ONTIER

PRIVACY AND DATA PROTECTION INTERNATIONAL TEAM

27th June 2017
#13

Index

CERTIFICATION AND CERTIFICATION BODIES

The GDPR specifically recognises and promotes the use of certifications and privacy seals as a voluntary way for organisations to show to their customers that they take data protection compliance seriously.

Current situation

Under the current Directive there is no formal recognition of data protection seals and / or certificates. Moreover, some Member States and sectors provide for non-compulsory seals and certifications for privacy. Examples of these voluntary seals and certifications include EuroPriSe (the European Privacy Seal which is a scheme across the EU mainly used within the IT sector) and France's own national seal scheme. A few private sector organisations such as TRUSTe and the European Interactive Digital Advertising Alliance ("EDDA") also have their own privacy seal schemes for members.

What's new?

Certification and Certification Bodies are addressed by an entirely new section of the GDPR. In fact, Member States unanimously supported this section throughout the negotiations and the drafting of the GDPR.

Article 42 of the GDPR states that Member States, national supervisory authorities, the European Data Protection Board ("EDPB") and the Commission itself shall "*encourage, in particular at 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 Regulation clearly pushes the idea of privacy certifications and seals, and lays down a framework for the adoption of such seals and certifications. The purpose of certification schemes is to provide organisations with a formally recognised way to show their customers and clients that they are in compliance with EU data protection law. This could be done, for example, by way of a badge that can be used on their website and on their publications. In addition to adherence of the GDPR by Data Controllers and Data Processors, seals and certification can be used to demonstrate the existence of appropriate safeguards that are put in place by the Data Controller or Data Processor such as increased transparency and accountability. It may also provide some mitigation against any enforcement actions in the event of an infringement of the GDPR and allow customers and clients to assess the level of data protection of a particular product or service being offered by a particular organisation.

An organisation may apply for a certification or seal by providing all the necessary information and by submitting its relevant processing activities to the relevant supervisory authority or accredited certified body that oversees the relevant scheme.

All seals and certifications will be voluntary so a Data Controller or a Data Processor's obligation under the GDPR will not be reduced if they have a seal or certification, but it may go towards supporting any investigation into its GDPR compliance.

Any certification or seal awarded has a maximum term of three years which can be renewed provided the Data Controller/Data Processor still meets the relevant criteria. If the criteria is not met, the certification is likely to be withdrawn.

All seals and certifications will be awarded by accredited certified bodies. Article 43 of the GDPR sets out the criteria to be met before a certified body becomes accredited. National

accreditation bodies and/or national supervisory authorities may accredit certified bodies (so that they can issue certificates, marks and/or seals), regardless of whether they are a public or private body, provided (inter alia) they:

a) can demonstrate their independence and expertise in relation to the subject matter of the certification;

b) have established procedures for the issuing, periodic reviewing and withdrawal of data protection certification, seals and marks;

c) have established procedures for handling complaints about infringement of the certification; and

d) can demonstrate that their tasks and duties do not result in a conflict of interest.

Specific criteria for accreditation will be developed by the national supervisory authorities or the EDPB and will be publicly available in due course. Accreditations for certification bodies will be issued for a maximum of five years and will be subject to renewals, as well as withdrawals in cases where the criteria for the accreditation are no longer met.

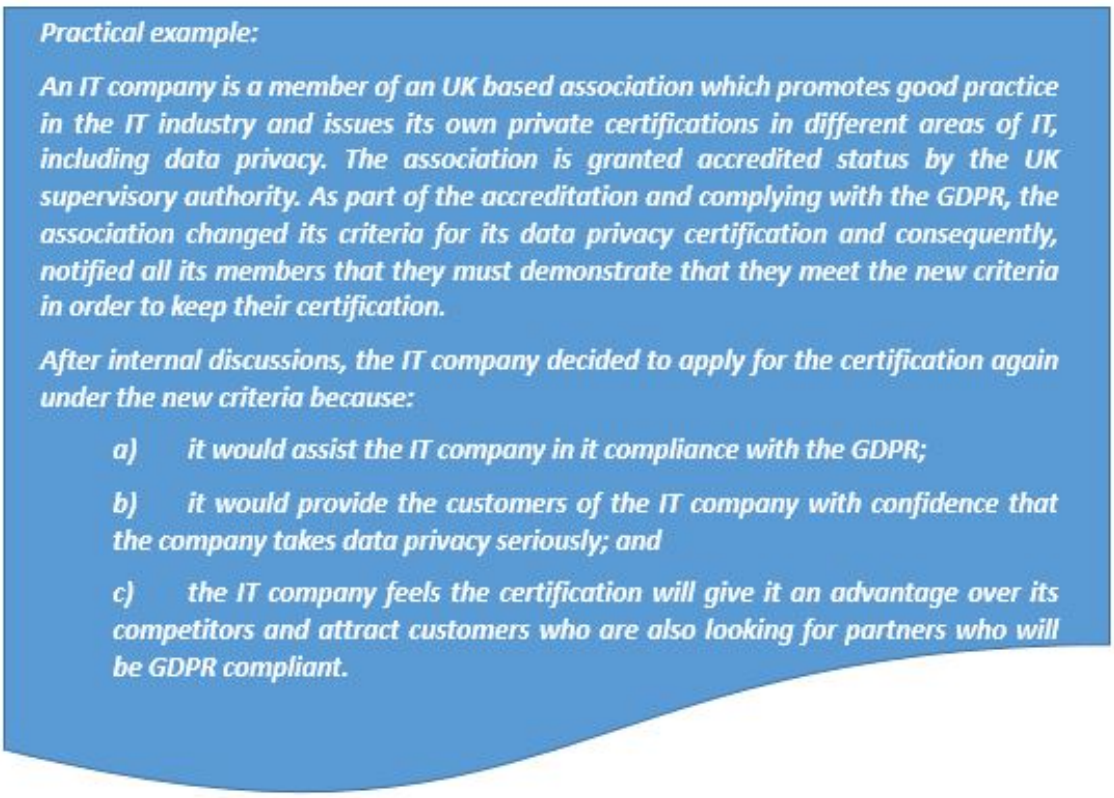
The EDPB is to maintain a publicly available register with all certification mechanisms, data protections seals and marks. The EDPB may also create a common ‘European Data Protection Seal’. The idea behind this is that there would be one uniform body to authenticate an organisation’s compliance with the GDPR.

It is expected that the Article 29 Working Party will issue guidelines on certifications in 2017 (no specific date has been set for this release at the time of writing). It is also expected that the existing seals or certification schemes currently in place around the EU will gradually be harmonised under the GDPR.

What to do to adapt?

Data Controllers and Data Processors should follow developments in relation to accreditation of applicable certification bodies and consider whether they wish to apply for such certification, seal or mark in due course. If a Data Controller or Data Processor already has existing privacy certifications, seals or marks, they should review the status of such certification, seal or mark to see if they remain compliant with the relevant criteria following any changes as a result of the GDPR. Finally, they should be prepared to re-apply under any revised rules and conditions.

A Data Controller may also wish to take into consideration whether a proposed Data Processor it is looking to contract with has a certification, seal or mark in relation to data protection to ensure that the Data Processor’s procedures in relation to data privacy are of a certain standard.



Practical example

An IT company is a member of an UK based association which promotes good practice in the IT industry and issues its own private certifications in different areas of IT, including data privacy. The association is granted accredited status by the UK supervisory authority. As part of the accreditation and complying with the GDPR, the association changed its criteria for its data privacy certification and consequently, notified all its members that they must demonstrate that they meet the new criteria in order to keep their certification.

After internal discussions, the IT company decided to apply for the certification again under the new criteria because:

a) it would assist the IT company in it compliance with the GDPR;

b) it would provide the customers of the IT company with confidence that the company takes data privacy seriously; and

c) the IT company feels the certification will give it an advantage over its competitors and attract customers who are also looking for partners who will be GDPR compliant.

TEAM

Joaquin Muñoz Rodríguez (Spain)
Pablo Uslé Presmanes (Spain)

Derek Stinson (UK)
Paula Enríquez (UK)

Ana Rocha (Portugal)
Joana Cunha de Miranda (Portugal)

Luca Pardo (Italy)
Giulio Ciompi (Italy)

Read more:

about us

Share on:

Linkedin Twitter

Subscribe:

our Newsletters

Contact us:

Website | LinkedIn

Rua Vitor Cordon Nº 10A - 1249 - 202 Lisboa | Portugal
Tel. (+351) 213 223 590 / Fax (+351) 213 223 599

Rua Pedro Homem de Melo, n.º 55, 8º piso - 4150 - 599 Porto | Portugal
Tel. (+351) 223 190 888 / Fax (+351) 220 924 945

PORTUGAL / **SPAIN** / **U.K** / BOLIVIA / / BRAZIL / CHILE / CHINA / COLOMBIA

USA / **ITALY** / MEXICO / PERU / VENEZUELA

This article is provided for information purposes only and does not constitute legal advice. Professional legal advice should be obtained before taking or refraining from any action as a result of the contents of this document. If you have any queries regarding this article, please contact CCA Ontier or ar@cca-ontier.com.