

Regulation (EU) 2016/679 of the European Parliament and of the Council
of 27 April 2016 on the protection of natural persons with regard to the
processing of personal data and on the free movement of such data, and repealing
Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)

CHAPTER IV

Controller and processor

Section 5

Codes of conduct and certification

Article 40

Codes of conduct

1 The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.

2 Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to:

- a fair and transparent processing;
- b the legitimate interests pursued by controllers in specific contexts;
- c the collection of personal data;
- d the pseudonymisation of personal data;
- e the information provided to the public and to data subjects;
- f the exercise of the rights of data subjects;
- g the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained;
- h the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32;
- i the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects;
- j the transfer of personal data to third countries or international organisations; or
- k out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79.

3 In addition to adherence by controllers or processors subject to this Regulation, codes of conduct approved pursuant to paragraph 5 of this Article and having general validity pursuant to paragraph 9 of this Article may also be adhered to by controllers or processors that are not subject to this Regulation pursuant to Article 3 in order to provide appropriate safeguards within the framework of personal data transfers to third countries or international organisations under

the terms referred to in point (e) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards including with regard to the rights of data subjects.

4 A code of conduct referred to in paragraph 2 of this Article shall contain mechanisms which enable the body referred to in Article 41(1) to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors which undertake to apply it, without prejudice to the tasks and powers of supervisory authorities competent pursuant to Article 55 or 56.

5 Associations and other bodies referred to in paragraph 2 of this Article which intend to prepare a code of conduct or to amend or extend an existing code shall submit the draft code, amendment or extension to the supervisory authority which is competent pursuant to Article 55. The supervisory authority shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation and shall approve that draft code, amendment or extension if it finds that it provides sufficient appropriate safeguards.

6 Where the draft code, or amendment or extension is approved in accordance with paragraph 5, and where the code of conduct concerned does not relate to processing activities in several Member States, the supervisory authority shall register and publish the code.

7 Where a draft code of conduct relates to processing activities in several Member States, the supervisory authority which is competent pursuant to Article 55 shall, before approving the draft code, amendment or extension, submit it in the procedure referred to in Article 63 to the Board which shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation or, in the situation referred to in paragraph 3 of this Article, provides appropriate safeguards.

8 Where the opinion referred to in paragraph 7 confirms that the draft code, amendment or extension complies with this Regulation, or, in the situation referred to in paragraph 3, provides appropriate safeguards, the Board shall submit its opinion to the Commission.

9 The Commission may, by way of implementing acts, decide that the approved code of conduct, amendment or extension submitted to it pursuant to paragraph 8 of this Article have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

10 The Commission shall ensure appropriate publicity for the approved codes which have been decided as having general validity in accordance with paragraph 9.

11 The Board shall collate all approved codes of conduct, amendments and extensions in a register and shall make them publicly available by way of appropriate means.

Article 41

Monitoring of approved codes of conduct

1 Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, the monitoring of compliance with a code of conduct pursuant to Article 40 may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the competent supervisory authority.

2 A body as referred to in paragraph 1 may be accredited to monitor compliance with a code of conduct where that body has:

Status: This is the original version (as it was originally adopted).

- a demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority;
- b established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;
- c established procedures and structures to handle complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make those procedures and structures transparent to data subjects and the public; and
- d demonstrated to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.

3 The competent supervisory authority shall submit the draft criteria for accreditation of a body as referred to in paragraph 1 of this Article to the Board pursuant to the consistency mechanism referred to in Article 63.

4 Without prejudice to the tasks and powers of the competent supervisory authority and the provisions of Chapter VIII, a body as referred to in paragraph 1 of this Article shall, subject to appropriate safeguards, take appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code. It shall inform the competent supervisory authority of such actions and the reasons for taking them.

5 The competent supervisory authority shall revoke the accreditation of a body as referred to in paragraph 1 if the conditions for accreditation are not, or are no longer, met or where actions taken by the body infringe this Regulation.

6 This Article shall not apply to processing carried out by public authorities and bodies.

Article 42

Certification

1 The Member States, the supervisory authorities, the Board and the Commission 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.

2 In addition to adherence by controllers or processors subject to this Regulation, data protection certification mechanisms, seals or marks approved pursuant to paragraph 5 of this Article may be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation pursuant to Article 3 within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (f) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including with regard to the rights of data subjects.

3 The certification shall be voluntary and available via a process that is transparent.

4 A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authorities which are competent pursuant to Article 55 or 56.

5 A certification pursuant to this Article shall be issued by the certification bodies referred to in Article 43 or by the competent supervisory authority, on the basis of criteria approved by that competent supervisory authority pursuant to Article 58(3) or by the Board pursuant to Article 63. Where the criteria are approved by the Board, this may result in a common certification, the European Data Protection Seal.

6 The controller or processor which submits its processing to the certification mechanism shall provide the certification body referred to in Article 43, or where applicable, the competent supervisory authority, with all information and access to its processing activities which are necessary to conduct the certification procedure.

7 Certification shall be issued to a controller or processor for a maximum period of three years and may be renewed, under the same conditions, provided that the relevant requirements continue to be met. Certification shall be withdrawn, as applicable, by the certification bodies referred to in Article 43 or by the competent supervisory authority where the requirements for the certification are not or are no longer met.

8 The Board shall collate all certification mechanisms and data protection seals and marks in a register and shall make them publicly available by any appropriate means.

Article 43

Certification bodies

1 Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, certification bodies which have an appropriate level of expertise in relation to data protection shall, after informing the supervisory authority in order to allow it to exercise its powers pursuant to point (h) of Article 58(2) where necessary, issue and renew certification. Member States shall ensure that those certification bodies are accredited by one or both of the following:

- a the supervisory authority which is competent pursuant to Article 55 or 56;
- b the national accreditation body named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council⁽¹⁾ in accordance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the supervisory authority which is competent pursuant to Article 55 or 56.

2 Certification bodies referred to in paragraph 1 shall be accredited in accordance with that paragraph only where they have:

- a demonstrated their independence and expertise in relation to the subject-matter of the certification to the satisfaction of the competent supervisory authority;
- b undertaken to respect the criteria referred to in Article 42(5) and approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63;
- c established procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks;
- d established procedures and structures to handle complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make those procedures and structures transparent to data subjects and the public; and
- e demonstrated, to the satisfaction of the competent supervisory authority, that their tasks and duties do not result in a conflict of interests.

3 The accreditation of certification bodies as referred to in paragraphs 1 and 2 of this Article shall take place on the basis of criteria approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63. In the case of accreditation pursuant to point (b) of paragraph 1 of this Article, those requirements shall complement those envisaged in Regulation (EC) No 765/2008 and the technical rules that describe the methods and procedures of the certification bodies.

4 The certification bodies referred to in paragraph 1 shall be responsible for the proper assessment leading to the certification or the withdrawal of such certification without prejudice to the responsibility of the controller or processor for compliance with this Regulation. The accreditation shall be issued for a maximum period of five years and may be renewed on the same conditions provided that the certification body meets the requirements set out in this Article.

5 The certification bodies referred to in paragraph 1 shall provide the competent supervisory authorities with the reasons for granting or withdrawing the requested certification.

6 The requirements referred to in paragraph 3 of this Article and the criteria referred to in Article 42(5) shall be made public by the supervisory authority in an easily accessible form. The supervisory authorities shall also transmit those requirements and criteria to the Board. The Board shall collate all certification mechanisms and data protection seals in a register and shall make them publicly available by any appropriate means.

7 Without prejudice to Chapter VIII, the competent supervisory authority or the national accreditation body shall revoke an accreditation of a certification body pursuant to paragraph 1 of this Article where the conditions for the accreditation are not, or are no longer, met or where actions taken by a certification body infringe this Regulation.

8 The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of specifying the requirements to be taken into account for the data protection certification mechanisms referred to in Article 42(1).

9 The Commission may adopt implementing acts laying down technical standards for certification mechanisms and data protection seals and marks, and mechanisms to promote and recognise those certification mechanisms, seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

Status: This is the original version (as it was originally adopted).

- (1) Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 ([OJ L 218, 13.8.2008, p. 30](#)).