

GDPR compliance



by



Day II
DPO Certification part I
Brussels 022019

Overview



abc

FAS

- Introduction to GDPR
- Changes
- Roadmap for implementation



DPO Day 1

- GDPR in practice
- Principles for data processing
- Legitimate interests and new rights
- Operational privacy



DPO Day 2

- DPO rule and functions
- Binding corporate rules
- Data protection impact assessment
- ISO 27001



CEP

- Best practices and methodology
- Managing the privacy compliance program
- Study cases
- Definitions

Agenda

Time	Topic
09:00 - 09:25	Recap : Compliance Summary
09:25 - 10:30	Legitimate interests
10:30 - 10:45	Management issues
10:45 - 11:05	
11:05 - 12:00	Consents
12:00 - 12:30	Demonstrate compliance To Do
12:30 - 13:30	
13:30 - 14:20	Demonstrate compliance Documentation
14:20 - 14:35	Breakout session
14:35 - 15:35	
15:35 - 16:00	Change management and tips



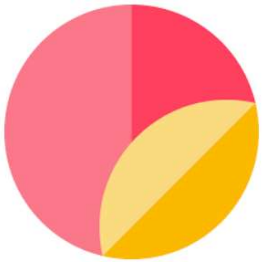
Access to the presentation



<https://www.eugdpr.institute/dpo-1/>



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

What is happening in the world?



There are data breaches everywhere, everyday.



Facebook Security Breach Exposes Accounts of 50 Million Users

CNIL (France)

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

CNPD (Lux)

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

FINANCE • EQUIFAX

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



Cambridge Analytica

Cathay Pacific faces probe over massive data breach

Under Armour

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

ICO (UK)

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

Organisation areas with risk exposure



- ✎ **Governance** – historic deficit in board accountability
- ✎ **Risk management** – GDPR processes are absent
 - ✎ no consideration of risks to rights and freedoms
- ✎ **GDPR Project team** – key issues needed to create a dedicated team, (un)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 throughout the roles
- ✎ **The scope of compliance** – unclear, because of the chain of processing activities are undefined
- ✎ **Process analysis** – significant inadequacies in relation to the data processing/protection principles.

IT and technical 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

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**

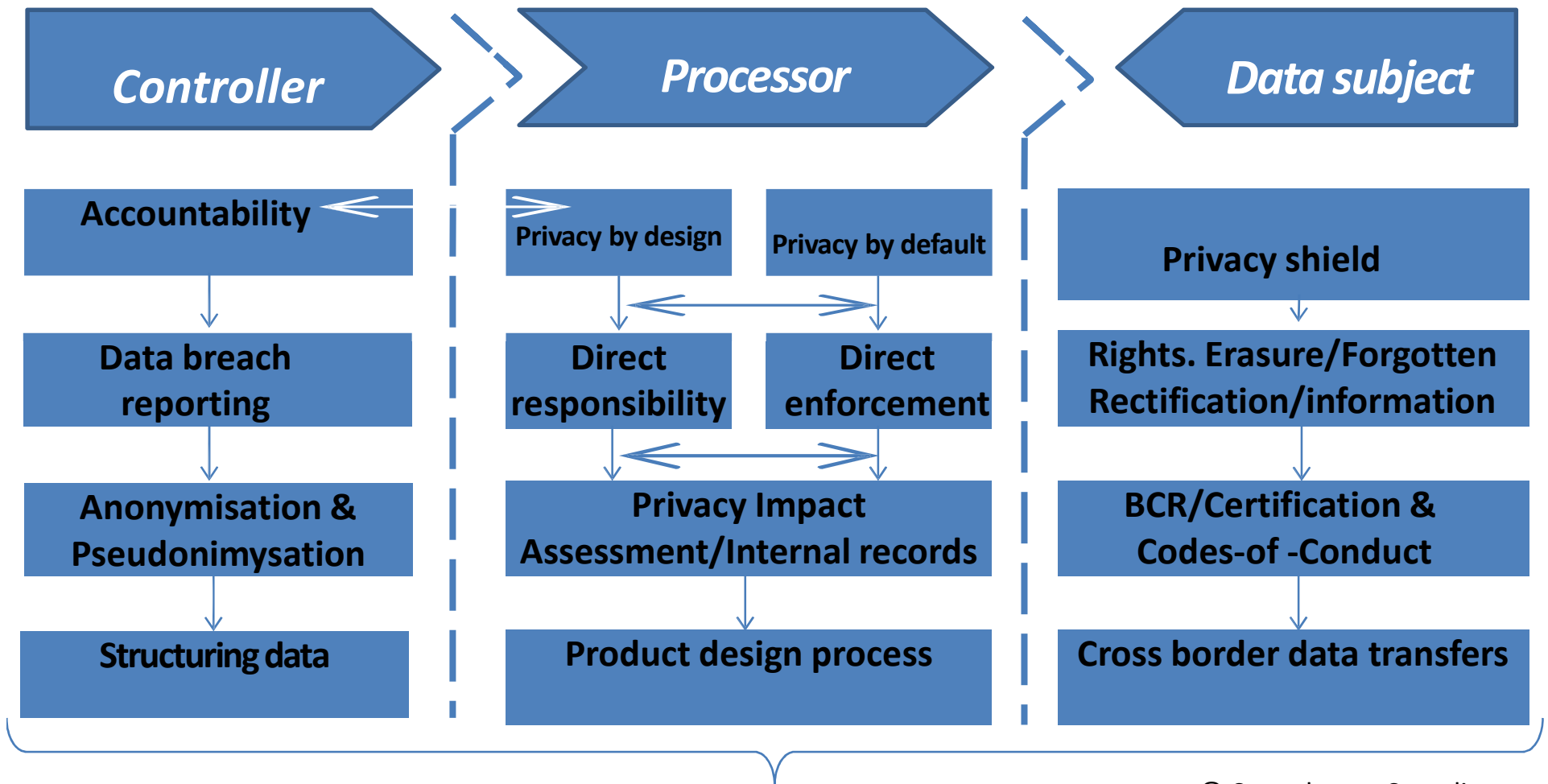


Proportionality

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

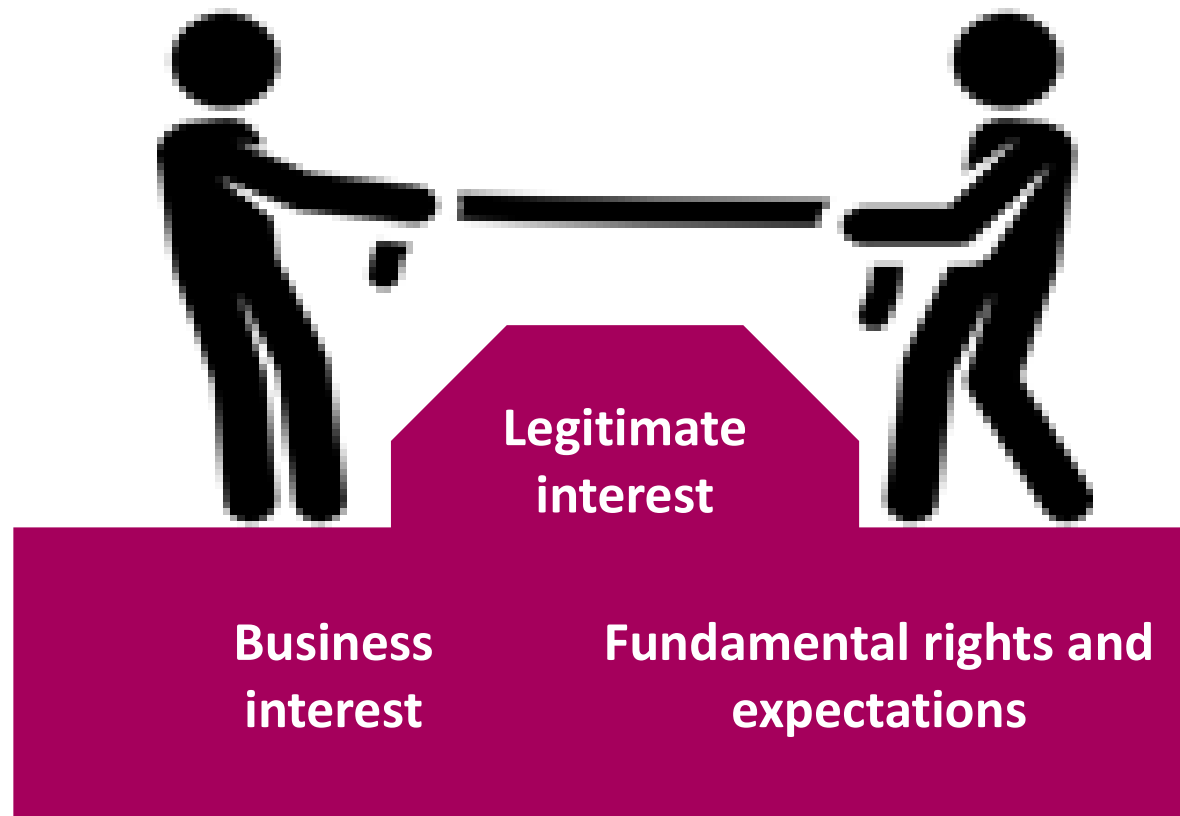
Assemble the Data Privacy & Protection Road Map & Framework



© Copenhagen Compliance

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

Legitimate interests



Legitimate interests



The processing of personal data is

- ✓ Required for an organization interests
- ✓ Does not impact the individual from a privacy perspective

Purpose

- ✓ Are you pursuing a legitimate interest?

Necessity

- ✓ Is the processing necessary for that purpose?

Balancing

- ✓ Do the individual's interests override the legitimate interest?

Legitimate interests



Principle 2: Purpose Limitation

- Only be collected for specified, explicit and legitimate purposes
 - Define up front what the data will be used for
- limit the processing to what is necessary to meet that purpose
- processing is necessary for the purposes pursued by the controller
 - or by a third party
- Interests are overridden by the interests or fundamental rights and freedoms of the data subject
 - needs protection of personal data, if the data subject is a child
 - Processing is carried out by authorities to perform their tasks
- Legitimate interests pursued by controllers in specific contexts

Identify the interests



✓ What is the purpose of the processing operation?	The first step is to identify to a legitimate interest
✓ Is the processing necessary to meet one or more specific organizational objectives?	If the processing operation is required to achieve a lawful business objective, then it is likely to be legitimate for the purposes of this assessment
✓ Is the processing necessary to meet one or more specific objectives of any Third Party?	It is useful to list all apparent interests in the processing, those of you as the Controller, as well as those of any Third Party
✓ Does the GDPR identify the processing activity as being a legitimate activity, subject to the completion of a balancing test and positive outcome?	Legitimate interests might be relied on where an data subject information is processed by a group of companies for the purposes of administration

The Necessity Test



<p>✓ Why is the processing activity important to the Controller?</p>	<p>A legitimate interest may be elective or business critical; however, even if the Controller's interest in processing personal data for a specific purpose is obvious and legitimate</p>
<p>✓ Why is the processing activity important to other parties the data may be disclosed to, if applicable?</p>	<p>A legitimate interest may be trivial or business critical, however, the organization needs to be able to clearly explain what it is</p>
<p>✓ Is there another way of achieving the objective?</p>	<ul style="list-style-type: none">• If there isn't, then clearly the processing is necessary; or• If there is another way but it would require disproportionate effort, then the processing is still necessary; or• If there are multiple ways of achieving the objective, then a Privacy Impact Assessment should have identified the least intrusive means of processing the data which would be necessary

The Balancing Test



✓ Would the individual expect the processing activity to take place?

If data subject would expect the processing to take place then the impact on the individual is likely to have already considered by them and accepted. If they have no expectation, then the impact is greater and is given more weight in the balancing test

✓ Does the processing add value to a product or service that the individual uses?

✓ Is the processing likely to negatively impact the individual's rights?

CASE STUDY I of II




- Umbrella Corp is an eCommerce company with a global presence for 45 years. The head office is in Germany and operates in 153 countries. This organization has 127000 on-payroll and has partnerships with 300+ 3rd party companies.
 - Thomas Benjamín is CIO
 - Mark Shields is the CRO to whom Sally (DPO) reports.
 - Michal James is CISO
- On DPO's directions, Thomas (CIO) is running a program to redesign the eCommerce to be compliant to GDPR.
- Post due-diligence, he identified that 47 mobile and web applications are used in EU and must be GDPR compliant.
- These applications are collecting personal and sensitive personal information from suppliers, employees, and various EU residents. Data collected from these EU residents is currently used by R&D, customer insights, sales, operation and various internal departments, consumers and suppliers.

CASE STUDY II/II



- The Controller has given you 70 days to make these applications GDPR compliant.
- Due Diligence: - Completed, 47 applications are collecting information from users and storing it in unstructured and structured databases.
 - Consumers have signed-up for using these applications, However, he does not have visibility whether it is being done on all the applications.
- You have been hired as an advisor to execute the GDPR program.
- You have to develop and perform the balancing test and necessity test to run this program.
 - Formulate Privacy Policy for GDPR.
 - Built technical administrative and awareness controls required for GDPR compliance.


Data Subjects Rights



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

NEW

To data portability *common format, even directly transmitted between controllers*




NEW



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

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




NEW



To restrict processing *limiting the data use or transfer*

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



Privacy is part of the general management system

- ✎ Documentation is the evidence of accountability and good governance

Privacy policy

- ✎ Supported by: document retention, destruction, info classification, breach management and others
- ✎ Assess and manage the impact of changes in policies
- ✎ Available to all the staff (awareness training)

Corporate defence

- ✎ 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 are 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 & organisational controls (art. 28, ISAE 3000 type 1, data protection seals and certifications)

Auditor's responsibility for GDPR compliance



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

Structure of the ISAE3000 report by the independent auditor



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

Discussion on Data Breach



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

Data Protection Officer



The DPO has an independent role
The role is about delivering compliance

DPO functions



Privacy governance



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
- ✎ Privacy is part of the general management system
 - ✎ Documentation is the evidence of accountability and good governance

Approach 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 organisations and individuals employed by them



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

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

Approach for governing privacy



Comprehensive regulation or sectorial laws?

EU (and Singapore) have adopted comprehensive legislation while other countries regulate different sectors

Governance of cross-border data flows

Disparities in national legislations have the potential to hamper data flows and raise constraints in trade development

– **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

– might lead to restricting innovation and raising costs



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				

Key challenges for compliance



Issue	Challenges	Resolution
<p>Cross-Border Data Transfers Art. 46</p> <p>Addresses transfer to national not deemed “adequate.”</p> <p>Lead data protection supervisory authority</p>	<p>Which mechanism to use</p> <p>Data in Cloud Environments</p>	<ul style="list-style-type: none"> • <u>Privacy Shield</u> (e.g. EU to the US, one directional only, general purpose solution) • <u>Standard Contract Clauses</u> with individual companies and vendors • <u>Binding Corporate Rules</u> challenging to complete before deadline, establish basic compliance first
<p>Third Party Compliance Art. 28</p>	<p>Working with third parties</p> <p>Cloud service providers</p>	<p>Third Party Triage</p> <ul style="list-style-type: none"> • One size fits all, e.g. large cloud companies • Team players • Laggards
<p>Data Protection Impact Assessments (DPIA) Art. 35</p>	<p>Binary “It is high risk” determination</p> <p>No clear guidelines for medium risk</p>	<p>WP 248 guidelines (High Risk)</p> <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 that produces a significant effect on the data subject? • Is the organisation performing systematic monitoring of data subjects, including in a publicly accessible area?

Key challenges for compliance



Issue	Challenges	Resolution
<ol style="list-style-type: none"> 1. Creating a Data Inventory 2. Information Held 3. Locating all personal data and mapping it 4. Art. 30 Record of processing activities 	<p>Relies on interviews with process owners</p> <p>Process owners may not always be aware of all the data and where it resides</p> <p>Affects internal controls, taking consent</p>	<p>Data classification and discovery</p> <p>Algorithms to go through the systems and identify the various types of data (eDiscovery)</p> <p>Manual inventory of data and documentation</p>
<ol style="list-style-type: none"> 1. Appointing a Data Protection Officer Art 37 someone to take responsibility for data protection compliance 	<p>Is a DPO always needed?</p> <p>Confusion between roles, DPO is more of an ombudsman (between Data Protection Authority and data subjects) than a officer</p>	<p>Worst case scenario if data is leaked can be used to identify need for a DPO</p> <ul style="list-style-type: none"> • Organizations with medical data need a DPO • Marketing data that can be cross-referenced to identify people would need a DPO
<ol style="list-style-type: none"> 1. Privacy by Design and Default. Art.25 2. Build deterministic failure into processing of personal data 	<p>No generally accepted standards for data protection by design and default</p> <p>Retrofitting existing legacy systems for data protection in a short time frame</p> <p>Data minimisation</p>	<p>Organizational (i.e. administrative) controls</p> <ul style="list-style-type: none"> • Background checks on employees, • Privacy policy training • Incident Response Plan • Breach Notification Plan • Controls for breakdown of legacy systems

Key challenges for compliance



Issue	Challenges	Resolution
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
Notice and Consent Art. 12-14, Art. 7,8	<ol style="list-style-type: none">1. Notice consent2. Notice Availability	Review data inventory
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 Sometimes it may not be feasible, or effort to be invested may outweigh the benefits	<ul style="list-style-type: none">• 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



Issue	Challenges	Resolution
Crafting a Privacy Policy Implied under Art. 32	Developing the correct content	The organization's commitment to the protection of personal data <ul style="list-style-type: none">• 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
Subject Access Requests	How much to invest in automating SARs?	The organization should update their procedures and plan how they will handle requests within the new timescales and provide any additional information.
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



Issue	Challenges	Resolution
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
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
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.

Discussion on Data Breach



Assess the potential impact
data breaches can have
on your business.

Operational privacy



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), a proper budget, qualifications and certifications (CV, identity and background checks) and communication to the supervisory authority
- ✎ For non-EU data controllers/processors; the 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; detail the legal reasons for processing data
- ✎ Procedure for secondary uses of personal data
 - ✎ How to manage personal information for other purposes other than it was originally collected
 - ✎ The mechanism for de-identifying data (art 89) for archiving purposes in the public interest, or scientific and historical research purposes, or statistical purposes

Demonstrate compliance



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 the processing, accountability for the responsible person and the response actions
- ✎ Procedure for children's consents
 - ✎ How to verify parents/guardians

Demonstrate compliance



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

- ✎ Policy for collection and use of sensitive personal data
 - ✎ How to document the 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



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



The 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 requests, 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

Discussion on Data Breach



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

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

Document Each Objective



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)

Document Each Objective



Corporate defense. Demonstrate compliance efforts (implementation measures, control improvement)

- ✎ Record of processing activities under the stakeholder 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)

Demonstrate compliance



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

Demonstrate compliance



- Responsibility of the controller (art 24)
- Responsibility of the controller in outsourcing (art 28)
- Records of processing activities (art 30)
- Records of data transfers (arts 45 to 49)
- Security of processing (art 32)
- Data protection impact assessment (arts 35 and 36)
- Data breach notification (art 33)
- Privacy by design and by default (art 25)
- Protocol for a data breach notification
- Procedure to obtain valid data privacy notices

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
 - ✎ Processes documented and tested!

Demonstrate compliance



Responsibility of the controller in outsourcing (art 28)

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

Demonstrate compliance



Records of processing activities (art 30)

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

Document Granularity



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

Case



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

Discussion on Data Breach



How will you address data breaches thru training and awareness?

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

Document Compliance



Data protection impact assessment (arts 35 and 36)

- ✎ DPIA guidelines and templates
- ✎ Consultation with 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 with the supervisory authority

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

Document Compliance



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)

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 advise would you give to The Safe Browsing team of The EUGDPR Institute to ensure GDPR Compliance on Google, Facebook and Twitter to make sure that primary issues like consent or showing a warning whenever it tries to collect your data without telling you.is taken into consideration to avoid issues with the DPA.



Differences



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

When is processing 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

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-ticket)



clicking an opt-in button or link online



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?

When submitting Yes, No 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/utills/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.

Profiling activities



Data Subject right to limit profiling and not be subjected to automated decision making

✎ Analytical Profiling

- ✎ Big data analytics has enabled the collation of scattered bits of PI & manufacture information.
- ✎ GDPR will safeguard against misuse of such information

✎ Extensive profiling, or

- ✎ automated-decision making (e.g. by scoring) with legal or similar significant effect
- ✎ e.g. financial institutions for automated loan approvals, e-recruiting, online marketing companies, and search engines with target marketing facilities

✎ WP 248 guidelines (High Risk)

- ✎ Is the organisation doing evaluation or scoring (including profiling and predicting) of aspects specific to the data subject?

Discussion case



- ✎ 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?



Discussion case



✎ 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?



Discussion case



✎ 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



Discussion case



- ✎ Can an 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.**



Step 4: Let's practice



Examples from “when” to “what”

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

Step 4: Let's practice



Ideas for the “what”?

✎ When candidates apply for a job

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

✎ When employees are hired

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

✎ When clients take part in a prize draw

✎ name, phone

Step 4: Let's practice



Ideas for the “what”?

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

Step 4: 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

Managing changes to comply



Change management



GDPR Impact



New or amended policies and record management



New operational roles and responsibilities, DPO role



Changes in IT tools, solutions, applications and infrastructure



Changes in contracts, agreements, consents, notices

Continuous improvement

Change management



GDPR Impact



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



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



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



Document compliance efforts
Get approvals for changes
Metrics for GDPR compliance

Change management



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

Accelerating GDPR compliance



Discussion on Data Breach



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

Discussion on Data Breach



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

Tips for data accountability



- ✎ Clear ownership of data in the privacy policy to coordinate GDPR compliance efforts
- ✎ **Data custodian for technical control** > system administration and technical measures such as encryption and backups
- ✎ **Data owner for functional control** > data management practices to comply with GDPR
- ✎ All types of data > ERP/CMR, cloud, on-premises, big data, and unstructured data
- ✎ Involve project stakeholders

Tips for data inventory



- ✎ A good map of records of processing activities saves time
- ✎ Consider all techniques
 - ✎ Interviews and workshops with data owners and process experts
 - ✎ Functional documentation and data flow maps
 - ✎ eDiscovery
- ✎ Classify data > confidential, restricted, private, public
- ✎ New personal data > online identifiers, location, biometric
- ✎ Logically grouped actions
- ✎ Prepare to maintain the records of processing activities

Tips for risk approach



- ✎ Prioritize remediation plans to riskier areas
- ✎ Most sensible data, most shared, most records
- ✎ Follow good info sec standards > ISO 27001/2
- ✎ Test procedures to address subject access requests and data breach notification > are they scalable?
- ✎ Operationalize changes such as data protection by design and DPIAs
- ✎ Validate data transfers
- ✎ Scramble, anonymize and pseudo-anonymize data

Non-GDPR compliance can be accomplished by:



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

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

Non-GDPR compliance can be accomplished by:



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

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

What did May 25th 2018 mean?



End of remediation actions

- ✎ Mandatory appointment of a DPO
- ✎ Completed records of processing activities
- ✎ Updated privacy notices and statements
- ✎ Renegotiated contracts with 3rd parties
- ✎ Reviewed user access and data quality
- ✎ Completed de-risking actions
- ✎ Completed training and awareness

What did May 25th 2018 mean?



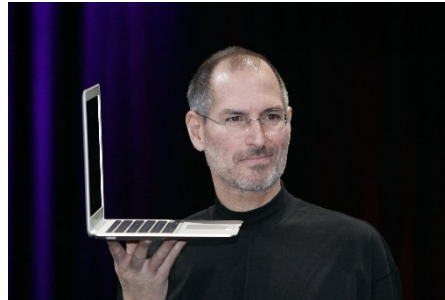
Start demonstrating the compliance efforts

- ✎ Documented privacy program and legal basis for processing activities
- ✎ Ongoing data lifecycle management according to the privacy policy, including data consents
- ✎ Monitoring data flows and audit trails
- ✎ Data privacy impact assessment procedure
- ✎ Incident response and breach notification procedure and privacy audits plan

Data Privacy and Protection Perspectives



What the friends think



What the mom thinks



What society think



What the boss thinks



What the family thinks



What we think

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



The GDPR Institute



www.copenhagencompliance.com



Human Capital Assessment Framework



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

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

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

Disclaimer



- The examples and scenarios in this presentation are for illustration purposes only, and not based on specific examples to be construed as particular advice on any practical legal issues.
- As always, contact your legal counsel for clarification and recommendations on legal issues. Copenhagen Compliance or The EUGDPR Institute is not licensed to provide legal advise.

Copyright notice



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

As always, when in doubt or for legal guidance, always contact your legal advisers. The EUGDPR Institute and Copenhagen Compliance are not licensed to provide any legal advice.