RIPE NCC
RIPE NETWORK COORDINATION CENTRE

GDPR 101 - A Practical Guide

Maria Stafyla
Legal Counsel
RIPE NCC

Maria Stafyla| 06 July 2018| GRNOG

GDPR In A Nutshell

- New law
- Governs the protection of **personal data**
- Describes the **rights of individuals**
- **Obligations** of the responsible parties
- Came into force on 25 May, 2018
- Repealed the EU Data Protection Directive

Basic Information

- Who does the GDPR apply to?
  - natural persons who are in the European Union
- What information does the GDPR apply to?
  - ‘personal data’
  - ‘special categories of personal data’
- Who has to comply with the GDPR?
  - ‘controllers’
  - ‘processors’

GDPR New Elements

- Territorial Scope
- Penalties
- Data breach notification obligation
- Strengthened data subject rights
- Privacy by design
- Data protection officer
- Records of processing activities

Applying the GDPR

The RIPE NCC Approach

First Questions We Answered (1)

- What data do we process?
  - Identified processes, services and tools where personal data is involved
  - Classified the various data sets depending on their criticality and sensitivity
  - Created catalogues of data sets, services and processes
- Evaluation of legal obligations based on our data mapping and inventory

First Questions We Answered (2)

- Does this data help us identify an individual?
- If yes, the GDPR applies!

Seven Principles

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Data accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

Six Legal Grounds

- **Consent**
- …necessary for the **performance of a contract**
- …necessary for compliance with **a legal obligation**
- …necessary to protect the **vital interests of the data subject**
- ..performance of a task carried out **in the public interest**
- …necessary for the purposes of the **legitimate interest** pursued by the controller or by a third party

GDPR in Data Lifecycle

Collection, Processing, Disposal

Data Processing Lifecycle - Step 1

- Data collection:
  - What data do we need?
  - For what reasons?
  - Do we need all this data or the purpose can be fulfilled with less?
  - Who provides us with this data?
  - Is there a valid legal ground for this processing?

Data Processing Lifecycle - Step 2

- Data processing:
  - For how long do we need the data?
  - Do we process the data for purposes other than the initial ones?
  - Do we share the data internally and/or with other organisations? If yes, for what reasons?
  - Where do we process the data?
  - Have we implemented sufficient technical and organisational measures ensuring security of the data?

Data Processing Lifecycle - Step 3

- Data Disposal:
  - When is the data no longer needed?
  - How do we dispose the data?
  - Do we delete and/or anonymise it?

Other Obligations

Some Examples of How We Prepared

Demonstrate Accountability

- Informed and documented decisions about our processing activities
- Information to the individuals
  - clear and transparent information
  - easy and plain language
  - easily accessible
- Maintaining our documentation

Data Subject Requests

- Right of individuals to be informed, get access, have their data rectified, erased etc.
- Procedures on how to treat these requests:
  - How do we recognise a valid request?
  - Is the requested information personal data?
  - What are the technical steps to be taken in order to comply with this request?

Data Breach Notification Obligation

- Obligation to notify the supervisory authority of a personal data breach within 72 hours
- Our procedure describes:
  - necessary steps for internal coordination
  - how to decide when the authorities must be notified of a data breach and what the notification requirements are
  - when it is necessary to inform the individuals too
- Kept our colleagues up-to-date
- Raised awareness

Records of Processing Activities

- Obligation of controllers and processors to maintain a record of their processing activities, unless derogation applies
- How we set up our records:
  - based on our data mapping and inventory
  - listed our (personal data) processing activities
  - filled out the rest information as required by law
  - procedure on how to maintain it

References

- GDPR and the RIPE NCC:
  - https://www.ripe.net/about-us/legal/corporate-governance/gdpr-and-the-ripe-ncc
- European Data Protection Board:
  - https://edpb.europa.eu/edpb_en
- Art.29 WP archived news:
  - ec.europa.eu/newsroom/article29/news-overview.cfm

Questions

mstafyla@ripe.net