Tilburg Institute for Law, Technology and Society
EC study on Article 42/43 GDPR
Tilburg Law School
EC study on Article 42/43 GDPR

- **February 2017**: Directorate-General for Justice and Consumers launches a request for services under the framework contract JUST/2014/DATA/FW/0038 regarding a **Study** on certification mechanisms, seals or marks under Articles 42 and 43 of Regulation (EU) 2016/679

- **June 2017**: Consortium including Tilburg Institute for Law, Technology, and Society (TILT) from Tilburg University, TNO (Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek, TNO) and CIVIC Consulting is retained

- **July 2017**: Research team (6) led by Prof. Dr. Ronald Leenes (Tilt) and Irene Kamara (Tilt) starts the research (market scan, case studies, surveys…)

- **February 2019**: Final report and annexes is published on EC website
General Methodology

- Full data protection
- Partly focusing on data protection
- Data protection related topics (cyber security)

Quick Scan
117 schemes identified

Cases study
15 schemes selected

- BSI BS 10012 (UK)
- TÜV Italia ISO/IEC 27001
- BSI ISO/IEC 27018 (UK)
- Certificazione ISDP 2003:2018 Data protection (IT)
- Datenschutzaudit beim ULD (DE)
- E-privacy app (DE)
- EuroPrise (DE)
- IkeepSafe Coppa Safe Harbor (US)
- Label CNIL digital safe boxes (FR)
- Health Personal Data Storage Agreement (FR)
- Myobi Privacy Seal (NL)
- Norea Privacy-Audit-Proof (NL)
- PrivacyMark System (JP)
- Privacy by Design Certification Ryerson (CA)
- TrustArc APEC CBPR certification (US)

Cases study
8 themes analyzed

- Scope
- Normative criteria
- Scheme arrangements
- Conformity assessment
- Certification issuance
- Renewal
- Monitoring
- Sanction policy
- Complaint and dispute management
### Cases Study: Selection criteria

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Art. 42, 43 GDPR criteria</td>
<td>Certification schemes need to <strong>be relevant to the scope of Article 42 GDPR</strong></td>
</tr>
<tr>
<td>Maturity of certifications and adoption (“success”)</td>
<td>Mature schemes that are <strong>already operational for several years</strong></td>
</tr>
<tr>
<td>Focus/topics of certifications</td>
<td>Criterion was <strong>derived by the wording of the GDPR</strong>. There are also several schemes that are not limited to a specific topic, but are generic, in the sense that they aim to cover compliance dealing with more than one topic</td>
</tr>
<tr>
<td>Territoriality of regulatory basis</td>
<td>There are also lessons to be learned from <strong>certification schemes in other jurisdictions</strong>, both national and regional</td>
</tr>
<tr>
<td>Concerned entity</td>
<td>Following the wording of the GDPR, articles 24 and 28, come up. <strong>Certifications may be addressed to either of the two entities, or to neither specifically</strong></td>
</tr>
</tbody>
</table>
## Cases Study: Certification models

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>All processes model</td>
<td>Multi-sector model</td>
<td>Dedicated GDPR provisions model</td>
</tr>
<tr>
<td>The scheme applies to all process types</td>
<td>The scheme applies to all or certain processes in all business activities</td>
<td>(‘single-issue’) The scheme helps to demonstrate with certain GDPR provisions</td>
</tr>
<tr>
<td>Dedicated processes model</td>
<td>Single-sector model</td>
<td>All GDPR model (‘comprehensive’)</td>
</tr>
<tr>
<td>The scheme applies to some dedicated processes included or not in a product range</td>
<td>The scheme applies to one specific business activity</td>
<td>The scheme helps to demonstrate compliance with all GDPR provisions</td>
</tr>
</tbody>
</table>
## Cases Study: Certification models

<table>
<thead>
<tr>
<th>Legal framework vs Standard vs Combined</th>
<th>International vs National</th>
<th>Fully public vs Public monitored vs Private</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normative basis: law</td>
<td>Subnational model</td>
<td>Certification by public authorities</td>
</tr>
<tr>
<td>The scheme is based on a legal framework (EU or non-EU one)</td>
<td>The scheme applies within a subdivision of the national territory</td>
<td>The scheme is fully managed by a public authority</td>
</tr>
<tr>
<td>Standard model</td>
<td>National model</td>
<td>Monitored</td>
</tr>
<tr>
<td>The scheme is based on a standard issued by a national or an international standardization body</td>
<td>The scheme applies to a national territory</td>
<td>A public authority plays a limited but active role (eg. Accreditation)</td>
</tr>
<tr>
<td>Combined model</td>
<td>EU-wide model</td>
<td>Privately owned</td>
</tr>
<tr>
<td>The schemes both refer to a regulation and to one or several other(s) normative basis (Technical standard(s) or and code of conduct)</td>
<td>The scheme applies to all the EU Member States</td>
<td>The scheme is fully managed by a private body without any public authority intervention</td>
</tr>
<tr>
<td>International model</td>
<td></td>
<td>International model</td>
</tr>
<tr>
<td>The scheme applies worldwide or, at least, in the EU and outside the EU</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Cases Study: Certification models

<table>
<thead>
<tr>
<th>Internally managed vs Out-sourced</th>
<th>SME friendly</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internally managed model</td>
<td>SME friendly model</td>
</tr>
<tr>
<td>The scheme owner manages the entire certification process</td>
<td>The scheme has an offer dedicated to SMEs</td>
</tr>
<tr>
<td>Out-sourced model</td>
<td></td>
</tr>
<tr>
<td>The scheme fully or partly out-source the certification process to external auditors</td>
<td></td>
</tr>
</tbody>
</table>
Conclusion

1. Diversity

- Linked to the nature of certification > highly flexible process
- Study’s choice to select as many models as possible
- Intrinsic diversity of data protection certification schemes on the market (DPC market)

2. Existing Data Protection Certification market goes beyond Article 42 GDPR scope

- Material/functional scope
  - Management system certification (BSI, TUV Italia)
  - Personal certification (…)
- Geographical scope
  - Subnational (ULD)
  - International (ISO)
- Origin
  - Non-EU schemes (Jipdec, TrustArc, Ikeepafe, PbD Ryerson)
- Scheme arrangements
  - Self-regulated (Europrise, ISDP 2003)
Conclusion

3. Two main normative models
   • Regulatory based model
     ➢ Regional, national or European laws (Europrise, ISDP 2003, CNIL, Ikeepsafe)
     ➢ International agreements (TrustArc CBPR)
   • Industrial standard based model
     ➢ ISO standards (ISO/IEC 27018, 27001)
     ➢ National Industrial standard (JIS Q 15001, BS 10012)

4. Two main challenges
   • Articulate Article 42/43 GDPR and ISO approaches
     ➢ GDPR above > Art.42 schemes on top of ISO ones
     ➢ GDPR aside > Art.42 schemes set for topics not yet covered by the ISO (IoT, genetics, children, cross-border flows)
     ➢ GDPR into > GDPR provisions added to ISO standards (ISO standards updated every 5 years)
   • Mutual recognition
     • Schemes approved by national supervisory authorities
     • Schemes developed outside the EU
Annex: full study available on EC website