Privacy in Road User Charging Systems
Background, Experience and Consequences

Friedemann Kirn
Version 0.01 / 12.06.2012
Agenda

- European legal Framework
- Toll Charger View
- Architectural Consequences
- Experience from the German tolling scheme
  - Legal Framework
  - Toll Collect Solution
- Conclusion

T·Systems
Some Basics
EU Charter of Fundamental Rights
(12/2000)

- Article 7 - Respect for private and family life
  - Everyone has the right to respect for his or her private and family life, home and communications.

- Article 8 - Protection of personal data
  1. Everyone has the right to the protection of personal data concerning him or her.
  2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
  3. Compliance with these rules shall be subject to control by an independent authority.
- Long Title: “... on the protection of individuals with regard to the processing of personal data and on the free movement of such data”.

- Article 2 - Definitions (For the purposes of this Directive):
  a) ‘personal data’ shall mean any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;
  b) ‘processing of personal data’ (‘processing’) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;
  ...
  h) ‘the data subject’s consent’ shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.
EU Directive 95/46
Important Claims

- Personal data must be
  - legitimately processed, i.e. by user consent, on contractual basis, ... (Art. 7),
  - fairly and lawfully processed (Art. 6.1a),
  - collected and processed for limited purposes only (Art. 6.1b),
  - adequate, relevant and not excessive in relation to that purposes → Data Avoidance (Art. 6.1c),
  - accurate and kept up to date (Art. 6.1d),
  - kept no longer than necessary → Limited Data Retention (Art. 6.1e),
  - processed in accordance with the data subject's other rights (Art. 8 and 9),
  - confidentially and securely processed (Art. 16 and 17),
  - transferred only to countries with adequate protection (Art. 25 and 26).

- The data subject has the right to
  - be informed about the collection of data relating to him/her (Art. 10),
  - request information about the data stored or processed relating to him/her (Art. 12).
Toll Charger / Government View
Toll Charger Perspective (Government perspective)
Drivers for Data Collection and Avoidance

**Data Avoidance**

- **Legal obligations**
  - Follow the standards and concepts of local and EU data privacy concepts

- **User acceptance**
  - Tolling schemes might suffer from an acceptance lack when the authority is perceived as "big brother"
  - A "big brother" image might result in a lower compliance rate (data privacy issues as a psychological excuse for toll dodgers)

- **Data is actually an operative burden**
  - Cost for security and auditing framework
  - Risk if security breaches (internal or external)
    - The more sensitive data is available, the higher is the potential damage

**Data Collection**

- **Legal obligations**
  - Especially public authorities might have to obey special fiscal rules
  - Proof of sound and consistent operation to shareholder/public
  - But: Collection for operative purposes is allowed, but needs to be anonymous/pseudonymous as early as possible

- **Supervision of Service Provider**
  - Collect data to check performance of provider
  - But: Performance can be assessed by statistical methods

- **Compliance check of subjects to toll (Enforcement)**
  - Collect data to check compliance of vehicles
  - But: Collection is only necessary in suspicious cases

- **Value added services (VAS)**
  - Offer value added services (e.g. traffic services) for traffic improvement and acceptance reasons
  - But: Statistical data is not affected if anonymized as early as possible
Architectural Consequences
Experience from the German Tolling Scheme
- Data privacy rules to be followed in Germany
  - Bundesdatenschutzgesetz (BDSG)
    - CRM-orders, Service-requests
  - Bundesfernstraßenmautgesetz (BFStrMG)
    - Track- and Enforcement Data = Tolling Data
Technology agnostic requirements in German tolling law (BFStrMG)

- No specific technology request on implementation by government
- Reference to data protection law (BDSG)
  - data avoidance and data economy
  - Necessity
- Design principles:
  - On Board Unit
  - Central processes
  - Data handling rules (processing, storage, deletion)
<table>
<thead>
<tr>
<th>Upon creation</th>
<th>Upon end of process</th>
<th>Upon end of de-registration process</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>immediate</strong></td>
<td><strong>nmF, Web-Logs</strong></td>
<td><strong>ergänzende Stammdaten</strong></td>
</tr>
<tr>
<td><strong>42 days</strong></td>
<td><strong>Kurzzeit-Doku., Betriebs-Logs</strong></td>
<td><strong>Verträge (&gt; 7 Jahre, &gt;=1 Jahr nach De-Reg.)</strong></td>
</tr>
<tr>
<td><strong>120 days</strong></td>
<td><strong>voll erstattete Reklamationen</strong></td>
<td><strong>Kernstamm-daten</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Mautdaten mit bes. Analysebedarf</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Vorgänge ohne Dokupflicht</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Rekla- und Forde rungsdaten</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Handelsbriefe</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Buchhaltungsdaten</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Starting date + deadline = 12 deletion classes**
Privacy by Design – the OBU On Bord Unit

- "Knows" the tolled sections
- All other track data are deleted immediately by the OBU and are not communicated
  - (following the data protection law "BDSG "not generated")
- The OBU is a "data avoidance machine"
Conclusion
Conclusion (1)

- Privacy is not only achievable; if done right it may be an economic success factor
- Involve stakeholders, experts and media openly
- If the legal requirements are applied consequently a smart client OBU architecture is the logical choice
- Other Solutions concepts require additional measures to be compliant
- Integrate privacy aspects in the tender requirements
- Non compliance to existing regulations should be prosecuted
Conclusion (2)

- Privacy is not an afterthought; it has to be integrated from the beginning by design - to be taken into account from the start.
- Privacy Requirements become a major legal risk if not taken seriously
  - For responsible persons in ministries and companies
  - For operation and success of RUC systems and revenue
- Privacy is a major political and public success factor for Tolling systems
- Data avoidance and data economy are key for tolling and enforcement solutions
Thank you for your attention

Contact:

Friedemann.Kirn@t-systems.com