Think about Data Protection

Petra Kauer-Ott
petra.kauer@switch.ch

Trust & Identity WG Meeting
14. March 2018, Bern
Goal

We are compliant with the different applicable data protection laws
But …

Data Protection Law compliant
3 Actors

- Cantonal Universities
  - Cantonal Data Protection Laws

- Federal Institutes of Technology

- SWITCH
  - Federal Data Protection Law
2 Purposes

University Administration

SWITCH edu-ID

User Purposes
How to get & deliver answers …

- Legal questions collected (regulations WG, 2014)
- Questions sent to different Data Protection Officers (2015)
- Several queries on federal data protection officer because of expected written answer (2015 - … )
- Legal developments in CH and EU observed (2014 - … )
- Participation in E-ID consultation (May 2017)
- Situation about social security number AHVN13 analysed with FHNW (2017)
- SWITCH edu-ID database declared (2017)
- Service Description elaborated (federation policies adopted; 2018)
Statements by Data Protection Officers

• Positive: „Lifelong use“ of SWITCH edu-ID
• Negative: Storing data after leaving Higher Education Institution

→ solution found ✓

Disallow to delete account (if no active affiliation)

Former affiliation & user consent
• Use of AHVN13 as attribute within SWITCH edu-ID?

• Legal assessment by SWITCH

• Legal advise:
  • Use of AHVN13 deemed as too delicate
  • Observe political development about usage of AHVN13

• Legislative project for wider applicability

Risk analysis (in German): https://projects.switch.ch/eduid/documents/
Legal aspects of the Service Description

• Data protection provisions (chapter 6.3)

• Provisions regarding warranty, liability, applicable law, place of jurisdiction etc.

https://www.switch.ch/edu-id/terms/
7 Privacy Principles

1. Lawfulness, fairness and transparency
2. Purpose limitations
3. Data minimisation
4. Accuracy
5. Storage limitations
6. Integrity and confidentiality
7. Accountability

- Use of data described
- Purposes described
- Data economy in federation
- Updates
- Deletion of accounts
- Data security
- Demonstrate compliance with principles
7 Privacy Principles

1. Lawfulness, fairness and transparency
2. Purpose limitations
3. Data minimisation
4. Accuracy
5. Storage limitations
6. Integrity and confidentiality
7. Accountability

Privacy by

- **Design**: technical integration
- **Default**: data protection friendly settings

7. **Accountability**

Demonstrate compliance with principles
How to protect data in general

1. **Apply law(s) and principles for processes & services**
   E.g., store & release only data necessary for the declared and current purpose

2. **Consult (local) Data Protection Officer**
   (knows local regulations as well as law)

3. **Apply specific policies**
   - Resource Registry → Data Release Policy (fill role of administrator)
   - Local (university) policies

4. **Inform & instruct staff and end users**
   - Clear user guides, Help, ToU, courses for IT and other staff
   - User awareness campaigns (security, data protection)
### How to protect data in SWITCH edu-ID?

<table>
<thead>
<tr>
<th>Secure storage of data</th>
<th>ISMS</th>
<th>ISMS/other</th>
<th>credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability of data</td>
<td>SLA</td>
<td>SLA</td>
<td>(updates)</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>access/policy</td>
<td>access/policy</td>
<td>credentials</td>
</tr>
<tr>
<td>Transparency</td>
<td>user consent, ToU, SLA</td>
<td>local ToU</td>
<td>My account</td>
</tr>
<tr>
<td>Accuracy (correctness of data)</td>
<td>verified email, mobile number, postal address</td>
<td>all transmitted attributes (verification)</td>
<td>ToU, updates</td>
</tr>
<tr>
<td>Data Economy (minimisation)</td>
<td>define minimal requirements</td>
<td>apply minimal requirements</td>
<td>user consent</td>
</tr>
<tr>
<td>Audits</td>
<td>ISMS</td>
<td>(right reserved)</td>
<td>inspection</td>
</tr>
<tr>
<td>Attribute Release Policy (ARP) in RR</td>
<td>approval process</td>
<td>approval by RRA admin</td>
<td>user consent</td>
</tr>
<tr>
<td>Federation trust layer</td>
<td>governance</td>
<td>community rules</td>
<td>membership</td>
</tr>
</tbody>
</table>
Current Law Situation

EU General Data Protection Regulation (GDPR) (Datenschutzgrundverordnung DSGVO):
- enforcement 25.5.2018
- important also for Switzerland
→ no immediate adaptations necessary (for SWITCH)

Revision of CH Federal Data Protection Act (Bundesgesetz über den Datenschutz DSG):
- includes adaptations for EU law
- delayed, expected earliest for end of 2018
- “compatibility” with GDPR
→ SWITCH will avoid double adjustments and apply CH law

New E-ID law
- simultaneously with data protection act or later
- impact possible if used as basic identity (but not directly on edu-ID)

https://www.eugdpr.org/
https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung.html
Tasks for the future

• Fill seat for **legal representative in Advisory Board** (mandate by SWITCH; hints welcome!)

• Analyse & compare **legal statements** of Data Protection Officers

• Analyse draft and final version of **FDPA**; prepare **changes** (if necessary)

• More detailed **description of data processing**

• Prepare process for **inspection of record** by users

• Prepare paper with **reasoning for universities**
Result:

We are compliant with the different applicable data protection laws