GDPR: From Regulation to coding
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
GDPR: From Regulation to coding

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
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
GDPR: From Regulation to coding
GDPR: From Regulation to coding

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 Master in IT Management

Executive Programme in
  . CIO Practices
  . CIO Leadership
  . IT Business Agility
  . Enterprise and IT Architecture
  . IT Sourcing
  . IT Management Consulting
Executive Master in Information Risk and Cybersecurity

Executive Programme in
  . Security Governance
  . Information Security
  . Cybersecurity

Executive Education in Information Security Management
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
S2 – IT Security Practices
S3 – Cybersecurity Workshop
G1 – The CIO Foundation
G2 – IT Governance Workshop
G3 – IT Risk and Legal concerns
M1 – Applications Build and Management
M2 – IT Services and Run Management
M3 – IT Sourcing Management
B1 – Enterprise Strategy and Architecture
B2 – Business Transformation
B3 – Digital Agility and Innovation
A1 – IT Finance and Portfolio Management
A2 – Soft Skills for IT professionals
A3 – Building Expert Opinion

Monday
Track-S

Thursday
Track-G

Wednesday
Track-M

Tuesday
Track-B

Monday
Track-A

© 2014 ictc.eu

© Copyright ICTC.EU 2017
GDPR
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
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
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)**

<table>
<thead>
<tr>
<th>Regulated Object</th>
<th>Personal Data</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Regulated Activity</th>
<th>Data Processing</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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, ...</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parties Involved</th>
<th>Data Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>One who can be identified directly or indirectly by reference to an identifier such a name, location data, identification number or other means</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Controller</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Natural or legal person which determines the purpose and means of the processing of personal data</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Processor</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Natural or legal person which processes personal data on behalf of the controller</td>
</tr>
</tbody>
</table>

| 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

<table>
<thead>
<tr>
<th>Principle</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lawfulness</td>
<td>- Processing is lawful as set out in GDPR (consent, legal obligation, vital interest, etc.)</td>
</tr>
<tr>
<td>Fairness &amp; transparency</td>
<td>- Data subject must be provided with sufficient information about the collection/processing of their data to understand possible risks</td>
</tr>
<tr>
<td>Purpose limitation</td>
<td>- Personal data must be collected for specified, explicit and legitimate purpose&lt;br&gt;- Personal data obtained for one purpose must not be processed for unrelated purpose</td>
</tr>
<tr>
<td>Data minimization</td>
<td>Both in the collection and processing, personal data has to be minimized as much as possible</td>
</tr>
<tr>
<td>Accuracy</td>
<td>Personal data should be accurate, kept up-to-date and reasonable steps must be taken to ensure that inaccurate personal data are erased or rectified without delay</td>
</tr>
<tr>
<td>Storage limitation</td>
<td>Data must be erased or effectively anonymised as soon as it is no longer needed for its original purpose</td>
</tr>
<tr>
<td>Right of withdraw consent (Art. 7)</td>
<td>Right to be informed (Art. 13 &amp; 14)</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>Right of erasure – Right to be forgotten (Art. 17)</td>
<td>Rights in relation to automated processing (Art. 22)</td>
</tr>
<tr>
<td>Right to object to processing (Art. 21)</td>
<td>Right to restrict processing (Art. 18)</td>
</tr>
</tbody>
</table>
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 of opt-in or opt-out.

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

GDPR: From Regulation to coding

Consent and choice

## GDPR: From Regulation to coding

### Right of withdraw consent

<table>
<thead>
<tr>
<th>Consent lifecycle</th>
<th>Consent given</th>
<th>Data collection</th>
<th>Consent Remove</th>
<th>No data collection</th>
<th>Consent given</th>
<th>Data collection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smartphone</td>
<td>Consent: Geolocation permission</td>
<td></td>
<td>Collect Geolocation info</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System</td>
<td>Consent: Geolocation info</td>
<td></td>
<td>Withdraw Consent</td>
<td>No data collection</td>
<td>Consent: Geolocation permission</td>
<td></td>
</tr>
<tr>
<td>Consent traceability</td>
<td>Consent given 01/01/2017 08:00</td>
<td></td>
<td>Legitimate process</td>
<td>Accountability</td>
<td>Consent removed 01/02/2017 08:00</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Consent given 01/03/2017 08:00</td>
<td></td>
<td>Legitimate process</td>
<td>Accountability</td>
<td>Consent given 01/03/2017 08:00</td>
<td></td>
</tr>
</tbody>
</table>

**Right of withdraw consent**

- **Consent given**: 01/01/2017 08:00
- **Consent removed**: 01/02/2017 08:00
- **Consent given**: 01/03/2017 08:00

**Legitimate process**

**Accountability**

**GDPR**: From Regulation to coding
Microsoft Privacy Statement

Last Updated: November 2016

What’s new?

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.

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.

How We Use Personal Data

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

Privacy notice

Summary

Table of contents

History

Topic summary
Right to be informed

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:
Changes introduced by a specific version of a privacy notice

**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 in-game chat for users who need it.

**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
Data 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
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 lifecycle Management**

- **Create**
- **Store**
- **Backup**
- **Share**
- **Destroy**

**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 lifecycle Management**

- Create
- Store
- Use
- Backup
- Destroy
- Share

**Phase: Share**

**How it is shared?**
- Mail
- Access right delegation
- File on USB stick

**Security mechanism in place**
- Access management
- Auditing
- Encryption

**GDPR: From Regulation to coding**
GDPR: From Regulation to coding

Data Management

**Data lifecycle Management**

- Create
- Store
- Use
- Share
- Destroy
- Backup

**Phase: Archive**

**Types of backup**

- DB,
- Email,
- Cloud

**Timing**

**Security mechanism in place**

- Access management
- Auditing
- Backup Encryption & Integrity
**Data lifecycle Management**

- **Create**
- **Store**
- **Use**
- **Share**
- **Backup**
- **Destroy**

**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
Security of personal Data

- Communication of a personal data breach to the data subject (Art. 34)
- Notification of a personal data breach to the supervisory authority (Art. 33)
- Security of processing (Art. 32)
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
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.
“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)

What is a privacy risk?

**Likelihood**: Represents the magnitude of a risk.

**Severity**: Represents the possibility for a risk to occur.

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

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

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).

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

# GDPR: From Regulation to coding

## Privacy Impact Assessment

**Template to describe personal data**

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

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

![Diagram](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

2.1. 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

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

2.2. Risk-treatment controls

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

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

3.1. Sources

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

#### 3.2. Feared events

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

3.2. Feared events

<table>
<thead>
<tr>
<th>Feared events</th>
<th>Prevention (Before)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unwanted modification of personal data</td>
<td>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</td>
</tr>
<tr>
<td>Use</td>
<td>The data are modified in other valid data, such that the processing operations have been or could be misused.</td>
</tr>
</tbody>
</table>
3.2. Feared events

<table>
<thead>
<tr>
<th>Feared events</th>
<th>Prevention (Before)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disappearance of personal data</td>
<td>The data are missing for personal data processings, which generates errors, malfunctions, or provides a different service than the one expected</td>
</tr>
<tr>
<td>Use</td>
<td>The data are missing for personal data processings which can no longer provide the expected service.</td>
</tr>
</tbody>
</table>
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

### 3.4. Risks

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

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

## 3.4. Risks

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

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

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

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 |

What can be done to mitigate risks?

- Reduce the impact
- Reduce the probability

Define Security Controls

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

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,
Security & Privacy
Security & Privacy

Security vs Privacy

Confidentiality

Information

Integrity

Availability

Confidentiality

Personal Data

(Sensitive)

Anonymity

Pseudonymity

Unobservability

Unlinkability

Integrity

Availability

Personal Data
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

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.

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

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

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, ...

Legal

Business

Technological

Application
GDPR: From Regulation to coding

Demonstrate the effectiveness of security controls

Where risks come from in ISO 27034?

- **Estimated Impact**
  - (4% annual turnover or 20Mi €)

**Context**
- Legal
- Business
- Technological

**Specification**
- Application

**Flow Diagram**
- Risks
- Security Requirements
- Security controls
Certification of Application Security

Demonstrate the effectiveness of security controls

Security Controls in ISO 27034

Security Activities
- What: Use Spring Security and activate X-XSS-Protection HTTP Response Headers
- Where: Implementation phase
- How much: 1 day
- Who: Back office Developer
- How: See code Snippet
- Documentation: https://docs.spring.io/spring-security/site/docs/current/reference/html=headers.html

Risk
Application can be vulnerable to XSS

Source
Technological Context

Required Level Of Trust
HIGH

Verification Process
- What: Create a test case to verify HTTP response header X-XSS-Protection HTTP Response Headers
- Where: Implementation phase
- How: See Code Snippet
- How much: 1 day
- Documentation: https://spring.io/blog/2014/05/23/preview-spring-security-test-web-security
GDPR: From Regulation to coding

Demonstrate the effectiveness of security controls

Privacy Security controls

- Phase Requirement
  - ASC: Privacy Impact Assessment
  - ASC: Cryptography requirements

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

- Phase Implementation
  - ASC: OWASP Top 10
  - ASC: OWASP Privacy Top 10

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

- Phase Release
  - 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

Application Management
Application Supply
Infrastructure Management
Application Audit

Application provisioning management
Application operation management
Application provisioning infrastructure management
Application operation audit
Application operation audit
Application operation audit

Utilization
Archival
Disposal
Disposal
Disposal

Utilization & Maintenance

Operation stages
Provisioning stages

Preparation
Realization
Transition
GDPR: From Regulation to coding

Demonstrate the effectiveness of security controls

Application Security Life Cycle Model (ISO 27034)
Threat modeling technique for privacy (LIDDUN)
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

Detectability: 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.

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.

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

Threat modeling technique for privacy (LIDDUN)

The analyst should create a "personalized" table, based on LIDDUN'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.

<table>
<thead>
<tr>
<th></th>
<th>L</th>
<th>I</th>
<th>N</th>
<th>D</th>
<th>D</th>
<th>U</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entity</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Data store</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Data flow</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Process</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Mapping LIDDUN 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)*

GDPR: From Regulation to coding

Threat modeling technique for privacy (LIDDUN)

Threat modeling technique for privacy (LIDDUN)

Non-repudiation of data flow

Source: https://distrinet.cs.kuleuven.be/software/linddun/nonrepudiation_DF.php
Privacy Framework
Nymity
GDPR: From Regulation to coding

Nymity Privacy Framework
# GDPR: From Regulation to Coding

## Nymity Privacy Framework

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. <strong>Maintain Governance Structure</strong></td>
<td>Ensure that there are individuals responsible for data privacy, accountable management, and management reporting procedures.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. <strong>Maintain Personal Data Inventory and Data Transfer Mechanisms</strong></td>
<td>Maintain an inventory of the location of key personal data storage or personal data flows, including cross-border, with defined classes of personal data.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. <strong>Maintain Internal Data Privacy Policy</strong></td>
<td>Maintain a data privacy policy that meets legal requirements and addresses operational risk and risk of harm to individuals.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. <strong>Embed Data Privacy Into Operations</strong></td>
<td>Maintain operational policies and procedures consistent with the data privacy policy, legal requirements, and operational risk management objectives.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. <strong>Maintain Training and Awareness Program</strong></td>
<td>Provide ongoing training and awareness to promote compliance with the data privacy policy and to mitigate operational risks.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. <strong>Manage Information Security Risk</strong></td>
<td>Maintain an information security program based on legal requirements and ongoing risk assessments.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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.
• 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)

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)

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

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)

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

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

• 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)

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
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 processed by the website.

Basic functionalities
Web Based application
Create a user profile
Subscription fee
Research engine based on a form
Online chat
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
• OWASP Privacy Top 10: https://www.owasp.org/index.php/OWASP_Top_10_Privacy_Risks_Project
• Privacy threat trees catalog: https://distrinet.cs.kuleuven.be/software/linddun/catalog.php