

**Comments by the Centre for Information Policy Leadership on the European Data Protection Board's Guidelines 4/2018 on the Accreditation of Certification Bodies under Article 43 of the General Data Protection Regulation (2016/679) – Annex 1**

**Adopted on 4 December 2018**

On 4 December 2018, the European Data Protection Board (“EDPB”) adopted its “Draft Annex to the Guidelines on the accreditation of certification bodies under Regulation (EU) 2016/679” (“Draft Annex”). The EDPB invited public comments on this document by 1 February 2019.

The Centre for Information Policy Leadership (CIPL)<sup>1</sup> welcomes the opportunity to submit the comment below. We are pleased to see the progress made on developing the guidelines which will ultimately help establish a certification framework both for GDPR compliance as well as data transfers under the GDPR. The goal of this limited comment is to facilitate consideration of the “specific needs of micro, small and medium-sized enterprises” as prescribed under Article 42(1) of the GDPR.

Section 4.3 of the Annex states that “[t]he accreditation body shall in addition to the requirement in 4.3.1 ISO/IEC 17065/2012 ensure on a regular yearly basis that the certification body has appropriate measures (e.g. insurance or reserves) to cover its liabilities in the geographical regions in which it operates”. CIPL suggests (1) that “liabilities” be defined to apply to a certification body’s ability to cover its general commercial liabilities and (2) that “available credit facilities” be added to “insurance or reserves” in the list of examples of such appropriate measures.

This definition of liabilities should not include liability under Article 83(4)(b) since it would be prohibitively expensive (if not impossible) to purchase liability insurance for fines stemming from violations of the GDPR itself. Without access to a readily available and affordable insurance product, under the current drafting, a prospective certification body would need to demonstrate sufficient reserves of up to “10,000,000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year” per violation. This requirement would introduce a significant upfront cost that would effectively prohibit all but the very largest entities from serving as a certification body. In addition, such a cost would functionally preclude most entities operating under a non-profit corporate structure. It is also unclear how this requirement would be met or evaluated by Supervisory Authorities that choose to act as certification bodies. In addition, introducing such initial costs for prospective certification bodies would ultimately increase the cost of a certification, thereby making an Article 42 certification impractical for micro, small and medium-sized enterprises.

CIPL is grateful for the opportunity to provide this brief and specific suggestion. We look forward to providing further input in the future as new issues arise. If you would like to discuss this comment or require additional information, please contact Bojana Bellamy, [bbellamy@huntonAK.com](mailto:bbellamy@huntonAK.com), Markus Heyder, [mheyder@huntonAK.com](mailto:mheyder@huntonAK.com), Nathalie Laneret, [nlaneret@huntonAK.com](mailto:nlaneret@huntonAK.com) or Sam Grogan, [sgrogan@huntonAK.com](mailto:sgrogan@huntonAK.com).

---

<sup>1</sup> CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 74 member companies that are leaders in key sectors of the global economy. CIPL’s mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL’s work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL’s website at <http://www.informationpolicycentre.com/>. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth LLP.