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

CHAPTER IV

Controller and processor

Section 1

General obligations

Article 24

Responsibility of the controller

1   Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

2   Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

3   Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.

Article 25

Data protection by design and by default

1   Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2   The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular,

such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

3 An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

Article 26

Joint controllers

1 Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by [**F1**domestic law]. The arrangement may designate a contact point for data subjects.

2 The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers *vis-à-vis* the data subjects. The essence of the arrangement shall be made available to the data subject.

3 Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

Textual Amendments

F1 Words in Art. 26(1) substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 20** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

Article 27

Representatives of controllers or processors not established in [F2**the United Kingdom]**

1 Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in [**F3**the United Kingdom].

2 The obligation laid down in paragraph 1 of this Article shall not apply to:

 a processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or

 b a public authority or body.

F43 . . . .

4 The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, [**F5**the Commissioner] and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation.

5   The designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves.

Textual Amendments

F2   Words in Art. 27 heading substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 21(2)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

F3   Words in Art. 27(1) substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 21(3)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

F4   Art. 27(3) omitted (31.12.2020) by virtue of The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 21(4)** (with reg. 5, Sch. 1 para. 80); 2020 c. 1, Sch. 5 para. 1(1)

F5   Words in Art. 27(4) substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 21(5)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

Article 28

Processor

1   Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

2   The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

3   Processing by a processor shall be governed by a contract or other legal act under [**F6**domestic law], that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

   a   processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by [**F7**domestic law]; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

   b   ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

   c   takes all measures required pursuant to Article 32;

   d   respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;

   e   taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

f   assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;

g   at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless [**F8**domestic law] requires storage of the personal data;

h   makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or [**F9**other domestic law relating to data protection].

4   Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under [**F10**domestic law], in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

5   Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.

6   Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in [**F11**paragraph 8] of this Article, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43.

F127   . . . .

8   [**F13**The Commissioner] may adopt standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article **F14**... .

9   The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.

10   Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

Textual Amendments

F6   Words in Art. 28(3) substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 22(2)(a)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

F7   Words in Art. 28(3)(a) substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 22(2)(b)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27...
CHAPTER IV Section 1
Document Generated: 2024-05-23

5

F8 Words in Art. 28(3)(g) substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 22(2)(c)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

F9 Words in Art. 28(3) substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 22(2)(d)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

F10 Words in Art. 28(4) substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 22(3)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

F11 Words in Art. 28(6) substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 22(4)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

F12 Art. 28(7) omitted (31.12.2020) by virtue of The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 22(5)** (with reg. 5, Sch. 1 para. 80); 2020 c. 1, Sch. 5 para. 1(1)

F13 Words in Art. 28(8) substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 22(6)(a)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

F14 Words in Art. 28(8) omitted (31.12.2020) by virtue of The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 22(6)(b)** (with reg. 5, Sch. 1 para. 80); 2020 c. 1, Sch. 5 para. 1(1)

Article 29

Processing under the authority of the controller or processor

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by [**F15**domestic law].

Textual Amendments

F15 Words in Art. 29 substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 23** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

Article 30

Records of processing activities

1   Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

  a   the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

  b   the purposes of the processing;

  c   a description of the categories of data subjects and of the categories of personal data;

  d   the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

- e   where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
- f   where possible, the envisaged time limits for erasure of the different categories of data;
- g   where possible, a general description of the technical and organisational security measures referred to in Article 32(1) **[F16**or, as appropriate, the security measures referred to in section 28(3) of the 2018 Act]**.

2   Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:
- a   the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
- b   the categories of processing carried out on behalf of each controller;
- c   where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
- d   where possible, a general description of the technical and organisational security measures referred to in Article 32(1) **[F17**or, as appropriate, the security measures referred to in section 28(3) of the 2018 Act]**.

3   The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

4   The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to **[F18**the Commissioner]** on request.

5   The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

Textual Amendments

F16   Words in Art. 30(1)(g) inserted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 24(2)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

F17   Words in Art. 30(2)(d) inserted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 24(3)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

F18   Words in Art. 30(4) substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 24(4)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27...
CHAPTER IV Section 2
Document Generated: 2024-05-23

7

Article 31

Cooperation with [F19the Commissioner]

The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with [F20the Commissioner in the performance of the Commissioner's tasks].

Textual Amendments

F19 Words in Art. 31 heading substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 25(2)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

F20 Words in Art. 31 substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 25(3)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

Section 2

Security of personal data

Article 32

Security of processing

1   Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

   a   the pseudonymisation and encryption of personal data;

   b   the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

   c   the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

   d   a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2   In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3   Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4   The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not

8

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27...
CHAPTER IV Section 2
Document Generated: 2024-05-23

process them except on instructions from the controller, unless he or she is required to do so by [**F21**domestic law].

Textual Amendments

F21 Words in Art. 32(4) substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 26** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

Article 33

Notification of a personal data breach to [**F22**the Commissioner]

1   In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to [**F23**the Commissioner], unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where [**F24**the notification under this paragraph] is not made within 72 hours, it shall be accompanied by reasons for the delay.

2   The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3   The notification referred to in paragraph 1 shall at least:
   a   describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
   b   communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
   c   describe the likely consequences of the personal data breach;
   d   describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4   Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5   The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable [**F25**the Commissioner] to verify compliance with this Article.

Textual Amendments

F22 Words in Art. 33 heading substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 27(2)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

F23 Words in Art. 33(1) substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 27(3)(a)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

F24 Words in Art. 33(1) substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 27(3)(b)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

F25   Words in Art. 33(5) substituted (31.12.2020) by The Data Protection, Privacy and Electronic
Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1
para. 27(4)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

Article 34

Communication of a personal data breach to the data subject

1   When the personal data breach is likely to result in a high risk to the rights and
freedoms of natural persons, the controller shall communicate the personal data breach to the
data subject without undue delay.

2   The communication to the data subject referred to in paragraph 1 of this Article shall
describe in clear and plain language the nature of the personal data breach and contain at least
the information and measures referred to in points (b), (c) and (d) of Article 33(3).

3   The communication to the data subject referred to in paragraph 1 shall not be required
if any of the following conditions are met:
  a   the controller has implemented appropriate technical and organisational protection
       measures, and those measures were applied to the personal data affected by the personal
       data breach, in particular those that render the personal data unintelligible to any person
       who is not authorised to access it, such as encryption;
  b   the controller has taken subsequent measures which ensure that the high risk to the
       rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to
       materialise;
  c   it would involve disproportionate effort. In such a case, there shall instead be a public
       communication or similar measure whereby the data subjects are informed in an equally
       effective manner.

4   If the controller has not already communicated the personal data breach to the data
subject, **[F26the Commissioner]**, having considered the likelihood of the personal data breach
resulting in a high risk, may require it to do so or may decide that any of the conditions referred
to in paragraph 3 are met.

Textual Amendments
   F26   Words in Art. 34(4) substituted (31.12.2020) by The Data Protection, Privacy and Electronic
   Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1
   para. 28** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

Section 3

Data protection impact assessment and prior consultation

Article 35

Data protection impact assessment

1   Where a type of processing in particular using new technologies, and taking into
account the nature, scope, context and purposes of the processing, is likely to result in a high

risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

2   The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

3   A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

     a   a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

     b   processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

     c   a systematic monitoring of a publicly accessible area on a large scale.

4   [**F27**The Commissioner] shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. **F28**...

5   [**F29**The Commissioner] may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. **F30**...

F316   . . . .

7   The assessment shall contain at least:

     a   a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

     b   an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

     c   an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

     d   the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

8   Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.]

9   Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

[**F32**10   In the case of processing pursuant to point (c) or (e) of Article 6(1), paragraphs 1 to 7 of this Article do not apply if a data protection impact assessment has already been carried out for the processing as part of a general impact assessment required by domestic law, unless domestic law provides otherwise.]

11   Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

Textual Amendments

F27   Words in Art. 35(4) substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 29(2)(a)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

F28   Words in Art. 35(4) omitted (31.12.2020) by virtue of The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 29(2)(b)** (with reg. 5, Sch. 1 para. 80); 2020 c. 1, Sch. 5 para. 1(1)

F29   Words in Art. 35(5) substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 29(3)(a)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

F30   Words in Art. 35(5) omitted (31.12.2020) by virtue of The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 29(3)(b)** (with reg. 5, Sch. 1 para. 80); 2020 c. 1, Sch. 5 para. 1(1)

F31   Art. 35(6) omitted (31.12.2020) by virtue of The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 29(4)** (with reg. 5, Sch. 1 para. 80); 2020 c. 1, Sch. 5 para. 1(1)

F32   Art. 35(10) substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 29(5)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

Article 36

Prior consultation

1   The controller shall consult [**F33**the Commissioner] prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

2   Where [**F34**the Commissioner] is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, [**F34**the Commissioner] shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Article 58. That period may be extended by six weeks, taking into account the complexity of the intended processing. [**F35**The Commissioner] shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until [**F36**the Commissioner has obtained information the Commissioner] has requested for the purposes of the consultation.

3   When consulting [**F37**the Commissioner] pursuant to paragraph 1, the controller shall provide [**F37**the Commissioner] with:

    a   where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;

    b   the purposes and means of the intended processing;

  c   the measures and safeguards provided to protect the rights and freedoms of data subjects
       pursuant to this Regulation;
  d   where applicable, the contact details of the data protection officer;
  e   the data protection impact assessment provided for in Article 35; and
  f   any other information requested by [**F38**the Commissioner].

4   [**F39**The relevant authority must consult the Commissioner] during the preparation of
a proposal for a legislative measure to be adopted by [**F40**Parliament, the National Assembly for
Wales, the Scottish Parliament or the Northern Ireland Assembly], or of a regulatory measure
based on such a legislative measure, which relates to processing.

[**F41**4A.   In paragraph 4, "the relevant authority" means—
  a   in relation to a legislative measure adopted by Parliament, or a regulatory measure based
       on such a legislative measure, the Secretary of State;
  b   in relation to a legislative measure adopted by the National Assembly for Wales, or a
       regulatory measure based on such a legislative measure, the Welsh Ministers;
  c   in relation to a legislative measure adopted by the Scottish Parliament, or a regulatory
       measure based on such a legislative measure, the Scottish Ministers;
  d   in relation to a legislative measure adopted by the Northern Ireland Assembly, or a
       regulatory measure based on such a legislative measure, the relevant Northern Ireland
       department.]

F425   . . . .

Textual Amendments

  F33   Words in Art. 36(1) substituted (31.12.2020) by The Data Protection, Privacy and Electronic
            Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1
            para. 30(2)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)
  F34   Words in Art. 36(2) substituted (31.12.2020) by The Data Protection, Privacy and Electronic
            Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1
            para. 30(3)(a)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)
  F35   Words in Art. 36(2) substituted (31.12.2020) by The Data Protection, Privacy and Electronic
            Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1
            para. 30(3)(b)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)
  F36   Words in Art. 36(2) substituted (31.12.2020) by The Data Protection, Privacy and Electronic
            Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1
            para. 30(3)(c)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)
  F37   Words in Art. 36(3) substituted (31.12.2020) by The Data Protection, Privacy and Electronic
            Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1
            para. 30(4)(a)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)
  F38   Words in Art. 36(3)(f) substituted (31.12.2020) by The Data Protection, Privacy and Electronic
            Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1
            para. 30(4)(b)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)
  F39   Words in Art. 36(4) substituted (31.12.2020) by The Data Protection, Privacy and Electronic
            Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1
            para. 30(5)(a)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)
  F40   Words in Art. 36(4) substituted (31.12.2020) by The Data Protection, Privacy and Electronic
            Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1
            para. 30(5)(b)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

Changes to legislation: *There are currently no known outstanding effects for the Regulation (EU) 2016/679 of the European Parliament and of the Council, CHAPTER IV. (See end of Document for details)*

F41   Art. 36(4A) inserted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 30(6)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

F42   Art. 36(5) omitted (31.12.2020) by virtue of The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 30(7)** (with reg. 5, Sch. 1 para. 80); 2020 c. 1, Sch. 5 para. 1(1)

Section 4

Data protection officer

Article 37

Designation of the data protection officer

1   The controller and the processor shall designate a data protection officer in any case where:

   a   the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

   b   the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

[^{X1}c   the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 or personal data relating to criminal convictions and offences referred to in Article 10.]

2   A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

3   Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.

4   In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may ^{F43}... designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.

5   The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.

6   The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.

7   The controller or the processor shall publish the contact details of the data protection officer and communicate them to [^{F44}the Commissioner].

Editorial Information

   X1   Substituted by Corrigendum to 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) (Official Journal of the European Union L 119 of 4 May 2016).

Textual Amendments

F43   Words in Art. 37(4) omitted (31.12.2020) by virtue of The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 31(2)** (with reg. 5, Sch. 1 para. 80); 2020 c. 1, Sch. 5 para. 1(1)

F44   Words in Art. 37(7) substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 31(3)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

Article 38

Position of the data protection officer

1   The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

2   The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

3   The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

4   Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.

5   The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with [F45domestic law].

6   The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

Textual Amendments

F45   Words in Art. 38(5) substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 32** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

Article 39

Tasks of the data protection officer

1   The data protection officer shall have at least the following tasks:

   a   to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to [F46other domestic law relating to data protection];

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27...
CHAPTER IV Section 5
Document Generated: 2024-05-23

15

    b   to monitor compliance with this Regulation, with **[**^{F47}other domestic law relating to data protection**]** and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

    c   to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;

    d   to cooperate with **[**^{F48}the Commissioner**]**;

    e   to act as the contact point for **[**^{F49}the Commissioner**]** on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

2   The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

Textual Amendments

  F46 Words in Art. 39(1)(a) substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 33(2)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

  F47 Words in Art. 39(1)(b) substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 33(2)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

  F48 Words in Art. 39(1)(d) substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 33(3)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

  F49 Words in Art. 39(1)(e) substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 33(3)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

Section 5

Codes of conduct and certification

Article 40

Codes of conduct

1   **[**^{F50}The Commissioner**]** 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 [**F51**the Commissioner] 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 **F52**... 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 [**F53**the Commissioner].

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 [**F54**the Commissioner, who] 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 [**F55**the Commissioner finds] that it provides sufficient appropriate safeguards.

6   Where the draft code, or amendment or extension is approved in accordance with paragraph 5, [**F56**the Commissioner] shall register and publish the code.

F577   . . . .

F578   . . . .

F579   . . . .

F5710   . . . .

F5711   . . . .

Textual Amendments

    F50   Words in Art. 40(1) substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 34(2)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

    F51   Words in Art. 40(2)(i) substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 34(3)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27...
CHAPTER IV Section 5
Document Generated: 2024-05-23

17

F52   Words in Art. 40(3) omitted (31.12.2020) by virtue of The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 34(4)** (with reg. 5, Sch. 1 para. 80); 2020 c. 1, Sch. 5 para. 1(1)

F53   Words in Art. 40(4) substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 34(5)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

F54   Words in Art. 40(5) substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 34(6)(a)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

F55   Words in Art. 40(5) substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 34(6)(b)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

F56   Words in Art. 40(6) substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 34(7)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

F57   Art. 40(7)-(11) omitted (31.12.2020) by virtue of The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 34(8)** (with reg. 5, Sch. 1 para. 80); 2020 c. 1, **Sch. 5 para. 1(1)**

Article 41

Monitoring of approved codes of conduct

1   Without prejudice to the tasks and powers of [**F58**the Commissioner] 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 [**F58**the Commissioner].

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

    a   demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of [**F59**the Commissioner];

    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 [**F60**the Commissioner] that its tasks and duties do not result in a conflict of interests.

F61 3   . . . .

4   Without prejudice to the tasks and powers of [**F62**the Commissioner] 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 [**F62**the Commissioner] of such actions and the reasons for taking them.

[^{X1}5   [^{F63}The Commissioner] shall revoke the accreditation of a body as referred to in paragraph 1 if the requirements 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.

Editorial Information

  X1   Substituted by Corrigendum to 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) (Official Journal of the European Union L 119 of 4 May 2016).

Textual Amendments

  F58   Words in Art. 41(1) substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 35(2)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

  F59   Words in Art. 41(2)(a) substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 35(3)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

  F60   Words in Art. 41(2)(d) substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 35(3)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

  F61   Art. 41(3) omitted (31.12.2020) by virtue of The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 35(4)** (with reg. 5, Sch. 1 para. 80); 2020 c. 1, Sch. 5 para. 1(1)

  F62   Words in Art. 41(4) substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 35(5)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

  F63   Words in Art. 41(5) substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 35(6)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

Article 42

Certification

1   [^{F64}The Commissioner] shall encourage ^{F65}... 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 [**F66**the Commissioner].

5   A certification pursuant to this Article shall be issued by the certification bodies referred to in Article 43 or by [**F67**the Commissioner], on the basis of criteria approved by [**F68**the Commissioner] pursuant to Article 58(3) **F69**... . 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, [**F70**the Commissioner], with all information and access to its processing activities which are necessary to conduct the certification procedure.

[**X1**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 criteria continue to be met. Certification shall be withdrawn, as applicable, by the certification bodies referred to in Article 43 or by [**F71**the Commissioner] where the criteria for the certification are not or are no longer met.]

8   [**F72**The Commissioner] shall collate all certification mechanisms and data protection seals and marks in a register and shall make them publicly available by any appropriate means.

Editorial Information

X1   Substituted by Corrigendum to 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) (Official Journal of the European Union L 119 of 4 May 2016).

Textual Amendments

F64   Words in Art. 42(1) substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 36(2)(a)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

F65   Words in Art. 42(1) omitted (31.12.2020) by virtue of The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 36(2)(b)** (with reg. 5, Sch. 1 para. 80); 2020 c. 1, Sch. 5 para. 1(1)

F66   Words in Art. 42(4) substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 36(3)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

F67   Words in Art. 42(5) substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 36(4)(a)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

F68   Words in Art. 42(5) substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 36(4)(b)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

F69   Words in Art. 42(5) omitted (31.12.2020) by virtue of The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 36(4)(c)** (with reg. 5, Sch. 1 para. 80); 2020 c. 1, Sch. 5 para. 1(1)

F70   Words in Art. 42(6) substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 36(5)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

F71   Words in Art. 42(7) substituted (31.12.2020) by The Data Protection, Privacy and Electronic
    Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1**
    para. 36(6) (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)
F72   Words in Art. 42(8) substituted (31.12.2020) by The Data Protection, Privacy and Electronic
    Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1**
    para. 36(7) (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

Article 43

Certification bodies

1   Without prejudice to the tasks and powers of [**F73**the Commissioner] under Articles 57
and 58, certification bodies which have an appropriate level of expertise in relation to data
protection shall, after informing [**F74**the Commissioner] in order to allow it to exercise its powers
pursuant to point (h) of Article 58(2) where necessary, issue and renew certification. [**F75**In
accordance with section 17 of the 2018 Act, those certification bodies may only be] accredited
by one or both of the following:

[**F76**a   the Commissioner;]

   b   [**F77**the UK 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 [**F78**the
        Commissioner].

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 [**F79**the Commissioner];

   b   undertaken to respect the criteria referred to in Article 42(5) and approved by [**F80**the
        Commissioner] 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 [**F81**the Commissioner], that their tasks and duties
        do not result in a conflict of interests.

3   [**X1**The accreditation of certification bodies as referred to in paragraphs 1 and 2 of this
Article shall take place on the basis of requirements approved by [**F82**the Commissioner].] 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 **[F83the Commissioner]** with the reasons for granting or withdrawing the requested certification.

[X16   The requirements referred to in paragraph 3 of this Article and the criteria referred to in Article 42(5) shall be made public by **[F84the Commissioner]** in an easily accessible form. **F85...]**

7   Without prejudice to Chapter VIII, **[F86the Commissioner or the UK 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.

F878   . . . .

F879   . . . .

F83   Words in Art. 43(5) substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 37(5)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

F84   Words in Art. 43(6) substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 37(6)(a)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

F85   Words in Art. 43(6) omitted (31.12.2020) by virtue of The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 37(6)(b)** (with reg. 5, Sch. 1 para. 80); 2020 c. 1, Sch. 5 para. 1(1)

F86   Words in Art. 43(7) substituted (31.12.2020) by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 37(7)** (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1)

F87   Art. 43(8)(9) omitted (31.12.2020) by virtue of The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), reg. 1(2), **Sch. 1 para. 37(8)** (with reg. 5, Sch. 1 para. 80); 2020 c. 1, Sch. 5 para. 1(1)

(**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).

Changes to legislation:
There are currently no known outstanding effects for the Regulation (EU) 2016/679 of the European Parliament and of the Council, CHAPTER IV.