



 **How could you develop training for this risk?**

 **How could you document your training efforts?**



Let`s play... add controls to risks



- ✎ Over collection of personal data
 - ✔ assign a data owner, inventory
- ✎ Incorrect or outdated personal data
 - ✔ validation campaigns, data audits, interface controls
- ✎ Unauthorized use or export by users
 - ✔ minimum access, training
- ✎ Unauthorized use or export by third parties
 - ✔ liability clauses, security requirements

Let`s play... add controls to risks



- ✎ Missing consents / data subjects unaware of uses
 - 🛡️ compulsory consent notices, process review
- ✎ Data subject cannot access or rectify their info
 - 🛡️ protocol for requests, forms on line
- ✎ Fragmented systems cannot retrieve or update all the data
 - 🛡️ updated inventory
- ✎ Personal data is hacked
 - 🛡️ network activity monitoring, firewall
- ✎ Personal data is kept longer than intended
 - 🛡️ automated deletion processes when data is flagged for deletion

1 – Identify the need



Early before **new** projects or revision of existing processes
for example, when considering a

- ✎ new system to store personal data
- ✎ change the use of already collected personal data
- ✎ new video surveillance system
- ✎ vulnerable data subjects (e.g. children)
- ✎ new database consolidating tables with personal information from other systems
- ✎ new algorithm to profile a particular type of client
- ✎ proposal to share personal data with a business partner
- ✎ impact of a new legislation

Existing processes → Recommended initial assessment

Doubts if needed → consult the Supervisory Authority and beg for mercy!

2 – Identify the flows



Process map start from the process or project documentation



Identify personal information in the process map



Consult with experts how personal information is collected, transferred, used and stored

 for existing and future purposes

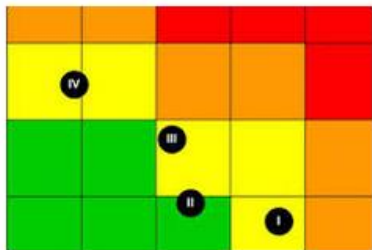
3- Consult on risks and controls



Consult all involved parties to have a 360° view, link risks to owners



Include current controls in the process map



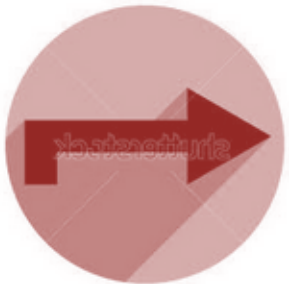
Assess the impact and frequency in a heat map (recommended), risk assessment in ISO 27001 (under 29100)

- Impact: fines, business continuity costs, loss of clients, reputational damage
- Risk must be assessed from the view of the data subject, not the business!

4 - Identify new measures



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



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



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

Step 5: Audit compliance



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

Step 5: Audit compliance



Process	KPI example
Training	% of staff (or hours) trained on privacy policies (participated/passed, type of program, levels)
Incident	# of privacy incidents (by system, location, repeated or new) # reported data breaches
Audits	# non conformities # action plans on-going (and past due)
Consents	% consents obtained
Access control	% of credential validated
Compliance	# requests # complains # new projects with DPIA

6 – Follow-up



Communicate to stakeholders, bottom-up and top-down



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












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

People to consult



Internal


-  Data protection officer (usually leading the DPIA)
-  Project management leaders and developers
-  CIO, CISO and other IT experts
-  Compliance officer
-  Legal department
-  Internal audit executive
-  Risk management officer
-  Future or current users
-  Senior managers

External

-  Potential data processors and vendors
-  Experts

Group discussion



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



Exercise



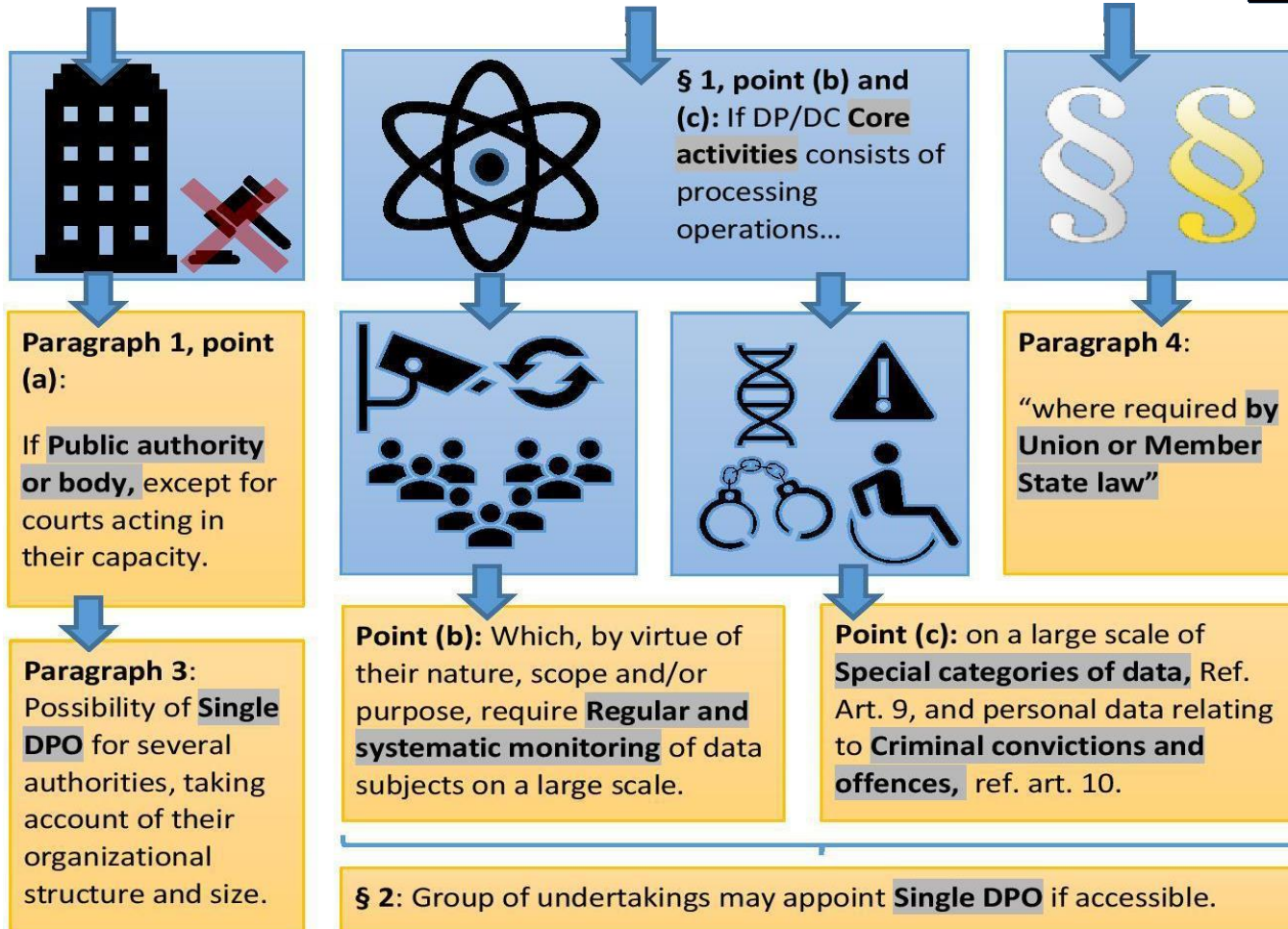
Case:

Imagine that you are the DPO of a large advertising company which monitors behaviours of individuals (*profiling*) and collects their personal data (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.

Task:

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

The Data Protection Officer (DPO)



Abbreviations

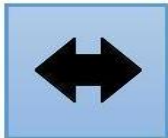
DC= Data Controller, DP = Data Processor, SA = Supervisory Authority. All article references: General Data Protection Regulation (GDPR), EU-2016/679

* 4: Addition: DC/DP has the right to appoint a DPO.

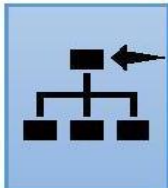
DPO's POSITION



Recruitment base: Article 37, § 5: The DPO shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practice and the ability to fulfil the tasks referred to in Art. 39.



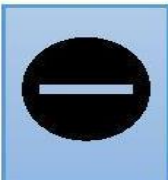
Conjunction: Art. 37 § 6: Employed by DC/DP or Service Contract (Independent).



Reporting: Article 38, § 3: DPO shall directly report to the highest management level of DC/DP.



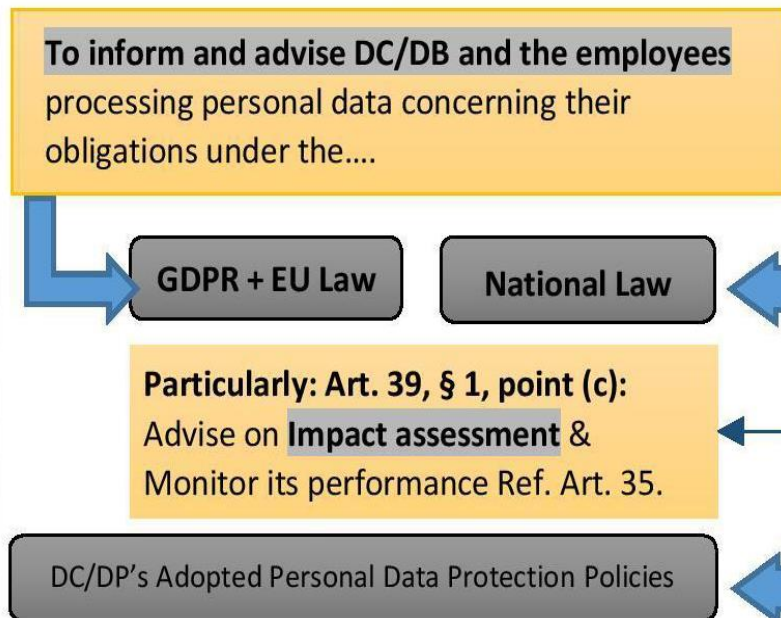
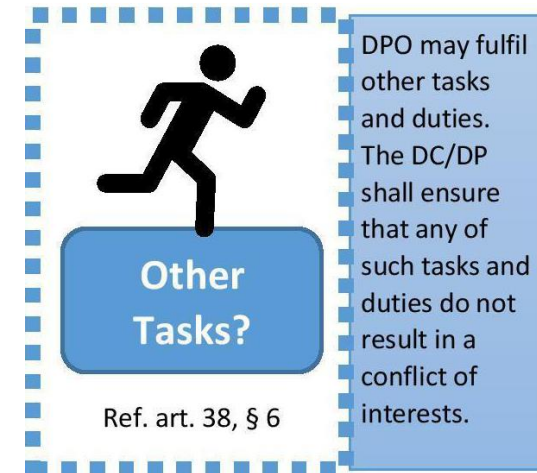
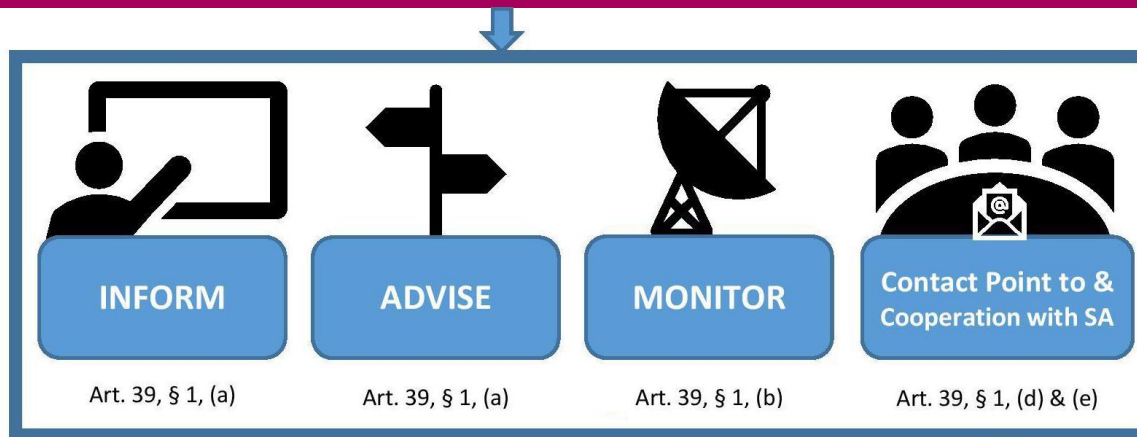
Confidentiality obligations: Article 38, § 5: DPO shall be bound by secrecy or confidentiality concerning the performance of tasks, in accordance with EU or member state law.



Independence: Recital 97 in fine: "should be in a position to perform their duties and tasks in an independent manner".

DPO TASK

Ref. art. 39



Art. 35, § 2: Seek the advice of the DPO, where designated, when carrying out a Data Protection Impact Assessment (DPIA)

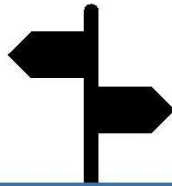
DPO TASK

Ref. art. 39



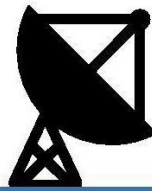
INFORM

Art. 39, § 1, (a)



ADVISE

Art. 39, § 1, (a)



MONITOR

Art. 39, § 1, (b)



Contact Point to &
Cooperation with SA

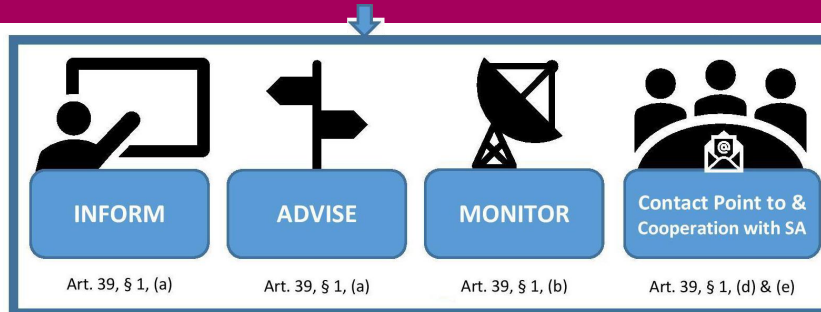
Art. 39, § 1, (d) & (e)

Art. 39, § 2: DPO shall (...) have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.




DPO TASK

Ref. art. 39




Art. 38, § 2: DC and DB shall *support the DPO in performing the tasks referred to in Art. 39* by providing the necessary:

- 
- 1) resources to carry out those tasks
 - 2) access to personal data and processing operations
 - 3) maintain DPO expert



Art. 24, § 2. + Recital No. 78:

"In order to demonstrate compliance with this Regulation, the Controller should adopt internal policies"



Article 39, paragraph 1, point (b): "Including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;"

Obligations of others to display DPO 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

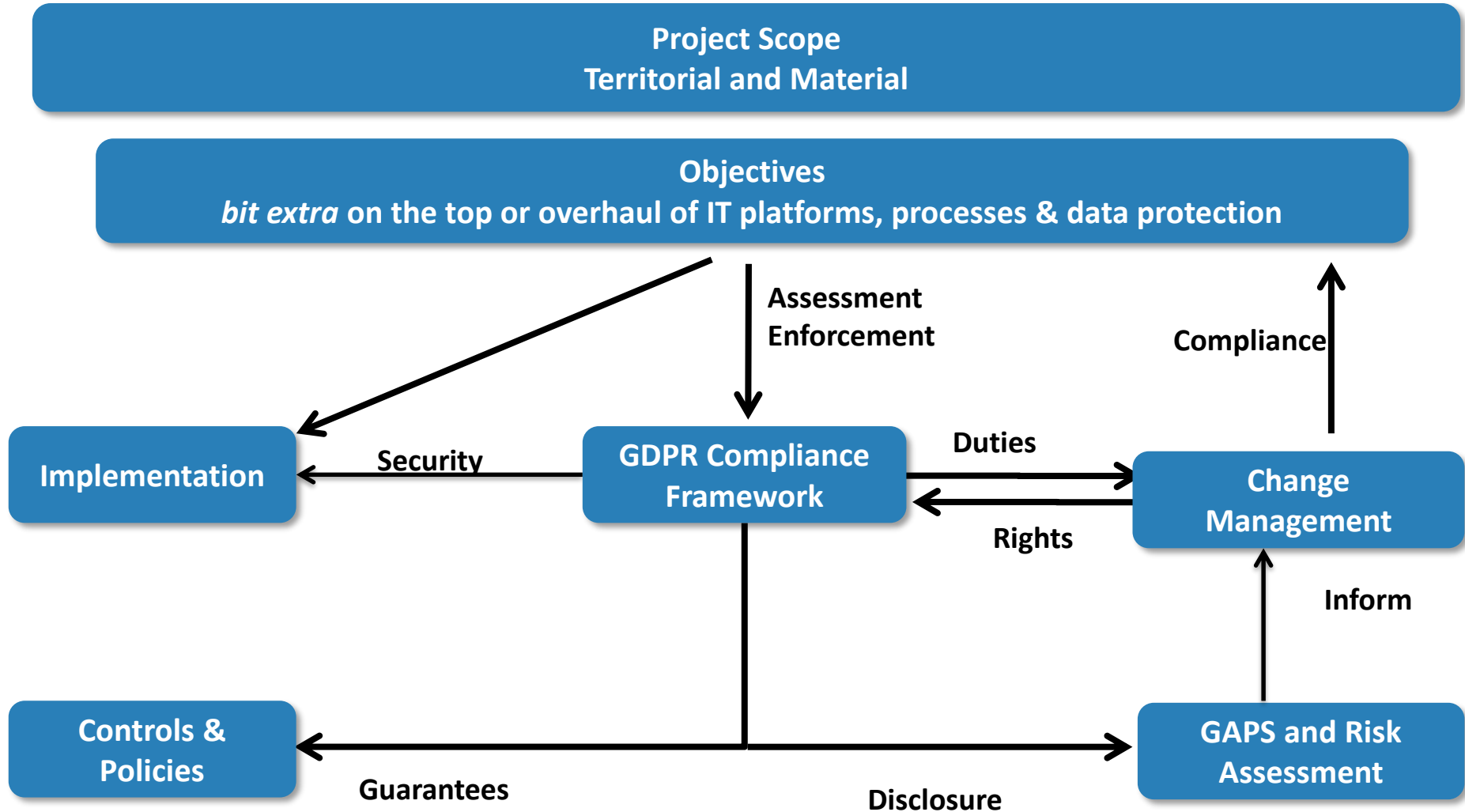
Obligations of others to display DPO

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	

What you have received?



Summary



The GDPR Institute



www.copenhagencompliance.com



Human Capital Assessment Framework



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

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

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

Useful GDPR links



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

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



Certification exam



<http://www.eugdpr.institute/gdpr-dpo/>

Copyright notice



The copyright of this work belongs to The GDPR 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 GDPR Institute®. Carrying out any unauthorized act in relation to this copyright notice may result in both a civil claim for damages and criminal prosecution. Info@eugdpr.institute