RIPE Database and GDPR Compliance

RIPE80 Lighting Talk, May 14, 2020

Michael "MiKa" Kafka, NetCaT
Ing. Dr. iur. Christof Tschohl, Research Institute – Digital Human Rights Center

RIPE Database:

- Accessible via web, whois, rdap (no authentication, authorisation)
- RIPE Database contains objects:
  - Internet resources (Addresses, ASnums etc..)
  - Organisations, Persons, Role, IRT (contact info, PII)
- Governed by mature and robust data protection and privacy policies
- **This talk is about:**
- PII (personally identifiable information) in objects and attributes **not sufficiently covered by data protection and privacy policies**

Storytime

- New business access
- My PII published without consent

```
-r -T inetnum 91▮▮▮▮▮▮▮▮
% Note: this output has been filtered.
%        To receive output for a database update, use the "-B" flag.

% Information related to '91.▮▮▮▮ - 91.▮▮▮▮'

% Abuse contact for '91.▮▮▮ - 91.▮▮▮ is 'abuse▮▮▮▮

inetnum:        91.▮▮▮▮ - 91.▮▮▮▮
netname:        KAFKAMICHAEL▮▮▮▮▮▮▮
descr:          Michael Kafka
descr:          ▮▮▮▮▮strasse
descr:          1230 Wien
country:        AT
status:         ASSIGNED PA
mnt-by:         ▮▮▮▮-MNT
mnt-lower:      ▮▮▮▮-MNT
created:        2020-02-▮▮▮▮
last-modified:  2020-02-▮▮▮▮
source:         RIPE

% This query was served by the RIPE Database Query Service version 1.97.1 (HER
```
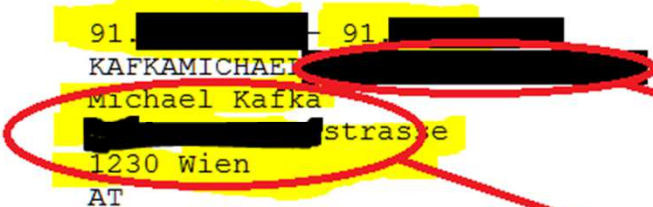
Suffix of netname: references a historic service-name from ISP

Full PII in descr:

Storytime

- Complained to ISP

- Was updated quickly (about 30 min)

Storytime

- RIPE DB history still displays old ("deleted") Info
- History out of direct control from my ISP

```
--show-version 1 91.██████████
% Version 1 of object "91.███████ - 91.████████"
% This version was a UPDATE operation on 2020-02-0████████
% You can use "--list-versions" to get a list of versions for an object.

inetnum:        91.███████ - 91.█████████
netname:        KAFKAMICHAEL-
descr:          Michael Kafka
descr:          ██████████████strasse
descr:          1230 Wien
country:        AT
status:         ASSIGNED PA
mnt-by:         █████████-MNT
mnt-lower:      █████████-MNT
created:        2020-02-05████████
last-modified:  2020-02-05████████
source:         RIPE

% This query was served by the RIPE Database Query Service version 1.97.1
```

Not only my ISP

- Asked friends with business access, similar picture

- Quick search shows lot of inetnums:
  - PII of customers in descr: attribute (not governed by privacy policies):
    - Statically assigned IP (together with name is PII according to GDPR)
    - Full name (natural person without any hint to a company)
    - Often street address
    - Commonly city and ZIP code
  - Several countries (.at .de .fr .nl and others)
  - Seems to be widespread (GDPR high-risk factor)

Reasonable Assumption:

- Inetnum: objects with PII in descr: (especially /32):
    - Are generated by scripts from deployment tools
    - Scripts are in use for many years (suffix) in netname:
    - Are not included in modelling of business processes ("forgotten knowledge")
    - Possibly not considered for data-subject's rights (e.g. right of access art. 15 GDPR)
- No malicious intent, more likely "negligence"

Joint Controllership RIPE/LIR

- LIR is controller (Art. 4 No 7 GDPR) regarding the content
  - PII in descr: is created by LIR
  - Processing by LIR is permitted (necessary), publication is unnecessary.
- RIPE is controller (Art. 4 No 7 GDPR) for RIPE-DB
  - DB functions including history is under control of RIPE
- This constitutes Joint Controllership Art. 26 GDPR
- Situation: RIPE together with LIR is liable for PII in descr: and netname:

Dataforwarding / Data Protection

- Right to access for data subject Art. 15 GDPR
  - LIR is possibly not aware
- Right of information for data subject Art. 13/14 GDPR
  - Queries to RIPE db, data forwarding e.g. through NRTM
  - Database downloads
  - Is likely to be violated (LIR doesn't know who is accessing RIPE db)
  - Is not fulfilled
- Data protection can't be guaranteed:
  - descr: and netname: attributes are not covered by data protection mechanisms:
    - E.g. rate limits
    - E.g. PII stripping in history or from NRTM

Conclusion PII and GDPR

- PII publication of end customer (natural person) is not lawful:
  - Processing justified by Art. 6 (1) lit b GDPR (fulfilling a contract), but publishing of PII of ISP customers is not necessary → violation of data minimization principle (Art. 5 (1) lit c GDPR)

- Data breach notification (proactive duty):
  - To authorities: Art. 33 GDPR (PII leaks into public)
  - To data subject: Art. 34 GDPR (high risk, less likely the case here)
  - Controllers (LIRs, maybe RIPE) most likely not aware

- Right to be forgotten, LIR perspective:
  - Art. 17 GDPR possibly can't be exercised because of RIPE db history (desc: attribute under control of LIR, history under control of RIPE)
  - Removal procedure covers in detail only: person, role, organization, irt
  - Additional, complicated steps necessary by data subject

Authors

- Michael "MiKa" Kafka
  - NetCaT GmbH, Austria
  - mika(at)net-cat(dot)at
  - RIPE Member
  - Network Engineer, Consulting, Trainings (CCSI)

- Ing. Dr. iur. Christof Tschohl
  - Research Institute – Digital Human Rights Center, Austria - Vienna
  - christof.tschohl(at)researchinstitute(dot)at
  - https://researchinstitute.at/en/christof-tschohl.html
  - https://researchinstitute.at/de/christof-tschohl.html (publications, German)
  - Digital Human Rights & Privacy