March 23, 2020

GDPR Codes of Conduct and Certification schemes – the ICO is "open for business"

Attorneys
Robert Lister

Accountability is a key element of GDPR compliance and Codes of Conduct and Certification schemes will, in the words of Ian Hulme, ICO Director of Regulatory Assurance, provide "a really good way" for data controllers and processors to demonstrate their commitment to it. While no such codes or certification schemes have yet been approved by the ICO, the UK regulator is promoting their uptake after finalising the criteria underpinning the establishment of both mechanisms in the UK with the European Data Protection Board.

Marking a significant step forward, the ICO is now formally inviting organisations to submit their sector-specific codes and scheme criteria for its approval. To assist with the process, the ICO has published guidance for organisations wanting to develop GDPR Codes of Conduct or Certification schemes.

Codes of Conduct

Under the GDPR, trade associations and other representative bodies may draw up codes of conduct that identify and address data protection issues that are important to their members. To encourage the development of codes of conduct, the ICO is offering advice on meeting the necessary criteria.

A draft code of conduct submitted to the ICO for approval will be assessed against specific criteria to ensure that it meets the expected standard. These include the code owner's ability to represent controllers or processors covered by its code, and identifying processing operations that the code covers and the categories of controllers or processors that it applies to, as well as what the data protection issues are that it intends to address. The code must also specify whether it is a national code or a code which covers processing activities in more than one EU Member State.

The code must also define suitable monitoring methods to assess member compliance with the code and outline appropriate action in cases of infringement. Codes of conduct covering the private sector, or any non-public bodies, will also have to identify an independent monitoring body to fulfil the code's monitoring requirements. The monitoring body must be "accredited" by the ICO against criteria that have now been formally approved by the EDPB. Code owners will therefore need to demonstrate to the ICO that the monitoring body can act free from sanctions or external influence, has the necessary expertise and resources, and has an open and transparent complaints-handling process. It will also be responsible for ensuring that the code remains relevant and up to date.

Certification schemes

UK organisations can now submit proposals to the ICO for Certification scheme criteria approval. Once scheme criteria have been approved, UK organisations can then, if desired, apply to the UK's national accreditation body, UKAS, to be accredited to deliver GDPR Certification schemes. This accreditation process could take up to 18 months.

Following scheme approval by the ICO and accreditation by UKAS of applicable certification bodies, controllers and processors will be able to apply for GDPR certification. The certification body will then assess the applicant organisation against ICO-approved certification scheme criteria, derived from GDPR principles and rules, as relevant to the scope of certification. Once an organisation has been successfully assessed by the accredited certification body, it will be issued with a data protection certificate, seal or mark relevant to that scheme.

As the ICO's guidance explains, any particular scheme could be quite general and be applied to a variety of different products, processes or services; or it could be specific, for example, secure storage and protection of personal data contained within a digital vault. Alternatively, the scope of the scheme could be focused on only one area of the GDPR, for example, transparency or automated decision-making.

Article 42(2) GDPR also allows for the use of certification schemes for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to GDPR for international transfers of personal data.

Comment

Whether you're considering signing up to a code of conduct or applying for certification under a GDPR scheme (once available), the message from the ICO is the same. As well as helping controllers and processors demonstrate compliance, both mechanisms can deliver a competitive advantage by engendering trust not only with individuals whose personal data is being processed but also between contracting parties who share personal data. Article 42(2) GDPR could also prove to be a significant provision in the context of legitimatising transfers of personal data to third countries.

However, membership of a code or holding a data protection certification will not reduce responsibility either inside or outside the scope of the code or scheme, and the ICO will also take into account both participation and non-adherence to a code or scheme criteria when enforcing the GDPR against organisations. In addition, given that no such codes or certification schemes have yet been approved by the ICO (and the accreditation process for certification bodies could be a slow process), it may be some time before controllers and processors can actually take advantage of either mechanism.