

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 (United
Kingdom General Data Protection Regulation)(Text with EEA relevance)

CHAPTER IV

Controller and processor

Section 1

General obligations

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 [F¹domestic 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 [F²domestic 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;

Changes to legislation: Regulation (EU) 2016/679 of the European Parliament and of the Council, Article 28 is up to date with all changes known to be in force on or before 27 September 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details) View outstanding changes

- 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 [^{F3}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 [^{F4}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 [^{F5}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 [^{F6}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.

^{F7}

8 [^{F8}The Commissioner] may adopt standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article ^{F9}... .

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

- F1** 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)
- F2** 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)
- F3** 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)

Changes to legislation: Regulation (EU) 2016/679 of the European Parliament and of the Council, Article 28 is up to date with all changes known to be in force on or before 27 September 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details) [View outstanding changes](#)

- F4** 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)
- F5** 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)
- F6** 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)
- F7** 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)
- F8** 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)
- F9** 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)

Changes to legislation:

Regulation (EU) 2016/679 of the European Parliament and of the Council, Article 28 is up to date with all changes known to be in force on or before 27 September 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations.

[View outstanding changes](#)

Changes and effects yet to be applied to the whole legislation item and associated provisions

- Art. 17(1)(g) inserted by [2024 c. 21 s. 31\(2\)](#)
- Art. 17(4)(5) inserted by [2024 c. 21 s. 31\(3\)](#)