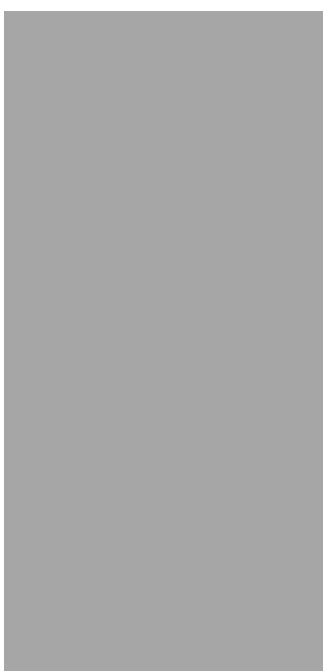


GDPR compliance



DPO Certification Training

Day 2

Agenda



Time	Topic
09:00 - 09:25	Introduction. Principles of Data Protection
09:25 - 10:30	Plan – DPO: The Need Part I
10:30 - 10:45	
10:45 - 11:05	Plan – Governance Plan
11:05 - 12:00	Plan – Key GRC Challenges
12:00 - 12:30	
12:30 - 13:30	Do – DPO: Part II. Objectives, Function, Skills
13:30 - 14:20	Do – DPO Part II: Organisation, Relationships,
14:20 - 14:35	
14:35 - 15:35	Improve – Privacy Governance
15:35 - 16:00	Improve – Demonstrate Compliance



Data Protection Officer



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

GDPR compliance summary



- ◆ The legal basis of IT and cyber security compliance
 - ◆ How is data collected, used, abused or misused?
 - ◆ Use of data exactly for the purpose it was collected
 - ◆ Consent from data subjects for secondary processing
 - ◆ Review change processes in processing personal data
 - ◆ Address violations, and remedies for correction
 - ◆ Regular reviews of data flow mapping, audits, risk assessments to ensure the legal basis has not changed
-
- ◆ GDPR is not privacy by choice, follow the privacy data!
 - ◆ Does not give the individual full control over the data
 - ◆ The reform simplifies and adds compliance complexity
 - ◆ The code-of-conduct and certification mechanism ensure structured and efficient means for compliance

Follow principles for data processing



**Processed lawfully,
fairly and
transparently**



**Processed in a manner
that ensures
appropriate security**



**Collected for specified,
explicit and legitimate
purposes**



**Accurate and, where
necessary, kept up to
date**



**Adequate, relevant
and limited to what is
necessary**



**Kept for no longer than
is necessary**



the controller be able to demonstrate **accountability**

- ✎ Being able to demonstrate **best efforts** to comply with the GDPR principles
- ✎ Proactive approach to properly manage personal data and to address privacy risks by a **structured privacy management program**



Proportionality

processing only if necessary for the attainment of the stated purpose

- ✎ Personal data must be adequate, relevant and not excessive in relation to the purposes
- ✎ By the data processor and controller
- ✎ Requires to use the less intrusive means of processing

Rights



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

To data portability
common format, even directly transmitted between controllers



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

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



To restrict processing
limiting the data use or transfer

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





One man army?

Data protection officer



Implementation team <> Maintenance team
Define a clear objective and responsibilities
Be a leader
Experience in project management, security,
training and legal
Commit time of process subject experts
Document all the project activities

Who needs a DPO?



The controller

AND

The processor

1. Processing is carried out by public authority

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

3. Business with a core activity

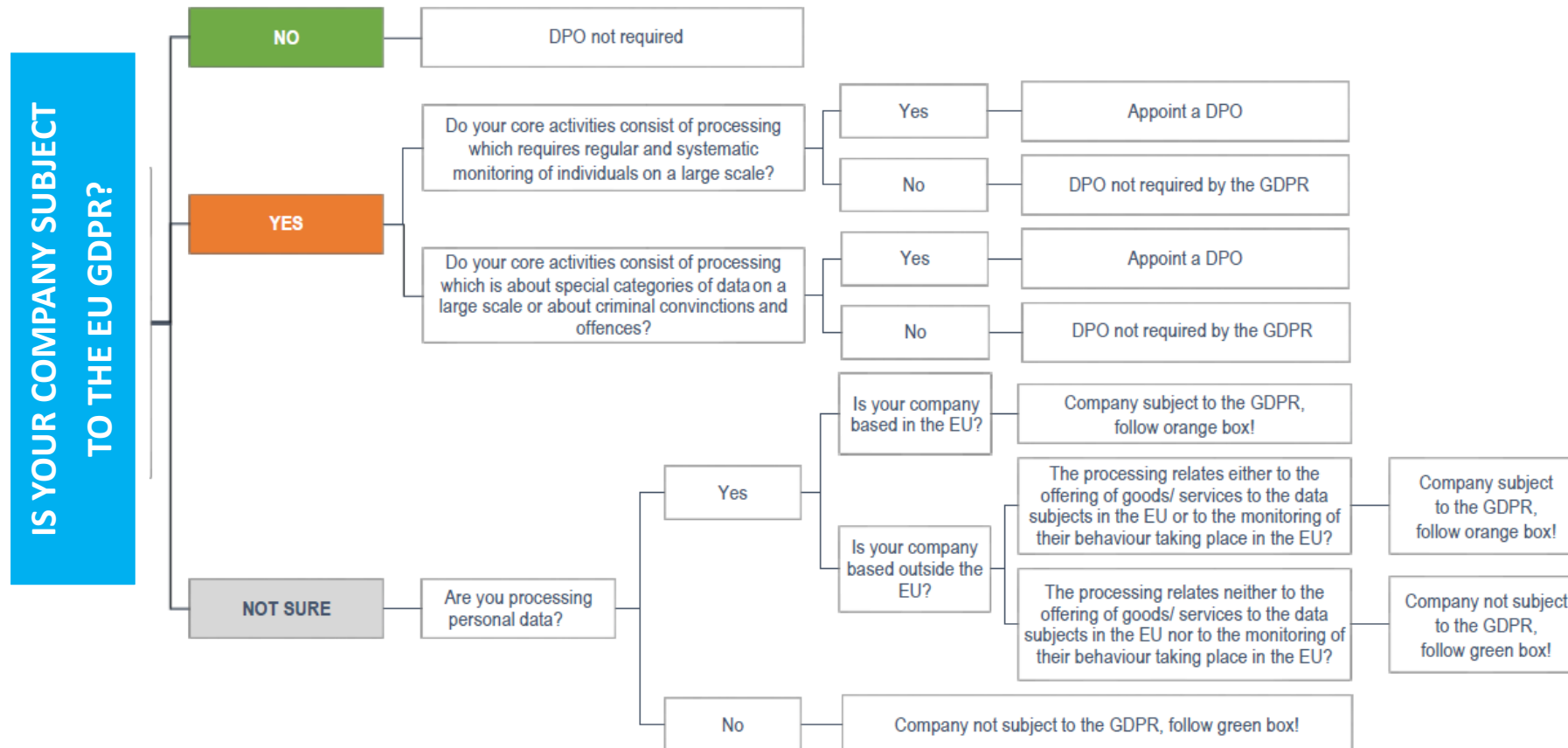
- Processing operations requiring monitoring of personal data at large scale

- Included hospitals for health data, marketing agency for customer web data, surveillance companies

- Excluded payroll for a commercial organization, health data by a single doctor

- Processing operations requiring monitoring of sensitive personal data at large scale relating to criminal convictions and offences

Who needs a DPO?



What does a DPO?



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

Independence to ensuring compliance

Employee or external consultant based on a service contract

Expertise in national and European data protection laws

Knowledge of the business sector and of the organization of the

Professional ethics and lack of conflict of interests

Groups may designate a single DPO

GDPR areas with GRC & IT exposure:




- Governance – historic deficit in board accountability.
- Risk management – processes are absent, no consideration of risks to rights and freedoms.
- GDPR Project team – key issues needed to create a dedicated, appropriately resourced project team.
- DPO – role needs to be entirely established: genuinely independent.
- Roles and responsibilities – typically do not include data protection or information security.
- Scope of compliance – unclear, because chain of processing undefined
- Process analysis – significant inadequacies in relation to the data processing principles.

10 core GDPR areas with risk exposure:



- PIMS – imited documentation – from policy downwards.
- ISMS – information security arrangements are inadequate and not integrated.
- Data subject rights – these have not been addressed; absence of transparency
- Limited available information in key GRC and IT security areas: controller-processor relationships, trans-border data processing, data protection policies and procedures,
- Confusion over consent and lawfulness of processing, interaction with *The Privacy and Electronic Communications Regulations*
- Not clear whether a DPO or DPIAs are mandatory or perhaps even a good idea.
- Inadequate information security – Cyber essentials not considered, no penetration testing, limited encryption.

 **Who can be a DPO? The chief risk officer, the compliance officer, the chief information security officer....**



GDPR Data Governance Plan



Build Program & Team	Identify Stakeholders	Allocate resources & budget	Appoint DPO	Define Program Mission and Goals
Assess Risks and Create Awareness	Conduct Data Inventory & Data Flow Analysis	Conduct Risk Assessment & Identify Gaps	Develop Policies, Procedures and Processes	Communicate Expectations and Conduct Training
Design & Implement Operational Controls	Obtain and Manage Consent	Data Transfers and 3 rd Party Management	Individual Data Protection Rights	Physical, Technical and Administrative Safeguards
Manage & 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 & External Reporting	Privacy Notice & Dispute Resolution Mechanism	Certification

Key Challenges for Compliance I/V



No.	Issue	Challenges	Resolution
1	Creating a Data Inventory Information Held Locating all personal data and mapping it Art. 30 Record of processing activities	Relies on interviews with process owners Process owners may not always be aware of all the data and where it resides Affects internal controls, taking consent	Data classification and discovery Algorithms to go through the systems and identify the various types of data Manual inventory of data and documentation
2	Appointing a Data Protection Officer Art 37 someone to take responsibility for data protection compliance	Is a DPO always needed? Confusion between roles, DPO is more of an ombudsman (between Data Protection Authority and data subjects) than a <i>officer</i>	Worst case scenario if data is leaked can be used to identify need for a DPO e.g. organisations with Medical data need a DPO Marketing data that can be cross-referenced to identify people would need a DPO
3	Data Protection by Design and Default. Art.25 (incorporates Art. 32 Information Security) Build deterministic failure into processing of personal data When systems fail they fail in a deterministic way (fail-safe), i.e. exposure is minimised.	No generally accepted standards for Data protection by design and default Retrofitting existing legacy systems for data protection in a short time frame (i.e. by May 2018). Re-thinking data processing activities (for data minimisation, data protection by default)	Organizational (i.e. administrative) controls e.g. Background checks on employees, Privacy policy training, Incident Response Plan, Breach Notification Plan, Controls for breakdown of legacy systems

Key Challenges for Compliance II/V



No.	Issue	Challenges	Resolution
4	Cross-Border Data Transfers Art. 46 Addresses transfer to national not deemed “adequate.” lead data protection supervisory authority	Which mechanism to use Data in Cloud Environments	Privacy Shield (e.g. EU to the US, one directional only, general purpose solution) Standard Contract Clauses with individual companies and vendors. Binding Corporate Rules (challenging to complete before deadline, establish basic compliance first)
5	Third Party Compliance Art. 28	Working with third parties Cloud service providers	Third Party Triage <ul style="list-style-type: none"> – One size fits all, e.g. large Cloud companies – Team players – Laggards
6	Data Protection Impact Assessments (DPIA) Art. 35	Binary “It is high risk” determination No clear guidelines for medium	WP 248 guidelines (High Risk) <ul style="list-style-type: none"> – Is the organisation doing evaluation or scoring (including profiling and predicting) of aspects specific to the data subject? – Does the processing involve automated decision making

Key Challenges for Compliance III/V



No.	Issue	Challenges	Resolution
7	Breach Notification Art. 33 Procedures to detect, report, investigate breaches	Meeting the 72 hours or without undue delay standard	Set up a war room and run through “worst case” scenarios Breach Notification Program
8	Notice and Consent Art. 12-14, Art. 7,8	1. Notice Consent 2. Notice Availability	Review Data Inventory
9	Right to Erasure or Right to be forgotten Art. 17	How to comply without creating disruption. Not all data may be possible to delete, e.g. in databases with data parts connected to each other etc. Sometimes it may not be feasible, or effort to be invested may outweigh the benefits.	Data Inventory and “worst case” scenarios. Would eliminating the data harm the data subjects, or other data subjects, or the organisation? A prior decision on data to be erased for each data process, along with the legal justifications for data that cannot be erased.

Key Challenges for Compliance IV/V



No.	Issue	Challenges	Resolution
10	Crafting a Privacy Policy Implied under Art. 32	Developing the correct content	The organisation's commitment to the protection of personal data Policy scope Principles for processing personal data Transfers to other business units Transfers to other business units Transfers to third parties Appendices Acts as a Master Document
11	Subject Access Requests	How much to invest in automating SARs?	The organisation should update their procedures and plan how they will handle requests within the new timescales and provide any additional information.
12	Lawful basis for processing personal data		The organisation should identify the lawful basis for their processing activity in the GDPR, document it and update the privacy notice to explain it.

Key Challenges for Compliance V/V



No.	Issue	Challenges	Resolution
13	Individuals Rights		The organisation should check their procedures to ensure they cover all the rights individuals have, including how they would delete personal data or provide data electronically and in a commonly used format.
14	Communicating Privacy Information		The organisation should review the current privacy notices and put a plan in place for making any necessary changes and future updates in time for GDPR implementation.
15	Individuals Rights		The organisation should check their procedures to ensure they cover all the rights individuals have, including how they would delete personal data or provide data electronically and in a commonly used format.

DPO functions



DPO 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)

Core functions of a DPO



- Implementation of compliance;
- Monitoring compliance;
- Follow up;
- Building awareness;
- Cooperation with DPAs;
- Advice the data controller, data processor and their employees;
- Assist Data Protection Impact Assessment;
- Act as a focal point of contact.
- Assist demonstration of compliance.

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

✎ Through separation of duties (art 38)

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

✎ Direct report to the CEO or highest management level

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





✎ Autonomous

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

Independence



Protected employment status

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

Separated budget

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

Professional qualities of an experienced manager








-  Access to independent legal counsel for non-lawyer DPOs

Requirements










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






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!

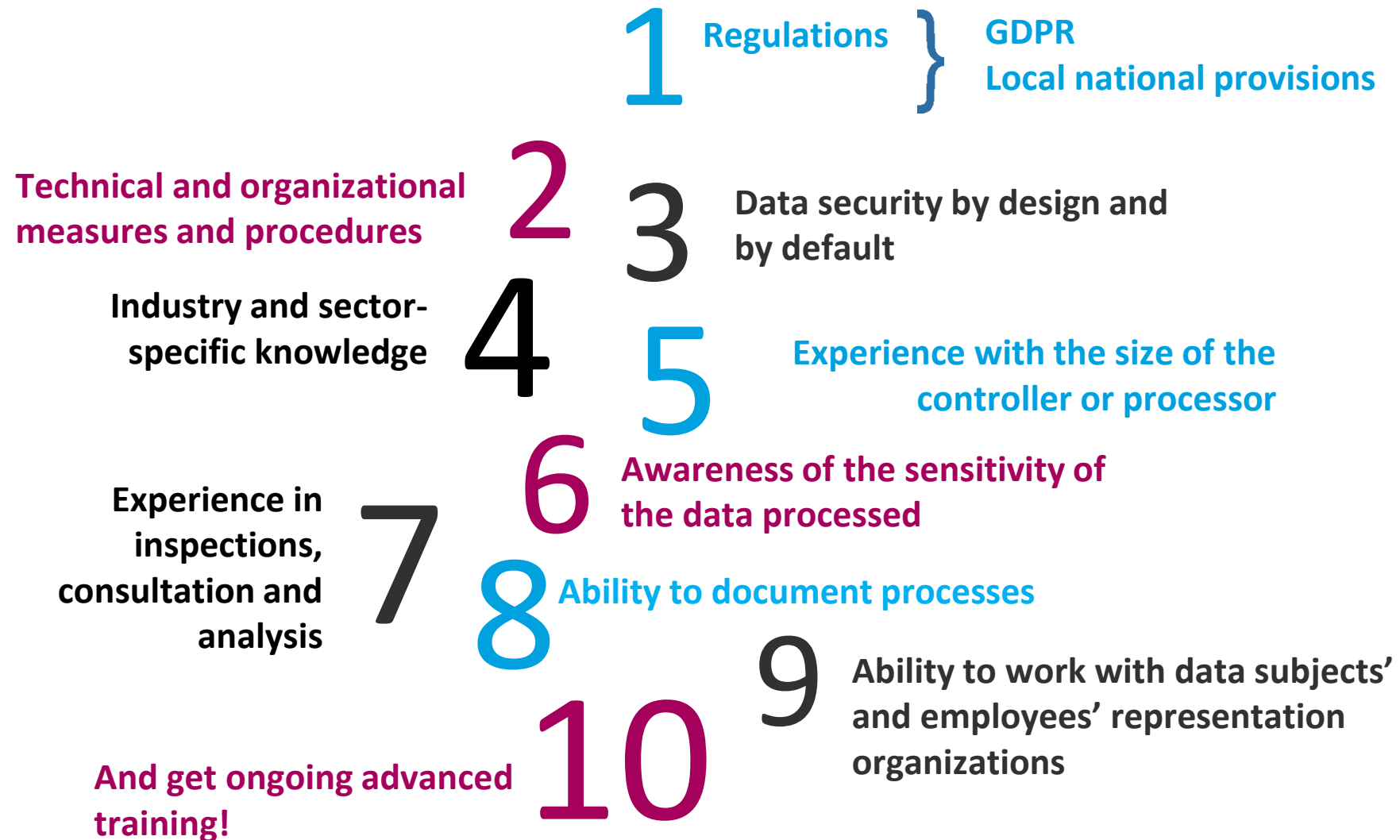
Independently, monitor compliance with the GDPR

-  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
-  Handle data subject requests

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

Skills



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

Voluntary



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

Relationship with the Board



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

Relationship with the CIO



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

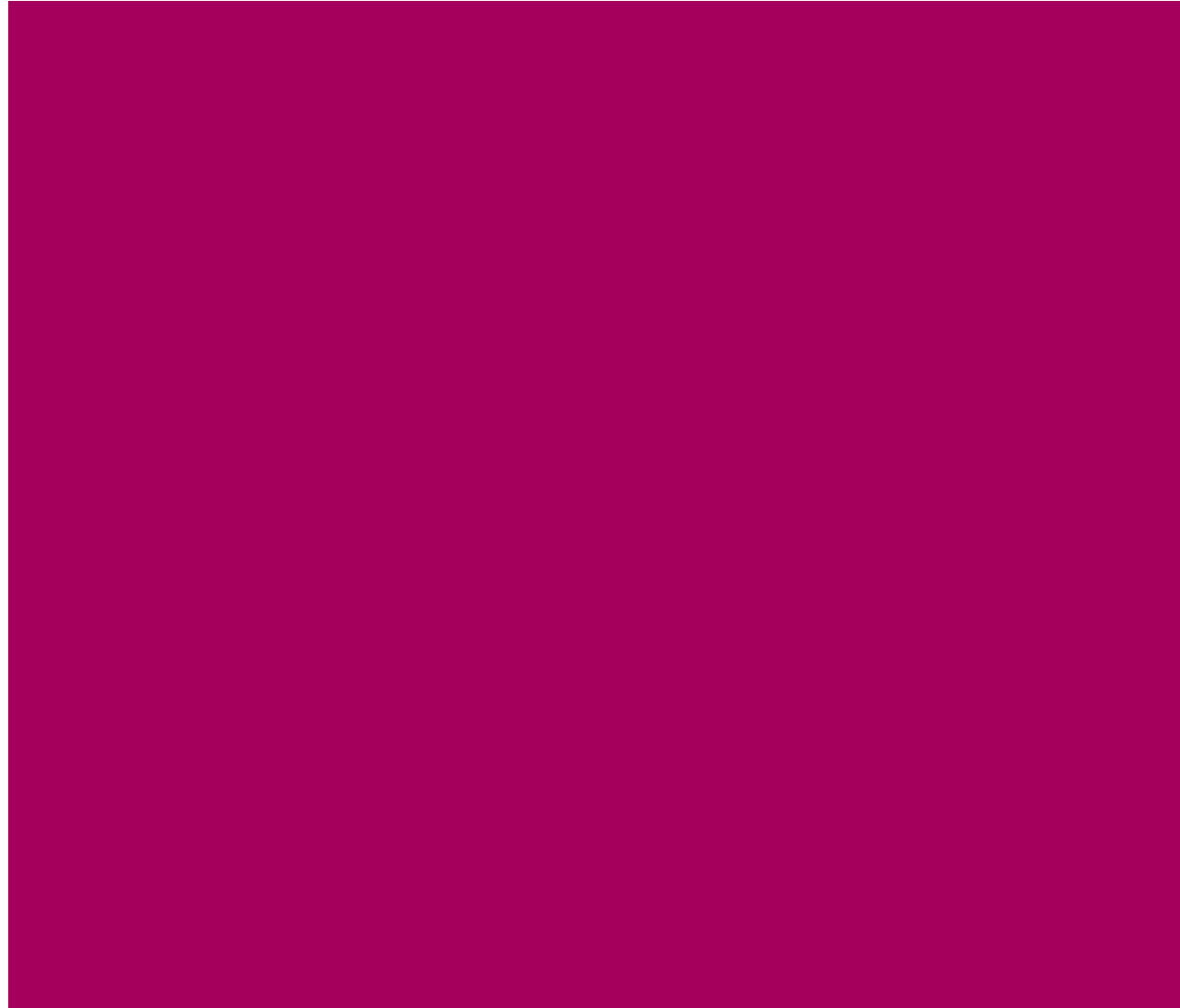
Breakout session/Discussion in groups



- What are the first three things you would do in your role as the DPO?
- In what manner, and how often, will you keep the board informed of your activities?
- What are the ethical responsibilities that you will maintain to ensure confidentiality?
- How will you maintain your independence while working closely with the organisation?
- How will you influence the use of DPIAs, privacy seals, and information security standards as a DPO?



Privacy governance



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 <i>Scope: Mkt, sales, HR, procurement systems</i>	Jan Hansen (DPO)	30 Oct	Done
Security Plan
Third Parties List				
Training Plan				

Operational privacy



How to demonstrate compliance?

Demonstrate compliance



- ✎ If required, board minute designating a DPO (art. 37, 38)
 - ✎ including evidence of independent reporting (org. chart, reports to the board), delegated tasks (contract, job description), proper budget, qualifications and certifications (CV, identity and background checks) and communication to supervisory authority
- ✎ For non-EU data controllers/processors, mandate to designate a representative in the EU and external communication in privacy notes and website (art. 27)
 - ✎ Privacy Officer, Privacy Counsel, CPO, Representative

Demonstrate compliance



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, retention, document destruction, marketing
- ✎ DPIAs for new or changing programs, systems, processes

Demonstrate compliance



Lawfulness of processing (art 6)

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

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

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

Demonstrate compliance



Consents (arts 7 and 8)

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

Demonstrate compliance



Transparent information (arts 12, 13 and 14)

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

Demonstrate compliance



Right of access (art 15)

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

✎ Subject Access Request procedure and similar

✎ Define the channels

- ✎ email, online form, in writing

✎ Formalize who is responsible for responding (on time)

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

✎ Define who controls/approves the final action

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

Breakout session/Discussion in groups



- Google, Facebook and Twitter are cracking down on apps that share information it shouldn't.
- Google is planning to roll out several changes designed to protect users on Android, e.g. the new rules that banned apps from displaying ads on your lock screen. These could potentially trick users into downloading unwanted software or sharing data that they don't want to.
- The Safe Browsing team of The EUGDPR Institute is laying out new restrictions on how apps collect a user's data. Under the new policy, apps must provide their privacy policy and prompt users to share their data. This applies to everything from a user's phone number to the list of apps installed on the phone.
- Applications which collect and transmit personal data not required for the app to function must tell users how the data will be used.
- If an app collects and transmits personal data unrelated to the functionality of the app then, prior to collection and transmission, the app must prominently highlight how the user data will be used and have the user provide affirmative consent for such use.
- 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 other advice would you give to The Safe Browsing team of The EUGDPR Institute to ensure GDPR Compliance on Google, Facebook and Twitter to make sure that primary issues like consent or showing a warning whenever it tries to collect your data without telling you is taken into consideration to avoid issues with the DPA.



Manage privacy risks



How to demonstrate compliance?

Demonstrate compliance



Responsibility of the controller (art 24)

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

Demonstrate compliance



Responsibility of the controller in outsourcing (art 28)

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

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

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

Data protection impact assessment (arts 35 and 36)

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

Demonstrate compliance



Data breach notification (art 33)

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

Demonstrate compliance



Privacy by design and by default (art 25)

- ✎ PIA policy for
 - ✎ new or
 - ✎ changes to existing } 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)

When processing is lawful?



- ✎ Data subject gives consent for one or more specific purposes
- ✎ Processing is necessary to meet contractual obligations entered into by the data subject
- ✎ Processing is necessary to comply with legal obligations of the controller
- ✎ Processing is necessary to protect the vital interests of the data subject
- ✎ Processing is necessary for tasks in the public interest or exercise of authority vested in the controller
- ✎ Purposes of the legitimate interests pursued by the controller

Privacy notices

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

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

Consents

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

Review consents

How consents should be given?



signing a consent statement on a paper

☐ I agree to

☐ I agree to the Google Terms of Service and Privacy Policy

ticking an opt-in box on paper or electronically (no pre-ticked)



clicking an opt-in button or link online

Yes

—Select—

Yes

No

selecting from equally prominent yes/no options

Data Protection:

☐ Email

☐ Post

☐ Telephone

choosing technical settings or preference dashboard settings



responding to an email requesting consent

Consent example



- Do you agree to the consent declaration below?

☐ Yes ☐ No

When submitting your information to [The Organization] you accept and consent to the following:

Collection of Personal Data

[The Organization] is an equal opportunity employer and makes all employment-related decisions entirely on merit and qualifications. Consequently, you should only include information relevant for the review of your application and **not include information about your race or ethnic origin, religion or belief, political opinion or sexual orientation or your union memberships. Please do also not include your social security number.**

Personal Information held by [The Organization] The personal information is held on an externally hosted database in the United States. Personal information is also held in manual form and on other computer systems. Personal information includes all information submitted by you.

Purposes for which Personal Information is used by [The Organization] Personal information about you may be held and processed by [The Organization] **for the purpose of recruitment.**

Consent example



Disclosures of Personal Information Personal information will be disclosed only in the following circumstances:

- Personal information will be disclosed to the extent required for the purposes listed above to [The Organization]'s affiliates worldwide, including affiliates located in countries outside of Europe.
- Personal information may be disclosed to public authorities and law enforcement agencies as permitted by law.

Security Measures [The Organization] ensures that adequate security measures to safeguard your information are in place throughout [The Organization], its affiliates and vendors, and also ensures that adequate safeguards are in place to protect your personal information if it is subsequently transferred to other [The Organization] entities or third parties.

Accurate Information and Deletion [The Organization] is committed to keeping data about you accurate and up to date. Therefore **please advise [The Organization] of relevant changes to your details.** [The Organization] will erase all information after 2 years.

Your rights You may access the personal information held about you by or on behalf of [The Organization] in order to review, edit, erase or to ascertain the purposes for which it is processed subject to certain criteria being met. Please contact [The Organization] HR for further information if you wish to obtain insight in your personal information.

Statistics Your information may be used for anonymous statistics for internal purposes in which case the information will be used collectively. **All personal data will be anonymized.**

Further information For further information on [The Organization]' Disclaimer and Privacy Policy please visit: www.ACME.com/utls/disclaimer.html

Profiling activities





Profiling activities

- Businesses should not make “decisions” about an individual if those decisions are solely based on automated processing, including profiling unless one of the certain specific legal criteria are met –
- typically requiring the individual’s “explicit consent”.
- The rule only applies, if the profiling produces “legal effects” concerning the individual or “similarly significantly affects the data subject.
- GDPR mentions explicitly refusal of online credit applications and E-recruitment of two such examples of automated decision-making.
- Data profiling where an individual’s direct identifying information has been removed through pseudonymisation will significantly reduce any privacy impact on the individual, mainly when keeping in mind the GDPR’s overarching support of Pseudonymisation.

- ✎ **ABC contacted via text message a number of former employees of subcontractor XYZ, who represents ABC as their customer service.**
- ✎ **ABC wanted to recruit employees who have been terminated or resigned at XYZ, after the Organization has chosen to move offices from the city where ABC has its headquarters.**
- ✎ **The employees have been contacted directly by text message ABC, despite having not been employed by the group.**

Discussion case



-  **Has ABC complied with the GDPR by using contact information on employees of a subcontractor in this context?**
-  **Can personal information given in another context be used to ensure terminated employees a job opportunity?**




 If ABC has obtained the information on legitimate terms in relation to their cooperation with XYZ, can ABC use employee data and commitments that are submitted in a different context and be in conflict with GDPR rules?



- ✎ **How could ABC have used personal data given for other purposes to be GDPR compliant?**
- ✎ **Let's discuss other alternatives than to invite the employees to a meeting where the employees could sign up**



 **Can a Organization contact former employees of a subcontractor directly when the Organization has daily cooperation with and is in daily contact with the employees and thus has contact information on them?**

 **Let's discuss the overall principles in relation to GDPR, the Organization must ask its subcontractors and partners they cooperate with, but where the daily management lies the partners/subcontractors.**

