Expected Legislative Impacts of GDPR and NIS

GDPR & NIS: Impacts since May 2018

Gerald.Quirchmayr@univie.ac.at
New legislation coming into effect (mainly) in 2018

• The legislation
  – The virtually unrecognized e-Privacy Directive is still being drafted now
Expected Legislative Impacts of GDPR and NIS

New legislation coming into effect (mainly) in 2018

- Status of preparedness
  - Who is aware of this legislation?
  - Who is still getting prepared for it?
  - Who has already tested the compliance of their current and future ICT systems?
  - What is the status of national legislation in EU Member States?
    - GDPR
    - NIS
Coping with the new legislation

- How far advanced are we?
  - Government institutions generally doing fine
  - Big companies (have) put in a lot of resources
  - SMEs are still worrying, some of them only now realizing their exposure and their critical role in the supply chain
Coping with the new legislation

- How far advanced are we?
  - Government institutions generally doing fine
  - Big companies (have) put in a lot of resources
  - SMEs are still worrying

- Where major trouble is expected to arise
  - Software development
  - Outsourcing SLAs – need to adapt
  - International supply chains
  - International service providers doing business in Europe
GDPR revisited
• Chapter 1 – General provisions
• Chapter 2 – Principles
• Chapter 3 – Rights of the data subject
• Chapter 4 – Controller and processor
• Chapter 5 – Transfers of personal data to third countries or international organisations
• Chapter 6 – Independent supervisory authorities
• Chapter 7 – Cooperation and consistency
• Chapter 8 – Remedies, liability and penalties
• Chapter 9 – Provisions relating to specific processing situations
• Chapter 10 – Delegated acts and implementing acts
• Chapter 11 – Final provisions
Expected Legislative Impacts of GDPR and NIS

GDPR Focus Areas

• Technological and organisational challenges
  – Right of data portability
  – Right to be forgotten
  – Privacy by default
  – Privacy by design
  – Risk-based approach
  – Effectiveness of security mechanisms in place to be monitored and controlled

• Procedural obligations
  – Keeping a registry of personal data processing
  – Data breach notification to the authority and / or the affected persons

• Penalties that finally hurt
  – Will they ever be imposed?
  – When will we see the first cases in court?
Conclusions drawn so far

• Those who have always done a good job in handling incidents are also doing it now.
• SMEs are pretty worried about cost and resourcing.
1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the varying likelihood and severity of risks to the rights and freedoms of natural persons and the nature of the personal data, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

a) the \textbf{pseudonymisation} and \textbf{encryption} of personal data;

b) the \textbf{ability to ensure} the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c) the \textbf{ability to restore} the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d) \textbf{a process for regularly} testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

\textbf{Requirements being pushed down the supply chain?}
2. In assessing the appropriate level of security, due account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

- Risk-oriented thinking forces to rethink some ways of doing things!
1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.
LLOYD'S
Emerging Risks Report 2017 - Technology

- Modelled scenarios
  - Cloud service provider hack
  - Mass vulnerability attack
Expected Legislative Impacts of GDPR and NIS

The house of cards model in detail...

Just remove one card....
The direct economic impacts of cyber events lead to a wide range of potential economic losses. For the cloud service disruption scenario in the report, these losses range from US$4.6 billion for a large event to US$53 billion for an extreme event; in the mass software vulnerability scenario, the losses range from US$9.7 billion for a large event to US$28.7 billion for an extreme event.

Economic losses could be much lower or higher than the average in the scenarios because of the uncertainty around cyber aggregation. For example, while average losses in the cloud service disruption scenario are US$53.1 billion for an extreme event, they could be as high as US$121.4 billion or as low as US$15.6 billion, depending on factors such as the different organisations involved and how long the cloud-service disruption lasts for.
Impact on software development

- Extended requirements catalogues
- Privacy impact analysis becomes mandatory as basis for risk estimation
- Documentation of personal data flows becomes mandatory
- Requirements engineering needs to take new legal obligations into account
- New testing requirements need to be introduced
- New standardized libraries will hopefully be developed to cover the new needed functionalities → a new vast playground for the open source community?

Documentation becomes a (legally important) asset.
Impact on supply chain management

- Pushing obligations down the supply chain will again put high demands on suppliers.
- Integrated control mechanisms along the supply chain will become necessary to allow for a continuous risk management process.
- Data breach notification along the supply chain will create new challenges.
- Technology and organisational concepts will have to support each other if legal compliance is to be achieved.

*Are we finally going towards integrated IT / systems planning?*
Impact on outsourcing

- Transfer of personal data outside Europe will become an even more important aspect.
- Chains of service providers in the form of (sub) contracting will create serious challenges.
- Risk estimation will be substantially more challenging in an outsourcing chain.
- Data breach notification processes will have to be developed across the outsourcing chain.
- Remote services of all kinds will have to be reviewed.
- Remote access mechanisms and interconnected systems will have to be assessed regarding the risk they cause for privacy.
- Personnel vetting will have to adhere to much higher standards than now.
Expected Legislative Impacts of GDPR and NIS

What can we expect? A brief reality check from ABC Australia.
Even shorter look at NIS
Article 7

Computer Emergency Response Team

1. Each Member State shall set up a Computer Emergency Response Team (hereinafter: "CERT") responsible for handling incidents and risks according to a well-defined process, which shall comply with the requirements set out in point (1) of Annex I. A CERT may be established within the competent authority.

2. Member States shall ensure that CERTs have adequate technical, financial and human resources to effectively carry out their tasks set out in point (2) of Annex I.

3. Member States shall ensure that CERTs rely on a secure and resilient communication and information infrastructure at national level, which shall be compatible and interoperable with the secure information-sharing system referred to in Article 9.

4. Member States shall inform the Commission about the resources and mandate as well as the incident handling process of the CERTs.

5. The CERT shall act under the supervision of the competent authority, which shall regularly review the adequacy of its resources, its mandate and the effectiveness of its incident-handling process.
Article 9

Secure information-sharing system

1. The exchange of sensitive and confidential information within the cooperation network shall take place through a secure infrastructure.

2. The Commission shall be empowered to adopt delegated acts in accordance with Article 18 concerning the definition of the criteria to be fulfilled for a Member State to be authorized to participate to the secure information-sharing system, regarding:
   - the availability of a secure and resilient communication and information infrastructure at national level, compatible and interoperable with the secure infrastructure of the cooperation network in compliance with Article 7(3), and
   - the existence of adequate technical, financial and human resources and processes for their competent authority and CERT allowing an effective, efficient and secure participation in the secure information-sharing system under Article 6(3), Article 7(2) and Article 7(3).

3. The Commission shall adopt, by means of implementing acts, decisions on the access of the Member States to this secure infrastructure, pursuant to the criteria referred to in paragraph 2 and 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 19(3).
Article 10

Early warnings

1. The competent authorities or the Commission shall provide early warnings within the cooperation network on those risks and incidents that fulfil at least one of the following conditions:
   - they grow rapidly or may grow rapidly in scale;
   - they exceed or may exceed national response capacity;
   - they affect or may affect more than one Member State.

2. In the early warnings, the competent authorities and the Commission shall communicate any relevant information in their possession that may be useful for assessing the risk or incident.

3. At the request of a Member State, or on its own initiative, the Commission may request a Member State to provide any relevant information on a specific risk or incident.

4. Where the risk or incident subject to an early warning is of a suspected criminal nature, the competent authorities or the Commission shall inform the European Cybercrime Centre within Europol.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 18, concerning the further specification of the risks and incidents triggering early warning referred to in paragraph 1.
Article 11
Coordinated response

1. Following an early warning referred to in Article 10 the competent authorities shall, after assessing the relevant information, agree on a coordinated response in accordance with the Union NIS cooperation plan referred to in Article 12.

2. The various measures adopted at national level as a result of the coordinated response shall be communicated to the cooperation network.
Article 14

Security requirements and incident notification

1. Member States shall ensure that public administrations and market operators take appropriate technical and organisational measures to manage the risks posed to the security of the networks and information systems which they control and use in their operations. Having regard to the state of the art, these measures shall guarantee a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimise the impact of incidents affecting their network and information system on the core services they provide and thus ensure the continuity of the services underpinned by those networks and information systems.

2. Member States shall ensure that public administrations and market operators notify to the competent authority incidents having a significant impact on the security of the core services they provide.

3. The requirements under paragraphs 1 and 2 apply to all market operators providing services within the European Union.
Article 14

Security requirements and incident notification

4. The competent authority may inform the public, or require the public administrations and market operators to do so, where it determines that disclosure of the incident is in the public interest. Once a year, the competent authority shall submit a summary report to the cooperation network on the notifications received and the action taken in accordance with this paragraph.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 18 concerning the definition of circumstances in which public administrations and market operators are required to notify incidents.

6. Subject to any delegated act adopted under paragraph 5, the competent authorities may adopt guidelines and, where necessary, issue instructions concerning the circumstances in which public administrations and market operators are required to notify incidents.
7. The Commission shall be empowered to define, by means of implementing acts, the formats and procedures applicable for the purpose of paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 19(3).

Some Questions

• Which enterprises count as critical infrastructure?
• How will resulting obligations be met in supply chain networks?
• Can NIS obligations be addressed in combination with GDPR obligations in on clean-up?

• Are the time lines of affected enterprises realistic?
• Do they put in the necessary resources?
Delayed introduction on the national level (NIS)

Watering down of the legislation (GDPR)

... due to an initial underestimation of the (commercial) consequences ...
A puzzle finally fitting together?

Just what we would need!