Codes of conduct and certifications

At a glance

The GDPR makes provision for the approval of codes of conduct ("Codes") and the accreditation of certifications, seals and marks to help controllers and processors demonstrate compliance and best practice.

Codes of conduct:

- Associations and representative bodies may prepare Codes for approval, registration and publication by a supervisory authority, or, where processing activities take place across member states, by the European Data Protection Board ("EDPB"). The EU Commission may declare Codes recommended by EDPB to have general validity within the EU.
- Codes may be approved in relation to a wide range of topics and adherence to Codes will help controllers and processors demonstrate compliance with GDPR obligations.
- Compliance with Codes will be subject to monitoring, which may be carried out by suitably qualified, accredited bodies. Controllers and processors who are found to have infringed a relevant code may be suspended from participation in the Code and reported to the supervisory authority.

Certifications, seals and marks:

- The establishment of data protection certification mechanisms and of seals and marks is to be encouraged.
- Certificates will be issued by accredited certifying bodies (yet to be established).
- Certification is voluntary but certification will enable controllers and processors to demonstrate compliance with the GDPR.
- Certificates will be valid for three years and subject to renewal.
- EDPB will maintain a publicly available register of all certification mechanisms, seals and marks.

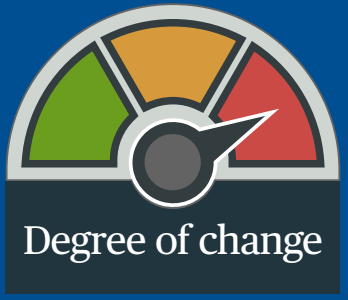
To do list

Codes of Conduct

- In order to get a head-start before the accreditation procedures are laid out by the supervisory authorities, processors (such as cloud providers) and controllers within specific sectors should consider identifying, or establishing, associations or representative bodies that could develop Codes for approval by supervisory authorities.

Certification, seals and marks

- Processors and controllers should follow developments in relation to the accreditation of certification bodies, and consider whether they will wish to apply for certification in due course.
- Once certification schemes are established, controllers should familiarise themselves with relevant schemes and take account of certifications, seals and marks when selecting their processors/ service providers.



Codes of conduct

Codes are an important component in broadening and adapting the tools for data protection compliance that controllers and processors can draw on, by way of a *"semi-self-regulating"* mechanism.

It is expected that Codes will provide authoritative guidance on certain key areas including:

- legitimate interest in specific contexts;
- pseudonymisation;
- exercise of data subjects' rights;
- protection of minors and modes of parental consent;
- proper implementation of privacy by design and by default, and security measures;
- security breach notification; and
- dispute resolution between controllers and data subjects.

The development and the approval of Codes are likely to deliver a number of benefits including:

- establishing and updating best practice for compliance in specific processing contexts;
- enabling data controllers and processors to commit to compliance with recognised standards and practices and be recognised for doing so;
- adherence to Codes can demonstrate that data importers (controllers as well as processors) located outside the EU / EEA have implemented adequate safeguards in order to permit transfers under Article 46; transfers made on the basis of an approved code of conduct together with binding and enforceable commitments of the importer to apply appropriate safeguards may take place without any specific authorisation from a supervisory authority and Codes may therefore offer an alternative mechanism for managing international transfers, standing on the same level as standard contractual clauses and BCR.

Approval of Codes

Codes proposed by associations or representative bodies in relation to data processing activities that affect only one member state are to be submitted to the competent supervisory authority, for comment and – subject to possible modifications or extensions – approval. If a Code covers processing operations in several Member States, it should be submitted to the EDPB for an opinion. Subject to possible modifications or extensions, the Code and the EDPB opinion may then be submitted to the European Commission which, upon due examination, may declare its general validity.

Codes are to be kept and made available in publicly accessible registers.

Monitoring of compliance

Monitoring of compliance with Codes will be carried out only by bodies accredited by the competent supervisory authority.

In order to become accredited such bodies will have to demonstrate:

- their independence and expertise;
- that they have established procedures to assess the ability of controllers and processors to apply the Code, and to monitor compliance, as well as periodically review the Code;
- the ability to deal with complaints about infringements; and
- that they have processes in place to avoid conflicts of interest.

Accreditations are revocable if the conditions for the accreditation are no longer met.

Certifications, seals and marks

The concept of certifying data processing operations is a significant development in creating a reliable and auditable framework for data processing operations. It is likely to be particularly relevant in the context of cloud computing and other forms of multi-tenancy services, where individual audits are often not feasible in practice.

Member States, supervisory authorities, the EDPB and the Commission are all encouraged to establish data protection certification mechanisms, seals and marks, with regard to specified processing operations.

Certifications are voluntary. The competent supervisory authority or the EDPB will approve criteria for the certifications. The EDPB may develop criteria for a common certification, the European Data Protection Seal.

There are two key advantages of certificates:

1. controllers and processors will be able to demonstrate compliance, in particular with regard to implementing technical and organisational measures.

2. certificates can demonstrate that data importers (controllers as well as processors) located outside the EU / EEA have implemented adequate safeguards for the purpose of Article 46; transfers made on the basis of an approved certification mechanism together with binding and enforceable commitments of the importer to apply appropriate safeguards may take place without any specific authorisation from a supervisory authority and certificates therefore offer an alternative mechanism for managing international transfers, standing on the same level as standard contractual clauses and BCR.

Certificates on processing operations will be issued for a period of three years, and are subject to renewal or withdrawal where the conditions for issuing the certificate are no longer met.

The EDPB is to maintain a publicly available register with all certification mechanisms, data protections seals and marks.

Certificates can be issued by – private or public - accredited certification bodies. National Accreditation Bodies and/or supervisory authorities may accredit certification bodies (so that they can issue certificates, marks and seals), that (*inter alia*):

- have the required expertise and are independent with regard to the subject matter of certification;
- have procedures to review and withdraw certifications, seals and marks;
- are able to deal with complaints about infringements of the certifications; and
- have rules to deal with conflicts of interest.

Criteria for accreditation will be developed by the supervisory authorities or the EDPB and will be publicly available.

Accreditations for certification bodies will be issued for a maximum of five years and are subject to renewals, as well as withdrawals in cases where conditions for the accreditation are no longer met.

Where can I find this?

Codes of conduct
Articles 24, 28(5) 32, 40, 41, 57, 58, 64, 70, 83
Recitals 77, 81, 98, 99, 148, 168

Certifications, seals and marks
Articles 24, 25, 28, 32, 42, 43
Recitals 77, 81, 100, 166, & 168