Tilburg Institute for Law, Technology and Society

EC study on Article 42/43 GDPR

Tilburg Law School

TILBURG UNIVERSITY

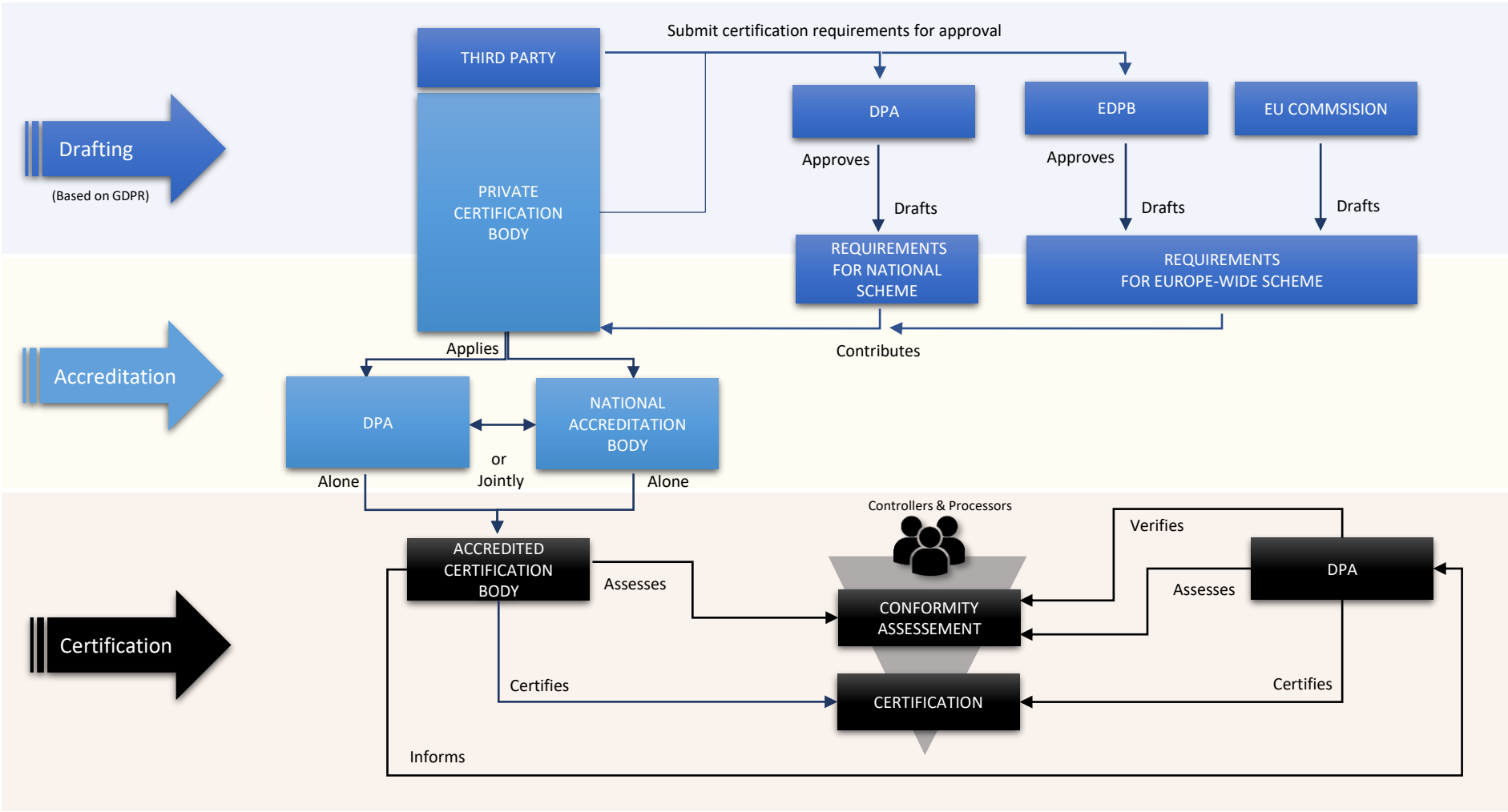
Understanding Society

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

TILBURG UNIVERSITY

Article 42/43 certification



TILBURG UNIVERSITY

General Methodology

Quick Scan
117 schemes identified

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

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

TILBURG UNIVERSITY

Cases Study : Selection criteria

Criteria	Details
Art. 42, 43 GDPR criteria	Certification schemes need to **be relevant to the scope of Article 42** GDPR
Maturity of certifications and adoption ("success")	Mature schemes that are **already operational for several years**
Focus/topics of certifications	Criterion was **derived by the wording of the GDPR**. 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
Territoriality of regulatory basis	There are also lessons to be learned from **certification schemes in other jurisdictions**, both national and regional
Concerned entity	Following the wording of the GDPR, articles 24 and 28, come up. **Certifications may be addressed to either of the two entities, or to neither specifically**

Cases Study: Certification models

All processes v. Dedicated processes	Multi-sector v. Single-sector	Single-issue certification vs Comprehensive certification
All processes model The scheme applies to all process types	**Multi-sector model** The scheme applies to all or certain processes in all business activities	**Dedicated GDPR provisions model ('single-issue')** The scheme helps to demonstrate with certain GDPR provisions
Dedicated processes model The scheme applies to some dedicated processes included or not in a product range	**Single-sector model** The scheme applies to one specific business activity	**All GDPR model ('comprehensive')** The scheme helps to demonstrate compliance with all GDPR provisions

TILBURG UNIVERSITY

Cases Study: Certification models

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

Cases Study: Certification models

Internally managed vs Out-sourced	**SME friendly**
Internally managed model The scheme owner manages the entire certification process	**SME friendly model** The scheme has an offer dedicated to SMEs
Out-sourced model The scheme fully or partly out-source the certification process to external auditors	

TILBURG UNIVERSITY

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

https://publications.europa.eu/en/publication-detail/-/publication/5509b099-707a-11e9-9f05-01aa75ed71a1/language-en/format-PDF/source-search

Tilburg University