Agenda

• NextDay.Vision
• Key concept
• Data controller, processor
• Principles and rights
• Data transfer vs. regulation
• Privacy shield and cloud act
• Questions?

Related to IT
with sample
Consulting & security awareness
Delegate DPO, CISO, CIO

Masters of Management in Security of Information Systems
HEG, Genève (CH)
Bachelor Degree in IT Engineering
HES Engineering School from Yverdons Les-Bains (CH)

Security and products certifications:
CSH, CEH, ECSA, MCSE, MCSA, MCAD, MCT

Worked for:

Training and certifications
OtpOne Everywhere

Protect files everywhere
Share sensitive files with everyone with a strong protection and identity check

OtpOne Enterprise

Protect files against internal attacks
Strengthen the Windows session
Reinforce the Windows application identity check
GDPR | RGPD | DSGVO

Key concepts
General Data Protection Regulation

Please note: this presentation will only summarize the GDPR, therefore there might be shortcuts
Key concepts

End user → Application

Wordpress | CRM | Google forms |.....

Private data
All types of data without any regulation

Somewhere
Data is stored.....

Somebody
Uses data or sells it...
Key concepts

GDPR VOCABULARY in a simple way:

• **Data subject**: the end user, the center of your GDPR related problem
• **Principles** are related to data protection and data management (expiry).
• **Rights** are related to the end user rights (right to access, etc.)
• The **processor** gets data, adds values, uses data (web form owner, etc.)
• The **controller** doesn’t use data (for himself), and does not add value ... (DC, store, back up, etc.)
• **Security by default**: data is protected without any configuration
• **Security by design**: the application is secured from the start and protects data by default
GDPR | RGPD | DSGVO

Data processor, data controller
Data controller (art. 24, 25, 26, 27)

- Collects data
- Shall implement appropriate technical and organisational measures to protect the private data
- Demonstrates the compliance of processing activities
- Shall answer data subject requests concerning rights
- The compliant controller is at risk of paying a fine of up to 4% of the global yearly turnover

You are the data controller
You are accountable.

I personally use Wordpress to get private data from my members. I am not responsible for the security of the Wordpress cloud I use.

GDPR: You are the controller, you are accountable, you have chosen this provider, this software.

It must be GDPR compliant.
Data processor (art. 28, 29, 30)

- Processes authorized data only
- Processes instruction documented by the controller only
- Does not have the right to engage another processor without the controller’s authorisation
- Should be governed by a contract
- Processors must keep records of data processing

Cloud services like Wordpress online, mail services, etc. are global processors.

A processor can also be a controller if he uses, modifies or adds value to the data.


*It must be GDPR compliant.*
Data controller & data processor

Data Controller

Your Company

Keep consent records
Analyze data
Use for purpose
Redefine purpose
Update decision record

Ask for consent

Data Processor

Software Vendor

Keep record of the decision and pass it over to Controller.
Gather and process subject's data.

Deliver data processing results

Data Subject

Your Website Visitors

Make the decision

Allow or deny

Validate the decision

Picture source: Quora.com
Questions 4 you

• You organize an event...
  .
• The backup is...
GDPR | RGPD | DSGVO

Principles and rights
Principles lawfulness, fairness and transparency

Related to Art. 5:

• Adequate, relevant, limited data, up-to-date
• Kept in a format allowing identification of data subjects for no longer than necessary
• Processed in a manner that ensures appropriate security

PIA = Privacy Impact Assessment
Principles lawfulness, fairness and transparency

Related to Art. 6, 7, 9:

• Users have given their consent to the specific processing (details in art. 7)

Or

• Data is necessary to the performance of a contract to which the data subject is party
• Data is necessary for compliance with legal obligation
• Data is necessary in order to protect the vital interests of the data subject.
Principles: lawfulness, fairness and transparency

Related to art. 7:

- I have read and agree to the terms & conditions and privacy & cookies notice, and understand that your company may contact me about products, services & offers that may be of interest, by email, SMS, phone etc.

NO
- don't bundle consent with agreements
- don't pre-fill tick boxes
- use granular consent options
- always name your organisation
- clearly mention the right to withdraw
- be detailed & specific, avoid ambiguity

I AGREE

Fields marked with an * are required
■ Name

Email

This form collects your [name and email] so that we can add you to our newsletter list for awesome project updates. Check out our privacy policy for the full story on how we protect and manage your submitted data!

☐ I consent to having ACME Inc collect my name and email!

Submit

Picture sources: 1wl.uk and ninjaforms.com
Principles: Purpose limitation

• Data shall be collected for specific, explicit and legitimate purpose.

PIA = Privacy Impact Assessment
Principles: Data minimization

• Data shall be adequate, applicable and restricted to what is necessary.
Principles: Storage limitation

- Data shall be stored in a form which allows identification of data subjects for no longer than is necessary.

For instance, use the database procedure to define archive bytes:

- Date of registration + 1 year = Archive (no direct access)
- Date of registration + 5 years = Delete data (local legal period)
Principles: Integrity and confidentiality

- Data shall be protected against unauthorized or unlawful processing, accidental loss, destruction, manipulation or damage. (art. 32)

Unauthorized access: Granular roles, strong identity check (2nd factor authentication)
Accidental loss: Backup and test restore process
Destruction: Backup, granular roles, strong identity check
Manipulation, damage: Encryption, granular roles, strong identity checks, pseudomization, anonymization

That not really new: Granular roles, strong identity check, backup, encryption
Principles: Accountability

• **The controller will be accountable** and capable of showing compliance.

**Document/register needed:**
- **Record of processing activities**
- Risk assessment & PIA
- Security awareness and training proof
- Nonconformity
- Incidents
- Private data policies (internal, external)

**Design, log & monitor:**
- Access control (role)
- Firewall, WAF, proxy
- System
- Vulnerabilities

---

Excel
Sharepoint
Office365

---

PRTG -> monitoring, logging and alert
Windows System log archive (group policy)
Nessus, openVAS -> test vulnerabilities and create report

.....
Data subject rights

• Of access (what do you know about me?) – art. 15
• Of modify/rectification (correct it) – art. 16
• Of erasure – art. 17
• Of restrictions (ex: oppose erasure, not use) - art. 23
• To object (ex: object against marketing use) – art. 21
• Of portability (ex: data migration, without any standard) – art. 20
Data subject rights

Functions you should have ready on your web application:

• Show all my data (all data, not only account information)
• Export all my data (all data, but no specific format is required)
• Modify my account
• Delete my account and all my data (except legal information)
• Enable, disable specific processing
Data subject rights

No automated decision making – art. 22
• You should define a manual step to make a decision.

To be informed – art. 13

Incident management process and active monitoring will help you when the monitoring alerts you or if you have any suspicion investigating the case, then define if it’s only an event or an incident

In case of incident:
• Inform the data subject as soon as possible
• You have 72 hours to inform the authority
Questions 4 you

• Category, and if is sensitive or not:
  • Birthday
  • Eyes color
  • End user weight
  • Heart rate but only if more as 100

• What is important to have prove your compliance?
GDPR | RGPD | DSGVO
Privacy vs. regulation
Data transfert vs. GDPR

https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde
# Data transfert vs. SWISS regulation

<table>
<thead>
<tr>
<th>Aménée</th>
<th>Niveau adéquat pour des personnes physiques</th>
<th>Niveau adéquat sous certaines conditions</th>
<th>Niveau insuffisant</th>
<th>Remarques</th>
<th>Autorité nationale de protection des données</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td>La loi s’applique également au traitement de données concernant des personnes morales.</td>
<td>Österreichische Datenschutzbehörde Hohenstaufengasse 3 AT-1010 Wien <a href="http://www.dsb.gv.at">www.dsb.gv.at</a></td>
</tr>
<tr>
<td>Autriche</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Azerbaïdjan</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Biélorussie</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Belgique</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bosnie-Herzégovine</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bulgarie</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chypre</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Croatie</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Danemark</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Data transfert vs. SWISS regulation

<table>
<thead>
<tr>
<th>Country</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Costa Rica</td>
<td>X</td>
<td>Les organismes qui adhèrent au Privacy Shield pour les données provenant de Suisse et qui figurent sur la liste du Département américain du commerce garantissent un niveau de protection adéquat au sens de l’art. 6, al. 1, LPD</td>
</tr>
<tr>
<td>Cuba</td>
<td>X</td>
<td>Federal Trade Commission FTC 600 Pennsylvania Avenue NW DC – 25080 Washington</td>
</tr>
<tr>
<td>Dominique</td>
<td>X</td>
<td>Federal Institute of Access to Public Information Av México 151, Col Del Carmen Coyoacán México DF 04100 <a href="http://www.ifai.org.mx">www.ifai.org.mx</a></td>
</tr>
<tr>
<td>Etats-Unis d'Amérique</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Grenade</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Guatemala</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Haiti</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Honduras</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Jamaïque</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Mexique</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Nicaragua</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Panama</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>République dominicaine</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Saint-Christophe-et-</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Nièvres</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sainte-Lucie</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Saint-Vincent-et-</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Grenadines</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

GDPR | RGPD | DSGVO
Privacy shield and cloud act
EU-US - Privacy shield


The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the US (limited to the Privacy Shield framework) as providing adequate protection.

Transborder data flows

The Swiss data protection law guarantees the protection of the private sphere for data processing carried out by persons in Switzerland. However, when data is transmitted abroad, an adequate level of its protection has to be provided for thereabouts.

The current regulations are as follows:

- Transborder data transfers briefly explained (PDF, 246 kB, 27.03.2017)

Certain data transmissions abroad must be announced to the FDPIC. Under certain circumstances, transmission is only allowed after concluding a special agreement. In some countries, transmission is problem-free to a great extent. The following list shows the levels of data protection worldwide:

- List of countries (in French) (PDF, 123 kB, 12.01.2017)
- The Council of Europe’s model contract (PDF, 71 kB, 13.05.2009)
- Guide of the Council of Europe (PDF, 88 kB, 13.05.2009)
- The standard contractual clauses of the European Union

Standard contract for the transborder outsourcing of data processing

https://www.privacyshield.gov/Swiss-US-Privacy-Shield-FAQs
EU - Switzerland - Privacy shield

HOW TO VERIFY AN ORGANIZATION’S PRIVACY SHIELD COMMITMENTS

The Privacy Shield List enables EU or Swiss companies to verify whether data can be transferred to a U.S.-based company under the Framework.

VIEW

CONTRACT REQUIREMENTS FOR DATA TRANSFERS TO A PROCESSOR

Data controllers in the EU and Switzerland are required to enter into a contract when a transfer is made for processing purposes only, regardless of whether the recipient is a Privacy Shield Participant. Under the Privacy Shield, this contract does not require prior approval and need not include standard contractual clauses.

VIEW

https://www.privacyshield.gov/welcome
(ii) Data transfers from Switzerland or the EU to the United States

... MailChimp is responsible for the processing of Personal Information we receive under each Privacy Shield Framework and subsequently transfer to a third party acting as an agent on our behalf. We comply with the Privacy Shield Principles for all onward transfers of Personal Information from the EU and Switzerland, including the onward transfer liability provisions. With respect to Personal Information received or transferred pursuant to the Privacy Shield Frameworks, we are subject to the regulatory enforcement powers of the U.S. Federal Trade Commission. In certain situations, we may be required to disclose Personal Information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.
Cloud act

The Clarifying Lawful Overseas Use of Data Act or CLOUD Act (H.R. 4943) is a United States federal law enacted in 2018.

The CLOUD Act had support of the Department of Justice and of major technology companies like Microsoft, Apple, and Google. The bill was criticized by several civil rights groups, including the Electronic Frontier Foundation, the American Civil Liberties Union, Amnesty International, and Human Rights Watch. These groups argued that the bill stripped away Fourth Amendment rights against unreasonable searches and seizures, since the government could enter into data rights sharing agreements with foreign countries and bypass U.S. courts, and affected users would not have to be notified when such warrants were issued. Some of these groups feared the government would not fully review requests from foreign countries for their citizens stored on servers in the U.S., potentially allowing such data to be used in bad faith in those countries.

https://en.wikipedia.org/wiki/CLOUD_Act
Questions 4 you

• What if I use a US Wordpress in the cloud service:
  • Do I need a contract?
  • Can a US policeman ask to access members private data without inform the end user? Is a judge required?

• What if I use a Wordpress in the cloud in Africa:
  • Do I need a contract?
  • Can a African policeman ask to access members private data without inform the end user? Is a judge required?
Do you need to have DPO on board?

- **Art 37:**
  - Large scale
  - Volume of data
  - The duration of permanency of the data
  - The geographical extension of the data
  - Type of data

- **WP27** guideline will help you to better understand the article 37 and the DPO role and attribution.

GDPR | RGPD | DSGVO
QUESTIONS

Philippe.kapfer@NextDay.Vision