GDPR: From Regulation to coding

Learning objectives (Session 1)

- Understanding the General Data Protection regulation and its impact on application and operations security
- Review major implementation methods and identify specific application security activities
- Explore risks sources and understand Application Security Controls (ASC)
- Understand data governance and develop Applications controls specifications

Learning objectives (Session 2)

- Use the Ashley Madison Data Leakage case
- Explore controls related to: Website & User Profile, Mobile applications, Localization / Tracking, Chat, Profiling, Sharing information with third parties
- Break-out group work
- Presentation of results to the class

GDPR: From Regulation to coding

Speaker

Georges ATAYA

Career Summary

- Professor and Academic Director (SBS-EM)
- Managing Director ICT Control advisory firm
- Past International Vice President at ISACA
- Past Partner Ernst & Young
- Deputy International CIO ITT World Directories
- Previously Project Manager and Senior IT Auditor

Expertise Summary

- IT Governance (development of Cobit 4 and COBIT 5)
- IT Governance and Value governance (co-author VALIT and supervision CGEIT BOK)
- Information Security Management (Co-author CISM Body of Knowledge)
- IT Audit and Governance
- Information security and risk
- Strategy and Enterprise Architecture and IT Sourcing

Education/ Certification

- Master in Computer Science (faculty of Sciences ULB)
- Postgraduate in Management (Solvay Brussels School ULB)
- CISA, CISM, CRISC, CISSP, CGEIT

Speaker

Alain CIESLIK

Career Summary

- Enterprise Security Architect (Stib)
- Security consultant
- ISO 27034 Lead Implementer & CISSP Trainer (Nitroxis)
- Java Development & Architecture

Expertise Summary

- Secure Development lifecycle
- Application security
- Security assessment
- Security Awareness
- Digital Forensics

Education / Certification

- Master in IT Management Solvay
- Master in computer Science
- Graduat en informatique de gestion
- ISO 27001 - 27034 Lead implementer
- CISSP, CSSLP , TOGAF
- SANS - GWAPT: Web Application Penetration tester

Executive Education in Information Security Management

Executive Education in IT Management

Executive Education in IT Management

Executive Master in IT Management

Executive Programme in

- CIO Practices
- CIO Leadership
- IT Business Agility
- Enterprise and IT Architecture
- IT Sourcing
- IT Management Consulting

Executive Education in Information Security Management

Executive Master in Information Risk and Cybersecurity

Executive Programme in

. Security Governance

. Information Security

. Cybersecurity

Lectured tracks and modules

S – track Info Security	G – track IT Governance	M – track IT Management	B – track Business Agility	A – track Activating skills
S1 – Information Security Management	**G1 – The CIO Foundation**	**M1 – Applications Build and Management**	**B1 – Enterprise Strategy and Architecture**	**A1 – IT Finance and Portfolio Management**
S2 – IT Security Practices	**G2 – IT Governance Workshop**	**M2 – IT Services and Run Management**	**B2 – Business Transformation**	**A2 – Soft Skills for IT professionals**
S3 – Cybersecurity Workshop	**G3 – IT Risk and Legal concerns**	**M3 – IT Sourcing Management**	**B3 – Digital Agility and Innovation**	**A3 – Building Expert Opinion**
Monday Track-S	Thursday Track-G	Wednesday Track-M	Tuesday Track-B	Monday Track-A

GDPR

GDPR: From Regulation to coding

Scope

- Regulates the processing of **personal data** (customers, employees, vendors, etc.)
- Replaces and harmonizes the European Directive 95/467EC
- Is **mandatory** and has serious **operational implications** for companies

GDPR: From Regulation to coding

Scope

Two main types of legislation

- Directives
  - Require individual implementation in each member state
  - Implemented by the creation of national laws approved by the parliaments of each member state
  - European Directive 95/46/EC is a directive
- Regulations
  - Immediately applicable in each member state
  - Require no local implementing legislation
  - The EU GDPR is a regulation

GDPR: From Regulation to coding

Timeline

- Adopted by the council of the European Union and the European Parliament in April 2016
- Provides for a two year implementation time period.
- The regulation is directly applicable in each member state, effective in May 2018
- Requires no local legislation implementation

GDPR: From Regulation to coding

Why bother ?

Financial Risk: Penalties up to 4% of annual revenues or 20 million

Reputational Risk: Fines and privacy violations can create negative press that erode customer confidence and brand equity

Operational Risk: Unless properly designed and implemented, patchwork efforts at GDPR create risks to the efficiency and reliability of operations

Opportunity to Improve Security: GDPR gives a positive Business case to improve security maturity within companies

GDPR: From Regulation to coding

Key concepts (Art. 4)

Regulated Object	**Personal Data** Any information relating to an identified or identifiable natural person; who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, location data, an online identifier, factors specific to the physical, physiological, genetic, economic, cultural or social identity of that person;
Regulated Activity	**Data Processing** Any operation or set of operations which is performed on personal data, whether or not by automated means, such as collection, recording, storage, use, disclosure by transmission, destruction, ...
Parties Involved	**Data Subject** One who can be identified directly or indirectly by reference to an identifier such a name, location data, identification number or other means **Controller** Natural or legal person which determines the purpose and means of the processing of personal data **Processor** Natural or legal person which processes personal data on behalf of the controller

Regulated Scope	• Controller or processor is establish in the EU (has real and sustainable economic activity in the EU)
	• Controller or processor is establish outside the EU but
	  • Offers goods or services to data subjects in the EU, or
	  • Monitoring the online behavior of data subjects in the EU

GDPR: From Regulation to coding

Principles relating to processing of personal Data

Principle	Description
Lawfulness	- Processing is lawful as set out in GDPR (consent, legal obligation, vital interest, etc.)
Fairness & transparency	- Data subject must be provided with sufficient information about the collection / processing of their data to understand possible risks
Purpose limitation	- Personal data must be collected for specified, explicit and legitimate purpose - Personal data obtained for one purpose must not be processed for unrelated purpose
Data minimizaton	Both in the collection and processing, personal data has to be minimized as much as possible
Accuracy	Personal data should be accurate, kept up-to-date and reasonable steps must be taken to ensure that inaccurate personal data are erased of rectified without delay
Storage limitation	Data must be erased or effectively anonymised as soon as it is no longer needed for its original purpose

GDPR: From Regulation to coding

Data Right Subjects

- Right of withdraw consent (Art. 7)
- Right to be informed (Art. 13 & 14)
- Right of access by the data subject (Art. 15)
- Right of erasure – Right to be forgotten (Art. 17)
- Rights in relation to automated processing (Art. 22)
- Right of rectification (Art. 16)
- Right to object to processing (Art. 21)
- Right to restrict processing (Art. 18)
- Right of portability (Art. 20)

Consent & Choice

GDPR: From Regulation to coding

Consent and choice

Consent: The data subject's indication of agreement to his/her personal data being processed

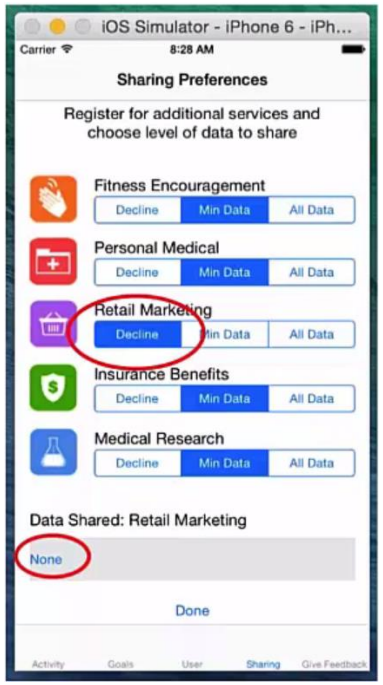
Choice: Data Subject as the option o opt-in or opt-out.

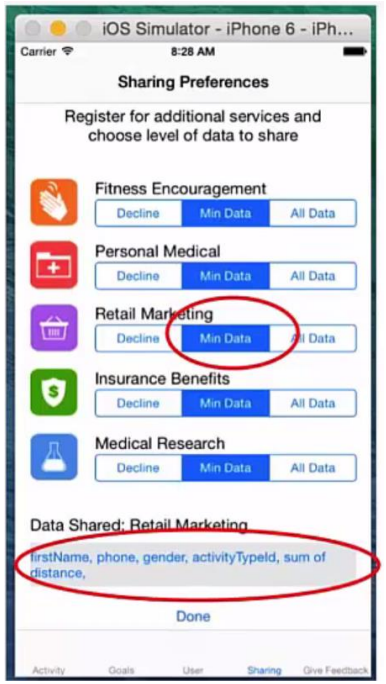
- Opt-out: Personal information will be process **unless** the data subject objects.
- Opt-in: Personal information will be processed **only if** the data subject agrees

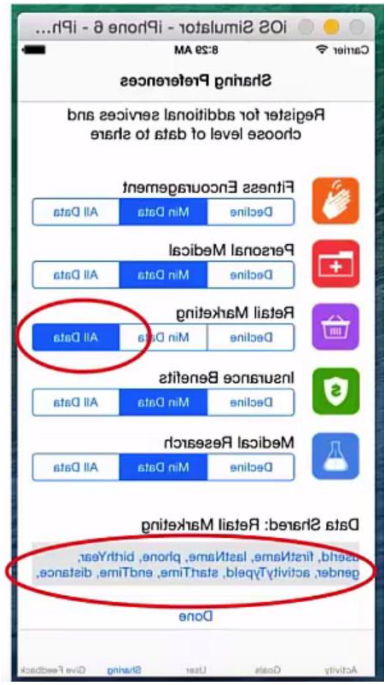
Source: http://www.dpoacademy.gr/webinars/ - https://youtu.be/GDzYry6GCFg?t=1857

GDPR: From Regulation to coding

Consent and choice



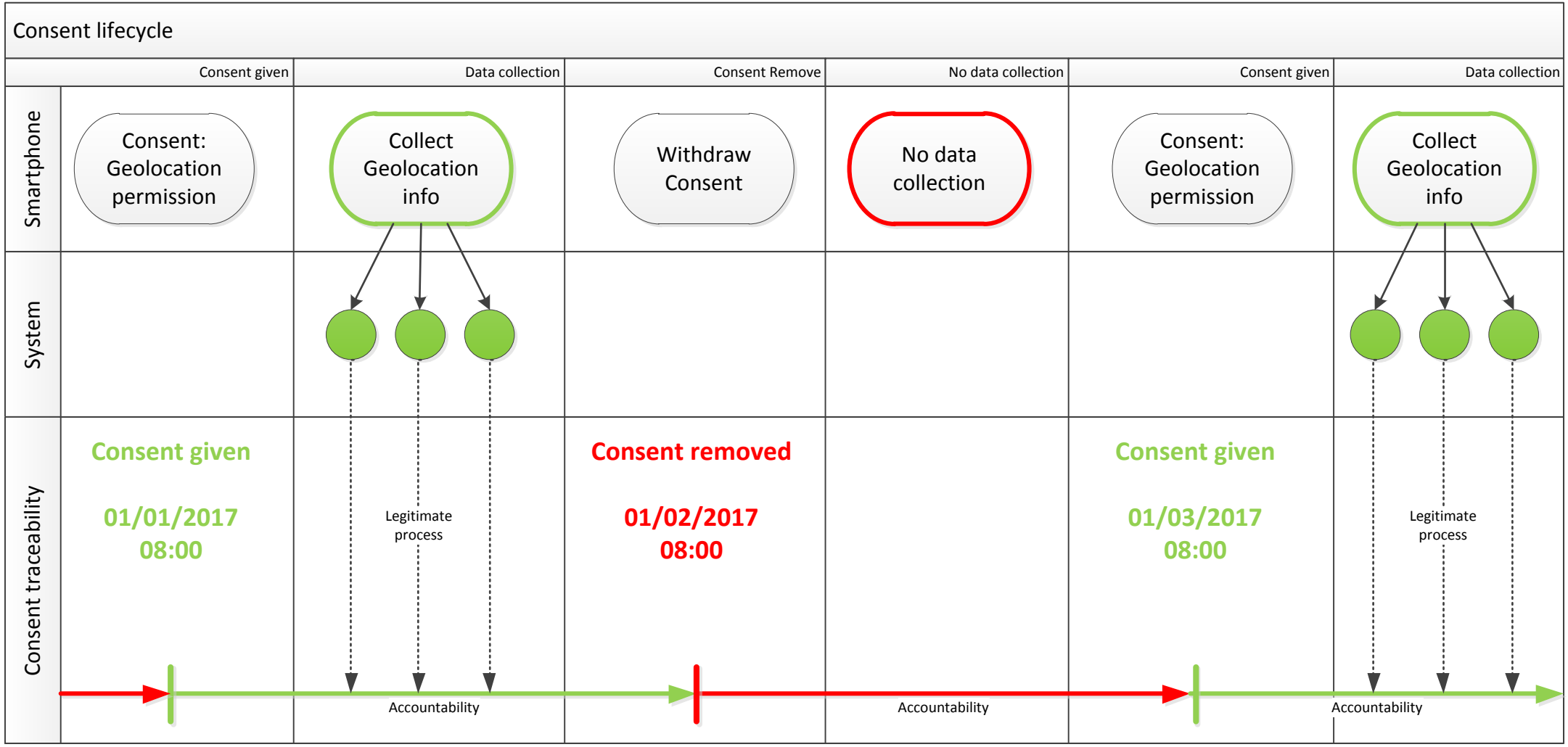




Source: http://www.dpoacademy.gr/webinars/ - https://youtu.be/GDzYry6GCFg?t=1857

GDPR: From Regulation to coding

Right of withdraw consent



GDPR: From Regulation to coding

Right to be informed

Microsoft Privacy Statement

Expand All

Print

History

Last Updated: **November 2016** What's new?

Privacy notice Summary

Your privacy is important to us. This privacy statement explains what personal data we collect from you and how we use it. We encourage you to read the summaries below and to click on "Learn More" if you'd like more information on a particular topic.

The product-specific details sections provide additional information relevant to particular Microsoft products. This statement applies to the Microsoft products listed below, as well as other Microsoft products that display this statement. References to Microsoft products in this statement include Microsoft services, websites, apps, software and devices.

Table of contents

Personal Data We Collect

How We Use Personal Data

Reasons We Share Personal Data

How to Access & Control Your Personal Data

Cookies & Similar Technologies

Microsoft account

Other Important Privacy Information

Product-specific details:

Bing

Cortana

Groove Music/Movies & TV

Microsoft Cognitive Services

Microsoft Health Services

Microsoft Translator

Topic summary

Personal Data We Collect

Microsoft collects data to operate effectively and provide you the best experiences with our products. You provide some of this data directly, such as when you create a Microsoft account, submit a search query to Bing, speak a voice command to Cortana, upload a document to OneDrive, purchase an MSDN subscription, sign up for Office 365, or contact us for support. We get some of it by recording how you interact with our products by, for example, using technologies like cookies, and receiving error reports or usage data from software running on your device. We also obtain data from third parties.

Learn More

Top of page

How We Use Personal Data

Microsoft uses the data we collect to provide you the products we offer, which

GDPR: From Regulation to coding

Right to be informed

Table of contents

Topic detail

Personal Data We Collect

Microsoft collects data to operate effectively and provide you the best experiences with our products. You provide some of this data directly, such as when you create a Microsoft account, submit a search query to Bing, speak a voice command to Cortana, upload a document to OneDrive, purchase an MSDN subscription, sign up for Office 365, or contact us for support. We get some of it by recording how you interact with our products by, for example, using technologies like cookies, and receiving error reports or usage data from software running on your device.

We also obtain data from third parties. For example, we supplement the data we collect by purchasing demographic data from other companies. We also use services from other companies to help us determine a location based on your IP address in order to customize certain products to your location.

You have choices about the data we collect. When you are asked to provide personal data, you may decline. But if you choose not to provide data that is necessary to provide a product or feature, you may not be able to use that product or feature.

The data we collect depends on the products and features you use, and can include the following:

Name and contact data. We collect your first and last name, email address, postal address, phone number, and other similar contact data.

Credentials. We collect passwords, password hints, and similar security information used for authentication and account access.

Demographic data. We collect data about you such as your age, gender, country, and preferred language.

Payment data. We collect data necessary to process your payment if you make purchases, such as your payment instrument number (such as a credit card number), and the security code associated with your payment instrument.

Usage data. We collect data about how you and your device interact with Microsoft and our products. For example, we collect:

GDPR: From Regulation to coding

Right to be informed

Change History for Microsoft Privacy Statement

Back to the privacy statement

November 2016

- In **How We Use Personal Data**, we updated **Advertising** to better clarify the use of your data by third parties to customize the ads you see.
- In **How to Access & Control Your Personal Data**, we updated **Your Communications Preferences**, clarifying how to modify your preferences.
- In **Other Important Information**, we updated the **Where We Store and Process Personal Data** section to reflect Microsoft's participation in the EU-U.S. Privacy Shield program.
- In **Bing**, we removed the Bing Rewards Program section, as Bing Rewards has been replaced by Microsoft Rewards.
- We added a new **Microsoft Cognitive Services** section to explain how we collect and use data when developers use the services. We also clarified that Microsoft Cognitive Services are not Enterprise Products under this privacy statement.
- We added a new **Microsoft Translator** section, to explain how Microsoft Translator, Collaborative Translations Framework, and Microsoft Translator Hub collect and use data.
- In **Windows**, we revised the **Telemetry & Error Reporting** section to reflect that wireless network identifiers are collected at the optional "Enhanced" level of telemetry rather than at the "Basic" level.
- We added a new **captioning** section in **Xbox** to explain how Microsoft incorporates a voice-to-text feature to provide captioning of in-game chat for users who need it.

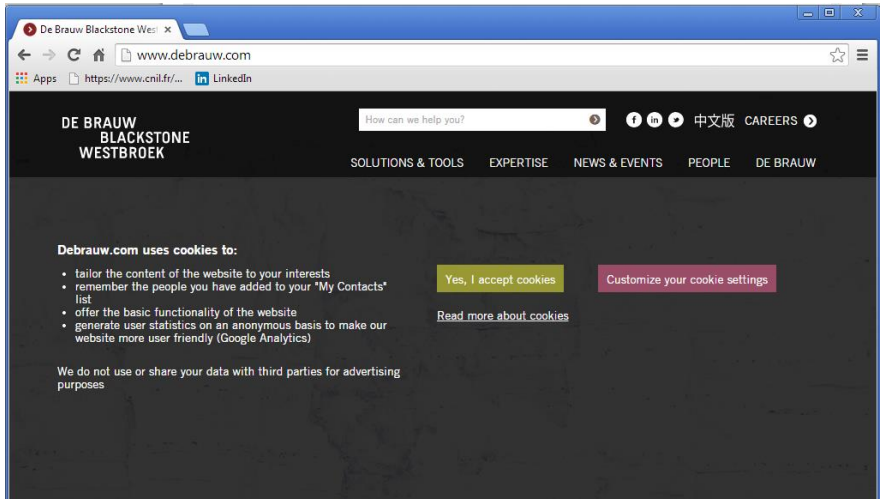
Changes introduced by a specific version of a privacy notice

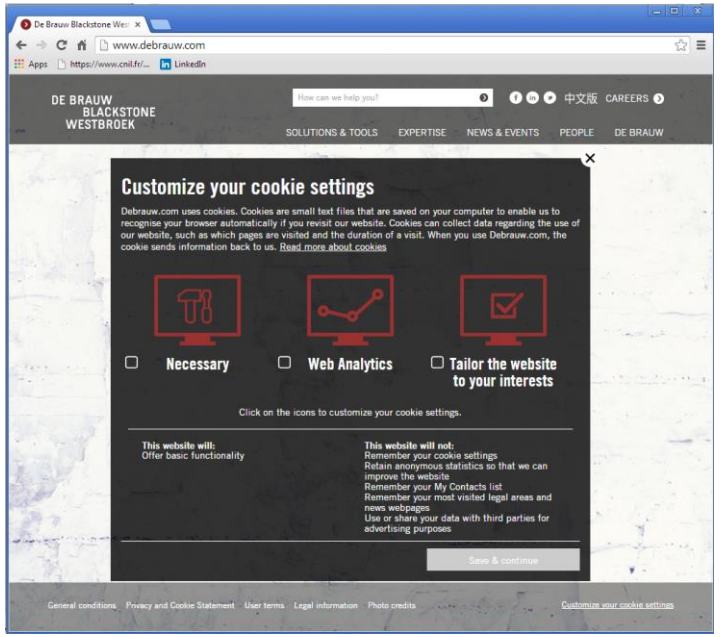
September 2016

In **Enterprise Products**, we added links to privacy notices that still apply to certain enterprise offerings.

GDPR: From Regulation to coding

Right to be informed



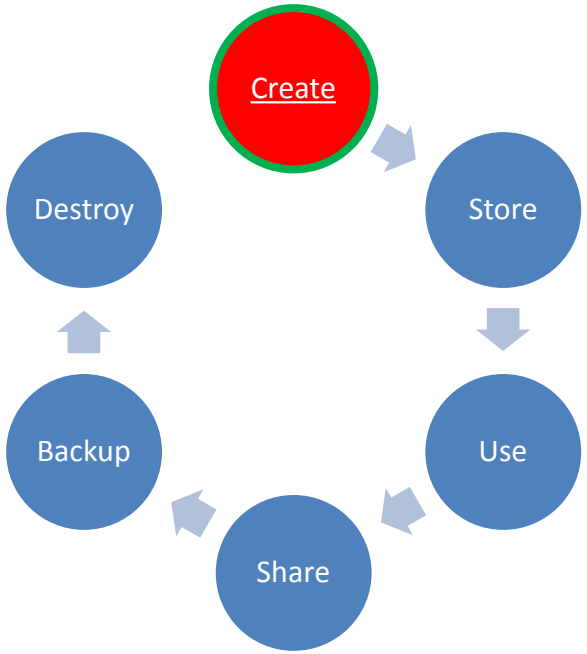


Data Management

GDPR: From Regulation to coding

Data Management

Data lifecyle Management



Phase: Create

Data

{ structured data , unstructured data}

Format

{Images, Text, Videos, Documents, Audio}

Data Origin

{Social Media, Web, Human input, Machine generated, …}

Data Consumers

{Human, Business Process, Internal Application, …}

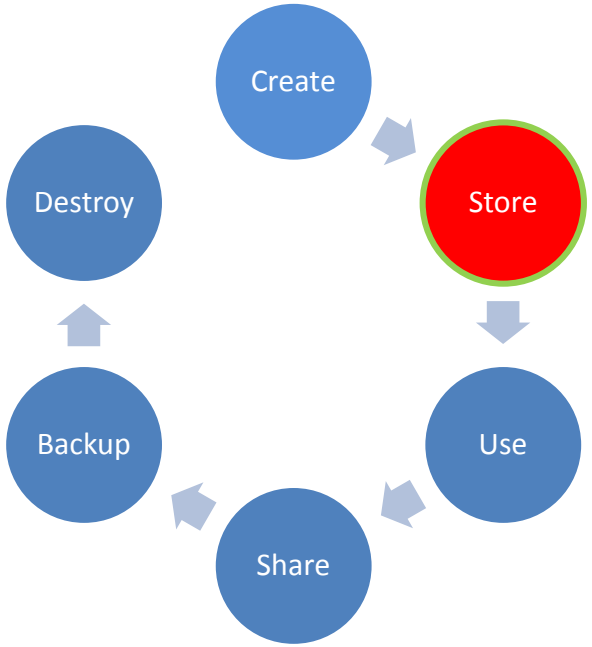
Quality

{Validation}

GDPR: From Regulation to coding

Data Management

Data lifecyle Management



Phase: Store

Different Storages => Different risks

- Disk
- Laptop
- USB
- Cloud
- Smartphone

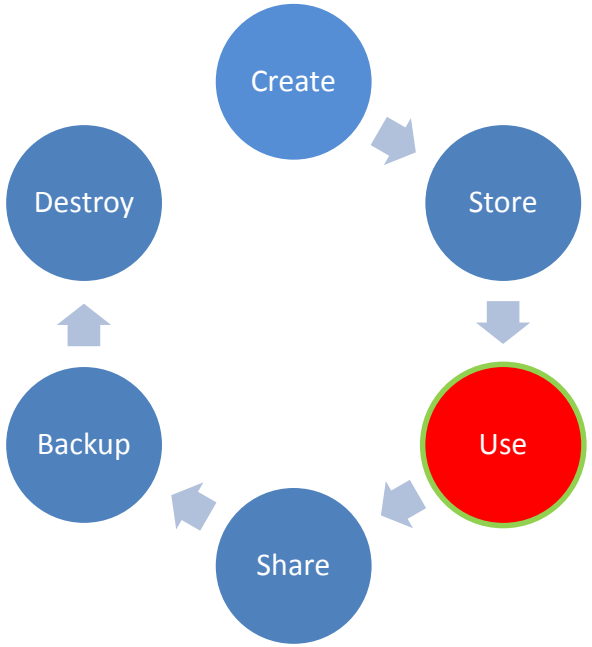
Security mechanism in place

- Access management
- Auditing
- Encryption
- Anonymization

GDPR: From Regulation to coding

Data Management

Data lifecyle Management



Phase: Use

Type of usage

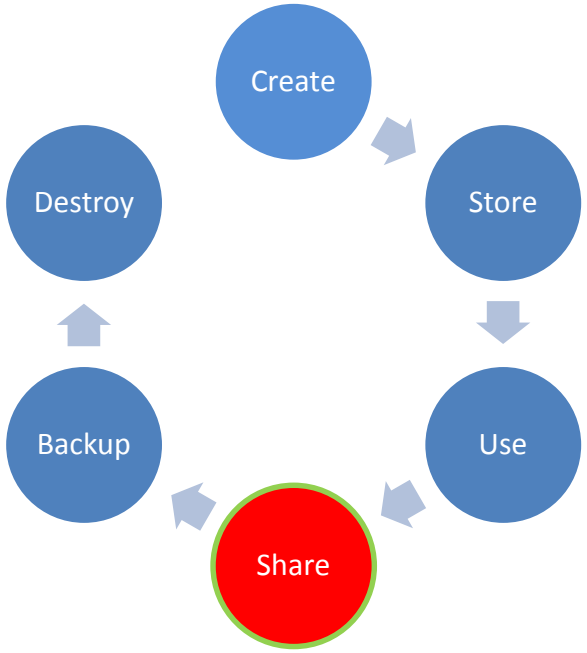
- Web application
- Mobile Application
- Business Intelligence
- Paper

Security mechanism in place

- Access management
- Auditing
- Encryption during transmission or processing

Data Management

Data lifecyle Management



Phase: Share

How it is shared ?

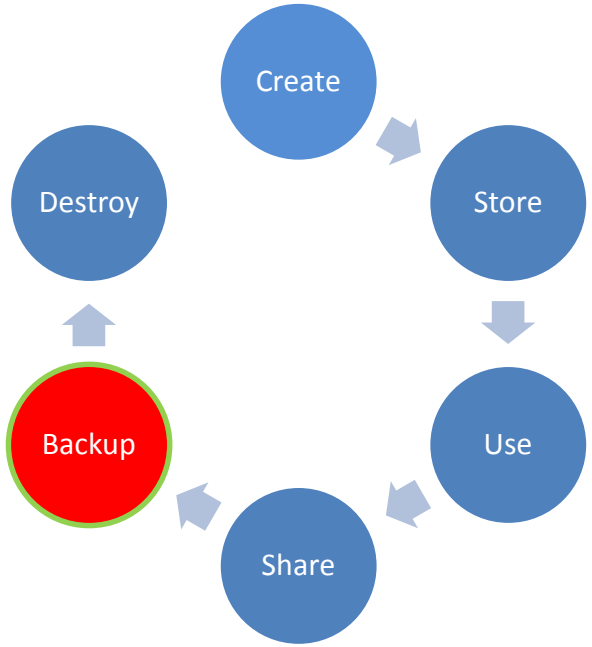
- Mail
- Access right delegation
- File on USB stick

Security mechanism in place

- Access management
- Auditing
- Encryption

Data Management

Data lifecyle Management



Phase: Archive

Types of backup

- DB,
- Email,
- Cloud

Timing

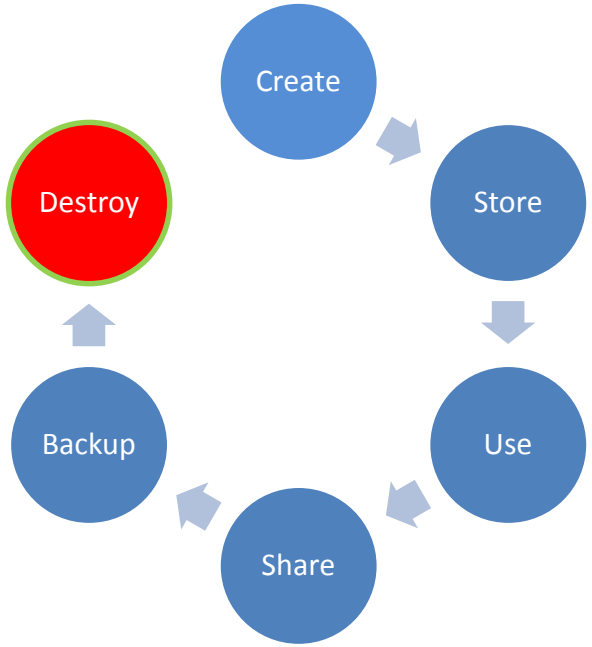
Security mechanism in place

- Access management
- Auditing
- Backup Encryption & Integrity

GDPR: From Regulation to coding

Data Management

Data lifecyle Management



Destruction

What is the destruction Trigger ?

- Human decision
- Automatic

What are the Retention periods ?

What is in scope ?

What are the guaranty ?

- Succeed or not
- What about the backup

Security & Privacy

GDPR: From Regulation to coding

Security of personal Data

Security of processing
(Art. 32)

Notification of a personal data breach to the supervisory authority
(Art. 33)

Communication of a personal data breach to the data subject
(Art. 34)

Security of personal Data

Article 32

Security of processing

1. Taking into account:

- The state of the art, the costs of implementation
- The nature, scope, context and purposes of processing
- The risk of varying likelihood and severity for the rights and freedoms of natural persons

=> Implement appropriate technical & administrative measures to ensure a level of security appropriate to the risk

Article 33

Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach:

- the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it
- notify the personal data breach to the supervisory authority competent
- unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons

Security of personal Data

Article 33

Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach:

- Likely to result in a high risk to the rights and freedoms of natural persons
- the controller shall communicate the personal data breach to the data subject without undue delay.

3 The communication to the data subject referred to in paragraph 1 shall not be required if

- the controller has implemented appropriate protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
- it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure

GDPR: From Regulation to coding

Privacy Risk

“Risk” is mentioned

75

times in the regulation

Privacy Risk

What is a privacy risk ?

A risk is a hypothetical scenario that describes:

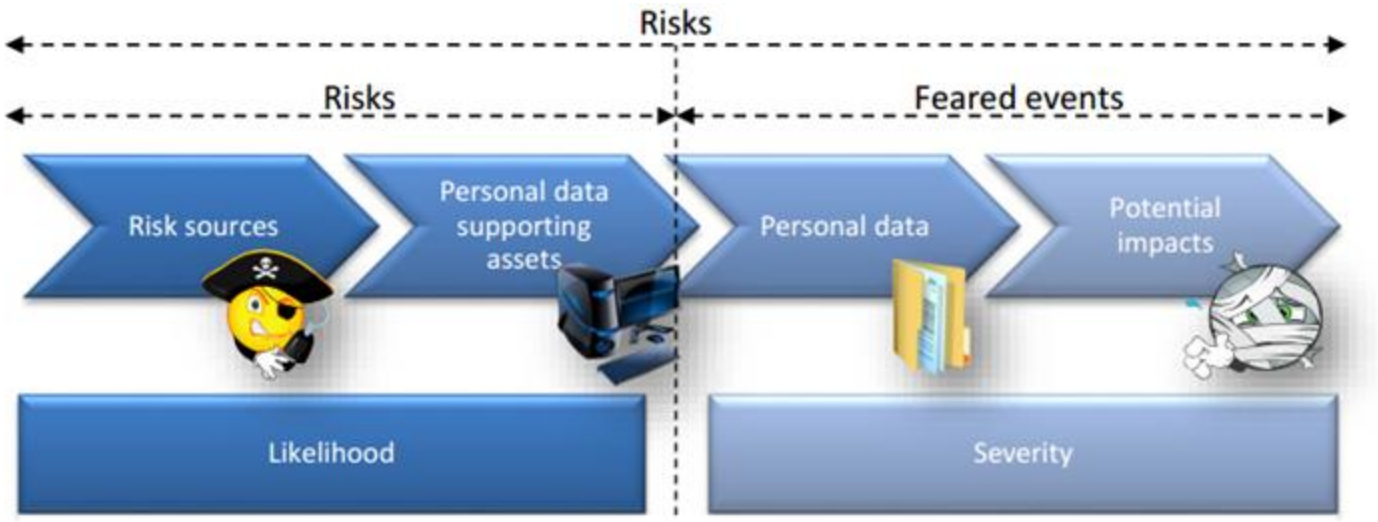
- how risk sources (e.g: an employee bribed by a competitor)
- could exploit the vulnerabilities in personal data supporting assets

  (e.g: the file management system that allow the manipulation of data)
- in a context of threats (e.g: misuse by sending mails)
- and allow feared events of occur (e.g: illegitimate access to personal data)
- on personal data (e.g: customer file)
- thus generating impacts on the privacy of data subjects (e.g: unwanted solicitations)

Source: https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf

Privacy Risk

What is a privacy risk ?



Likelihood: Represents the magnitude of a risk.

Severity: Represents the possibility for a risk to occur.

Source: https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf

Privacy Risk

How is a PIA conducted ?

The compliance approach implemented by carrying out a PIA is based on the respect for privacy principles:

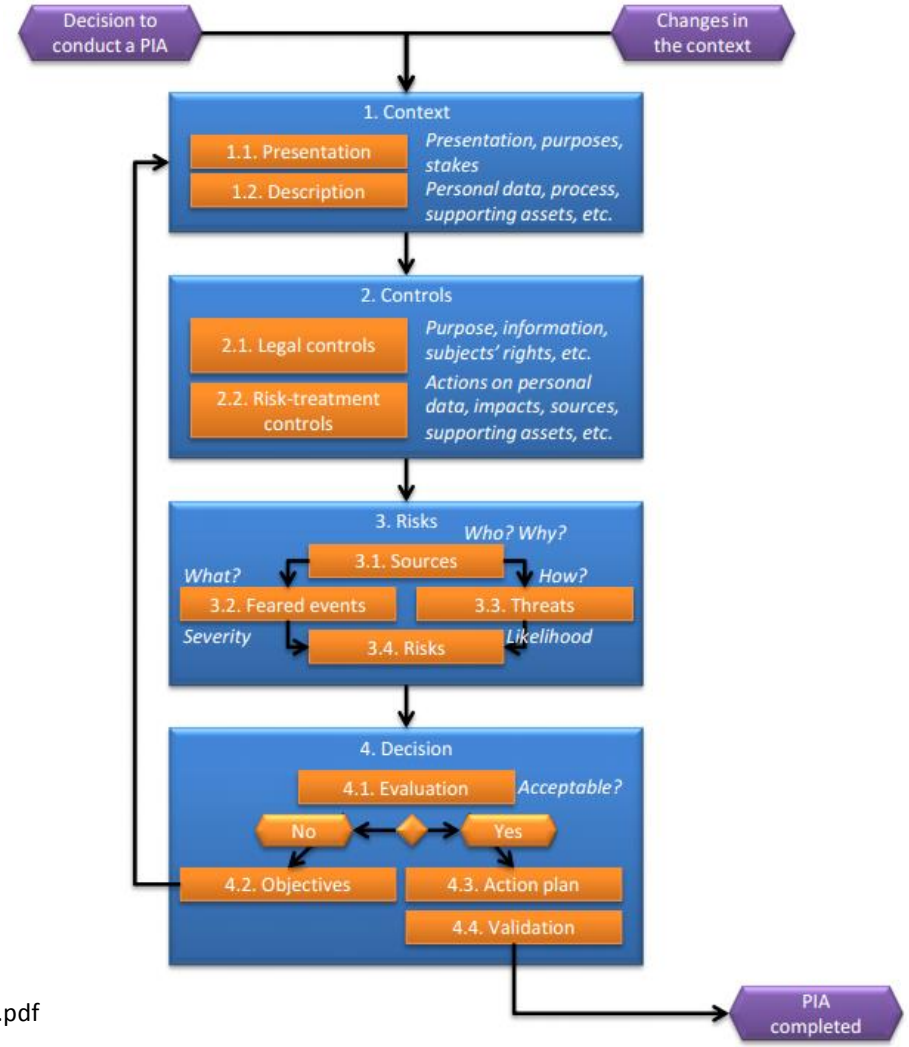
- respect for legal principles for privacy protection
- management of risks related to the security of personal data and having an impact on data subjects' privacy

Source: https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf

GDPR: From Regulation to coding

Privacy Impact Assessment

CNIL approach



In summary, to comply with GDPR, it is necessary to:

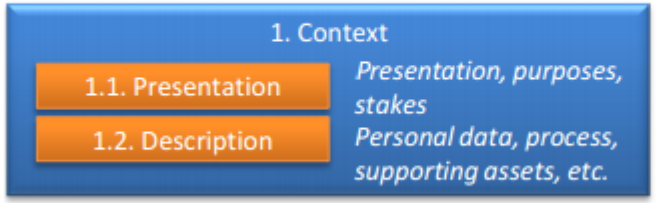
1. Define and describe the context of the processing of personal data under consideration and its stakes;
2. Identify existing or planned controls
3. Assess privacy risks to ensure they are properly treated;
4. make the decision to validate the manner in which it is planned to comply with privacy principles and treat the risks,

Source: https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf

GDPR: From Regulation to coding

Privacy Impact Assessment

Context phase: gain a clear view of the processing(s) of personal data under consideration

Step	Description	Report
		❑ Presentation of the processing(s) of personal data under consideration ❑ Description of the scope ❑ Detailed description of the scope

Source: https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf

Privacy Impact Assessment

1.1. General description

- Describe the processing(s) of personal data under consideration, its(their) purposes and stakes
- Identify the data controller and the processors.

1.2. Detailed description

Define and describe the scope in detail:

- the personal data concerned, their recipients and retention periods;
- description of the processes and personal data supporting assets for the entire personal data life cycle (from collection to erasure).

Source: https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf

GDPR: From Regulation to coding

Privacy Risk

Type	Sub-type	Example
Personal Data	Identification Data	
	Personal Life	Living habits, marial status, ..
	Professional Life	Education, training, CV
	Economic and Financial	Income, financial situation, …
	Connection Data	IP address, logs, ..
Personal Data perceived as sensitive	Location Data	Travel, GPS Data, GSM Data
	Social security number	
	Bank Data	
Sensitive Data	Health Data	Biometric, Genetic, Health records
	Political, Racial / Ethical, Philosophical	

Source: https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-2-Tools.pdf

GDPR: From Regulation to coding

Privacy Impact Assessment

Template to describe personal data

Personal Data	Data sub-type	Category	Data Subject	Data subject is under 16 year	People with access to them	Data Source	Retention Period
List the data	Select data sub-type	Common Sensitive	Customer Employees Job applicants	Yes No		Where the data is coming from	How long the data can be kept

Source: https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-2-Tools.pdf

GDPR: From Regulation to coding

Privacy Impact Assessment

Controls phase: build the system that ensures compliance with privacy principles

Step	Description	Report
	2. Controls 2.1. Legal controls — *Purpose, information, subjects' rights, etc.* 2.2. Risk-treatment controls — *Actions on personal data, impacts, sources, supporting assets, etc.*	❑ List of selected controls ❑ Detailed description of the controls

Source: https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf

GDPR: From Regulation to coding

Privacy Impact Assessment

Controls phase: build the system that ensures compliance with privacy principles

2.1. Legal controls (mandatory)

1. purpose: specified, explicit and legitimate purpose
2. minimization: limiting the amount of personal data to what is strictly necessary
3. quality: preserving the quality of personal data
4. retention periods: period needed to achieve the purposes, in the absence of another legal obligation imposing a longer retention period
5. information: respect for data subjects' right to information
6. consent: obtaining the consent of the data subjects or existence of another legal basis justifying the processing of personal data
7. right to object: respect for the data subjects' right of opposition
8. right of access: respect for the data subjects' right to access their data
9. right to rectification: respect for the data subjects' right to correct their data and erase them

Source: https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf

Privacy Impact Assessment

Controls phase : build the system that ensures compliance with privacy principles

2.2. Risk-treatment controls

Impact	Prevention (Before)	Detection (During)	Correction (After)
Administrative	Security awareness and technical training	- Security reviews and audits	- Penalty
Technical	anonymization,encryption, backups, data partitioning, logical access control, etc	- Audit Trails	- Restore the system
Physical	Locks and keys	- Motion detectors.	- Fire extinguishers

Source: https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf

Privacy Impact Assessment

Risks phase : gain a good understanding of the causes and consequences of risks.

Step	Description	Report
		❑ Risk map ❑ Detailed description of the risks

Source: https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf

Privacy Impact Assessment

3.1. Sources

Impact	Prevention (Before)
Internal human sources	Employees, IT managers, trainees, managers
External human sources	Recipients of personal data, authorized third parties15, service providers, hackers, visitors, activists, competitors, customers, …
Non-human sources	Malicious code of unknown origin (viruses, worms, etc.), water (pipelines, waterways, etc.), flammable, corrosive or explosive materials, natural disasters, epidemics, animals

Source: https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf

3.2. Feared events

Feared events		Prevention (Before)
Illegitimate access to personal data	Storage	The data are copied and saved to another location without being further used.
	Redistribution	The data are disseminated more than necessary and beyond the control of the data subjects
	Use	The data are used for purposes other than those planned and/or in an unfair manner

Source: https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf

3.2. Feared events

Feared events		Prevention (Before)
Unwanted modification of personal data	Malfunction	The data are modified, which will not be used correctly, the processing liable to cause errors, malfunctions, or no longer provide the expected service
	Use	The data are modified in other valid data, such that the processing operations have been or could be misused.

Source: https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf

3.2. Feared events

Feared events		Prevention (Before)
Disappearance of personal data	Malfunction	The data are missing for personal data processings, which generates errors, malfunctions, or provides a different service than the one expected
	Use	The data are missing for personal data processings which can no longer provide the expected service.

Source: https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf

Privacy Impact Assessment

3.3. Threats

- Theft of a laptop
- Unintentional disclosure of information while talking;
- Influence (phishing, social engineering, bribery)
- pressure (blackmail, psychological harassment)
- Unwanted modifications to data in databases;
- Errors during updates
- configuration or maintenance;
- infection by malicious code

Source: https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf

Privacy Impact Assessment

3.4. Risks

Scale for severity: Severity represents the magnitude of a risk.

Impact	Description	Physical Impact	Moral Impact	Material Impact
Negligible	Data subjects either will not be affected or may encounter a few inconveniences, which they will overcome without any problem	- Transient headaches	- Feeling of invasion of privacy without real or objective harm	- Receipt of unsolicited mail
Limited	Data subjects may encounter significant inconveniences, which they will be able to overcome despite a few difficulties	- Lack of care leading to a minor but real harm	- Feeling of invasion of privacy without irreversible damage	- Lost opportunities of comfort (i.e. cancellation of leisure, termination of an online account)

Source: https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-2-Tools.pdf

Privacy Impact Assessment

3.4. Risks

Scale for severity: Severity represents the magnitude of a risk.

Impact	Description	Physical Impact	Moral Impact	Material Impact
Significant	Data subjects may encounter significant consequences, which they should be able to overcome albeit with real and serious difficulties	- Alteration of physical integrity for example following an assault, an accident at home, work, etc.	- Feeling of invasion of privacy with irreversible damage	- Loss of housing - Loss of employment - Separation or divorce - Financial loss as a result
Maximum	Data subjects may Encounter significant, or even irreversible, consequences, which they may not overcome	- Death (e.g. murder, suicide, fatal accident	- Loss of family ties - Inability to sue	- Financial risk - Substantial debts - Inability to work

Source: https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-2-Tools.pdf

3.4. Risks

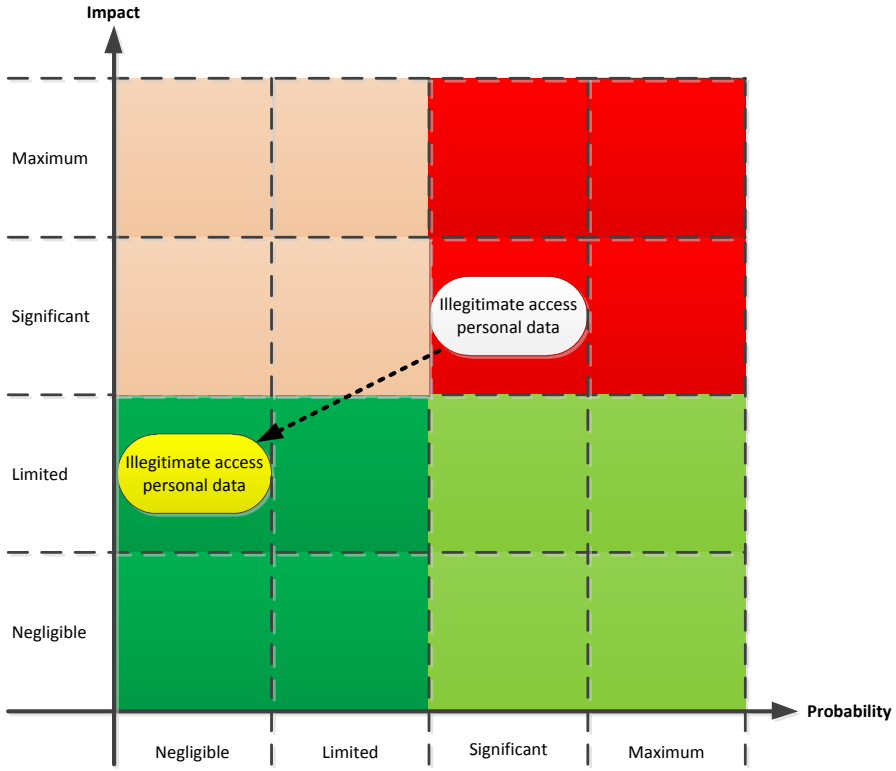
Scale for likelihood: Likelihood represents the feasibility of a risk to occur.

Likelihood	Description
Negligible	it does not seem possible for the selected risk sources to materialize the threat by exploiting the vulnerability **e.g.** theft of paper documents stored in a room protected by a badge reader and access code
Limited	it seems difficult for the selected risk sources to materialize the threat by exploiting the vulnerability **e.g.** theft of paper documents stored in a room protected by a badge reader).
Significant	it seems possible for the selected risk sources to materialize the threat by exploiting the vulnerability **e.g.** theft of paper documents stored in offices that cannot be accessed without first checking in at the reception
Maximum	it seems extremely easy for the selected risk sources to materialize the threat by exploiting the vulnerability **e.g.** theft of paper documents stored in the public lobby

Source: https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-2-Tools.pdf

Privacy Impact Assessment

3.4. Risks



What can be done to mitigate risks ?

- Reduce the impact
- Reduce the probability

Define Security Controls

Source: https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-2-Tools.pdf

GDPR: From Regulation to coding

Privacy Impact Assessment

Decision Phase. decide whether to accept or not the manner in which the PIA was managed and the residual risks

Step	Description	Report
		❑ Rationale to validate the PIA ❑ If applicable, action plan(s)

Source: https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf

GDPR: From Regulation to coding

Privacy Impact Assessment

Risks with a high severity and likelihood: these risks must be absolutely avoided or reduced by implementing security controls that reduce both their severity and their Likelihood

Risks with a high severity but a low likelihood: these risks must be avoided or reduced by implementing security controls that reduce both their severity and their likelihood

Risks with a low severity but a high likelihood: these risks must be reduced by implementing security controls that reduce their likelihood

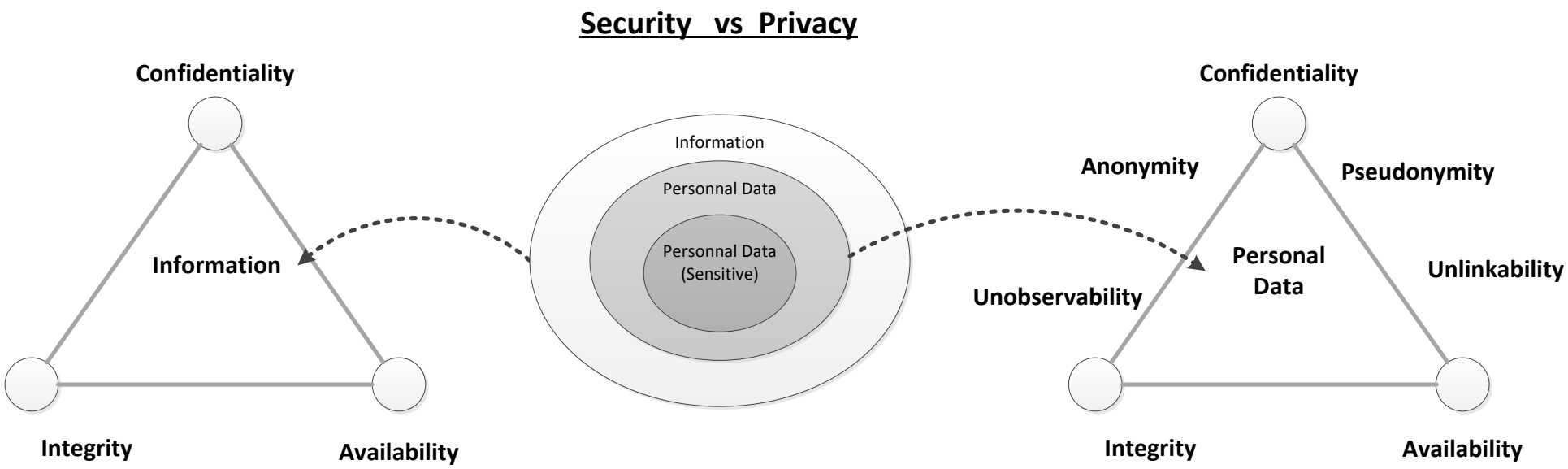
Risks with a low severity and low likelihood: it should be possible to take these risks,

Source: https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-2-Tools.pdf

Security & Privacy

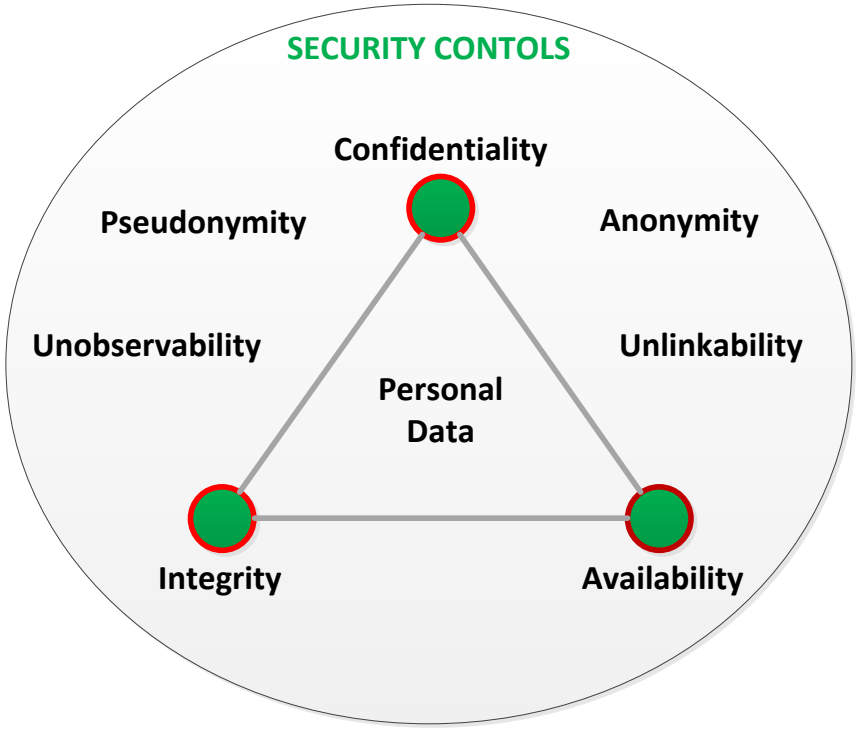
GDPR: From Regulation to coding

Security & Privacy



GDPR: From Regulation to coding

Security & Privacy



Privacy Controls

- Authentication
- Authorization
- Auditing
- Non-repudiation
- Encryption
- Hashing
- File Signature
- Architecture
- Privacy Design technics
- Database Design technics

Privacy by Design

7 principles

- Proactive not reactive; Preventative not remedial

It anticipates and prevents privacy invasive events before they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred — it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.

- Privacy as the default setting

Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business Practice

- Privacy embedded into design

Privacy by Design is embedded into the design and architecture of IT systems and business practices

- Full functionality – positive-sum, not zero-sum

Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made

Privacy by Design

7 principles

- End-to-end security – full lifecycle protection

Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish

- Visibility and transparency – keep it open

Component parts and operations remain visible and transparent, to users and providers.

- Respect for user privacy – keep it user-centric

Privacy by Design requires architects and operators to keep the interests of the individual by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric

Design Strategies

Data Oriented strategies

4 data oriented strategies can support the unlinkability protection goal and primarily address the principles of necessity and data minimization

Minimise

the amount of personal data that is processed should be restricted to the minimal amount possible

Hide

Any personal data, and their interrelationships, should be hidden from plain view.

It can be achieve by the use of encryption of data (when stored, or when in transit), anonymisation or the use of pseudonyms

Source: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

Design Strategies

Data Oriented strategies

Separate

Personal data should be processed in a distributed fashion, in separate compartments whenever possible. By separating the processing or storage of several sources of personal data that belong to the same person, complete profiles of one person cannot be made

Aggregate

Personal data should be processed at the highest level of aggregation and with the least possible detail in which it is (still) useful.

Source: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

Design Strategies

Process Oriented strategies

Inform

The INFORM strategy corresponds to the important notion of transparency

Whenever data subjects use a system, they should be informed about which information is processed, for what purpose, and by which means

Control

The data subjects should be provided agency over the processing of their personal data

Source: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

Design Strategies

Process Oriented strategies

Enforce

A privacy policy compatible with legal requirements should be in place and should be enforced.

This strategy supports the accountability principles

Demonstrate

The final strategy, DEMONSTRATE, requires a data controller to be able to demonstrate compliance with the privacy policy and any applicable legal requirements. This strategy supports the accountability principles

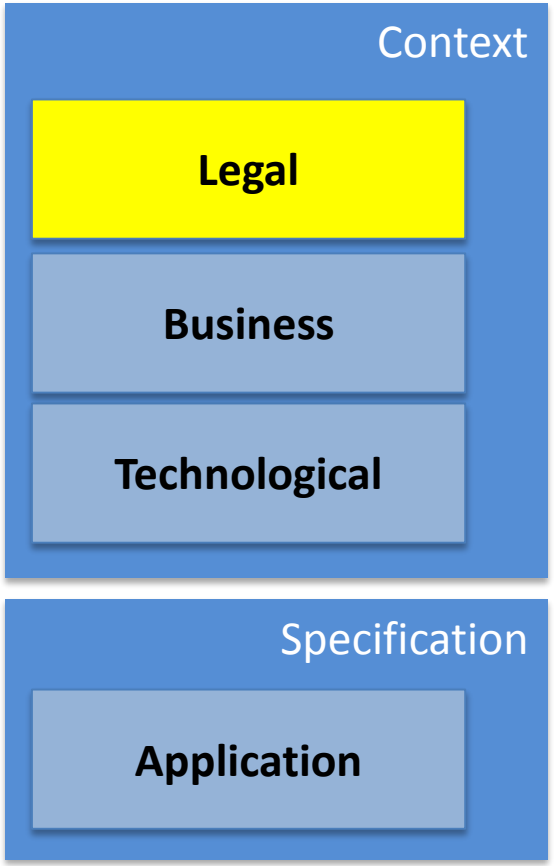
Source: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

Demonstrate the effectiveness of security controls

GDPR: From Regulation to coding

Demonstrate the effectiveness of security controls

Where risks come from in ISO 27034?



Global Data Protection Act
Patriot Act, …

PCI-DSS
Internal Policies, …

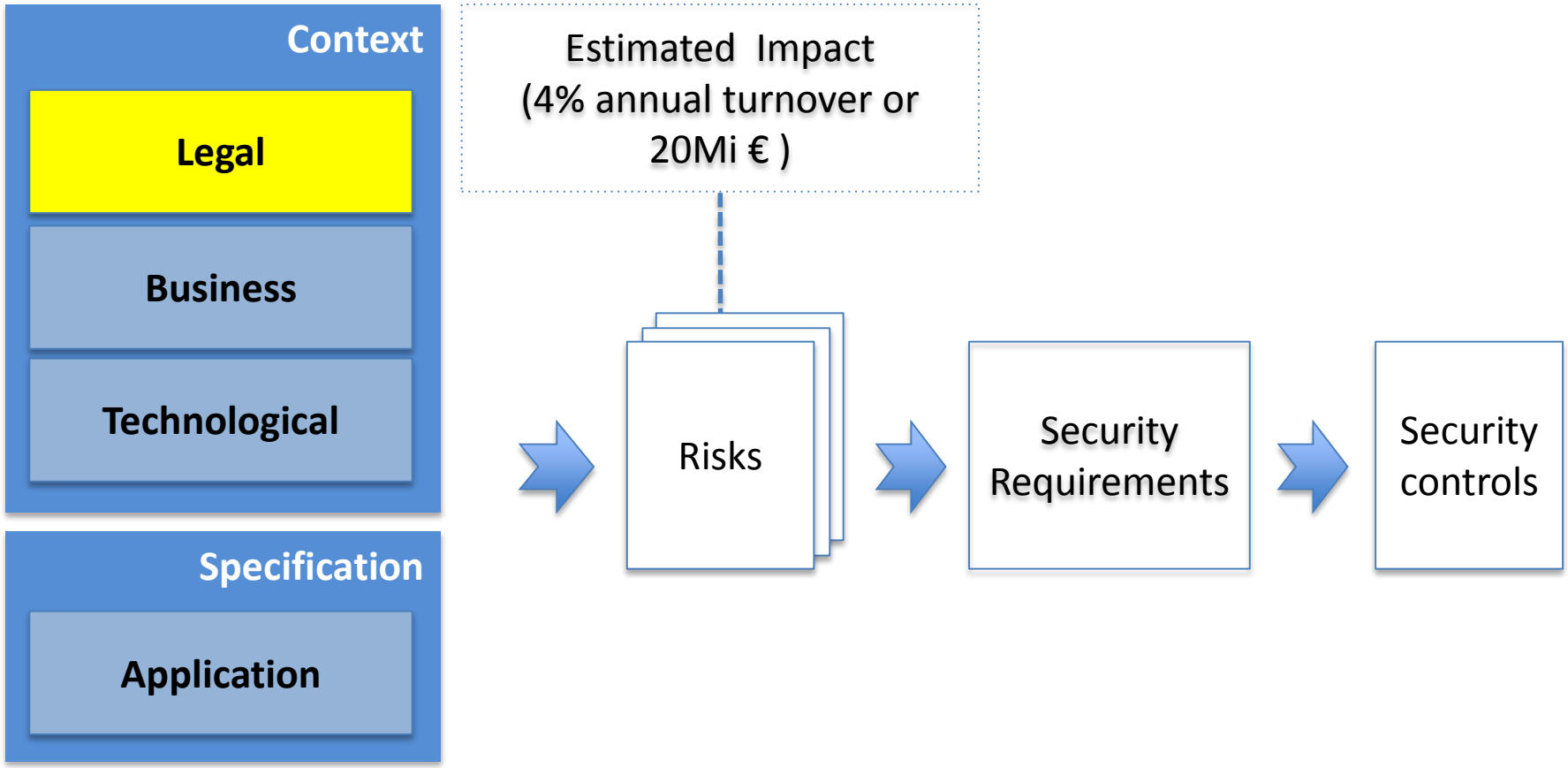
Java, C#, C++,…

File Upload
Dashboards
Sending mails, …

GDPR: From Regulation to coding

Demonstrate the effectiveness of security controls

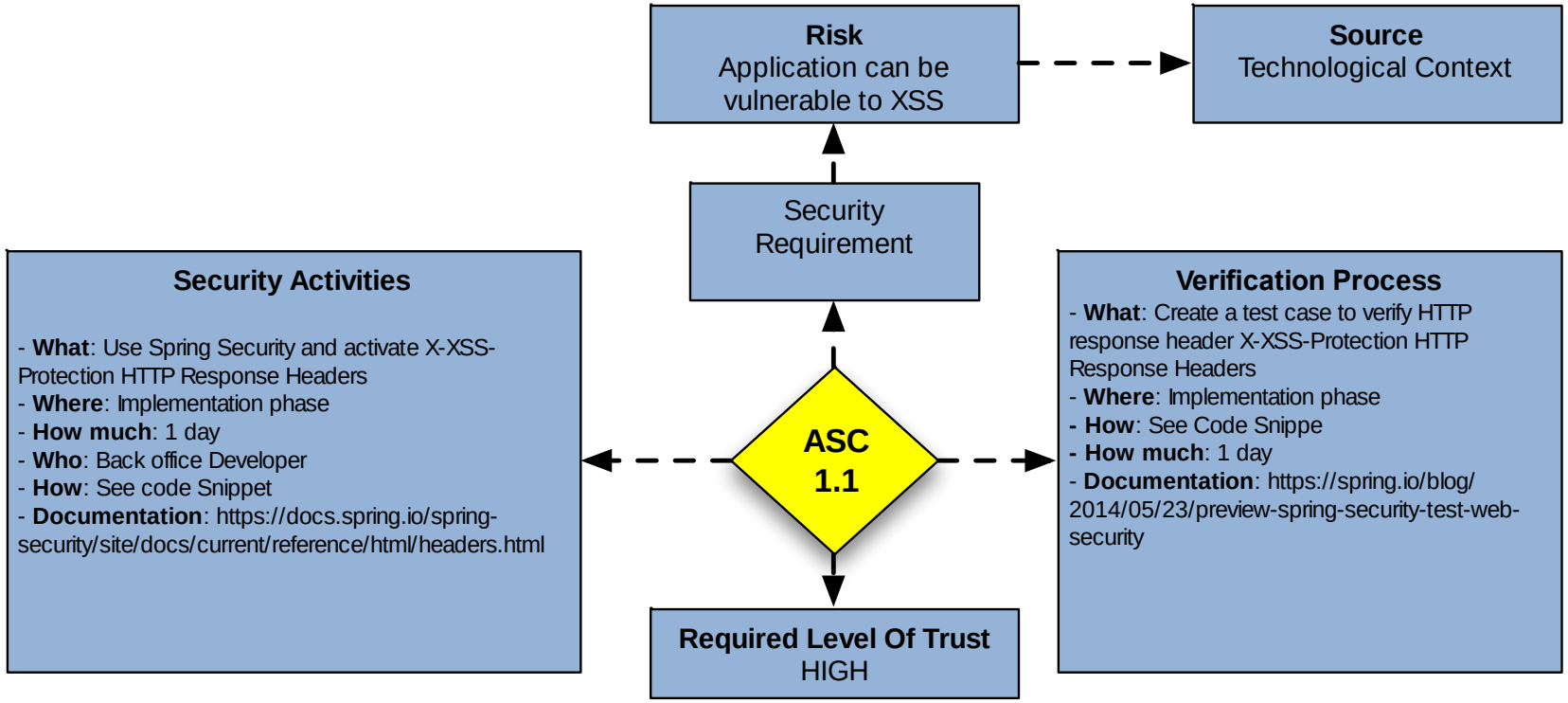
Where risks come from in ISO 27034?



Certification of Application Security

Demonstrate the effectiveness of security controls

Security Controls in ISO 27034



GDPR: From Regulation to coding

Demonstrate the effectiveness of security controls

Privacy Security controls

- ASC: Privacy Impact Assessment
- ASC: Cryptography requirements

- ASC: Privacy Design
- ASC: Secure Architecture Design
- ASC: Threat Modeling

- ASC: Owasp Top 10
- ASC: Owasp Privacy Top 10

- ASC: Static Code Analyzer
- ASC: Security and Privacy testing
- ASC: OWASP ASVS

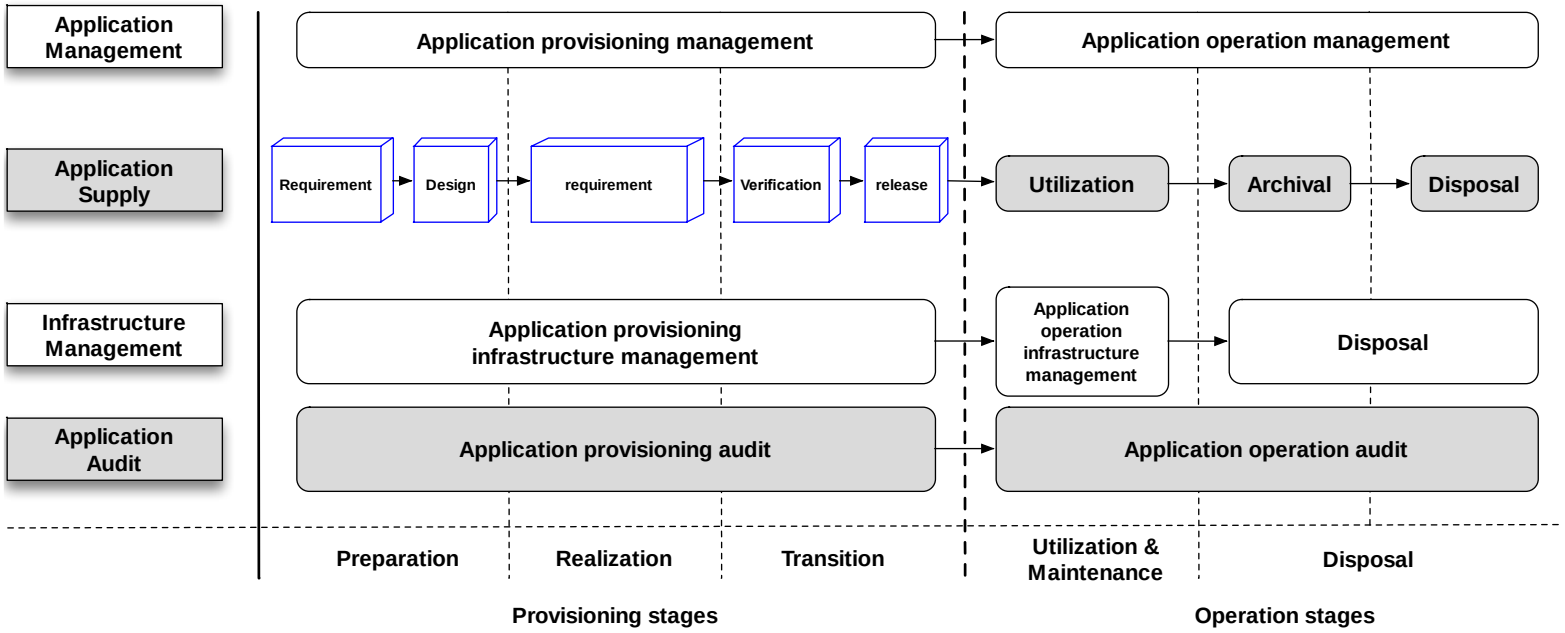
- ASC: Server Hardening
- ASC: Incident Response

GDPR: From Regulation to coding

Demonstrate the effectiveness of security controls

Application Security Life Cycle Model (ISO 27034)

Map your current Development life cycle with the reference model

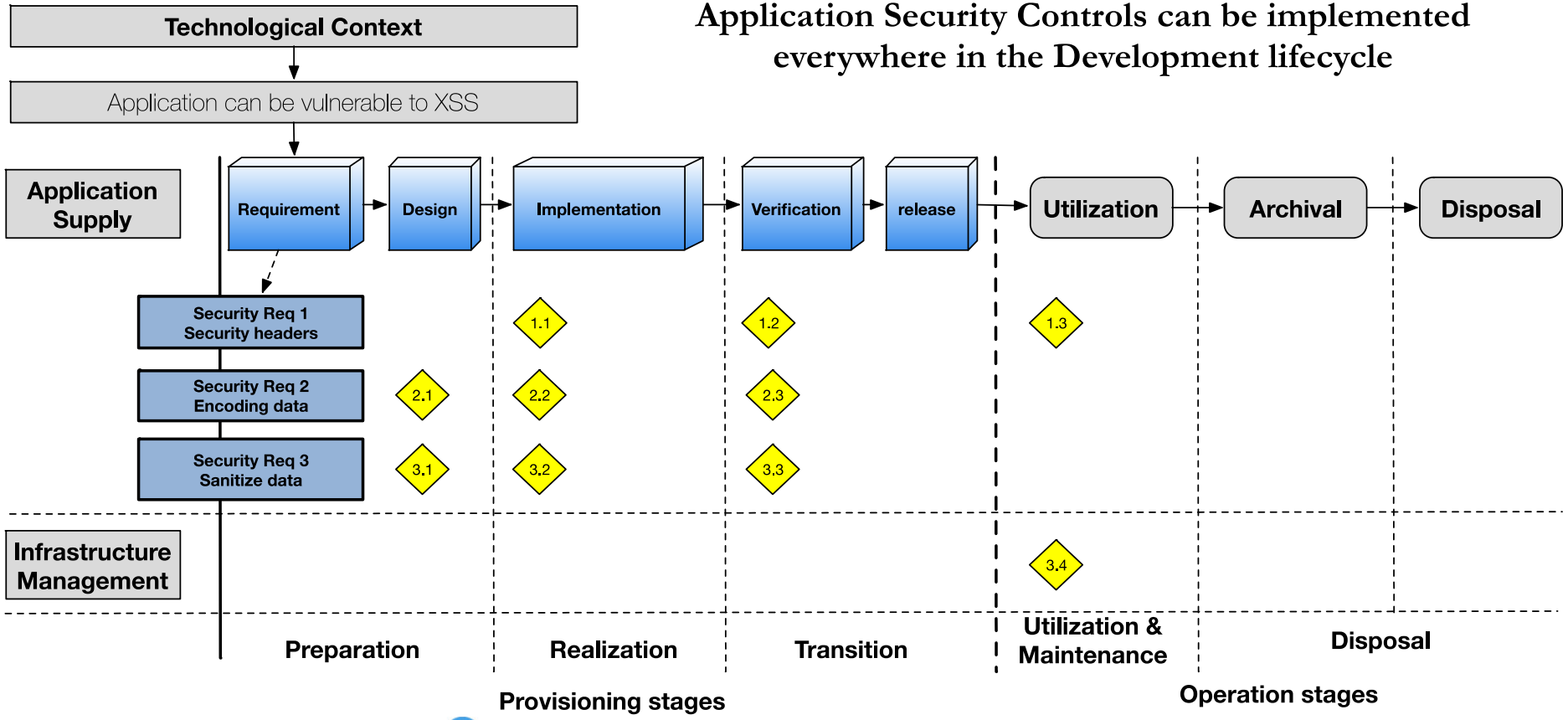


GDPR: From Regulation to coding

Demonstrate the effectiveness of security controls

Application Security Life Cycle Model (ISO 27034)

Application Security Controls can be implemented everywhere in the Development lifecycle



Secure Application Development

ICT CONTROL
Your Trusted Advisor

Solvay Brussels School Economics & Management

Cogentas.ca
Application Security Institute

Threat modeling technique for privacy (LIDDUN)

GDPR: From Regulation to coding

Threat modeling technique for privacy (LIDDUN)

Linkability: Being able to sufficiently distinguish whether 2 IOI (items of interest) are linked or not, even WITHOUT knowing the actual identity of the subject of the linkable IOI.

Identifiability: Being able to sufficiently identify the subject within a set of subjects

Non-repudiation: Not being able to deny a claim

Dectectability: Being able to sufficiently distinguish whether an item of interest (IOI) exists or not.

Information Disclosure: Information disclosure enables an attacker to gain valuable information about a system

Content Unawareness: Being unaware of the consequences of sharing information.

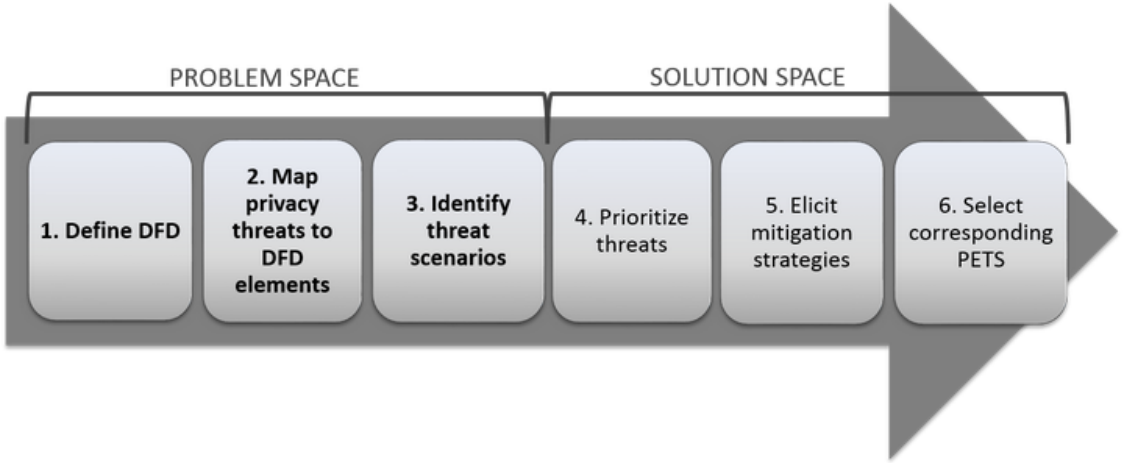
Non-compliance: Not being compliant with legislation, regulations, and corporate policies.

Source: https://distrinet.cs.kuleuven.be/software/linddun/linddun.php

GDPR: From Regulation to coding

Threat modeling technique for privacy (LIDDUN)

The LINDDUN methodology is a threat modeling technique that encourages analysts to consider privacy issues in a systematic fashion.



The LINDDUN methodology steps

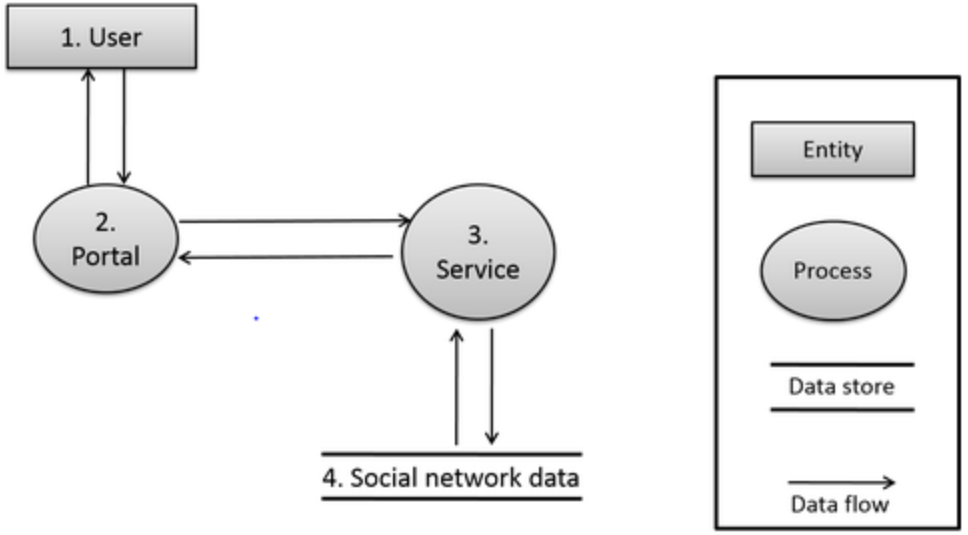
LINDDUN consists of six steps, as illustrated in the LINDDUN methodology steps illustration below. The first three steps are considered the core LINDDUN steps, as they focus on the problem space and aim at identifying the privacy threats in the system. The three remaining steps are more solution-oriented and aim at translating the threats that were identified into viable strategies and solutions that can mitigate the threats.

Source: https://distrinet.cs.kuleuven.be/software/linddun/linddun.php

GDPR: From Regulation to coding

Threat modeling technique for privacy (LIDDUN)

The DFD for the Social Network application is shown in the figure below (and in step 1 of the step-by-step example). In the DFD, the user is represented as an entity to interact with the system. The social network application contains two processes (the portal and the service) and one data store that contains all the personal information of the users.



The data flow diagram (DFD) of the Social Network application

Source: https://distrinet.cs.kuleuven.be/software/linddun/linddun.php

GDPR: From Regulation to coding

Threat modeling technique for privacy (LIDDUN)

The analyst should create a "personalized" table, based on LINDDUN's mapping table, which contains a row for each of the individual elements of the created DFD. This table can then be used as checklist throughout the elicitation phase, as each "x" in the table highlights a potential threat to the system that requires further analysis.

	L	I	N	D	D	U	N
Entity	X	X				X	
Data store	X	X	X	X	X		X
Data flow	X	X	X	X	X		X
Process	X	X	X	X	X		X

Mapping LINDDUN threat categories (Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, Non-compliance) to DFD element types.
*(**Hover over the X's to receive more information related to the X's applicability**)*

Source: https://distrinet.cs.kuleuven.be/software/linddun/linddun.php

GDPR: From Regulation to coding

Threat modeling technique for privacy (LIDDUN)

LINDDUN
PRIVACY THREAT MODELING

Home | LINDDUN summary | About | Material

Home » Catalog

LINDDUN threats

- **Linkability**
  - Linkability of entity
  - Linkability of data flow
  - Linkability of data store
  - Linkability of process
- **Identifiability**
  - identifiability of entity
  - identifiability of data flow
  - identifiability of data store
  - identifiability of process
- **Non-repudiation**
  - non-repudiation of data flow
  - non-repudiation of data store
  - non-repudiation of process
- **Detectability**
  - detectability of data flow
  - detectability of data store
  - detectability of process
- **Disclosure of information**
- **Unawareness**
  - Unawareness of entity
- **Non-compliance**
  - policy and consent non-compliance

Privacy threat trees catalog

Please use the menu on the left to browse through the catalog. The trees are categorized according to their corresponding DFD element type.

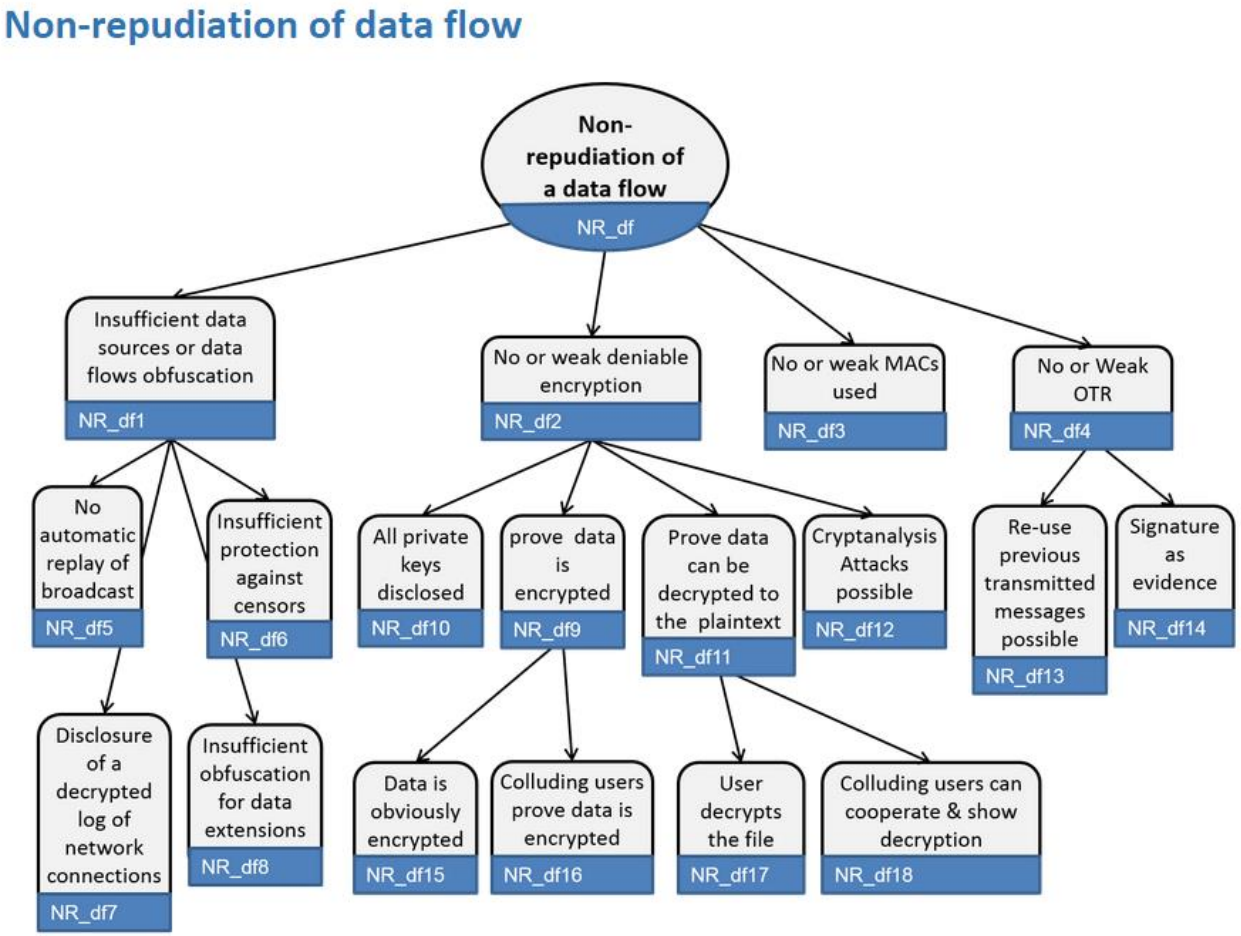
You can access the original LINDDUN paper here. We refer to the LINDDUN in a nutshell webpage for more information about the latest LINDDUN methodology steps (an up-to-date tutorial will be available soon).

Note that the STRIDE trees are only added for completeness. Ideally a thorough security analysis has already been performed or will be performed in parallel with LINDDUN.

Source: https://distrinet.cs.kuleuven.be/software/linddun/catalog.php

GDPR: From Regulation to coding

Threat modeling technique for privacy (LIDDUN)



Source: https://distrinet.cs.kuleuven.be/software/linddun/nonrepudiation_DF.php

Privacy Framework
Nymity

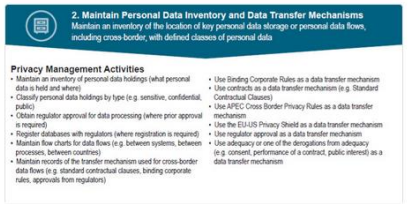
GDPR: From Regulation to coding

Nymity Privacy Framework


1. Maintain Governance Structure
Ensure that there are individuals responsible for data privacy, accountable management, and management reporting procedures

Privacy Management Activities
- Assign responsibility for data privacy to an individual (e.g. Privacy Officer, Privacy Counsel, CPO)
- Engage senior management in data privacy (e.g. at the Board of Directors, Executive Committee)
- Appoint a Data Protection Officer/Official (DPO) in an independent oversight role
- Assign responsibility for data privacy throughout the organization (e.g. Privacy Network)
- Maintain roles and responsibilities for individuals responsible for data privacy (e.g. job descriptions)
- Conduct regular communication between the privacy office, privacy network and others responsible/accountable for data privacy
- Engage stakeholders throughout the organization on data privacy matters (e.g. information security, marketing, etc.)
- Report to internal stakeholders on the status of privacy management (e.g. board of directors, management)
- Report to external stakeholders on the status of privacy management (e.g. regulators, third-parties, clients)
- Conduct an Enterprise Privacy Risk Assessment
- Integrate data privacy into business risk assessments/reporting
- Maintain a Privacy Strategy
- Maintain a privacy program charter/mission statement
- Require employees to acknowledge and agree to adhere to the data privacy policies

1. Maintain Governance Structure


2. Maintain Personal Data Inventory and Data Transfer Mechanisms
Maintain an inventory of the location of key personal data storage or personal data flows, including cross-border, with defined classes of personal data

Privacy Management Activities
- Maintain an inventory of personal data holdings (what personal data is held and where)
- Classify personal data holdings by type (e.g. sensitive, confidential, public)
- Obtain regulator approval for data processing (where prior approval is required)
- Register databases with regulators (where registration is required)
- Maintain flow charts for data flows (e.g. between systems, between processes, between countries)
- Maintain records of the transfer mechanism used for cross-border data flows (e.g. standard contractual clauses, binding corporate rules, approvals from regulators)
- Use Binding Corporate Rules as a data transfer mechanism
- Use contracts as a data transfer mechanism (e.g. Standard Contractual Clauses)
- Use APEC Cross Border Privacy Rules as a data transfer mechanism
- Use the EU-US Privacy Shield as a data transfer mechanism
- Use regulator approval as a data transfer mechanism
- Use adequacy or one of the derogations from adequacy (e.g. consent, performance of a contract, public interest) as a data transfer mechanism

2. Maintain Personal Data Inventory and Data Transfer Mechanisms


3. Maintain Internal Data Privacy Policy
Maintain a data privacy policy that meets legal requirements and addresses operational risk and risk of harm to individuals

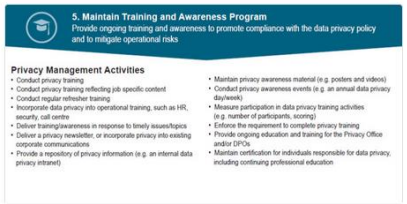
Privacy Management Activities
- Maintain a data privacy policy
- Maintain an employee data privacy policy
- Maintain an organizational code of conduct that includes privacy
- Document legal basis for processing personal data
- Integrate ethics into data processing (Codes of Conduct, policies and other measures)

3. Maintain Internal Data Privacy Policy


4. Embed Data Privacy Into Operations
Maintain operational policies and procedures consistent with the data privacy policy, legal requirements, and operational risk management objectives

Privacy Management Activities
- Maintain policies/procedures for collection and use of sensitive personal data (including biometric data)
- Maintain policies/procedures for collection and use of children and minors' data
- Maintain policies/procedures for maintaining data quality
- Maintain policies/procedures for the de-identification of personal data
- Maintain policies/procedures to review processing conducted wholly or partially by automated means
- Maintain policies/procedures for secondary uses of personal data
- Maintain policies/procedures for obtaining valid consent
- Maintain policies/procedures for secure destruction of personal data
- Integrate data privacy into use of cookies and tracking mechanisms
- Integrate data privacy into records retention practices
- Integrate data privacy into hiring practices
- Integrate data privacy into the organization's use of social media
- Integrate data privacy into Bring Your Own Device (BYOD) policies/procedures
- Integrate data privacy into health & safety practices
- Integrate data privacy into interactions with works councils
- Integrate data privacy into practices for monitoring employees
- Integrate data privacy into use of CCTV/video surveillance
- Integrate data privacy into use of geo-location (tracking and or location) devices
- Integrate data privacy into policies/procedures regarding access to employees' company e-mail accounts
- Integrate data privacy into e-discovery practices

4. Embed Data Privacy Into Operations


5. Maintain Training and Awareness Program
Provide ongoing training and awareness to promote compliance with the data privacy policy and to mitigate operational risks

Privacy Management Activities
- Conduct privacy training
- Conduct privacy training reflecting job specific content
- Conduct regular refresher training
- Incorporate data privacy into operational training, such as HR, security, call centre
- Deliver training/awareness in response to timely issues/topics
- Deliver a privacy newsletter, or incorporate privacy into existing corporate communications
- Provide a repository of privacy information (e.g. an internal data privacy intranet)
- Maintain privacy awareness material (e.g. posters and videos)
- Conduct privacy awareness events (e.g. an annual data privacy day/week)
- Measure participation in data privacy training activities (e.g. number of participants, scoring)
- Enforce the requirement to complete privacy training
- Provide ongoing education and training for the Privacy Office and/or DPOs
- Maintain certification for individuals responsible for data privacy, including continuing professional education

5. Maintain Training and Awareness Program


6. Manage Information Security Risk
Maintain an information security program based on legal requirements and ongoing risk assessments

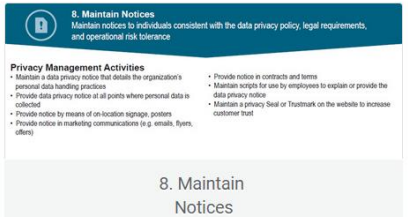
Privacy Management Activities
- Integrate data privacy risk into security risk assessments
- Integrate data privacy into an information security policy
- Maintain technical security measures (e.g. intrusion detection, firewalls, monitoring)
- Maintain measures to encrypt personal data
- Maintain an acceptable use of information resources policy
- Maintain procedures to restrict access to personal data (e.g. role-based access, segregation of duties)
- Integrate data privacy into a corporate security policy (protection of physical premises and hard assets)
- Maintain human resource security measures (e.g. pre-screening, performance appraisals)
- Integrate data privacy into business continuity plans
- Maintain a data-loss prevention strategy
- Conduct regular testing of data security posture
- Maintain a security certification (e.g. ISO)

6. Manage Information Security Risk


7. Manage Third-Party Risk
Maintain contracts and agreements with third-parties and affiliates consistent with the data privacy policy, legal requirements, and operational risk tolerance

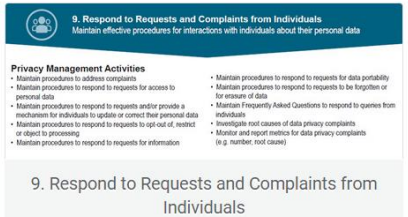
Privacy Management Activities
- Maintain data privacy requirements for third parties (e.g. clients, vendors, processors, affiliates)
- Maintain procedures to execute contracts or agreements with all processors
- Conduct due diligence around the data privacy and security posture of potential vendors/processors
- Conduct due diligence on third party data sources
- Maintain a vendor data privacy risk assessment process
- Maintain a policy governing use of cloud providers
- Maintain procedures to address instances of non-compliance with contracts and agreements
- Conduct ongoing due diligence around the data privacy and security posture of vendors/processors
- Review long-term contracts for new or evolving data privacy risks

7. Manage Third-Party Risk


8. Maintain Notices
Maintain notices to individuals consistent with the data privacy policy, legal requirements, and operational risk tolerance

Privacy Management Activities
- Maintain a data privacy notice that details the organization's personal data handling practices
- Provide data privacy notice at all points where personal data is collected
- Provide notice by means of on-location signage, posters
- Provide notice in marketing communications (e.g. emails, flyers, offers)
- Provide notice in contracts and terms
- Maintain scripts for use by employees to explain or provide the data privacy notice
- Maintain a privacy Seal or Trustmark on the website to increase customer trust

8. Maintain Notices


9. Respond to Requests and Complaints from Individuals
Maintain effective procedures for interactions with individuals about their personal data

Privacy Management Activities
- Maintain procedures to address complaints
- Maintain procedures to respond to requests for access to personal data
- Maintain procedures to respond to requests and/or provide a mechanism for individuals to update or correct their personal data
- Maintain procedures to respond to requests to opt-out of, restrict or object to processing
- Maintain procedures to respond to requests for information
- Maintain procedures to respond to requests for data portability
- Maintain procedures to respond to requests to be forgotten or for erasure of data
- Maintain Frequently Asked Questions to respond to queries from individuals
- Investigate root causes of data privacy complaints
- Monitor and report metrics for data privacy complaints (e.g. number, root cause)

9. Respond to Requests and Complaints from Individuals


10. Monitor for New Operational Practices
Monitor organizational practices to identify new processes or material changes to existing processes and ensure the implementation of Privacy by Design principles

Privacy Management Activities
- Integrate Privacy by Design into system and product development
- Maintain PIA/DPIA guidelines and templates
- Conduct PIAs/DPIAs for new programs, systems, processes
- Conduct PIAs or DPIAs for changes to existing programs, systems, or processes
- Engage external stakeholders (e.g., individuals, privacy advocates) as part of the PIA/DPIA process
- Track and address data protection issues identified during PIAs/DPIAs
- Report PIA/DPIA analysis and results to regulators (where required) and external stakeholders (if appropriate)

10. Monitor for New Operational Practices


11. Maintain Data Privacy Breach Management Program
Maintain an effective data privacy incident and breach management program

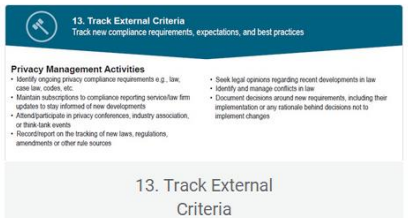
Privacy Management Activities
- Maintain a data privacy incident/breach response plan
- Maintain a breach notification (to affected individuals) and reporting (to regulators, credit agencies, law enforcement) protocol
- Maintain a log to track data privacy incidents/breaches
- Monitor and report data privacy incident/breach metrics (e.g. nature of breach, risk, root cause)
- Conduct periodic testing of data privacy incident/breach plan
- Engage a breach response remediation provider
- Engage a forensic investigation team
- Obtain data privacy breach insurance coverage

11. Maintain Data Privacy Breach Management Program


12. Monitor Data Handling Practices
Verify operational practices comply with the data privacy policy and operational policies and procedures, and measure and report on their effectiveness

Privacy Management Activities
- Conduct self-assessments of privacy management
- Conduct Internal Audits of the privacy program (i.e. operational audit of the Privacy Office)
- Conduct ad-hoc walk-throughs
- Conduct ad-hoc assessments based on external events, such as complaints/breaches
- Engage a third party to conduct audits/assessments
- Monitor and report privacy management metrics
- Maintain documentation as evidence to demonstrate compliance and/or accountability
- Maintain certifications, accreditations or data protection seals for demonstrating compliance to regulators

12. Monitor Data Handling Practices


13. Track External Criteria
Track new compliance requirements, expectations, and best practices

Privacy Management Activities
- Identify ongoing privacy compliance requirements e.g., law, case law, codes, etc.
- Maintain subscriptions to compliance reporting service/law firm updates to stay informed of new developments
- Attend/participate in privacy conferences, industry association, or think-tank events
- Record/report on the tracking of new laws, regulations, amendments or other rule sources
- Seek legal opinions regarding recent developments in law
- Identify and manage conflicts in law
- Document decisions around new requirements, including their implementation or any rationale behind decisions not to implement changes

13. Track External Criteria

GDPR: From Regulation to coding

Nymity Privacy Framework

1. Maintain Governance Structure
Ensure that there are individuals responsible for data privacy, accountable management, and management reporting procedures

2. Maintain Personal Data Inventory and Data Transfer Mechanisms
Maintain an inventory of the location of key personal data storage or personal data flows, including cross-border, with defined classes of personal data

3. Maintain Internal Data Privacy Policy
Maintain a data privacy policy that meets legal requirements and addresses operational risk and risk of harm to individuals

4. Embed Data Privacy Into Operations
Maintain operational policies and procedures consistent with the data privacy policy, legal requirements, and operational risk management objectives

5. Maintain Training and Awareness Program
Provide ongoing training and awareness to promote compliance with the data privacy policy and to mitigate operational risks

6. Manage Information Security Risk
Maintain an information security program based on legal requirements and ongoing risk assessments

GDPR: From Regulation to coding

Nymity Privacy Framework

7. Manage Third-Party Risk
Maintain contracts and agreements with third-parties and affiliates consistent with the data privacy policy, legal requirements, and operational risk tolerance

8. Maintain Notices
Maintain notices to individuals consistent with the data privacy policy, legal requirements, and operational risk tolerance

9. Respond to Requests and Complaints from Individuals
Maintain effective procedures for interactions with individuals about their personal data

10. Monitor for New Operational Practices
Monitor organizational practices to identify new processes or material changes to existing processes and ensure the implementation of Privacy by Design principles

11. Maintain Data Privacy Breach Management Program
Maintain an effective data privacy incident and breach management program

12. Monitor Data Handling Practices
Verify operational practices comply with the data privacy policy and operational policies and procedures, and measure and report on their effectiveness

13. Track External Criteria
Track new compliance requirements, expectations, and best practices

GDPR: From Regulation to coding

Nymity Privacy Framework

2. Maintain Personal Data Inventory and Data Transfer Mechanisms
Maintain an inventory of the location of key personal data storage or personal data flows, including cross-border, with defined classes of personal data

- Maintain an inventory of personal data holdings (what personal data is held and where)
- Classify personal data holdings by type (e.g. sensitive, confidential, public)
- Maintain flow charts for data flows (e.g. between systems, between processes, between countries)

Source: https://www.nymity.com/data-privacy-resources/privacy-management-tools/maintain-personal-data-inventory.aspx

GDPR: From Regulation to coding

Nymity Privacy Framework

4. Embed Data Privacy Into Operations
Maintain operational policies and procedures consistent with the data privacy policy, legal requirements, and operational risk management objectives

Integrate data privacy into

- use of cookies and tracking mechanisms
- records retention practices
- direct marketing practices
- e-mail marketing practices
- telemarketing practices
- digital advertising practices (e.g., online, mobile)

Source: https://www.nymity.com/data-privacy-resources/privacy-management-tools/embed-data-privacy-into-operations.aspx

GDPR: From Regulation to coding

Nymity Privacy Framework

4. Embed Data Privacy Into Operations
Maintain operational policies and procedures consistent with the data privacy policy, legal requirements, and operational risk management objectives

Integrate data privacy into

- hiring practices
- the organization's use of social media practices
- Bring Your Own Device (BYOD) policies/procedures
- health & safety practices
- use of CCTV/video surveillance
- use of geo-location (tracking and or location) devices

Source: https://www.nymity.com/data-privacy-resources/privacy-management-tools/embed-data-privacy-into-operations.aspx

GDPR: From Regulation to coding

Nymity Privacy Framework

- Maintain technical security measures (e.g. intrusion detection, firewalls, monitoring)
- Maintain measures to encrypt personal data
- Maintain procedures to restrict access to personal data (e.g. role-based access, segregation of duties)

Source: https://www.nymity.com/data-privacy-resources/privacy-management-tools/manage-information-security-risk.aspx

GDPR: From Regulation to coding

Nymity Privacy Framework

- Maintain a data privacy notice that details the organization's personal data handling practices
- Provide data privacy notice at all points where personal data is collected

Source: https://www.nymity.com/data-privacy-resources/privacy-management-tools/maintain-notices.aspx

GDPR: From Regulation to coding

Nymity Privacy Framework

- Maintain procedures to respond to requests for data portability
- Maintain procedures to respond to requests to be forgotten or for erasure of data

Source: https://www.nymity.com/data-privacy-resources/privacy-management-tools/maintain-procedures-privacy-inquiries-complaints.aspx

GDPR: From Regulation to coding

Nymity Privacy Framework

10. Monitor for New Operational Practices
Monitor organizational practices to identify new processes or material changes to existing processes and ensure the implementation of Privacy by Design principles

- Integrate Privacy by Design into system and product development
- Conduct PIAs/DPIAs for new programs, systems, processes
- Conduct PIAs or DPIAs for changes to existing programs, systems, or processes

Source: https://www.nymity.com/data-privacy-resources/privacy-management-tools/monitor-new-operational-practices.aspx

GDPR: From Regulation to coding

Nymity Privacy Framework

11. Maintain Data Privacy Breach Management Program
Maintain an effective data privacy incident and breach management program

- Maintain a log to track data privacy incidents/breaches
- Monitor and Report data privacy incident/breach metrics (e.g. nature of breach, risk, root cause)

Source: https://www.nymity.com/data-privacy-resources/privacy-management-tools/maintain-notices.aspx

Questions

Part II: Exercise

Exercise

Ashley Madison hack
15 July 2015

What did hackers take from Ashley Madison and why?
The Ashley Madison hackers have posted personal information like e-mail addresses and account details from 32 million of the site's members

Impacts

Company reputation

On 24 August 2015, a pastor and professor at the New Orleans Baptist Theological Seminary committed suicide citing the leak that had occurred six days before

On 24 August 2015, Toronto police announced that two unconfirmed suicides had been linked to the data breach, in addition to "reports of hate crimes connected to the hack

Fake Profiles: A very high number of the women's accounts were created from the same IP address suggesting

GDPR: From Regulation to coding

Exercise

Ashley Madison hack

Timing
Case presentation: 10’
Break-out work: 20’
Group presentations: 60’

Exercise

Ashley Madison hack
15 July 2015

The company "find love" is willing to develop a dating website

The company is well aware of Ashley Madison case. A big attention as to be given to the security and the privacy of personal data that will be process by the website

Basic functionalities
Web Based application
Create a user profile
Subscription fee
Research engine based on a form
Online chat

GDPR: From Regulation to coding

Exercise

Ashley Madison hack
15 July 2015

Future functionalities

Case 1
- Building a more detail profile: Hobbies, Culture, Politics, Religion, …
- Process these data to create a psychological profile

Case 2
- Build a mobile application with Geolocation services, follow your users and propose matching profile close to their location

Case 3
- Like Ashley Madison, restrict the registration to persons already in relation and interested in having an affair

References

- **General Data Protection Regulation:** http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC
- **The International Association of Privacy Professionals: https://iapp.org/**
- **Nymity Privacy Framework**: www.nymity.com
- **Anonymisation**: https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf
- **Owasp Privacy Top 10**: https://www.owasp.org/index.php/OWASP_Top_10_Privacy_Risks_Project
- **Privacy By Design:** https://en.wikipedia.org/wiki/Privacy_by_design
- **Privacy By Design 7 Principles:** https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf
- Privacy by Redesign: https://iapp.org/media/presentations/12Symposium/CS12_Privacy_by_ReDesign_PPT.pdf
- Retention period: http://www.debrauw.com/wp-content/uploads/2015/01/EU-Retention-Guide-2014.pdf
- OWASP Privacy Top 10: https://www.owasp.org/index.php/OWASP_Top_10_Privacy_Risks_Project
- ENISA: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design
- Privacy threat trees catalog: https://distrinet.cs.kuleuven.be/software/linddun/catalog.php