RIPE NCC
RIPE NETWORK COORDINATION CENTRE

GDPR Explained

Serge Radovcic
Chief Communications Officer
RIPE NCC

December 2018 | Government Roundtable Riyadh

The Road to GDPR

The RIPE NCC and Data Protection

- **We collect and publish *personal data***
- **The registration authority for Internet number resources in our service region (76 countries)**
  - Operating the **publicly-available** RIPE Database
  - Maintaining **non public** registration information
- **We have important role in the operation of the Internet (globally)**
  - Accountability and clear governance procedures are vital!

Data Protection at the RIPE NCC

- **We were already governed by the EU Data Protection Directive (1995) which was incorporated into Dutch Law**
- **In 2006 the RIPE Community established the Data Protection Task Force (DPTF)**
  - Recommended steps to ensure full compliance of the Directive
  - The DPTF developed procedures and a legal framework for the RIPE NCC
- **Data Protection Report**
  - https://www.ripe.net/about-us/legal/ripe-ncc-data-protection-report

Involvement in Legislative Discussions

- **2009: EU public consultation on the legal framework for the fundamental right of the protection of personal data**
- **We submitted an opinion:**

  “[…]

  *The RIPE NCC considers that personal data related to the operators of the Internet should be **easily available** to each other, **both inside and outside the EU**, in order for those individuals to be able to contact one another to coordinate the **proper functioning of the Internet around the world**.*

  […]”

GDPR

General Data Protection Regulation

- Adopted in April 2016
- Replaces the EU Data Protection Directive
- Became applicable on 25 May 2018

GDPR: The Basics

- **Who does it offer protection to?**
  - Natural persons who are in the EU
  - ***Any citizen*** whose personal data is processed by an organisation established in the EU
- **What information does it cover?**
  - ‘Personal data’ (name, email address, phone number, ID numbers, photos, videos, etc.)
- **Who has to comply?**
  - ‘Controllers’, ’Processors’ established in EU or those doing business with individuals residing in the EU

GDPR at the RIPE NCC

Our preparations for the GDPR

- **A good opportunity for a general review of all data sets processed by the RIPE NCC**
- **March 2017: internal project team established**
  - Review all personal data processed by the RIPE NCC
  - Project team consists of two legal counsels and two security officers
  - Supported by staff throughout the organisation
  - Engagement with external legal counsels and industry partners
  - Communication and consultations with RIPE community

Our preparations for the GDPR

- **Catalogue of all data sets processed by the RIPE NCC**
- **Reviewed our compliance with GDPR**
- **Main areas of focus:**
  - RIPE Database
  - Retention of personal data
  - Internal processing of personal data
  - Other RIPE NCC services

The RIPE Database

- **The purpose described in Article 3 of the RIPE Database Terms and Conditions**
  - *“Facilitating coordination between network operators (network problem resolution, outage notification etc)”*
  - Established by the RIPE Community and the Data Protection Task Force
- **For this purpose, it is crucial to have publicly-available contact information of individuals**
  - Such as in the event of a cyber attack - requires quick contact between operators with no direct (business) relations

Retention of Personal Data

- **We carefully reviewed the purpose of every data set**
- **Focus on RIPE Registry data**
  - Information about old non-publicly available personal data
  - Registry role similar to Land Register
  - Historic information important to resolve potential future disputes over registration of Internet number resources

Internal Processing of Personal Data

- **Review of internal policies, including:**
  - Who is authorised to have access to data
  - How personal data is stored (security aspects)
  - Ensuring that we are fully GDPR compliant

Other RIPE NCC Services

- RIPE Atlas
- Meeting registration
- Websites operated by the RIPE NCC
- Mailing lists
- And more…

Further details

- **Series of RIPE Labs articles describing the GDPR preparations**
  - https://labs.ripe.net/gdpr
- **RIPE NCC webpages dedicated to GDPR**
  - https://www.ripe.net/about-us/legal/corporate-governance/gdpr-and-the-ripe-ncc

GDPR: What’s New?

Increased Territorial Scope (1)

- **Applicable to controllers/processors established in the EU**
- **And controllers/processors that are not established in the EU, if they:**
  - Offer goods/services to data subjects in the EU, *or*
  - Monitor the behaviour (e.g. for marketing purposes) of data subjects who are in the EU
  - They **must** also **comply** => Extra-territorial effect

Increased Territorial Scope (2)

- **Obligation to comply with GDPR**
- **Among other things, obligation to appoint a legal *representative* based in the EU**
- **Unless an exception applies:**
  - a) Processing is occasional and it does **not** involve special categories of personal data (e.g. health data, etc.)
  - b) They are a ***public authority or body***
- **The representative offers a European-facing point of contact for individuals and local data protection authorities**

Data Protection Officer (DPO)

- **Obligation in certain cases, such as:**
  - Public authority or body
  - Large scale amounts of personal Data
- **This also applies to controllers and processors not established in the EU**
- **NOTE: this is a Different role than of the EU *representative***
  - The same DPO can be used for several bodies
  - The DPO must have expert knowledge of data protection
  - Contact details of DPO must be published

Data Subject Rights

- **Strengthened rights for individuals**
- **Non-exhaustive list:**
  - Right to be informed (how it will be used)
  - Right of access to someone’s data
  - Right to be forgotten
  - Right to data portability

Data Breach Notification Obligation

- **Obligation to notify personal data breaches to:**
  - Local supervisory authority **within 72 hours**
  - The data subject - only if the breach involves a **high risk** for them
- **Not every breach requires notification**
- **Risk assessment is required**

Privacy by Design

- **Data protection principles embedded into business processes from the design state**
  - From day one of design
  - Only collecting data that is needed
  - And how is the data stored and deleted?
- **Not a new concept, but first time as a legal requirement**
- **Certification mechanisms can help to demonstrate compliance (e.g. ISO)**

Penalties

- **Right of data protection authorities to impose administrative fines in case of infringements**
- **Decision based on the circumstances and various other factors**
- **Depending on the type of infringement, fines may vary**
  - Up to 20 Million EUR or up to 4% of annual global turnover
- **Not the only available repercussion**
  - e.g. warnings, force to comply

Questions

Serge Radovcic
sr@ripe.net