



GENERAL
DATA
PROTECTION
REGULATION



FAS
Foundation

DPO
Masterclass

CEP
Practitioner



Day 3. Brussels 16th May 2019

All Links



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

The impact of Data Privacy & Protection in Business



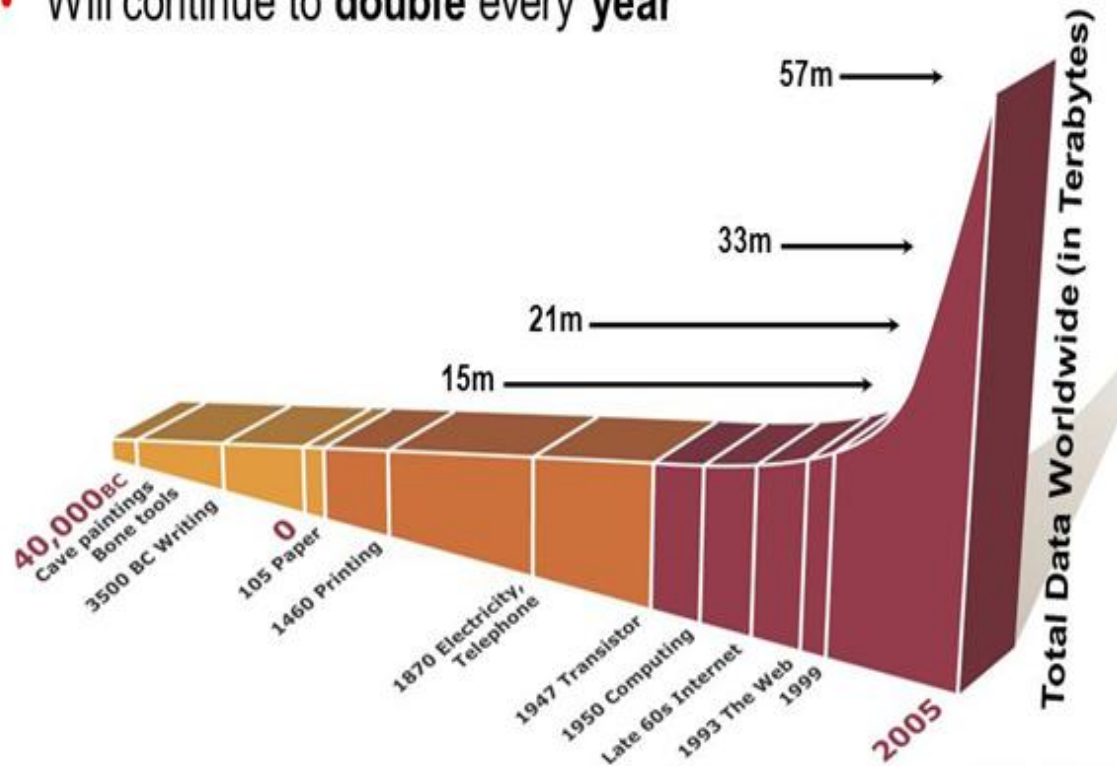
- Increasing number of regulations do not render more jobs & growth
- Net neutrality rules could create the next Google or Facebook
 - Google or Facebook rivals are in Russia & China, with no net neutrality rules
- The largest firms benefit at the expense of smaller due to complexities
- Increased government power at the cost of consumer freedom
- The impact on value chain in the upcoming 5G networks in Europe
 - US and China where consumers have adopted pre-5G products and services
- GDPR is the data and IT platform for a “level the playing field”
 - Empowers European consumers
- GDPR’s impact on the advertising market in Europe
- GDPR’s negative impact on venture investment in Europe¹
 - The declines result in projected losses projected between 3,000-30,000 jobs.
- However, the GDPR is now the “global gold standard.”

¹Federal Trade Commission (FTC) and two academics at the Illinois Institute of Technology.

Data Proliferation



- More data created in last **2 yrs** than in the past **40,000 yrs**
- Total data **quadrupled** in the last **2 yrs**
- Will continue to **double** every **year**



- 90% of world's existing data created in the last 2 years
- 1 Billion - pieces of content on Facebook/daily
- 2.5 Quintillion - generated by people everyday
- 6 Billion - hours of video watched on YouTube every month
- 271 Million - Monthly active users on Twitter
- 2.7 Zetabytes - Amount of data in the digital universe

Privacy principles



General best practices when collecting, storing, using and disclosing personal information

Represent the core around which data or privacy protection has evolved

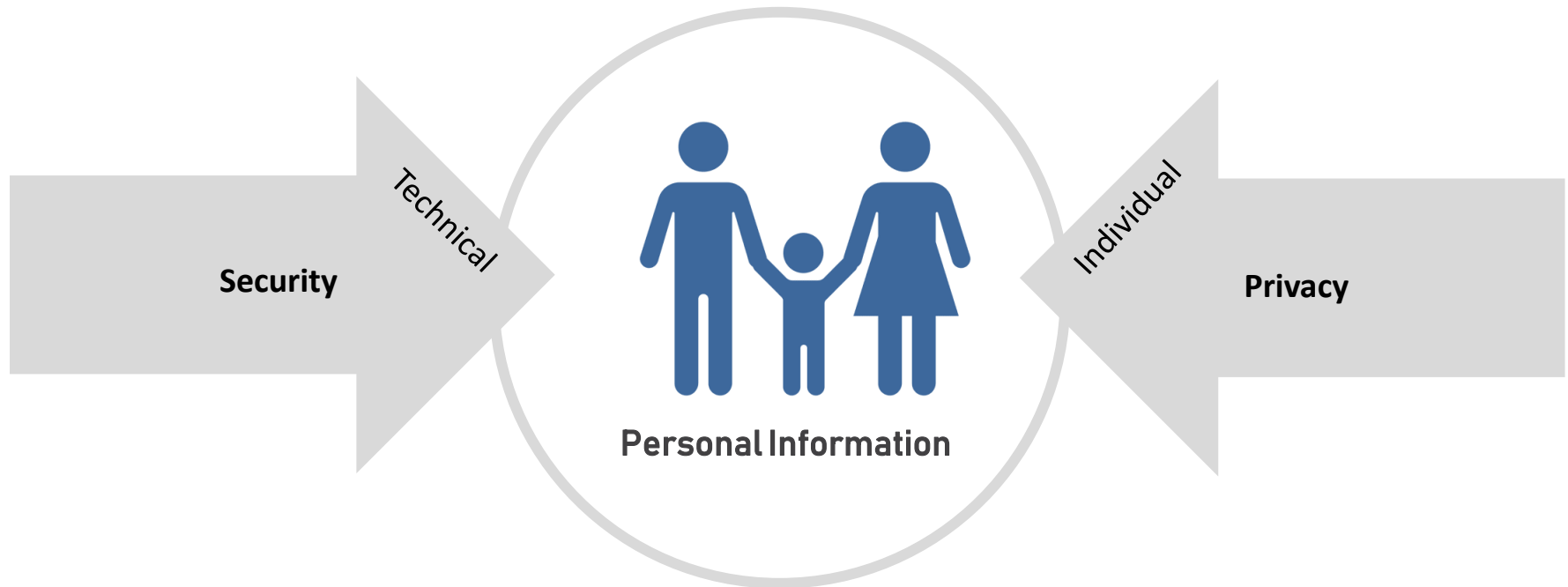


Developed before the internet era and have been resilient enough to withstand the test of time

Privacy is a human issue



GDPR requires companies handling EU residents' data to undertake major operational, privacy and security reforms



Considerably More Than Just a Privacy Policy Update

Data privacy



Data privacy



Ability to limit access and control the use of personal data

Communication privacy

Ability to communicate with others without being monitored by other people or organizations



Information privacy

Ability to determine when and to what extent personal information is collected, used, stored, processed transmitted and deleted

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

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

Key challenges for compliance 1



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 2



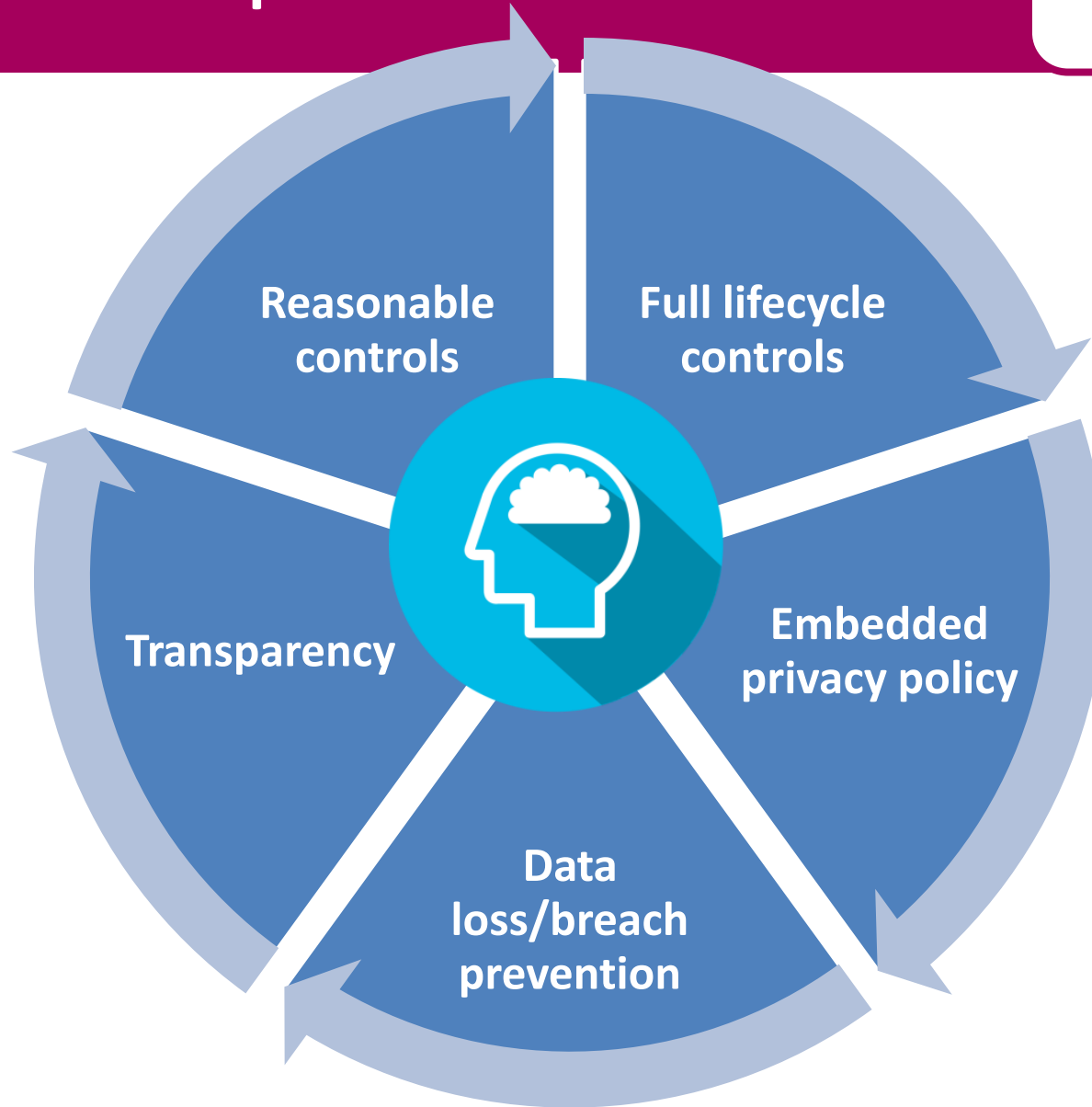
Issue	Challenges	Resolution
<p>Creating a Data Inventory</p> <p>Information Held</p> <p>Locating all personal data and mapping it</p> <p>Art. 30 Record of processing activities</p>	<p>Relies on interviews with process owners</p> <p>Process owners may not always be aware of all the data and where it resides</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>
<p>Appointing a Data Protection Officer Art 37 someone to take responsibility for data protection compliance</p>	<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
<p>Privacy by Design and Default. Art.25</p> <p>Build deterministic failure into processing of personal data</p>	<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 3











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
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

GDPR Principles in Practice

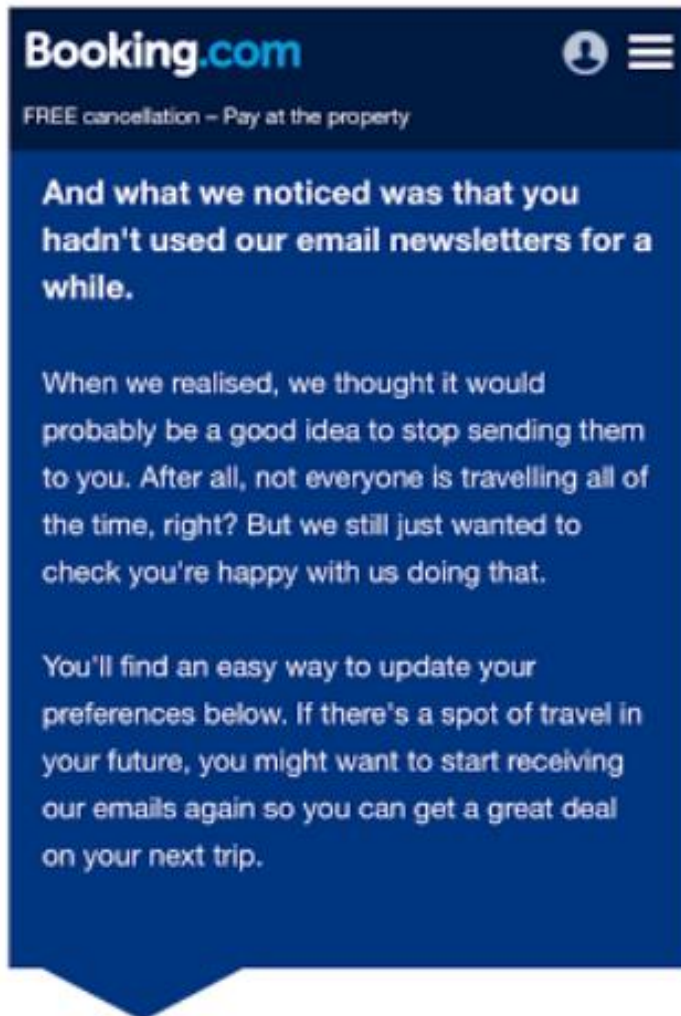


List of Policies to create



-  **Personal data privacy policy**
-  **Data privacy impact assessments policy**
-  **Consent management policy**
-  **Data retention policy (for personal data)**
-  **Subject access request management procedure**
-  **Data breach / incident management procedure**
-  **Privacy by design and default**
-  **Data processors addendum to contracts**

An example



I'd like to receive deals and offers again!

Update my preferences



[Head to Booking.com](#)

How to react after receiving a data subject request?

- ✎ How and when you got the consent
- ✎ What the consent covers
- ✎ How to demonstrate the processing according to the consent
- ✎ Where the data was stored and how it was accessed

How to prepare a GDPR compliance plan



Base the privacy program on the ISO 27001

- ✎ Accepted data security framework
- ✎ RoPA as a live management tool

Embedding data privacy into operations

- ✎ Privacy controls in policies and procedures
- ✎ Training and awareness
- ✎ Periodic testing of compliance and control evidence
- ✎ Respond to complaints and SARs
- ✎ Test the data privacy incident and breach management plan

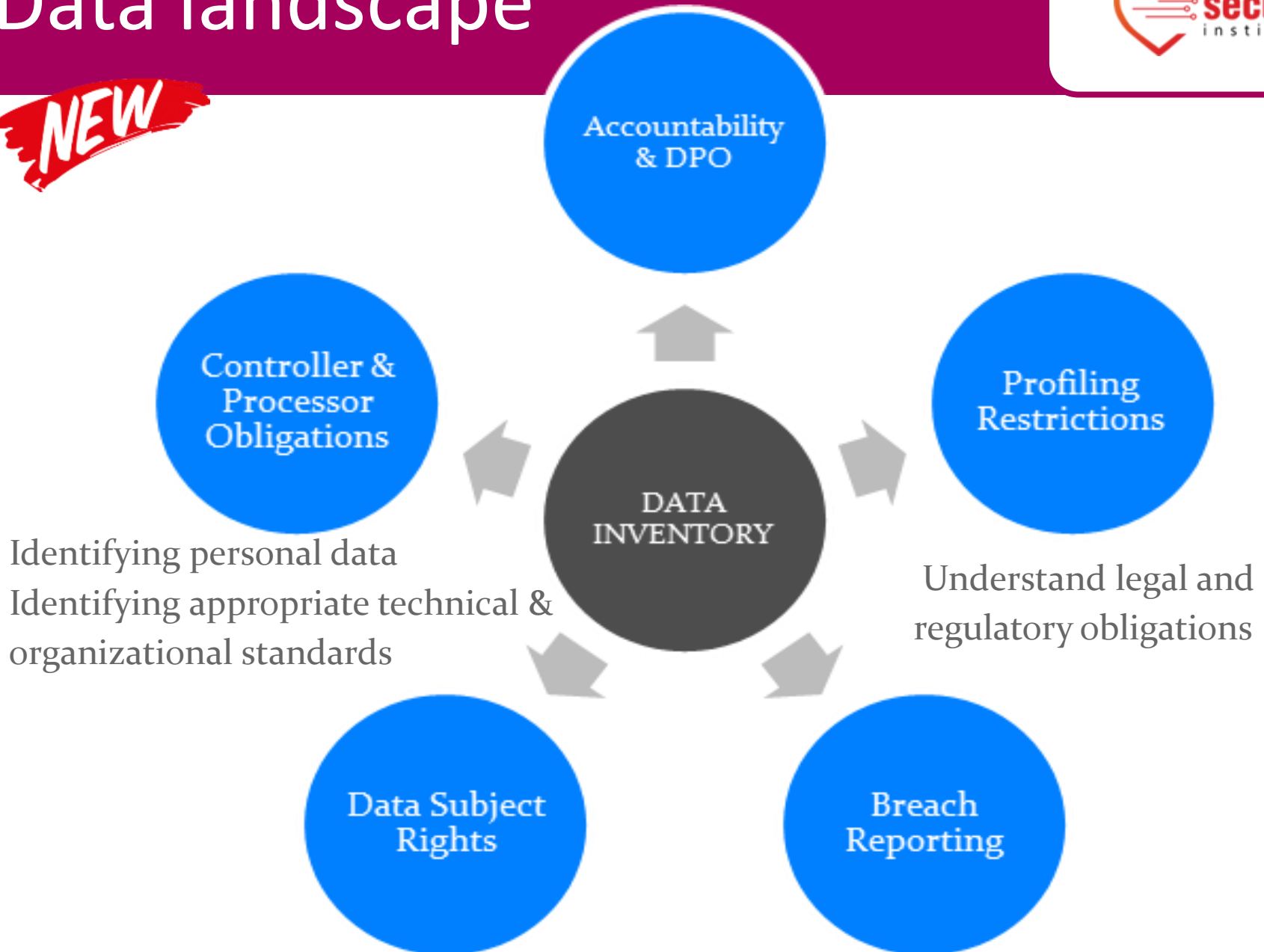
Privacy impact assessments

- ✎ Templates and procedure based on ISO
- ✎ Third party risk: avoid sub-processors and data exports

Data landscape



NEW



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 and genuinely independent



Data accountability

responsibility to use data for business

- Roles and responsibilities** typically do not include data protection or information security
- Scope of compliance** unclear because of undefined chain of processing
- Process analysis** significant inadequacies in relation to the data processing principles

GDPR Best Practices and Standards

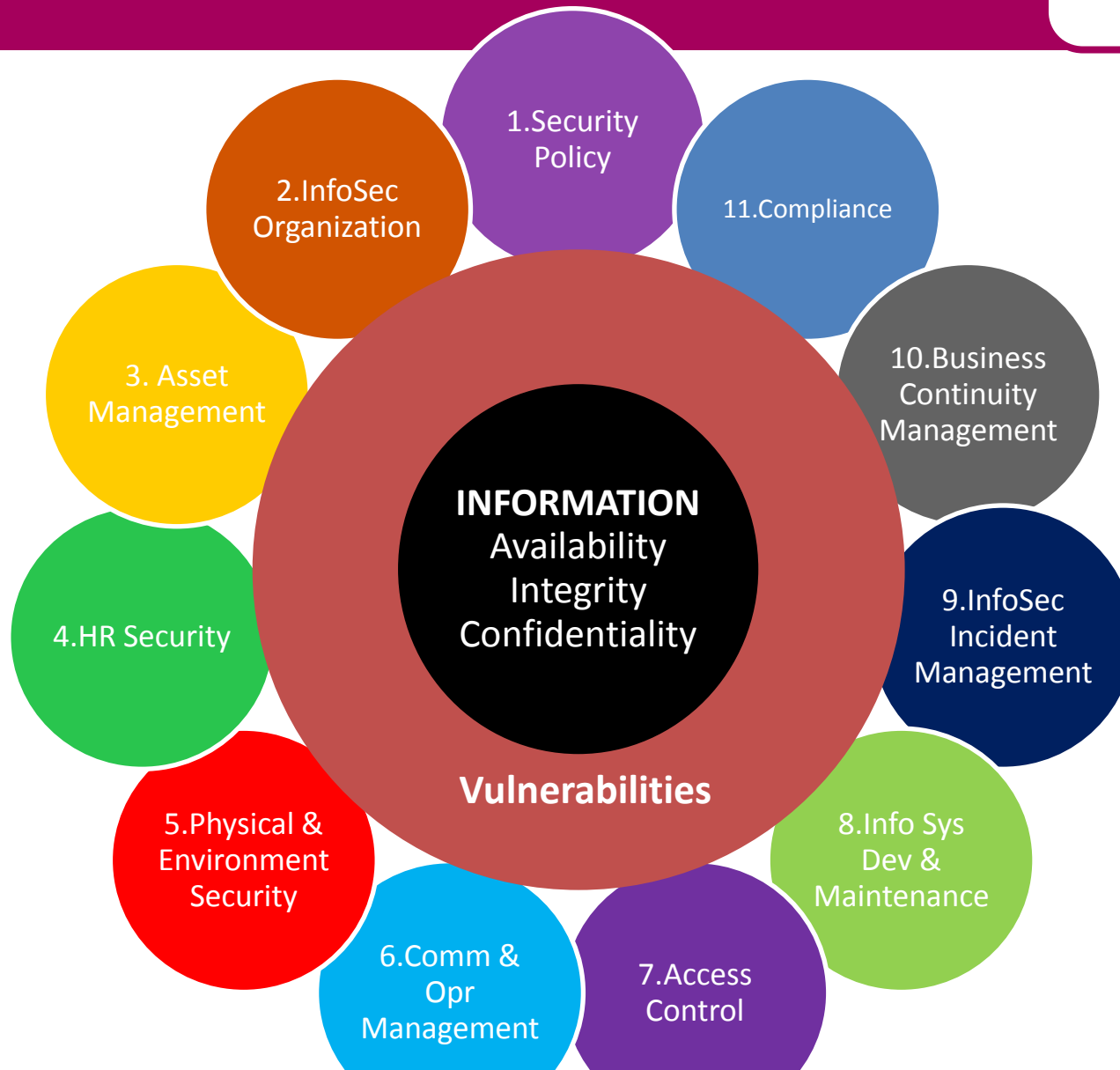


ISO 27001

PCI DSS

NIST Guidance

Domains of ISO 27001



Confidentiality

- ✎ Ensuring that information is accessible only to those authorized to have access

Integrity

- ✎ Safeguarding the accuracy and completeness of information and processing methods

Availability

- ✎ Ensuring that authorized users have access to information and associated assets when required

Comparison



GDPR

ISO 27001

Purpose

Protects individuals with regard to the processing of personal data

Define, implement, maintain and improve a security management system

Scope

All the personal information that the organizations handle, either digital or on-paper

All information systems at organizations

Comparison



GDPR

ISO 27001

Safety measures

Based on the impact on the rights of data subjects after leaks, thefts or damage to their personal data

Based on the importance of the information for the organization

Legitimacy, correctness, transparency

The data is processed in a lawful, correct and transparent manner in comfort of the interested party

The data is processed in the way the organization considers correct and responds to their needs

Comparison



GDPR

ISO 27001

Purpose limitations

The data is collected for specific, explicit, legal and legitimate purposes and processed only for those

No constraints

Data minimization

The data collected is only the necessary for the stated purpose

No constraints

ISO 27001 and GDPR



ISO27001 and GDPR



1. ASSURANCE

- ✎ Use of certification schemes providing assurance managing information security risks

2. NOT JUST PERSONAL DATA

- ✎ Protects customer information
- ✎ Protects your information assets
- ✎ Includes electronic information and in hard copy format

3. CONTROLS AND SECURITY FRAMEWORK

- ✎ Selection of technical and organizational controls to mitigate risks

4. PEOPLE, PROCESSES AND TECHNOLOGY

- ✎ Protects from technology-based risks
- ✎ Educates poorly informed staff
- ✎ Corrects ineffective procedures

5. ACCOUNTABILITY

- ✎ Requires security regimes to be supported by top leadership
- ✎ Requires a senior individual who takes accountability
- ✎ Mandates clear accountability for data protection

6. RISK ASSESSMENTS

- ✎ Conducts regular risk assessments to identify threats and vulnerabilities that can affect your information assets, and to take steps to protect that data

7. CONTINUAL IMPROVEMENT

- ✎ Requires that ISMS is constantly monitored, updated and reviewed,
- ✎ It evolves as business with continual improvement, reducing risks

8. TESTING AND AUDITS

- ✎ Requires organizations to carry out regular testing and audits to prove that its security regime is working effectively

9. CERTIFICATION

- ✎ Requires organisations to ensure that security controls are designed.
- ✎ Deliver an independent, expert assessment to confirm if adequate measures or safeguards are implemented to protect your data

Define adequate safeguards



- Controllers and processors may only transfer personal data to third countries that do not provide for adequate protection (non-adequate countries),
 - if the controller or processor has provided adequate safeguards
- The data transfer provisions require processors/controllers to implement adequate safeguards, with full GDPR scope
 - The interpretation of this requirement means that processors should provide “adequate safeguards” insofar as their own obligations are concerned.
 - The DPAs interpret the transfer requirement on the controller “to offer adequate safeguards.”
 - The current provision is that both controllers processors are required to impose “adequate safeguards” in case of transfers to all third parties in a non-adequate country

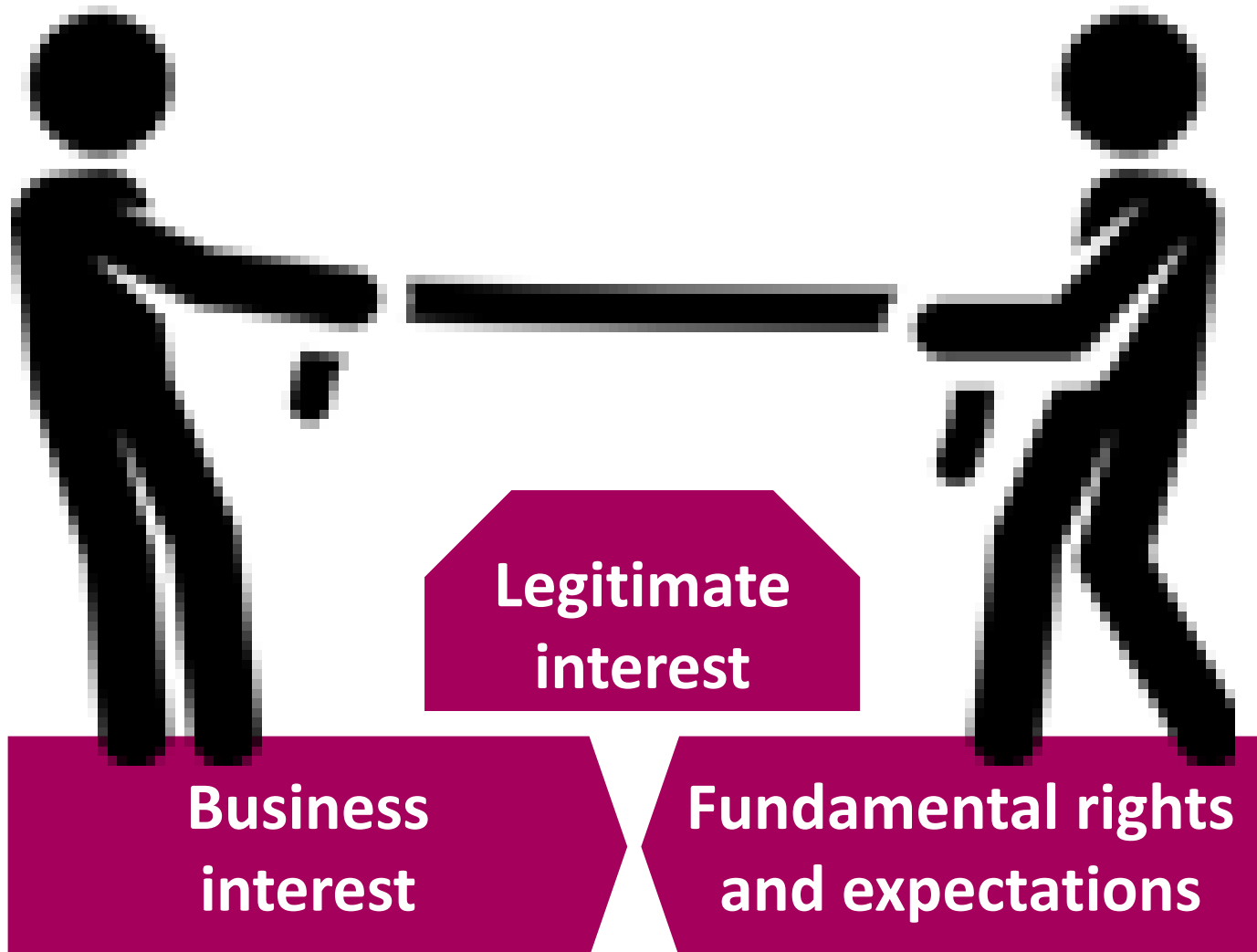
Legitimate interests



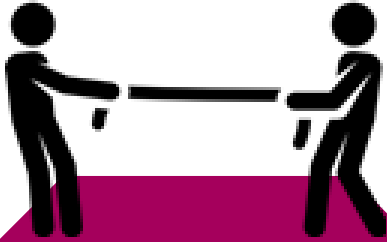
Requirements

Practice

Legitimate interests



Legitimate interests



**Legitimate
interest**

Test



The processing of personal data is

1) required for an organization interests, and
2) does not impact the individual from a privacy perspective

1) purpose

Are you pursuing a legitimate interest?

2) necessity

Is the processing necessary for that purpose?

3) balancing

Do the individual's interests override the legitimate interest?

Legitimate interests



Checklist

- ✓ **We have checked that legitimate interests is the most appropriate basis**
- ✓ **We understand our responsibility to protect the individual's interests**
- ✓ **We have conducted a legitimate interests assessment (LIA) and kept a record of it, to ensure that we can justify our decision**
- ✓ **We have identified the relevant legitimate interests**
- ✓ **We have checked that the processing is necessary and there is no less intrusive way to achieve the same result**
- ✓ **We have done a balancing test, and are confident that the individual's interests do not override those legitimate interests**
- ✓ **We only use individuals' data in ways they would reasonably expect, unless we have a very good reason**

Legitimate interests



Checklist

- ✓ **We are not using people's data in ways they would find intrusive or which could cause them harm, unless we have a very good reason**
- ✓ **If we process children's data, we take extra care to make sure we protect their interests.**
- ✓ **We have considered safeguards to reduce the impact where possible**
- ✓ **We have considered whether we can offer an opt out**
- ✓ **If our LIA identifies a significant privacy impact, we have considered whether we also need to conduct a DPIA**
- ✓ **We keep our LIA under review, and repeat it if circumstances change**
- ✓ **We include information about our legitimate interests in our privacy notice**

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?**

The Balancing Test



<p>✓ Is the processing likely to result in unwarranted harm or distress to the Individual?</p>	
<p>✓ What is the nature of the data to be processed? Does data of this nature have any special protections under GDPR?</p>	<p>If processing special categories of personal data, an Article 9 condition must be identified as the lawful basis of processing (e.g. explicit consent, employment and social security, vital interests, public interest, etc)</p>
<p>✓ Has the personal information been obtained directly from the individual, or obtained indirectly?</p>	<p>If the information was obtained directly from the data subject then you should take due consideration of the notice of fair processing (e.g. the privacy notice)</p>

Study case



- 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.

Study case



- 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.

Automated decision making



Profiling



fully automated decision-making
(*machine learning*)



ability to make decisions by
technological means without
human involvement

decisions on an
individual cannot be
solely based on
automated processing

unless the individual
gives an explicit
consent

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?

Automated decision making



There are three exemptions when they apply in processing the data:

- is necessary for entering into, or performance of, a contract between the data subject and a data controller;
 - is authorised by a union or member state law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
 - is based on the data subject's explicit consent.
-
- Article 13 states that data subjects have the right to an explanation of the logic involved.
 - GDPR does not forbid profiling. It requires the transparency of all operations, appropriate statistical procedures and accuracy of data.
 - Requires a strong emphasis on the right to opt out that is enforced in all areas where consent is involved, not just profiling.

Discussion case



FSA fines HSBC over £3 million for data security breach

HSBC Life UK Limited, HSBC Actuaries and Consultants Limited and HSBC Insurance Brokers Limited have been fined £1,610,000, £875,000 and £700,000 respectively by the Financial Services Authority (FSA) following an investigation into their customer data security measures. The measures were inadequate and failed to prevent customers' confidential details against risks including identify theft. The fines would have been £2,300,000, £1,250,000 and £1,000,000 respectively but HSBC cooperated fully and agreed to settle at an early stage of the investigation.

The FSA's investigation into the firms' data security systems and controls highlighted the following. There were inadequate protections to guard against financial crime (including the theft of customer details). A floppy disk and a CD containing unencrypted customer data were sent by post or courier to third parties. Hard copies of confidential customer information were not locked away in cabinets. Staff were insufficiently trained on how to manage data security risks. The firms had previously been warned by HSBC Group about the need for robust data security controls.



The FSA has said that firms must ensure that their data security systems and controls are constantly reviewed not least in order to guard against identify theft. The FSA has made it clear that in areas where it has warned firms generally about the need to improve their data security measures, they should expect fines to increase in order to deter others and to foster change in the sector.

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 a company 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.**




Discussion case



Website attack affecting our customers

We are very sorry to tell you that on Thursday 22nd October a criminal investigation was launched by and sustained cyberattack on our website on Wednesday 21st October. The investigation is ongoing data may have been accessed:

- ▶ Names
- ▶ Addresss
- ▶ Dates of birth
- ▶ Email addresses
- ▶ Telephone numbers
- ▶ TalkTalk account information
- ▶ Credit card details and/or bank details

 **TalkTalk exposed the names, addresses, dates of birth, phone numbers and email addresses of more than 150k customers**

 **U.K. the Information Commissioner's Office fined at 400k GBP**

 **TalkTalk appeared in headlines associated with a lack of security and lost more than 100k customers**

GDPR and HR



GDPR Principles in Practice



Lawfulness

- ✎ **Transparent processing to data subjects**
- ✎ **Controls to process data according to consents**

Purpose and storage limitation

- ✎ **Specific and clear purpose**
- ✎ **Erase information after use**

Accuracy

- ✎ **Controls to maintain the quality, the integrity and against data loss**

Employee new rights



- ✎ Ask for a (free) copy of all their HR-related information**
- ✎ Correct or ask for correction information (e.g. using a self-service portal to update information)**
- ✎ Only use their personal data for the purposes informed in the consents**

Remember: employees, former employees, interns, part-time employees, contractors

How to write a consent for an employee



- ✎ Commitment for privacy and compliance
- ✎ Explain the employee rights
- ✎ Comprehensive examples of personal information maintained by HR
- ✎ Describe how and why the data is collected (e.g. by external recruiters)
- ✎ Describe how the data is transferred and protected
- ✎ Describe how criminal conviction data is managed

Supporting GDPR HR policies



HR Related Policies

- ✎ **Policies on the disclosure of personal data (covering internal and external disclosures) including:**
 - ✎ **Legal obligations on the organization to disclose, for example to meet Inland Revenue requirements or to provide information to company auditors**
 - ✎ **Cases in which the employee will be informed of the request for disclosure**
 - ✎ **Checks to carry out on credentials of those seeking disclosure.**
 - ✎ **The position regarding the disclosure of sensitive data**
 - ✎ **The position regarding disclosure which would involve transfer of personal data outside the European Economic Area**
 - ✎ **the review of non-regular disclosures**
- ✎ **Policy on how spent disciplinary notices are handled (part of disciplinary procedure)**
- ✎ **Document retention policy, including deletion and destruction guidelines**

Supporting GDPR HR policies



HR Related Policies

- ✎ **Personal data security policy including:**
 - ✎ **Guidelines for using fax and e-mail to transmit confidential information**
 - ✎ **The use of laptops and homeworking generally**
 - ✎ **The security of paper files**
 - ✎ **Audit trails**
 - ✎ **The use of shared facilities.**
 - ✎ **Subject rights procedures**
 - ✎ **Interview policy and guidelines**
 - ✎ **Practices for monitoring employee (CCTV/video surveillance)**
 - ✎ **Policy on the provision of confidential references**
- Also, serious breaches of data protection policies should be a disciplinary offence to impart the importance of compliance to staff**

Processing of HR data



Only process employee data on the basis ...

✎ 1- to fulfill an employment contract and legal obligations

✎ draft and manage the contract

✎ prepare payroll

✎ monitor worked time and activities such as work travel

✎ calculate payroll taxes, pension and insurance

✎ 2- to fulfil an employer's legitimate interests

✎ Protect the employee health and safety (e.g. warning, emergencies)

Get an explicit consent signed by employees

✎ a contract clause is not longer accepted (not separated)

✎ explain how HR-related data is processed and trasfered

HR training topics for GDPR



- What constitutes unauthorized processing and how to avoid it
- How deceit may be used to obtain information illegally from the organization
- General guidelines for line managers recognizing that they process employee personal data on behalf of the organization, and their responsibilities
- General guidelines on how to identify and action the exercise of subject rights
- General guidelines for those who 'wear different hats' working for two or more companies or trustees (i.e. 'Chinese walls')

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

Discussion case



A ridesharing company (*i.e.* URBAN GO) based on a mobile app offers a platform where drivers and riders can register to use its service

The company collects names, addresses, driving licenses, bank account details and location data of drivers and riders

The company has appointed a fintech solutions provider to process the payment of fares and driver's salaries

1. Who is a data controller, data processor and data subject

2. Based on your role, develop an outline of strategy to ensure data protection

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

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.

Overview



Global Data Privacy Laws



Worldwide privacy laws



HIPAA Health Insurance Portability and Accountability Act

1996/2009



Personal information

Medical records
Health status
Healthcare payment details

Key provisions

Right to request and correct personal medical information
Limited the conditions to disclose health information
Develop a privacy policy
Appoint a privacy official

Covered entities

Providers of health plans (insurers)
Health care providers (hospitals, dentists)
Subcontractors (claims processing, health analysis)

Penalties

Civil
100 to 50k USD per occurrence
Max 1.5M USD
Criminal
Imprisonment

Worldwide privacy laws



FCRA Fair Credit Reporting Act

1970 / FACTA 2003



Personal information

Personal financial information
Consumer files
Consumer-reporting information

Key provisions

Right to request and correct personal information
Right to opt-out for marketing contact
Limited disclose on reports
Real disposal of information

Covered entities

Credit reporting agencies

Penalties

Civil
1K USD per consumer damage
Max 2.5k USD per violation
Victims of identify theft can file a separated law suit
Criminal

Worldwide privacy laws



US Privacy Act

1974



Personal information

Personal data of US citizen and lawful foreign residents
Social security number usage

Key provisions

No disclosure without Consent rule
Right to receive a notice for voluntary or mandatory collection of personal information

Covered entities

US Federal government agencies
Government contractors

Penalties

Civil
up to 5K USD for willful disclosures
Criminal
for the agency officer

Worldwide privacy laws



Australian Privacy Act

2012



Personal information

Information or opinion about an individual whose identity is apparent or can be reasonably ascertained
Health, employment and credit data

Key provisions

Choice to opt-out of any direct marketing
Allows the use of pseudonyms
Limit international data exports

Covered entities

Most government sectors
Some private organizations

Penalties

Civil
up to 140K EUR for individuals
up to .7M EUR for companies

Worldwide privacy laws



BDSG Federal Data Protection Act

1995



Personal information

Personal relationships: name, address, e-mail, IP address
Factual circumstances: income, taxes, ownership
Sensitive personal data: health, racial, political, lifestyle

Key provisions

Extended the EU directive
Explicit consent in advance
Notify data breaches
Provisions for email marketing as well as online privacy, covering cookies, traffic and location data

Covered entities

Both government and private sectors

Penalties

Civil
up to 300K EUR per violation
Criminal
Imprisonment up to 2 years

Worldwide privacy laws



IT Amendment Act

2008



Personal information

related to a natural person which either directly or indirectly or in combination with other information can lead to identification of an individual

Key provisions

Implemented reasonable security practices and procedures (ie. ISO 27001)

Covered entities

Public and private companies, NGOs, national and foreign

Penalties

Civil
up to 622k EUR

Worldwide privacy laws



PIPEDA Personal Info Protection and Electronic Doc Act

2012



Personal information

Any factual or subjective information, recorded or not, about an identifiable individual

Key provisions

10 fair information principles
Document all personal information handling practices
Appoint a privacy officer
Limit international data exports to countries w/same protection

Covered entities

Private organizations, covers personal information in the course of a commercial activity

Penalties

Civil
up to 163K EUR per violation

Payment Card Industry Data Security Standard



Definition

Information security standard covering payment card and cardholder data
Cardholder data is scoped by GDPR

How it helps GDPR?



Methodology for securing cardholder data
Encryption of critical data
Identify and remediate vulnerabilities (i.e. penetration tests)
Implement strong access control measures
Daily review of security events and logs
Guidance on conducting data protection impact assessments

NIST Guidance



Definition

Frameworks and methods to help organizations to deal with cyber risks
I.e. NIST 800-53 on privacy policy

How it helps GDPR?



How to identify different types of information that are processed, stored, or transmitted
How to assess risks
How to maintain a record of security controls
Develop security architectures to allocate security controls including monitoring communications

California Consumer Privacy Act of 2018



Who Is Protected by the CCPA?

- Protects “consumers,” and natural persons; are California residents
- The rights do not extend to legal persons e.g. corporations (4(1).[1])

Who or What Is Regulated by the CCPA?

- A business that collects “personal information” from consumers
- Does business in California for profit/shareholders financial benefit
- Must meet or surpass one of the following thresholds:
 - \$25 million in annual gross revenue
 - Receive for commercial purposes, sell, or share for commercial purposes, the personal information of 50,000 or more consumers
 - Derive +50% of annual revenue from selling consumers’ personal information
- *Personal information is information that identifies, relates, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.*

California Consumer Privacy Act of 2018 compared to GDPR

- **CCPA** excludes “publicly available information,” (i.e. lawfully available via government records).
 - **The GDPR** identifies “special categories of personal data” that are entitled to extra protection
- CCPA recognizes personal information as a single category that may be composed of different kinds of data. Art. 9.
- **The CCPA** regulates businesses (statutorily defined) under the law.
 - **The GDPR** regulates the “controllers” who determine what personal data is collected and the “processors” who process personal data on behalf of controllers. Art. 4(7)-(8).
- **The CCPA** is limited to the location/residency (California) of the consumer. Focused on protecting the rights of California resident

California Consumer Privacy Act of 2018 compared to GDPR



- **The GDPR** regulates businesses in the EU, regardless of the personal data collected concerns EU citizens or not.
- **The GDPR** also regulates businesses located outside the EU that offer goods or services in the EU and process the data of EU citizens
- **Like the CCPA, the GDPR** allows data subjects to request information about the personal data that the controller has collected about them, though it distinguishes personal data obtained from the data subject and personal data obtained from outside parties.

California Consumer Privacy Act of 2018 compared to GDPR



- CCPA grants consumers the right to request that businesses delete any personal information that the business has collected from the them.
- The CCPA does not grant consumers the right to request that a business delete personal information obtained from someone other than the consumer
- The CCPA indicates circumstances where a business need not comply with a consumer request to delete personal information.
 - The GDPR contains a provision, the “right to be forgotten allowing data subjects the right to have personal data concerning them deleted by the data. Data subjects enjoy this right regardless of the source from which the data was obtained. Art. 17.
 - The GDPR’s right to be forgotten is also qualified by exceptions

California Consumer Privacy Act of 2018 compared to GDPR



CCPA requires that businesses that sell consumer personal data, or disclose personal information for a business purpose, provide data regarding these practices to the consumer upon request.

The consumer may seek the following information:

- The categories of personal information collected
- The categories of personal information that were sold, and the category/categories of 3rd parties to whom the information was sold
- The categories of personal information that the business disclosed

The CCPA allows consumers to demand that businesses cease and desist from selling their personal information, referring to this as “the right to opt out.” The CCPA adopts an “opt in” when selling a child’s personal information: here affirmative parental consent is required

California Consumer Privacy Act of 2018 compared to GDPR - Summary



Both GDPR and CCPA seek to protect personal privacy, however:

1. The CCPA is a statute about disclosure and transparency applicable to Californian residents only.
2. It requires businesses to proactively disclose to consumers the kinds of personal information that they collect and to tell consumers if they plan to sell consumers' personal data.
3. It gives consumers the right to request the specific personal data that businesses have collected about them, to request that the information be deleted, and to opt out of the sale of their personal information to third parties.
4. The liability portion of the statute subjects covered businesses to lawsuits when their failure to "implement and maintain reasonable security procedures and practices" results in the unauthorized disclosure of personal information

California Consumer Privacy Act of 2018 compared to GDPR - Summary



Both GDPR and CCPA seek to protect personal privacy, however:

1. The CCPA has relatively little to say about what security procedures and practices are “reasonable.”
2. The GDPR is a more comprehensive, “General” regulation. It has wider outreach and goes into greater detail as to how personal data should be protected, particularly:
 1. Data controllers & processors generally must maintain specific records regarding their processing of personal data, use encryption, undertake data protection impact assessments prior to using personal data and must designate a data protection officer where the controller or processor processes personal data on a large scale.
 2. GDPR grants rights to consumers that the CCPA does not. The GDPR gives data subjects the right to request that those who control their personal information rectify any mistakes contained therein, the right to request that restrictions be placed on the use of their data

Worldwide privacy laws



U.S. State and Federal

GDPR

PIPEDA

Definition of personal data and regulated forms

Under U.S. law, personal information is generally defined as an individual's name in combination with a set of specified data elements such as a Social Security number. All U.S. breach notification laws regulate electronic personal information. A handful of state laws, insurance regulations, and federal laws such as HIPAA also regulate non-electronic personal information.

Personal data under the GDPR has a broad definition, meaning information in any form relating to an identified or identifiable individual, with particular sensitivity to information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, and sex life or sexual orientation.

Similar to the GDPR, PIPEDA has defined personal information very broadly, meaning information in any form about an identifiable individual. Also similar to the GDPR, personal information can mean information about an individual's race, national or ethnic origin, religion, age, marital status, medical, education or employment history, financial information, or views or opinions about the individual as an employee.

Who must be notified

Entities that may require notification include affected individuals, state attorneys general, various state agencies, law enforcement, consumer reporting agencies, and media. Notice to industry-specific regulators may also be required.

Entities that may require notification include data subjects, competent state data protection authority (national breaches), lead supervisory authority (cross-border breaches), or multiple supervisory authorities.

Entities that may require notification are the Privacy Commissioner of Canada and affected individuals. The notifying organization is also required to notify any other entity that may be able to reduce the risk of harm to individuals. This could, depending on the circumstances of the breach, include entities such as law enforcement authorities or credit reporting agencies.

Worldwide privacy laws



US State and Federal

GDPR

PIPEDA

U.S. law, the GDPR, and PIPEDA each require a multi-factor risk assessment to determine whether notification is required to affected individuals and others, taking into consideration the nuances in each law's standard of harm.

Risk of harm standard

When specified in U.S. law, risk of harm is typically defined as risk of financial harm or identity theft.

Unlike the focus on financial harm under U.S. law, the GDPR standard for notification to supervisory authorities is a breach that is likely to result in a risk to the rights and freedoms of affected individuals. The standard for notification to affected individuals is a breach that is likely to result in a high risk to the individuals' rights and freedoms.

PIPEDA harmonizes with the GDPR in that the consideration of harm goes beyond financial harm. Under PIPEDA, notification to the Privacy Commissioner and affected individuals is required when a breach creates a real risk of significant harm to an individual, including considerations for bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, and identity theft.

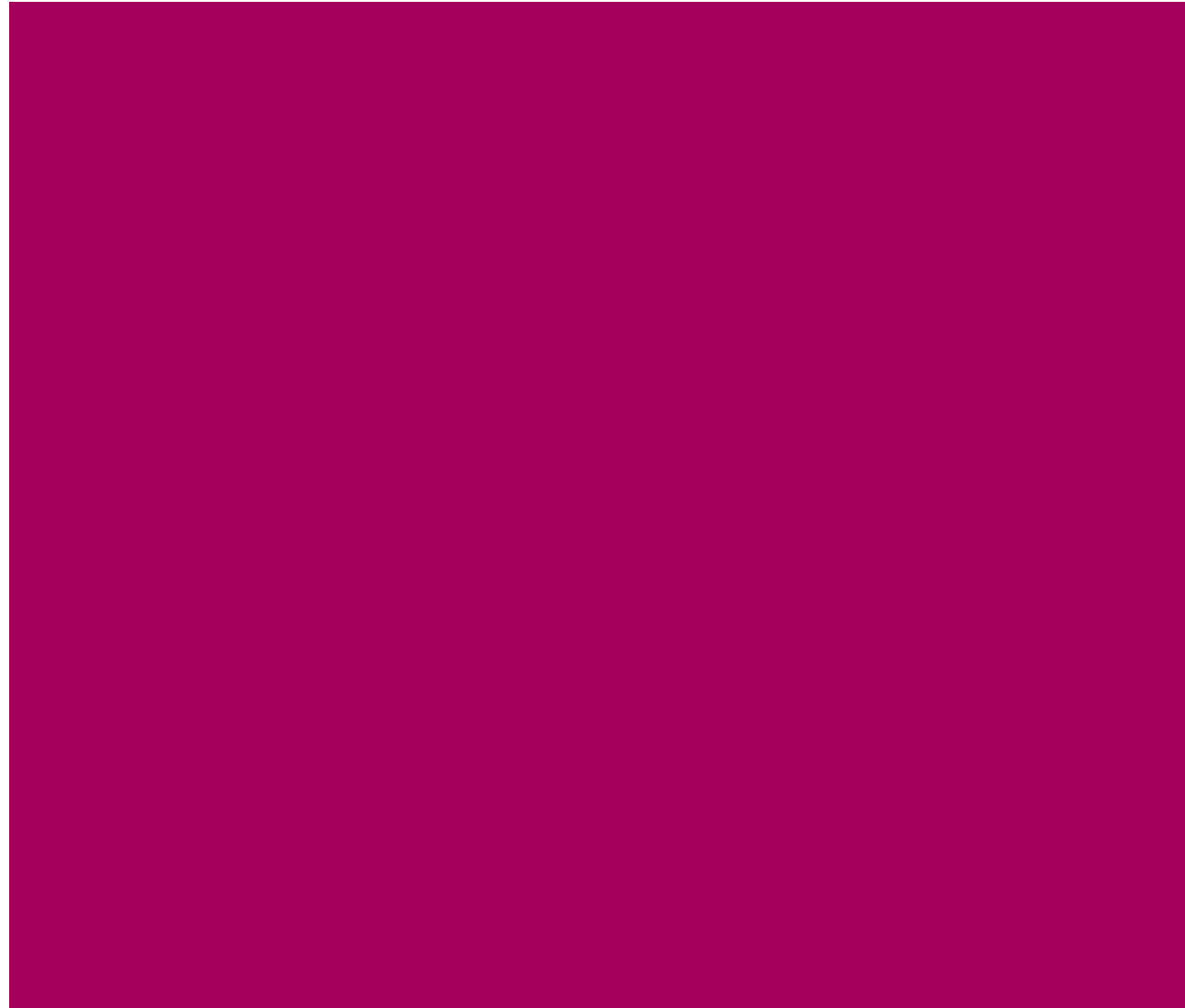
Notification timeframes

Generally, notification is required in the most expeditious manner possible, without unreasonable delay. In recent years, the trend is toward a more specific timeline, typically 30–45 days from breach discovery.

For supervisory authorities, notice is required "without undue delay and, where feasible, not later than 72 hours." For data subjects, notice is required "without undue delay."

Notification of individuals affected by the breach should occur as soon as feasible after determining that a breach has occurred.

GDPR Glossary



Binding Corporate Rules (BCR)



- Personal data protection policies which are adhered to by a controller or processor.
 - The policies are related and established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor.
- The data transfers are to one or more third countries within a group of undertakings or group of enterprises engaged in a joint economic activity

Chapter 5, Article 4, Article 45, Article 46, Article 49, Article 57, Article 58, Article 64, Article 70, Recital 107, Recital 108, Recital 110, Recital 168

Biometric Data



- Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person.
- The data allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data (identification by comparison of fingerprints)

Consent



- A *yes* given as clear affirmative action.
- Any freely given, specific, informed and unambiguous indication of the data subject's wishes
- The data subject provides a statement or
 - an agreement, to signify agreement to the processing of personal data relating to him or her

Chapter 2, Article 4, Article 6, Article 7, Article 8, Article 9, Article 13, Article 14, Article 15, Article 17, Article 22, Article 24, Article 32, Article 33, Article 34, Article 40, Article 41, Article 49, Article 70, Article 79, Article 83, Recital 29, Recital 32, Recital 33, Recital 38, Recital 40, Recital 42, Recital 43, Recital 45, Recital 50, Recital 51, Recital 54, Recital 65, Recital 68, Recital 71, Recital 74, Recital 79, Recital 111, Recital 112, Recital 113, Recital 126, Recital 155, Recital 161, Recital 171

Legal Basis for Processing



- which items of personal data to collect, ie the content of the data;
- the purposes the data are to be used for;
- which individuals to collect data about;
- whether to disclose the data, and if so, who to;
- whether subject access and other individuals' rights apply ie the application of exemptions; and
- how long to retain the data or whether to make non-routine amendments to the data.

Data Protection by Design- Default



- PIA / Privacy by Design Tool – a more granular questionnaire and checklist based tool powered by configurable templates and rules engines to meet your PIA, DPIA, and PbD obligations
- The controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default
- DPIAs are an important part of privacy by design and by default, which is a process of ensuring that all personal data collection, processing, storage and destruction measures are designed to secure privacy.
- privacy by design as "an approach to projects that promotes privacy and data protection compliance from the start
- This is expanded in the GDPR to include "by default", which essentially insists that the organisation ensures that *all* such projects take privacy into account.

Data Protection Impact Assessments



Use a set of questions to determine whether a DPIA may be necessary:

- Will the project involve the collection of new information on individuals?
- Compel individuals to provide information about themselves?
- Will information about individuals be disclosed to organisations or people who have not previously had routing access to the information?
- Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
- Using new technology that might be perceived as privacy-intrusive?
- Will the project result in decisions being made or taking action against individuals in ways that could have a significant impact on them?
- Is the information about individuals likely to raise privacy concerns or expectations?
- Will the project require you to contact individuals in ways they may find intrusive?

Consent Obligations



- data subjects can request that information be erased if they withdraw consent or there is an issue with the underlying legality of the processing
- data subject withdraws consent to processing, as there is no other legal justification for processing
- data subject's consent for fulfilment of a contract, and if the processing is automated
- To gain explicit consent, ensure that it is very clear to the data subject what they are agreeing to: simply adding a reference to profiling into a consent form, for instance, isn't likely to pass any sort of legal test.

Cookie, Online Tracking, and Marketing Reform



- includes biometric, genetic , health information, as well as online identifiers used to identify a person
- if customers view their personal data online, allow your customers to edit their personal data.
- For online services, there must be an automated way for individuals to raise their right to object.
- a "dashboard" that allows the data subjects to see an overview of all relevant processing, change their consent and update or correct their personal data

72 Hour Data Breach Reporting



- The capability of reporting data breaches to supervisory authorities within 72 hours;
- Pre-determined security levels, combined with clarity on roles and responsibilities and tested reporting procedure to ensure that the right decisions about breach reporting are made
- Data breach reporting requirements are consistent across EU, who must be told what and by when

Records of Processing Activities



- records of processing activities is carried out on the individual's personal information
- An examination could identify improvements or alternative activities that eliminate the risk of breaching the storage limitation principle
- DPIAs are used to identify specific risks to personal data as a result of processing activities
- Significance of their role in a PIMS could be compared to security risk assessments

Data Portability and Erasure



- Data subject access requests introduces new rights, on data portability, and erasure
- data subjects can request copies of their personal data in a useful electronic format.
- The right aims to improve the accessibility of information
- The right to receive the personal data which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided
- Being able to transfer that data to another controller.

Subject Access Rights



- an individual has the right to obtain confirmation that their data is being processed by the data controller, access to that personal data and any other supplementary information to help explain the data revealed to that individual
- Additional administrative burden on organisations to identify, respond and have suitable systems in place to answer all requests within just one month
- If a request is made in electronic form, then the information should also be provided in a commonly used electronic form, or an alternative format

International Data Transfers



- Cloud services may transmit data to a third country#
- Controllers will have to meet the usual requirements of the Regulation with regard to international data transfer.
- This includes having a legitimate reason for the transfer, asserting the data protection principles, applying appropriate controls or measures to protect the personal data (such as model contract clauses), and informing the data subject of the transfer of their personal data.

Codes of Conduct and Certifications



- A code of conduct is a starting point to instruct a culture of accountability. It depends on the exact nature of your business, its third-party suppliers and the industry
- A holistic approach is necessary to ensure the six privacy principles of the GDPR are understood and implemented across the organisation
- Consider a safe bet for assurance of information security if no approved code of conduct has been established, and there is no formally recognised certification mechanism to prove compliance with the GDPR

Controller



- The natural or legal person, public authority, agency or other body which,
 - alone or jointly with others,
- determines the purposes and means of the processing of personal data;
 - where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law

All about The Controller is mentioned in the following:



- Chapter 4, Chapter 8, Article 3, Article 4, Article 5, Article 6, Article 7, Article 8, Article 9, Article 11, Article 12, Article 13, Article 14, Article 15, Article 16, Article 17, Article 18, Article 19, Article 20, Article 21, Article 22, Article 23, Article 24, Article 25, Article 26, Article 27, Article 28, Article 29, Article 30, Article 31, Article 32, Article 33, Article 34, Article 35, Article 36, Article 37, Article 38, Article 39, Article 40, Article 41, Article 42, Article 43, Article 44, Article 46, Article 47, Article 48, Article 49, Article 56, Article 57, Article 58, Article 60, Article 62, Article 65, Article 70, Article 79, Article 81, Article 82, Article 83, Article 85, Article 90, Recital 10, Recital 13, Recital 18, Recital 22, Recital 23, Recital 24, Recital 25, Recital 26, Recital 28, Recital 29, Recital 36, Recital 39, Recital 40, Recital 42, Recital 43, Recital 45, Recital 47, Recital 48, Recital 49, Recital 50, Recital 51, Recital 57, Recital 59, Recital 60, Recital 63, Recital 64, Recital 65, Recital 66, Recital 68, Recital 69, Recital 71, Recital 73, Recital 74, Recital 77, Recital 78, Recital 79, Recital 80, Recital 81, Recital 82, Recital 83, Recital 84, Recital 86, Recital 85, Recital 89, Recital 90, Recital 92, Recital 94, Recital 95, Recital 97, Recital 98, Recital 99, Recital 101, Recital 108, Recital 109, Recital 113, Recital 114, Recital 115, Recital 122, Recital 124, Recital 127, Recital 131, Recital 126, Recital 145, Recital 146, Recital 148, Recital 153, Recital 61, Recital 132, Recital 143, Recital 144, Recital 147, Recital 156, Recital 164, Recital 168, Recital 171, Recital 173

Cross-Border Processing



When the controller or processor is established in more than one Member State;

- Processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union or
- Processing of personal data takes place in the context of the activities of a single establishment of a controller or processor in the Union
 - but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

All about "cross-border" in Article 4, Article 56, Recital 5, Recital 53, Recital 138

Data Erasure



Also known as the Right to be Forgotten,

- Data erasure entitles the data subject to have the data controller erase his/her personal data,
- Cease further dissemination of the data, and
- *Potentially* have third parties cease processing of the data

Data erasure is mentioned in: Article 17, Recital 65, Recital 66

Data Protection Officer



An expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures outlined in the GDPR

Article 13, Article 14, Article 30, Article 33, Article 35, Article 36, Article 37, Article 38, Article 39, Article 47, Article 57, Recital 77, Recital 97

Pseudonymisation



The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person

Article 4, Article 6, Article 25, Article 32, Article 40, Article 89, Recital 26, Recital 28, Recital 29, Recital 75, Recital 85, Recital 156

Encryption

- Personal data that is protected with a unique key, ensuring that data is only accessible/readable to authorised people

Article 6, Article 32, Article 34, Recital 83

Data Portability



The requirement for controllers to provide the data subject with a copy of his or her data in a format that allows for easy use with another controller

Article 13, Article 14, Article 20, Recital 68, Recital 73, Recital 156

International Organisation



An International organisation and its subordinate bodies governed by public international law,
– any other body, set up by, or based on an agreement between two or more countries

International Organisation: Chapter 5, Article 4, Article 13, Article 14, Article 15, Article 28, Article 30, Article 40, Article 42, Article 44, Article 45, Article 46, Article 49, Article 50, Article 58, Article 70, Article 71, Article 83, Article 85, Article 96, Article 97, Recital 6, Recital 101, Recital 102, Recital 103, Recital 105, Recital 106, Recital 107, Recital 108, Recital 112, Recital 139, Recital 153, Recital 168, Recital 169

Enterprise



A natural or legal person engaged in economic activity, irrespective of its legal form

- including partnerships or associations regularly engaged in an economic activity

Enterprise: Article 4, Article 30, Article 40, Article 42, Article 47, Article 88, Recital 13, Recital 37, Recital 98, Recital 110, Recital 132, Recital 167

- Any structured set of personal data
 - which is accessible according to specific criteria:
 - whether centralised or decentralised
 - dispersed on a functional or geographical basis

Article 2, Article 4, Recital 15, Recital 31, Recital 67

Genetic Data



- Personal data relating to the inherited or acquired genetic characteristics of a natural person
- gives unique information about the physiology or the health of that natural person
- Results, in particular, from an analysis of a biological sample from the natural person in question

Group of Undertakings



- Controlling undertaking and its controlled undertakings
- The controlling undertaking can exert a dominant influence over the other undertakings by virtue, of ownership and financial participation
- The rules which govern it or the power to have personal data protection rules implemented.
- An undertaking which controls the processing of personal data in affiliations is regarded, as a group of undertakings.

Article 4, Article 36, Article 37, Article 47, Article 88, Recital 36, Recital 37,
Recital 48, Recital 110

Main Establishment



- a controller with establishments and central administration in more than one Member State
- unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union
- the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;
- a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union
- the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation

Article 4, Article 56, Article 60, Article 65, Recital 36, Recital 124, Recital 126

Personal Data



- Any information relating to an identified or identifiable natural person ('data subject');
- an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier
- to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

Personal Data



Chapter 5, Article 1, Article 2, Article 3, Article 4, Article 5, Article 6, Article 7, Article 9, Article 10, Article 11, Article 13, Article 14, Article 15, Article 16, Article 17, Article 18, Article 20, Article 19, Article 21, Article 22, Article 23, Article 25, Article 27, Article 28, Article 29, Article 30, Article 32, Article 33, Article 34, Article 35, Article 37, Article 38, Article 39, Article 40, Article 42, Article 44, Article 45, Article 46, Article 47, Article 49, Article 50, Article 53, Article 57, Article 58, Article 70, Article 77, Article 79, Article 80, Article 83, Article 85, Article 86, Article 88, Article 89, Article 90, Article 98, Recital 1, Recital 2, Recital 3, Recital 4, Recital 5, Recital 6, Recital 7, Recital 9, Recital 10, Recital 11, Recital 12, Recital 13, Recital 14, Recital 15, Recital 16, Recital 17, Recital 18, Recital 19, Recital 20, Recital 22, Recital 23, Recital 24, Recital 26, Recital 27, Recital 28, Recital 29, Recital 31, Recital 32, Recital 33, Recital 34, Recital 35, Recital 36, Recital 37, Recital 38, Recital 39, Recital 40, Recital 42, Recital 43, Recital 45, Recital 46, Recital 47, Recital 48, Recital 49, Recital 50, Recital 51, Recital 52, Recital 53, Recital 54, Recital 55, Recital 56, Recital 57, Recital 58, Recital 59, Recital 60, Recital 61, Recital 62, Recital 63, Recital 64, Recital 65, Recital 66, Recital 67, Recital 68, Recital 69, Recital 70, Recital 71, Recital 72, Recital 73, Recital 75, Recital 78, Recital 80, Recital 81, Recital 83, Recital 84, Recital 85, Recital 86, Recital 87, Recital 88, Recital 89, Recital 90, Recital 91, Recital 96, Recital 97, Recital 101, Recital 102, Recital 103, Recital 104, Recital 105, Recital 108, Recital 110, Recital 111, Recital 112, Recital 113, Recital 115, Recital 116, Recital 122, Recital 123, Recital 124, Recital 127, Recital 129, Recital 139, Recital 142, Recital 153, Recital 154, Recital 155, Recital 156, Recital 157, Recital 158, Recital 159, Recital 160, Recital 162, Recital 164, Recital 166, Recital 170

What did May 25th 2018 mean?



Start demonstrating the compliance efforts

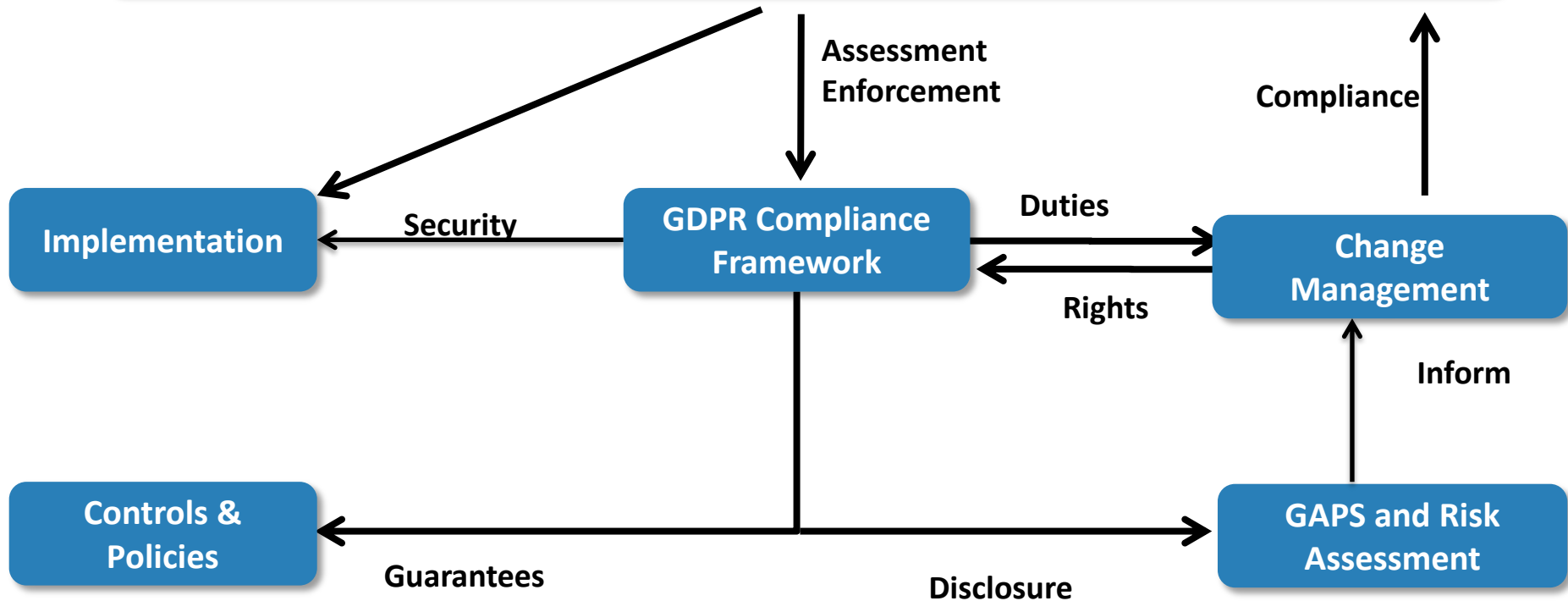
- ✎ Documented privacy program and legal basis for processing activities
- ✎ Ongoing data lifecycle management according to the privacy policy, including data consents
- ✎ Monitoring data flows and audit trails
- ✎ Data privacy impact assessment procedure
- ✎ Incident response and breach notification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

Summary



Project Scope
Territorial and Material

Objectives
bit extra on the top or overhaul of IT platforms, processes & data protection



The Info Sec 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
- **[EU Data Protection Board](https://edpb.europa.eu/edpb_en)**
- **https://edpb.europa.eu/edpb_en**
- **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/>



All Links



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

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