RSAConference2018

San Francisco | April 16 – 20 | Moscone Center

SESSION ID: SEM-M01

TEN PITFALLS TO AVOID IN GDPR

FREDDY DEZEURE

Next Month

- 25 May 2018 –>
- Protection of personal data in e-society
- Single legal basis for all 28 (27) Member States
- Regulation –> no enabling legislation needed
- Adaptations in national law may be made

10 Pitfalls to Avoid

1. Wait and see
2. Fix and forget
3. Your DPO
4. It can’t be that bad
5. Let’s patch
6. I have consent
7. Transfer
8. I need consent
9. Forget from logs
10. Pseudonymise?

1. Wait And See

Art. 24: Implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Measures shall be reviewed and updated where necessary.

- You have to comply by May 2018
- You have to be able to demonstrate compliance by May 2018
- You have to continue to comply over time

Identify why you collect and process personal data, how much, how you keep them up to date, how long and how you protect them.

- Document and maintain the documentation.

Collect and determine the purpose later?

Recital 50: “Processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected”

2. Fix and Forget

This is not a fluke, to be resolved in 2018

GDPR is here to stay

Your applications (hopefully) are here to stay

They will evolve

There will be more

Your users and the DPA may want more

Prepare for the long run, put a framework in place and build internal competence

3. Your DPO

- You have to provide sufficient resources and autonomy
- Avoid conflict of interest with the business / IT
- If possible, internalize this competence
- Possible to combine with CISO/CSO
- The responsibility remains top level

4. It Can't Be That Bad

- Personal data breach ***or*** a complaint by a subject

- Notification to the DPA, by the **controller,** within 72 hours after the controller becomes aware and ***if*** there *is a risk*
- If high risk: communication to data subjects, **coordinated** with DPA

Possible consequences:

- Administrative fine up to 4% or 20mio€
- Victim damage compensation
- Potentially criminal prosecution

5. Let's Patch

Data protection should not be an afterthought

Art. 25&32: Data protection by design and by default.

Controller takes appropriate technical and organizational measures both at the time of the determination of the means for processing and at the time of the processing itself.

Measures to comply take into account the state of the art, the cost, the type of processing and the risk.

Special case: cloud infrastructure

Is completely within scope.

All GDPR compliance aspects are applicable and the controller is accountable.

6. I Have Consent

Accept processing of data for all purposes, including transfer to third parties? Consent was given to a third party, which transferred the data to you?

The performance of a contract is conditional on consent to processing of personal data not necessary for the performance of that contract?

Consent in an intelligible and easily accessible form, using clear and plain language, not containing unfair terms.

The processing is necessary for the purpose.

Every organization in the chain complies.

7. Someone else is doing it for me

Processor: Art. 28

Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

8. I Need Consent

Six lawful grounds. Read beyond a.

a. Consent
b. Necessary for a contract
c. Compliance with a legal obligation
d. Vital interests of a person
e. Task in the public interest
f. Legitimate interest
   - Recital 47, 49

Recital 47

Legitimate interest **may** provide a legal basis

- Data subject is a client or an employee
- Processing strictly necessary for the prevention of fraud
- Processing for direct marketing purposes

If reasonably expected by the data subject

Recital 49

- Processing of personal data to ***the extent strictly necessary and proportionate*** for the ***purposes of ensuring network and information security*** … constitutes a ***legitimate interest***.
- No need for consent of the data subjects.
- Purpose of the processing and its justification should be documented
- Precautions are needed to ***for other purposes***.

9. Forget From Logs?

Article 17 : “Right to erasure ('right to be forgotten')”

(1)The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a)The data are no longer necessary for the purpose
(b)Withdrawal of consent
(c) …
(d) The data was unlawfully processed
(e) …
(f) …

These conditions would very likely not apply for your security logs.

10. Pseudonymise?

Article 32 : "Security of processing"

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 risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security **appropriate** to the risk, including as appropriate:

a) the pseudonymisation and encryption of personal data (...)

=> It depends...

The Risk Of Logs

Logs could be exposed to

- Third parties – by breaches
- Internal access for other purposes – illegitimate use
- Internal access by security staff – illegitimate use

-> Store the logs in a secure manner

-> Restrict access, also internally

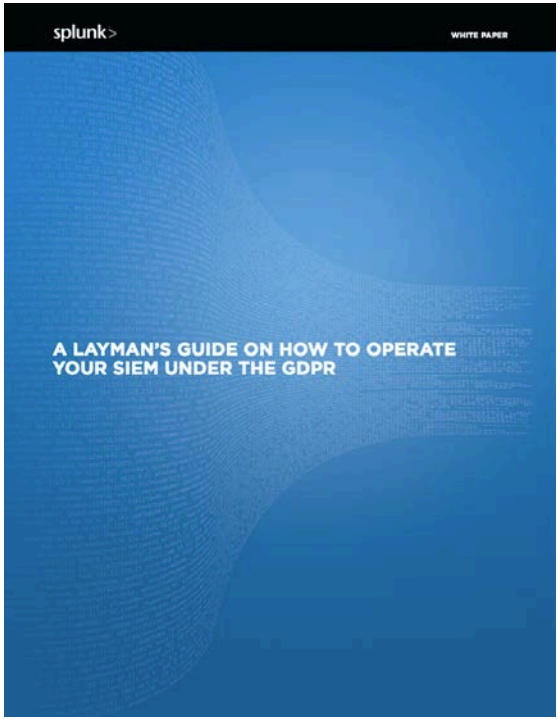
-> Additional mitigation of risk by pseudonymisation

- In case the risk is considered high
- Access to combined information only when needed for incident response
- Based on four-eye principle

Logs: A GDPR Opportunity

- Monitor to ensure the security of the processing (compliance, certification)
  - Include cloud infrastructure!
- Prevent breaches by monitoring logs
- Provide **early** alert to a personal data breach
- Mitigate the risk by rapid incident response
- Assess the nature and impact of a breach
  - Which and how much data was impacted ?
  - Since when ?
  - What is the risk ?

More On GDPR And Your SIEM



Take Away

- GDPR is also for you
- GDPR is not necessarily a problem for you
- GDPR could be an opportunity for you
- It’s a culture, not a process

Apply What You Have Learned Today

Next week you should:

- Identify the existing GDPR plan within your organization

In the first three months following this presentation you should:

- Understand how the GDPR impacts your NIS operations
- Document your processes

Within six months you should:

- Understand how your NIS operations can foster the GDPR compliance of your organisation
- Fine-tune your systems/processes in order to maximize their impact
- Document the added value

Thank You

Don’t Hide The Risk, Manage It

FreddyDezeure.eu