

*Article 3*

*Amendments to Regulation (EU) 2016/679 (GDPR)*

Regulation (EU) 2016/679 is amended as follows:

1. Article 4 is amended as follows:

(a) in point 1, the following sentences are added:

‘Information relating to a natural person is not necessarily personal data for every other person or entity, merely because another entity can identify that

natural person. Information shall not be personal for a given entity where that entity cannot identify the natural person to whom the information relates, taking into account the means reasonably likely to be used by that entity. Such information does not become personal for that entity merely because a potential subsequent recipient has means reasonably likely to be used to identify the natural person to whom the information relates.’

(b) the following points are added:

‘(32) ‘terminal equipment’ means terminal equipment as set out in Article 1(1) of Directive 2008/63/EC;

(33) for ‘electronic communications networks’ the definition of Article 2(1) of Directive (EU) 2018/1972 shall apply;

(34) ‘web browser’ means web browser as defined in Article 2(11) of Regulation (EU) 2022/1925;

(35) ‘media service’ means a media service as defined in Article 2(1) of Regulation (EU) 2024/1083;

(36) ‘media service provider’ means a media service provider as defined in Article 2(2) of Regulation (EU) 2024/1083;’

(37) ‘online interface’ means an online interface as defined in Article 3(m) of Regulation (EU) 2022/2065.’

(38) “scientific research” means any research which can also support innovation, such as technological development and demonstration. These actions shall contribute to existing scientific knowledge or apply existing knowledge in novel ways, be carried out with the aim of contributing to the growth of society’s general knowledge and wellbeing and adhere to ethical standards in the relevant research area. This does not exclude that the research may also aim to further a commercial interest.’

2. Article 5 (1)(b) is replaced by the following:

‘collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), be considered to be compatible with the initial purposes, independent of the conditions of Article 6(4) of this Regulation, (‘purpose limitation’);’

3. Article 9 is amended as follows:

(a) in paragraph 2, the following points are added:

‘(k) processing in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model, subject to the conditions referred to in paragraph 5.

(l) processing of biometric data is necessary for the purpose of confirming the identity of a data subject (verification), where the biometric data or the means needed for the verification is under the sole control of the data subject.’

(b) the following paragraph is added:

‘5. For processing referred to in point (k) of paragraph 2, appropriate organisational and technical measures shall be implemented to avoid v the collection and otherwise processing of special categories of personal data. Where, despite the implementation of such measures, the controller identifies special categories of personal data in the datasets used for training, testing or validation or in the AI system or AI model, the controller shall remove such data. If removal of those data requires disproportionate effort, the controller shall in any event effectively protect without undue delay such data from being used to produce outputs, from being disclosed or otherwise made available to third parties.’

4. In Article 12, paragraph 5 is replaced by the following:

‘5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character or also, for requests under Article 15 because the data subject abuses the rights conferred by this regulation for purposes other than the protection of their data, the controller may either:

- (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or
- (b) refuse to act on the request.

The controller shall bear the burden of demonstrating that the request is manifestly unfounded or that there are reasonable grounds to believe that it is excessive.’

5. In Article 13, paragraph 4 is replaced by the following:

‘4. Paragraphs 1, 2 and 3 shall not apply where the personal data have been collected in the context of a clear and circumscribed relationship between data subjects and a controller exercising an activity that is not data-intensive and there are reasonable grounds to assume that the data subject already has the information referred to in points (a) and (c) of paragraph 1, unless the controller transmits the data to other recipients or categories of recipients, transfers the data to a third country, carries out automated decision-making, including profiling, referred to in Article 22(1), or the processing is likely to result in a high risk to the rights and freedoms of data subjects within the meaning of Article 35.’

6. In Article 13, paragraph 5 is added:

‘5. When the processing takes place for scientific research purposes and the provision of information referred to under paragraphs 1, 2 and 3 proves impossible or would involve a disproportionate effort subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing, the controller does not need to provide the information referred to under paragraphs 1, 2 and 3. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available.’

7. In Article 22, paragraphs 1 and 2 are replaced by the following:
- ‘1. A decision which produces legal effects for a data subject or similarly significantly affects him or her may be based solely on automated processing, including profiling, only where that decision:
- (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller regardless of whether the decision could be taken otherwise than by solely automated means;
  - (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
  - (c) is based on the data subject's explicit consent.’
8. Article 33 is amended as follows:
- (a) paragraph 1 is replaced by the following:

‘1. In the case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall without undue delay and, where feasible, not later than 96 hours after having become aware of it, notify the personal data breach via the single-entry point established pursuant to Article 23a of Directive (EU) 2022/2555 to the supervisory authority competent in accordance with Article 55 and Article 56. Where the notification to the supervisory authority is not made within 96 hours, it shall be accompanied by reasons for the delay.’
  - (b) the following paragraph is added:

‘1a. Until the establishment of the single-entry point pursuant to Article 23a of Directive (EU) 2022/2555, controllers shall continue to notify personal data breaches directly to the competent supervisory authority in accordance with Article 55 and Article 56.’
  - (c) the following paragraphs are added:

‘6. The Board shall prepare and transmit to the Commission a proposal for a common template for notifying a personal data breach to the competent supervisory authority referred to in paragraph 1 as well as for a list of the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person. The proposals shall be submitted to the Commission within [OP date = nine months of the entry into application of this Regulation]. The Commission after due consideration reviews it, as necessary, and is empowered to adopt it by way of an implementing act in accordance with the examination procedure set out in Article 93(2).

7. The template and the list referred to in paragraph 6 shall be reviewed at least every three years and updated where necessary. The Board shall submit its assessment and possible proposals for updates to the Commission in due time. The Commission after due consideration of the proposals reviews them and is empowered to adopt any updates following the procedure in paragraph 6.’
9. Article 35 is amended as follows:
- (a) paragraphs 4, 5 and 6 are replaced by the following:

‘4. The Board shall prepare and transmit to the Commission a proposal for a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1.

5. The Board shall prepare and transmit to the Commission a proposal for a list of the kind of processing operations for which no data protection impact assessment is required.

6. The Board shall prepare and transmit to the Commission a proposal for a common template and a common methodology for conducting data protection impact assessments.’

(b) the following paragraphs are inserted:

‘6a. The proposals for the lists referred to in paragraphs 4 and 5 and for the template and methodology referred to in paragraph 6 shall be submitted to the Commission within [OP date = 9 months of the entry into application of this Regulation]. The Commission after due consideration reviews them, as necessary, and is empowered to adopt them by way of an implementing act in accordance with the examination procedure set out in Article 93(2).

6b. The lists and the template and methodology referred to in paragraph 6a shall be reviewed at least every three years and updated where necessary. The Board shall submit its assessment and possible proposals for updates to the Commission in due time. The Commission after due consideration of the proposals reviews them and is empowered to adopt any updates following the procedure in paragraph 6a.

6c. Lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment and of the kind of processing operations for which no data protection impact assessment is required established and made public by supervisory authorities remain valid until the Commission adopts the implementing act referred to in paragraph 6a.’

10. The following article is added:

‘Article 41a

- (1) The Commission may adopt implementing acts to specify means and criteria to determine whether data resulting from pseudonymisation no longer constitutes personal data for certain entities.
- (2) For the purpose of paragraph 1 the Commission shall:
  - (a) assess the state of the art of available techniques;
  - (b) develop criteria and or categories for controllers and recipients to assess the risk of re-identification in relation to typical recipients of data.
- (3) The implementation of the means and criteria outlined in an implementing act may be used as an element to demonstrate that data cannot lead to reidentification of the data subjects.
- (4) The Commission shall closely involve the EDPB in the preparations of the implementing acts. The EPDB shall issue an opinion on the draft implementing acts within a deadline of 8 weeks as of the receipt of the draft from the Commission.
- (5) The Implementing Acts shall be adopted in accordance with the examination procedure referred to in Article 93(3).’

11. In Article 57(1) is amended as follows:
  - (a) point (k) is deleted;
12. In Article 64(1), point (a) is deleted.
13. In Article 70(1), point (h) is deleted.
14. In Article 70(1), the following points are inserted:

‘(ha) prepare and transmit to the Commission a proposal for a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment and for which no data protection impact assessment is required, pursuant to Article 35.

(hb) prepare and transmit to the Commission a proposal for a common template and a common methodology for conducting data protection impact assessments, pursuant to Article 35.

(hc) prepare and transmit to the Commission a proposal for a common template for notifying a personal data breach to the competent supervisory authority as well as for a list of the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person pursuant to Article 33’
15. After Article 88, the following articles are added:

‘Article 88a

*Processing of personal data in the terminal equipment of natural persons*

  - (1) Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person is only allowed when that person has given his or her consent, in accordance with this Regulation.
  - (2) Paragraph 1 does not preclude storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person, based on Union or Member State law within the meaning of, and subject to the conditions of Article 6, to safeguard the objectives referred to in Article 23(1).
  - (3) Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person without consent, and subsequent processing, shall be lawful to the extent it is necessary for any of the following:
    - (a) carrying out the transmission of an electronic communication over an electronic communications network;
    - (b) providing a service explicitly requested by the data subject;
    - (c) creating aggregated information about the usage of an online service to measure the audience of such a service, where it is carried out by the controller of that online service solely for its own use;
    - (d) maintaining or restoring the security of a service provided by the controller and requested by the data subject or the terminal equipment used for the provision of such service.
  - (4) Where storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person is based on consent, the following shall apply:

- (a) the data subject shall be able to refuse requests for consent in an easy and intelligible manner with a single-click button or equivalent means;
- (b) if the data subject gives consent, the controller shall not make a new request for consent for the same purpose for the period during which the controller can lawfully rely on the consent of the data subject;
- (c) if the data subject declines a request for consent, the controller shall not make a new request for consent for the same purpose for a period of at least six months.

This paragraph also applies to the subsequent processing of personal data based on consent.

- (5) This Article shall apply from [OP: please insert the date = 6 months following the date of entry into force of this Regulation]

#### Article 88b

##### *Automated and machine-readable indications of data subject's choices with respect to processing of personal data in the terminal equipment of natural persons*

- (1) Controllers shall ensure that their online interfaces allow data subjects to:
  - (a) Give consent through automated and machine-readable means, provided that the conditions for consent laid down in this Regulation are fulfilled;
  - (b) decline a request for consent and exercise the right to object pursuant to Article 21(2) through automated and machine-readable means.
- (2) Controllers shall respect the choices made by data subjects in accordance with paragraph 1.
- (3) Paragraphs 1 and 2 shall not apply to controllers that are media service providers when providing a media service.
- (4) The Commission shall, in accordance with Article 10(1) of Regulation (EU) 1025/2012, request one or more European standardisation organisations to draft standards for the interpretation of machine-readable indications of data subjects' choices.

Online interfaces of controllers which are in conformity with harmonised standards or parts thereof the references of which have been published in the *Official Journal of the European Union* shall be presumed to be in conformity with the requirements covered by those standards or parts thereof, set out in paragraph 1.

- (5) Paragraphs 1 and 2 shall apply from [OP: please insert the date = 24 months following the date of entry into force of this Regulation].
- (6) Providers of web browsers, which are not SMEs, shall provide the technical means to allow data subjects to give their consent and to refuse a request for consent and exercise the right to object pursuant to Article 21(2) through the automated and machine-readable means referred to in paragraph 1 of this Article, as applied pursuant to paragraphs 2 to 5 of this Article.
- (7) Paragraph 6 shall apply from [OP: please insert the date = 48 months following the date of entry into force of this Regulation].

## Article 88c

### *Processing in the context of the development and operation of AI*

Where the processing of personal data is necessary for the interests of the controller in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model, such processing may be pursued for legitimate interests within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, where appropriate, except where other Union or national laws explicitly require consent, and where such interests are overridden by the interests, or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Any such processing shall be subject to appropriate organisational, technical measures and safeguards for the rights and freedoms of the data subject, such as to ensure respect of data minimisation during the stage of selection of sources and the training and testing of AI an system or AI model, to protect against non-disclosure of residually retained data in the AI system or AI model to ensure enhanced transparency to data subjects and providing data subjects with an unconditional right to object to the processing of their personal data.’