Client Alert | Data, Privacy & Cybersecurity / Technology

Guidelines on the Certification Mechanisms under the GDPR

July 2019

Authors: Tim Hickman, Kimberly Sharp

The European Data Protection Board ("**EDPB**") has published guidelines on the use of the certification mechanism under the GDPR. Certifications are intended to help businesses provide evidence of compliance with the GDPR. The guidelines provide insight into the relevant criteria that will be considered when assessing applications for certification.

Overview

The primary purpose of certifications is to provide businesses with a formal means of demonstrating compliance with their obligations under the General Data Protection Regulation (the "**GDPR**"). Certification typically comes with an associated visual symbol (e.g., a badge or emblem that can be displayed on published documents and websites, confirming that the relevant business satisfies the requirements of the relevant seal or certification). The GDPR provides for a voluntary system of accreditation, under which businesses may adhere to the requirements of a certification scheme, for the purpose of demonstrating compliance with the GDPR.

The EDPB has published Guidelines 1/2018 on certification and identifying certification criteria in accordance with Article 42 and 43 of the GDPR (the "**Guidelines**"). The primary aim of the Guidelines is to identify overarching criteria that may be relevant in assessing certification mechanisms. The EDPB specifically states that the Guidelines will be relevant for Data Protection Authorities, certification bodies and businesses (whether acting as controllers or processors) when defining their own GDPR compliance strategy, and considering certification as a means to demonstrate compliance.

Certification under the GDPR

Article 42(1) of the GDPR allows for the creation of certification schemes, for the purpose of enabling businesses to demonstrate compliance with the GDPR. However, implementing a certification scheme is a difficult and time-consuming exercise. The GDPR therefore imposes a legal obligation on EU Member States, Data Protection Authorities, the EDPB, and the European Commission, to take steps to encourage the establishment of data protection certification schemes, and the use of data protection seals and marks, for the purpose of demonstrating GDPR compliance. Recital 100 of the GDPR explains that certification schemes are intended to enhance transparency and compliance with the GDPR, and allow individuals to easily understand the level of GDPR compliance that a business has achieved.

EDPB Guidelines – What can be certified under the GDPR?

The Guidelines focus on helping businesses to demonstrate compliance with the GDPR. When assessing any data processing activity, the following three core components must be considered:

- the personal data being processed, and the GDPR compliance requirements triggered by that processing;

- the technical systems used to carry out the processing – i.e., the relevant hardware and software, relevant staffing arrangements, and so on; and
- internal rules, processes, and procedures governing the relevant processing activities.

EDPB Guidelines – Certification Criteria

The Guidelines set out guidance on the criteria that certification schemes should use to assess the level of compliance achieved by businesses. The EDPB has stated that the criteria should focus on:

- verifiability (i.e., whether compliance with the relevant criterion can be assessed and confirmed);
- significance (i.e., how important the relevant criterion is to determining GDPR compliance); and
- suitability (i.e., how appropriate the relevant criterion is for the purposes of assessing GDPR compliance).

These criteria need to be clear, comprehensible and capable of practical implementation. The Guidelines go on to set out issues that certification schemes will be expected to address before they can be accredited by the EDPB. These include ensuring that certification schemes are capable of verification, are tailored to the relevant target audience (e.g., specific industry sectors) and interoperable with other standards (e.g., relevant ISO standards).

Impact on businesses

In principle, certification mechanisms will provide businesses with the ability to demonstrate that their processing activities are GDPR-compliant, allowing them to improve transparency for affected individuals and other businesses with whom they interact. There could also be financial benefits for businesses, as adherence to approved certification mechanisms is a factor Data Protection Authorities must consider as a mitigating factor when imposing fines under the GDPR (Article 83(2)(j) of the GDPR).

On the other hand, most businesses have no real experience of using certification schemes in a data protection context, and the fact that the EDPB felt it necessary to issue almost 30 pages of Guidelines on this topic indicates that significant clarifications were needed. Moreover, assessing GDPR compliance, even in relation to a single processing activity, is often a complex task that requires a significant investment of time.

Consequently, there remain potential pitfalls for businesses that seek to participate in, and rely on, certification schemes to demonstrate their GDPR compliance. Businesses should therefore welcome the Guidelines with cautious optimism, being aware of the potential benefits that certification has to offer, but equally being cognizant of the fact that early adoption may not be a smooth process.

White & Case LLP
5 Old Broad Street
London EC2N 1DW
United Kingdom

T +44 20 7532 1000