Analyzing GDPR Compliance of Named Data Networking

Casey Tran, Reza Tourani, Gaurav Panwar, Satyajayant Misra, Travis Machacek
General Data Protection Regulation (GDPR)

Data Protection Officer (DPO)
Compliance
25 May 2018
Data Breaches
Personal Data
Harsh Fines for Risky/Critical Systems
Money Saved for Prepared Systems
NDN Relevance of GDPR Compliance
Motivation and Background

Recent Initiatives

Addressing Compliance via:
- Retrofitting old Systems and Assessing new technologies

Relevant fines tracked by CMS.Law

ETID-118, Failure to Separate Personal Data
ETID-226, Application Semantics
ETID-34, Failure to respond to data erasure
ETID-422, Lost ability to track and access data

• IoT Networks
• Software Defined Networking API
• Storage Systems
• Access Control
Our GDPR Analysis of NDN

- **Rights of Data Subject**
  - Naming: Articles 6, 9
  - Caching: Articles 12, 15-18, 21
  - Forwarding: Article 15
  - Trust: Articles 15

- **NDN’s Relevant Features**
  - Responsibilities of Data Controller & Processor
    - Naming: Articles 5, 6, 29, 35
    - Caching: Articles 5-7, 13, 14, 25, 29, 30, 32-34
    - Forwarding: Articles 28, 30, 32, 35
    - Trust: Articles 5, 9, 32

---

<table>
<thead>
<tr>
<th>No.</th>
<th>Article Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Lawfulness of processing</td>
</tr>
<tr>
<td>9</td>
<td>Processing of special data categories</td>
</tr>
<tr>
<td>12</td>
<td>Transparent information communication</td>
</tr>
<tr>
<td>15</td>
<td>Right of access by the data subject</td>
</tr>
<tr>
<td>16</td>
<td>Right to rectification</td>
</tr>
<tr>
<td>17</td>
<td>Right to erasure</td>
</tr>
<tr>
<td>18</td>
<td>Right to restriction of processing</td>
</tr>
<tr>
<td>21</td>
<td>Right to object</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>No.</th>
<th>Article Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Principles of processing</td>
</tr>
<tr>
<td>6</td>
<td>Lawfulness of processing</td>
</tr>
<tr>
<td>7</td>
<td>Conditions for consent</td>
</tr>
<tr>
<td>12</td>
<td>Conditions for data collection</td>
</tr>
<tr>
<td>14</td>
<td>Conditions for indirect data collection</td>
</tr>
<tr>
<td>25</td>
<td>Protection by design and by default</td>
</tr>
<tr>
<td>28</td>
<td>Processor</td>
</tr>
<tr>
<td>29</td>
<td>Processing under controller’s authority</td>
</tr>
<tr>
<td>30</td>
<td>Records of processing activity</td>
</tr>
<tr>
<td>32</td>
<td>Security of processing</td>
</tr>
<tr>
<td>33</td>
<td>Data breach notification</td>
</tr>
<tr>
<td>34</td>
<td>Data protection impact assessment</td>
</tr>
</tbody>
</table>
### Naming

*Arts. 5, 6, 29, 35*

<table>
<thead>
<tr>
<th>Data Packet</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
</tr>
<tr>
<td><strong>MetalInfo</strong> (content type, freshness period, …)</td>
</tr>
<tr>
<td><strong>Content</strong></td>
</tr>
<tr>
<td><strong>Signature</strong> (signature type, key locator, signature bits, …)</td>
</tr>
</tbody>
</table>

- Outside core NDN forwarding operations?
- Does the name contain sensitive or identifying information?
- If the name contains any identifier, can it be controlled?
Caching
Arts. 5, 6, 7, 12, 13, 14, 15, 16, 17, 18, 21, 25, 29, 30, 32, 33, 34

- Can the data be located upon request?
- Processing is only insertion and deletion of cache? Proof?
- Will the data be transferred?
- Is there a possibility that personally identifiable information will be cached?

[Diagram of Content Store and FIB with GDPR sign]
Stateful Forwarding
Arts. 15, 28, 30, 32, 35

More than PIT and FIB operations, or will access control/custom forwarding strategies be used?

Can sensitive producers know who accessed their data?

How will records of data trail be kept if needed?
Built-in-Trust
5, 9, 15, 32

Data Packet

<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>MetaInfo</td>
</tr>
<tr>
<td>Content</td>
</tr>
<tr>
<td>Signature</td>
</tr>
</tbody>
</table>

- Are users identifiable in the trust schema?
- Do trust schemas reveal sensitive information?
- How can eviction of certificates revealing sensitive chains of trusts be evicted?
Experimental Results on a per node basis.

Fundamental Compliance Requirements:
Logging and Encryption
Logging Experimental Results

End-to-End Latency of Logging Levels

Effect of Logging on CPU Utilization

(a) No Caching
(b) 25% Cache Hit Rate
(c) 50% Cache Hit Rate

Logging Levels
- None
- Cache
- All

CPU Utilization (%)
Experimental Results of Encryption

Impact of Data Decryption during cache hit

Effect of Encryption on CPU Utilization

(a) 25% Cache Hit Rate

(b) 50% Cache Hit Rate
Concluding Discussion and Insights

**Consumer Identification**

**Timely Request Processing**

**Distributed Auditing Framework**

**Compliance at Application Layer**
Thank you!

Q & A and discussion in breakout room!