Webinar:
Understanding Certifications, Seals and Marks under the GDPR

Thursday, 27 October 2016

Centre for Information Policy Leadership
Hunton & Williams LLP

Webinar Agenda

1. Introduction by Bojana Bellamy
2. Understanding certifications, seals and marks under the GDPR
3. Understanding the respective roles of stakeholders
4. Key benefits
5. Initial Recommendations
6. Key challenges and open questions and areas where further work and guidance is needed
7. Next Steps
   - CIPL Working Session, Brussels on 8 November 2016
   - CIPL white paper on Certifications and Seals under the GDPR

Centre for Information Policy Leadership
Hunton & Williams LLP

GDPR Project Objectives

Consistent interpretation by all Member States and stakeholders

Consistent further implementation by Member States, EU Commission and DPAs/EDPB

Constructive, forward-thinking and future-proof interpretation enabling EU Digital Single Market and data-driven innovation, while protecting privacy

Best practices, opportunities and challenges in the implementation

Bridging stakeholders and building trust

Centre for Information Policy Leadership
Hunton & Williams LLP

5 Project Focus Topics

Data Privacy Programmatic Management

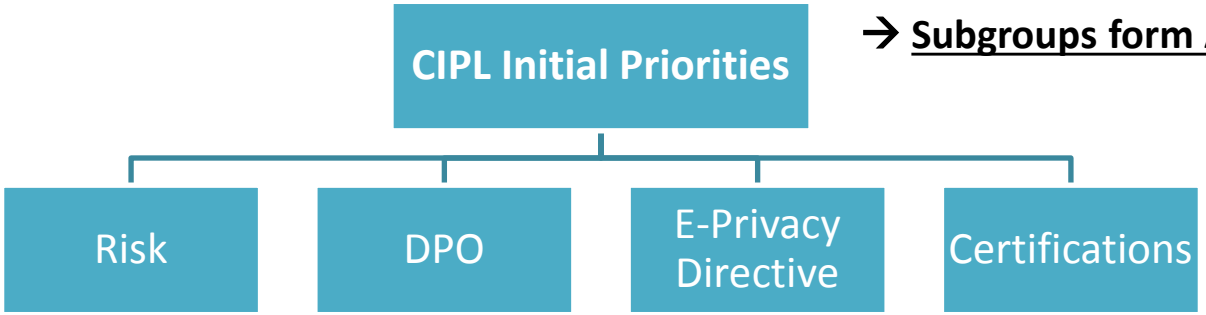
Core Principles and Concepts

Individual Rights

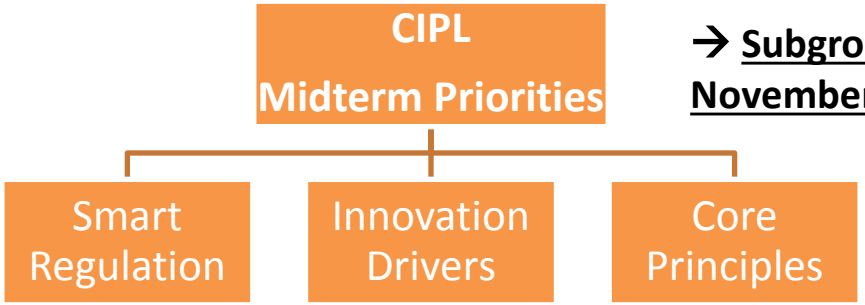
International Data Transfers

Relationship with EU DPAs and Smart Regulation

Project Work Plan 2016 – March 2017



→ **Subgroups form April**



→ **Subgroups staggered from November**

Project Activities

Internal	External
• **Steering Committee and calls** • **Subgroups and calls** • **Deep dive webinars on priority topics** • **All project participants calls**	• Workshop reports, papers and written submissions • Engagement with EU DPAs , Commission and national governments • Workshop I (16 March, Amsterdam) • WP29 FabLab (26 July, Brussels) • EU Commission Workshop (27 July, Brussels) • Workshop II (19 September, Paris) • Working Session on Seals, Certifications and Codes of Conduct (8 November, Brussels) • Workshop III (March 2017, Madrid or Rome, TBC)

Certification

Member States, DPAs, the EDPB and the EU Commission must encourage establishment of certifications: *(42(1),(3)); see also (57(1)(n); (70)(1)(n))*

- At **national** and particularly at **EU level**
- For use by **controllers** and **processors**
- **Voluntary** and available through a transparent process

Controllers and processors may use certifications to: *(42(1),(2); see also (46(2)(f))*

- Demonstrate **compliance** with the Regulation
- Demonstrate safeguards in third countries for **data transfers**
- Certifications must be coupled with enforceable commitments by the controllers or processors in the third country to apply such safeguards

Certification does not reduce GDPR compliance obligations or prejudice the tasks and powers of the DPAs *(42(4))*

- But it is one factor that DPAs must take into account in determining **administrative fines** *(83(2)(j)*

Certification (cont.)

Certifications issued by "certification bodies" or the DPA: *(42(5); see also 57(1)(o); 58(1)(c) and (2)(h); 58(3)(f))*

- On the basis of **criteria approved by the DPA (national) or the EDPB (European DP Seal)**
- Last up to three years and are renewable *(42(7))*
- Can be withdrawn by certification bodies or DPAs if the certification requirements are no longer met
- EDPB maintains a publicly available register of all certifications, seals and marks *(42(8)); see also 43(6); 70(1)(o))*

To obtain certification from a certification body or DPA, organisations must: *(42(6))*

- Provide all relevant information about the processing activities they seek to certify
- Provide access to these activities

The Commission's role: *(43(8)); (43(9)); see also Art 92, on the exercise of delegation*

- May adopt delegated acts to specify the requirements for the certifications *(43(8)); see also Art 92, on the exercise of delegation*
- May adopt implementing acts laying down technical standards for certifications and mechanisms to promote or recognise certifications

Certification Bodies

Issue, renew and withdraw certifications *(43(1))*

- Must have an appropriate level of data protection expertise
- Before each certification, the certification body must seek DPA approval *(See also (58(2)(h))*
- Responsible for the assessment leading to certification or withdrawal of certification *(43)(4))*
- Must provide to the competent DPAs the reasons for granting or withdrawing certifications *(43(5))*

Must be accredited by DPAs and/or national accreditation bodies *(43)(1)(a) and (b), 43(3), 43(4), see also 64(1)(c); 57(1)(p); (70(1)(p))*

- For a maximum of 5 years
- On the basis of criteria approved by the DPA or the EDPB
- (Separate requirements in the case of accreditation by a national accreditation body)
- DPAs and EDPB must make public the accreditation criteria for certification bodies (and certification criteria) *(46(6); see also 42(8) and 70(1)(o)*
- The DPA or national accreditation body can revoke the accreditation of a certification body *(43(7))*

Conditions for accreditation of certification bodies *(43(2))*

- Demonstrate independence and expertise;
- Undertake to respect the approved certification criteria;
- Establish procedures for issuing, periodic review and withdrawal of certification;
- Establish transparent complaint-handling mechanisms;
- Demonstrate absence of conflicts of interest

Centre for Information Policy Leadership
Hunton & Williams LLP

Benefits of Certifications

For organizations

- Enable and demonstrate GDPR compliance and accountability – to internal management and the Board, to DPAs, consumers, business partners
- Builds trust among public, DPAs and customers
- Support and create compliance scalability for SMEs and startups
- Support effective and practical privacy programs developed by relevant subject matter expertise
- Use as cross-border mechanism when coupled with binding commitments
- Potential global reach and interoperability with other privacy marks and certifications
- Potential mitigating factor in connection with GDPR enforcement and sanctions

For DPAs

- Shared, more efficient and more far-reaching supervision and enforcement through certification bodies
- Deliver better and long term compliance
- Drive more transparency

For individuals

- More trust in organisations
- More effective and rigorous protection and compliant resolution
- More transparency

For business partners and the ecosystem

- More trust and assurance of protection in ecosystem
- Greater speed of doing business and avoidance of protracted negotiations about privacy and security

Centre for Information Policy Leadership
Hunton & Williams LLP

CIPL Initial Recommendations

Certifications should be:

- Effectively incentivised and clearly accompanied by benefits for certified organisations, otherwise organisations will be reluctant to invest time and money in obtaining and maintaining certifications (in addition to the many other certifications they are subject to (ISO, SOX, etc)
- Helpful, recognisable, trusted and wanted by individuals
- Flexible, scalable and affordable to serve different purposes and types and sizes of organisations – controllers and processors, large and SMEs, start ups etc.
- Available both for overall privacy program and capability to comply, as well as a product, process and service
- Technologically neutral
- Harmonised (criteria, process, scope, effect) at EU level, with a preference for European DP Seal; national certifications should be used for organisations whose services and products are limited to a single Member State
- Consistent and taking into account other systems (such as ISO Standards, Privacy Shield, and CBPR)
- Aligned with BCR and given to BCR approved companies
- Efficient (appropriately fast) and effective in terms of certification process
- Effective and recognized/accepted means for demonstrating compliance
- Informed by other third party privacy and security certification systems, such as APEC CBPR and ISO standards
- Handled by third party certification bodies, rather than by DPAs, to save resources

Centre for Information Policy Leadership
Hunton & Williams LLP

Key Challenges and Questions

Nature and Effect of Certifications

- What is certified: a product / service, a process, or privacy program?
- Does certification certify compliance, or having an infrastructure or program that can deliver compliance?
- What level of protection does the certification signify?
- Certification as mitigating factor in enforcement and sanctions
- Up-to-date standards, reflecting current expertise and the most recent techniques?

Scope of Certifications

- Co-existence of national and EU-wide certifications
- BCR as a form of certification and how to join and evolve the two concepts?
- Extraterritorial effect and relation of certifications to other certification mechanisms - Privacy Shield, APEC CBPR, Japan Privacy Mark, ISO Cloud Privacy and Security certification

Process of Certification

- How can the process of certification be kept simple, efficient, scalable and sufficiently fast? (Contrast to the BCR process.)

Centre for Information Policy Leadership
Hunton & Williams LLP

Key Challenges and Questions cont.

Cooperation/roles of multiple "Certifications Stakeholders":

- Who should develop and draft the standards/criteria for certification? (Commission; DPAs; EDPB – all have roles; who should take the lead?
- Do private sector organisations (certification bodies, companies, etc.) have a role?
- Should the Commission take the lead and draft a baseline/template certification to ensure consistency?
- What exactly are the Commission's delegated/implementing acts?
- How do we understand the role of the Member States? ("Encourage" certifications (Art. 42(1) and ensure that certification bodies are properly accredited (Art 43(1))
- What issues should any WP29 guidance address at this stage?
- What is the role of private sector bodies at this stage in terms of advancing GDPR certifications?

Centre for Information Policy Leadership
Hunton & Williams LLP

Next Steps

- CIPL GDPR Project Working Session on Seals, Certifications, and Codes of Conduct
  - 8 November 2016
  - Brussels, Belgium

- CIPL white paper on Certifications and Seals under the GDPR
  - In progress

Centre for Information Policy Leadership
Hunton & Williams LLP

GDPR Certification Actors

Member States	DPAs	EDPB	Commission	Certification Bodies	National Accreditation Body	Private Sector Organizations
Encourage Certifications (42(1))	Encourage Certifications (42(1); 57(1)(n))	Encourage Certifications (42(1)); 70(1)(n)	Encourage certifications (42(1))	Issue/renew/withdraw certifications (42(5); 42(7); 43(1))	Accredit Certification Bodies (43(1)(b))	Draft/propose certification criteria and Mechanisms
Ensure that Certification Bodies are accredited (43(1))	Approve accreditation criteria for Certification Bodies (43(1)(b);(43(3); 64(1)(c); 57(1)(p))	Approve accreditation criteria for Certification Bodies (43(3)); 64(1)(c); 70(1)(p))	"lay down technical standards for cert. mechs. and mechs. to promote and recognize cert. mechs" (through implementing acts)(43(9)) [Create accreditation criteria for Cert. Bodies ?]			Provide input into creation of certification criteria
	Approve certification criteria (42(5); 43(2)(b); 57(1)(n))	Approve certification criteria (42(5); 43(2)(b)); 70(1)(q)(provide opinion to Commission)	Specify requirements for cert. mechs. (through delegated and implementing acts)(43(8) [Adopt certification criteria ?]			Become certified (and attendant tasks, such as providing information and access to Certification Bodies and enter into safeguards commitments with c-b parties) (42(6); 46(2)(f)
	Accredit Certification Bodies (43(1)(a); 43(7); 57(1)(q); 58(3)(e))	Accredit Certification Bodies (70(1)(o))				
	Publicize accreditation criteria and certification criteria (43(6))	Publicize in Register Certification Mechanisms (accredited certification bodies) and certified organizations in third countries (42(8); 43(6); 70(1)(o))				
	Issue/renew/withdraw certifications (42(5); 42(7); 43(1);57(1)(o); 58(1)(c) and (2)(h)); 58(3)(f))					

Centre for Information Policy Leadership
Hunton & Williams LLP

GDPR Certification Tasks

Encourage Certifications	Approve accreditation criteria for Certification Bodies	Ensure that Certification Bodies are accredited	Accredit Certification Bodies	Specify requirements for Cert Mechs and lay down technical standards for Cert Mechs and Mechs to promote and recognize Cert Mechs	Draft/Propose Certification Criteria/Mech	Approve/Adopt Certification Criteria/Mechanisms	Issue/renew/withdraw certifications to controllers or processors	Publicize accreditation criteria and certification criteria and mechs
DPAs (42(1); 57(1)(n))	DPAs (43(1)(b); 43(3); 64(1)(c); 57(1)(p))		DPAs (43(1)(a); 43(2); 43(7); 57(1)(q); (58)(3)(e)			DPAs (42(5); 43(2)(b); (57)(1)(n))	DPAs (42(5); 42(7); 43(1); 57(1)(o); 58(1)(c); 58(2)(h); 58(3)(f)	DPAs (43(6))
EDPB (42(1); 70(1)(n)	EDPB (43(3); 64(1)(c); (70)(1)(p);		EDPB (70(1)(o)			EDPB (42(5); 43(2)(b); 70(1)(q) (opinion to Comm.)		EDPB (42(8); 43(6); 70(1)(o)
Member States (42(1))		Member States (43(1))						
Commission (42(1);	Commission (through implementing acts) (43(9)) [?]			Commission (through delegated and implementing acts)(43(8) and (9)	Commission (through delegated or implementing acts) (43(8) and (9)) [?]	Commission (through delegated or implementing acts) (43(8) and (9)) [?]; 92(3) and (5))		
	National Accreditation Bodies under Regulation (EC) No 765/2008 and specified technical rules (43)(3)		National Accreditation Body (43(1)(b))					
							Certification Bodies (with approval/input by the DPA) (42(5); 42(7); (43(1))	
					Private Sector			

Q&A Discussion

If you would like to ask a question, please hit *7 (star 7) to unmute your phone.

Please hit *6 (star 6) to mute your phone again.

Bojana Bellamy
President
Centre for Information Policy Leadership

Contacts

Bojana Bellamy
President
Centre for Information Policy Leadership
Bbellamy@hunton.com

Markus Heyder
Vice President & Senior Policy Advisor
Centre for Information Policy Leadership
Mheyder@hunton.com

Hielke Hijmans
Senior Policy Advisor
Centre for Information Policy Leadership
Hhijmans@hunton.com

Centre for Information Policy Leadership
www.informationpolicycentre.com

Hunton & Williams Privacy and Information Security Law Blog
www.huntonprivacyblog.com

FOLLOW US ON
linkedin.com/company/centre-for-information-policy-leadership

FOLLOW US ON TWITTER
@THE_CIPL