A Brief Overview of GDPR

6th SIG-NOC Meeting

Nicole Harris

Head of Trust and Identity Operations

Utrecht, Netherlands

27th November 2017

When and Who

Comes into effect on 25th May 2018

Impacts pretty much everyone as covers controllers and processors “in the Union” and data subjects “in the Union” (Recitals 22 and 23)

Directive to Regulation

Directive = each Member State can interpret differently

Regulation = required to be implemented as is in all Member States
(but interpretation is still happening)

Main Change?

TO

Why?

It’s OK to Process Personal Data!

“seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and **to ensure the free flow of personal data between Member States**.”
(Recital 3)

And…it’s only about PERSONAL data

That Pesky IP thing

"Natural persons **may be associated** with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them." (Recital 30)

"unauthorised **reversal** of pseudonymisation" (Recital 75)

"'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such **additional information is kept separately** and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person" (Definitions, Article 4)

Technology is Mentioned as Good!

DATA PROTECTION BY DESIGN

Encryption

- Mitigates breaches, (recital 83, articles 62 + 32)

Pseudonymisation

- Reduces risks (many places)

Training / Exercises

- Tests Readiness (many places)

Lawful Reasons to Process

CONSENT	•The data subject has unambiguously given their consent.
CONTRACTUAL	•Processing is necessary for the performance of a contract to which the data subject is party.
LEGAL OBLIGATION	•Processing is necessary for compliance with a legal obligation to which the data controller is subject.
VITAL INTEREST	•Processing is necessary in order to protect the vital interests of the data subject.
PUBLIC INTEREST	•Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed.
LEGITIMATE INTEREST	•Processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by the third party or parties to whom the data are disclosed.

7 Step Assessment for Legitimate Interests (from REFEDS)

STEP ONE

- Check that Legitimate Interests is the best approach.

STEP TWO

- Qualify the legitimacy of the request – lawful, clearly articulated, real need.

STEP THREE

- Determine whether the processing is necessary to achieve the goal.

7 Step Assessment for Legitimate Interests

STEP FOUR

- Balance the data controller's needs against the interests of the subjects.

STEP FIVE

- Identity safeguards you can put in place (tech design etc).

STEP SIX

- Demonstrate (publish) compliancy.

STEP SEVEN

- Allow the user to opt-out.

Consent

Consent should be given by a clear **affirmative** act establishing a **freely given**, specific, informed and unambiguous indication of a data subject's agreement.
(Recital 32)

Network and Information Security

"The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems. "

(Recital 49)

Retention Periods

- You must define a retention period – who wants to keep forever?
- Pseudonymise / anonymise for statistical reasons.
- Ticketing example:
  - When ticket is live: you have legitimate interests in the full contact details and other personal information.
  - When it is still of interest for statistical reasons - delete / mask individual data.
  - When it is still of interest for trends – keep minimum information about type of issue / possibly org name.
  - When is non of the information of interest?

Breaches

All Breaches	• You must document all breaches
Risks to Rights and Freedoms of Individuals	• Must report to Data Protection Authority within 72 hours
High Risks to Rights and Freedoms	• Must also inform individual (unless mitigated)

What to do?

- Take a risk based approach – where are you really exposed and what are the real implications?
- Use legitimate interests.
- Do a brief review on your processes.
- Write down what you do and WHY you do it
- Use privacy notices - make sure your org has at least one you can reference.
- Don’t panic.

Questions

- **How much explicit permission do we need to take & hold netflow logs?**
  - You don’t – see legitimate interests. Consider retention period.
- **How much explicit permission do we need to take & hold eduroam logs?**
  - You don’t – see legitimate interests. Also, eduroam will provide advice.
- **Can we hold any client staff contact information without explicit permission?**
  - Run that through the 7 step plan.
- **I have a phone number for a client that they haven't explicitly given as an official number.**
  - Run that through the 7 step plan.
- **Their link is down, landline not answering, can I use that number?**
  - I would – the risks of the incident are higher than the needs of the individual.
- **Just how paranoid do we need to be?**
  - Just because you are paranoid, doesn’t mean they aren’t out to get you!

Questions

- **Measurement Lab network – can we participate?**
  - Do you have a contract / agreement with them?
  - Do you pass personal data?
  - Run through risk assessment.

Thank you

Any Questions?

nicole.harris@geant.org

GÉANT

Networks · Services · People

www.geant.org