GDPR and You

February 2018

About Me

- Consultancy
  - Trusted Strategic Advisor
  - Board Member EclecticIQ
  - Advisor SpyCloud, Intel471, Phantom Cyber
- Thirty years at the European Commission
  - Head of CERT-EU
  - COO, CRO at the Joint Research Centre (3000 scientists)
  - Internal and external audit
- Five years as CIO in private industry

GDPR Scope

Any information relating to an ***identified*** or ***identifiable natural*** person

- IP, DNA, fingerprint, credit card, username, address, email address, phone number…

- Processed by an ***establishment in the EU***
- Or related to ***data subjects in the EU***
- Or related to ***behavior taking place in the EU***

- ***Even if at no cost***

Roles

Controller

- A **Controller** is the natural or legal person who determines the purpose and means of the processing of personal data

Processor

- A **Processor** is a natural or legal person that processes personal data on behalf of a controller. The Controller remains responsible to make sure the processor applies the relevant measures to comply

Responsibilities

- Controllers and Processors need to **maintain a record of their processing activities** and **be able to demonstrate compliance**

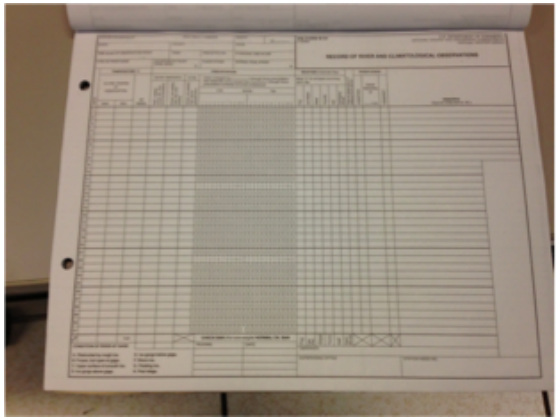
General Principles

- Processing should be ***lawful, fair and transparent***.
- Collected for ***specific, explicit and legitimate purpose***.
- ***Adequate, relevant and limited*** to what is necessary for the purpose.
- ***Accurate***
- ***Not kept longer than necessary for the purpose***.
- Processed in a manner that ensures ***security and confidentiality***.

Controller is responsible for and has to be able to demonstrate compliance with these principles (“accountability”)

What Does This Mean?

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



Document all this and have processes in place to maintain and update the documentation.

Data Subject Rights

- Data subjects have a right of **access, rectification, transfer, removal**

- And the right not to be subjected to automated decision-making (profiling).

Breach Impact

- Consequence of a personal data breach ***or*** a complaint by a subject

- Notification within 72 hours to supervisory authority ***if*** there *is a risk*
- If high risk: communication to data subjects, coordinated with supervisor

Possible consequences:
- Administrative fine up to 4% of world-wide annual turnover
- Victim damage compensation
- Criminal prosecution

Waiver
- The controller or processor should be exempt from liability if it proves that it is not in any way responsible for the damage.

Mitigation

Measures to comply take into account the risk;

- In case of high risk -> perform an impact assessment (PIA) to determine appropriate mitigation measures;
- Appropriate technical and organisational measures, taking into account the state of the art
  - Pseudonymise & encrypt;
  - Ensure confidentiality, integrity, availability and resilience of processing systems
  - Backup & restore;
  - Test effectiveness.

Specific Risks 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

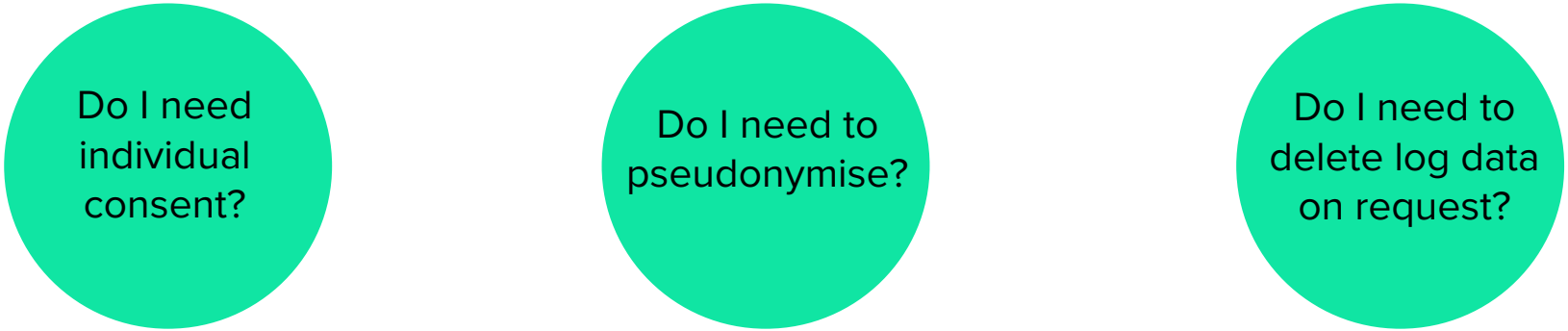
-> Restrict access, also internally

-> 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

Storing and analysing log data in compliance with the GDPR

Frequently Asked Questions



Read Beyond (a)

Article 6 spells out six lawful grounds:

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

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 ***avoid use for other purposes***.

Pseudonymise?

Article 32 : "Security of processing"

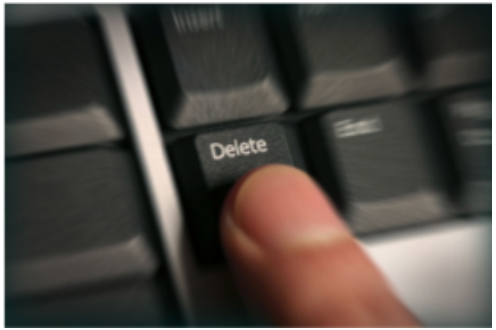
1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical 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...

Delete?

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) …

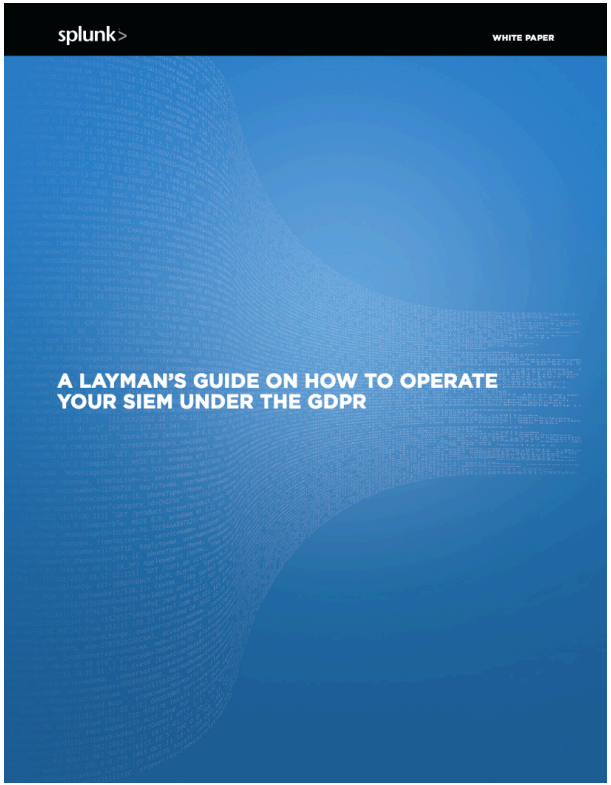
These conditions would very likely not apply for your Network and Information Security logs.

“An IP address is personal data – this doesn’t mean there is a problem”

Logs as Opportunity

- Demonstrate compliance, including by certification
- Monitor the measures to ensure the security of the processing
- 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


splunk>
WHITE PAPER
A LAYMAN'S GUIDE ON HOW TO OPERATE YOUR SIEM UNDER THE GDPR

Take Aways

- GDPR is also for you
- GDPR is not necessarily a problem for you
- GDPR could be an opportunity for you
- Prepare well for May 2018

Thank You

Don’t Hide The Risk, Manage It

freddy.dezeure@gmail.com
dezeuref@gmx.com
freddy.dezeure@protonmail.com