May 17, 2019

UK's ICO invites enquiries from organisations considering developing a GDPR certification scheme

Attorneys
Rohan Massey

The UK Information Commissioner's Office ("ICO") is welcoming enquiries from organisations that are considering developing a General Data Protection Regulation ("GDPR") certification scheme. The announcement comes alongside updated ICO guidance on certification under the GDPR, as the European Data Protection Board ("EDPB") completes a round of consultations with a view to adopting a full set of guidelines and annexes on certification, identifying certification criteria and the accreditation of certification bodies. Member States and supervisory authorities such as the ICO, along with the EDPB and the European Commission, are required to encourage the use of certification mechanisms as a means to enhance transparency and compliance with the GDPR. The submission process for certification schemes will open once the EDPB guidelines are finalised.

Certification under the GDPR

Article 42(1) GDPR provides that:

"The Member States, the supervisory authorities, the [European Data Protection] Board and the European Commission shall encourage, in particular at the Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account."

The GDPR says that certification is also a means to demonstrate data protection by design and by default and that appropriate technical and organisational measures are in place to ensure data security. Certification may also support transfers of personal data to third countries or international organisations. The EDPB is drafting guidelines on certification as an appropriate safeguard for international transfers of personal data.

Certification is therefore a voluntary method for an organisation to demonstrate compliance with GDPR, in line with the accountability principle. The ICO describes it as a practical way for data controllers and processors to demonstrate data protection to other businesses, individuals and regulators, and to give customers a means to quickly assess the level of data protection of a particular product or service, which provides transparency both for individuals and in business-to-business relationships.

Certification in the UK

The ICO guidance explains what the certification framework in the UK will involve. The ICO will publish accreditation requirements for certification bodies to meet. Certification bodies will be accredited by the UK's national accreditation body, UKAS, which will maintain a public register. The ICO will approve and publish certification scheme criteria which will be derived from GDPR principles and rules. Certification scheme criteria must be auditable (i.e. specify objectives and how they can be achieved so as to demonstrate compliance) and inter-operable with other standards, for example ISO standards. Controllers and processors can then apply for certification for their processing operations and services. Accredited certification bodies, using independent assessors, can assess eligibility and issue certification against those criteria. Once an organisation has been successfully assessed, it will be issued with a data protection certificate, seal or mark relevant to that scheme. Certification is valid for a maximum of three years, subject to periodic reviews. Certifications can be withdrawn if the organisation no longer meets the certification criteria.

Across EU Member States, the EDPB will collate all EU certification schemes in a public register. There is also scope for a European Data Protection Seal where scheme criteria are approved by the EDPB for use in all Member States.

Scope of a certification scheme

The ICO explains that the scope of a certification scheme could be general or specific, for example, secure storage and protection of personal data contained within a digital vault. Certification can therefore relate to a specific personal data processing operation or set of operations. Those processing operations will be assessed against the certification scheme criteria by the accredited certification body.

Certification can only be issued to data controllers and data processors and cannot therefore be used to certify individuals, for example, data protection officers. Article 42(2) of the GDPR also allows for the use of certification schemes to demonstrate the existence of appropriate safeguards provided by controllers or processors that are not subject to GDPR for international transfers of personal data.

Next steps

There are as yet no approved certification schemes or accredited certification bodies for issuing GDPR certificates. Once the certification bodies have been accredited to issue GDPR certificates, this information will be published on the ICO's and UKAS's websites. Final publication of certification and accreditation guidelines and annexes is expected this summer. Once the EDPB accreditation requirements are finalised, the ICO will submit its own additional requirements to EDPB for its opinion. Following final approval of the certification annex, the ICO can start accepting certification schemes for approval.

Comment

The ICO is promoting certification schemes as a way for organisations to gain a competitive advantage by enabling businesses or individuals to distinguish which processing activities, operations and services meet GDPR data protection requirements and they can "trust" with their personal data. Indeed, the ICO suggests that, when contracting work to third parties, to help meet its due diligence requirements under the GDPR, an organisation may wish to consider whether they hold a GDPR certificate for their processing operations.

The ICO nevertheless forewarns organisations that while certification can help demonstrate compliance, it does not reduce their data protection responsibilities. Whilst certification will be considered as a mitigating factor when the ICO is considering imposing a fine, non-compliance with a certification scheme could also be a reason for issuing a fine.