

Data Protection and GDPR Policy

Document Owner and Author:	Simply Third Sector
Date Drafted	August 2025
Date for Review	August 2026
Date Approved by the Board of Trustees	August 2025

Contents

Introduction to GDPR	4
1. Definitions (Art:4)	4
1.1 Data Subject.....	4
1.2 Contact Information.....	4
2. Principles of the GDPR (Art:5)	4
3. Lawful Processing	5
3.1 By Consent	5
3.2 By Contract	5
3.3 By Legal Obligation	6
3.4 By Public Task.....	6
3.5 Special Category Data (Art:9).....	6
4. Employees (Human Resources)	6
4.1 Taxation (HM Revenue & Customs)	6
4.2 Pensions	7
4.3 Vital Interest	7
4.4 By Public Task.....	7
4.5 Legitimate Interest.....	7
4.6 Enhanced DBS Checks.....	7
5. Individual Rights.....	8
5.1 The Right to be Informed (Arts 12-14)	8
5.2 The Right of Access (Art:15)	9
5.3 The Right to Rectification (Art:16).....	9
5.4 The Right to Erase (The Right to be Forgotten) (Art:17)	9
5.5 The Right to Restrict Processing (Art:18).....	9
5.6 The Right to Data Portability (Art:20)	9
5.7 The Right to Object (Art:21)	9
5.8 Rights in Relation to Automated Decision Making and Profiling (Art:22)	10
6. Operational Policies & Procedures – The Context	10
7. Personnel	10
7.1 Data Protection Officer	10
7.2 Data Controller	10
7.3 Data Processor	10

7.4 Access to Data.....	10
7.5 Training	10
8. Collecting & Processing Personal Data.....	11
9. Information Technology	11
9.1 Data Protection by Design/Default.....	11
9.2 Data Processing Equipment	11
9.3 Data Processing Location.....	11
9.4 Data Backups	11
9.5 Obsolete or Dysfunctional Equipment (Disposal of Removable Storage Media)	11
10. Data Subjects.....	12
10.1 Rights of Access, Rectification, and Erasure.....	12
10.2 Right of Portability	12
10.3 Data Retention Policy	12
11. Privacy Impact Assessment	13
11.1 Trustees' Data	13
11.2 Volunteers'/Members' Data	13
11.3 Supporters' & Enquirers' Data	13
11.4 Care Leaver Data	13
12. Third Party Access to Data	13
13. Data Breach	14
14. Privacy Policy & Privacy Notices	14
Appendix 1: Extracts of Relevant Articles from the GDPR	15
Article-4: Definitions.....	15
Article 6: Lawfulness of processing	18
Article 8: Conditions Applicable to Child's Consent	19
Article 9: Processing of Special Categories of Personal Data	19
Article 12: Transparent information, communication, and modalities for the exercise of the rights of the data subject.....	21
Article 13: Information to be provided where personal data are collected from the data subject	23
Article 24: Responsibility of the Controller	24
Article 25: Data protection by design and by default.....	24

Introduction to GDPR

Under the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018, and the retained EU General Data Protection Regulation (EU GDPR), Roots South West (hereinafter referred to as “the Charity” (Community Interest Company)) is required to comply with data protection laws and undertakes to do so. This policy is tailored to ensure the protection of personal data, particularly for 16-17 year old care leavers, who are considered vulnerable young people under safeguarding legislation (Children Act 1989/2004). Throughout this policy document, numbers prefixed by “Art:” (e.g., (Art:5)) refer to the relevant Article(s) in the GDPR. For ease of access, extracts of relevant GDPR Articles are contained in the Appendix to this Policy.

1. Definitions (Art:4)

The definitions of terms used in this policy are the same as those detailed in Article-4 of the GDPR.

1.1 Data Subject

A data subject is an identifiable individual person about whom the Charity holds personal data, including 16-17 year old care leavers, who may be vulnerable due to their care experiences.

1.2 Contact Information

For the purposes of this Policy, “Contact Information” means any or all of the person’s:

- Full name (including any preferences about how they like to be called).
- Full postal address.
- Telephone and/or mobile number(s).
- E-mail address(es).
- Social media IDs/Usernames (e.g., Facebook, Skype, WhatsApp).
- For care leavers: care history, health data, housing status, or other special category data relevant to their support needs.

2. Principles of the GDPR (Art:5)

The Charity will ensure that all personal data it holds will be:

- a) processed lawfully, fairly, and in a transparent manner, using age-appropriate communication for 16-17 year old care leavers as required by Art. 12.
- b) collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes shall not be incompatible with the initial purposes.

c) adequate, relevant, and limited to what is necessary for the purposes for which they are processed, including only data essential for supporting care leavers (e.g., care plans, health needs).

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

e) kept in a form that permits identification of data subjects for no longer than necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes subject to implementation of appropriate technical and organizational measures required by the GDPR to safeguard the rights and freedoms of individuals, particularly vulnerable care leavers.

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures, with enhanced safeguards for special category data of care leavers.

3. Lawful Processing

The Charity will obtain, hold, and process all personal data in accordance with the GDPR for the following lawful purposes. In all cases, the information collected, held, and processed will include Contact Information (as defined in 1.2 above).

3.1 By Consent

a) People, including 16-17 year old care leavers, who are interested in and wish to be kept informed of the activities of the Charity.

b) Subject to the person's consent, this may include information selected and forwarded by the Charity on activities relevant to those of the Charity by other organizations. Consent from 16-17 year olds will be obtained using age-appropriate, simplified explanations, with capacity assessed and advocates or guardians involved where necessary (Art. 8). Consent must be verifiable and recorded.

Note: this will not involve providing the person's personal data to another organization.

The information collected may additionally contain details of any areas of interest about which the person wishes to be kept informed.

The information provided will be held and processed solely for the purpose of providing the information requested by the person.

3.2 By Contract

People who sell goods and/or services to, and/or purchase goods and/or services from the Charity.

The information collected will additionally contain details of:

- a) The goods/services being sold to or purchased from the Charity.
- b) Bank and other details necessary and relevant to the making or receiving of payments for the goods/services being sold to or purchased from the Charity.

The information provided will be held and processed solely for the purpose of managing the contract between the Charity and the person for the supply or purchase of goods/services.

3.3 By Legal Obligation

People where there is a legal obligation on the Charity to collect, process, and share information with a third party, including data sharing with local authorities or social services for care planning or safeguarding of 16-17 year old care leavers under the Children Act (1989/2004) or HM Revenue & Customs payroll information on employees.

The information provided will be held, processed, and shared with others solely for the purpose of meeting the Charity's legal obligations.

3.4 By Public Task

The Charity may process personal data for safeguarding or supporting 16-17 year old care leavers as a public task, including collaboration with public bodies like social services to ensure continuity of care or protection from harm.

3.5 Special Category Data (Art:9)

For 16-17 year old care leavers, the Charity may process special category data (e.g., health, ethnicity, care history, or criminal records) under GDPR Art. 9(2) lawful bases, such as:

- a) Explicit consent, obtained in an age-appropriate manner with advocate support if needed.
- b) Substantial public interest, such as safeguarding vulnerable young people or complying with statutory care obligations.

The information will be processed with enhanced safeguards, including encryption and restricted access, and only for purposes directly related to supporting care leavers.

4. Employees (Human Resources)

4.1 Taxation (HM Revenue & Customs)

For managing an employee's PAYE and other taxation affairs, the information collected will additionally contain details, as required by HM Revenue & Customs, of:

- a. The person's National Insurance Number.
- b. The person's taxation codes.
- c. The person's salary/wages, benefits, taxation deductions & payments.

d. Such other information as may be required by HM Revenue & Customs.

4.2 Pensions

For managing an employee's statutory pension rights, the information collected will additionally contain details, as required by the Charity's pension scheme (National Employees Savings Trust, NEST), of:

- a. The person's National Insurance Number.
- b. The person's salary/wages, benefits, taxation & payments.
- c. Such other information as may be required by the NEST scheme.

4.3 Vital Interest

The Charity undertakes no activities that require the collection, holding, and/or processing of personal information for reasons of vital interest.

4.4 By Public Task

See Section 3.4 for processing related to public tasks for care leavers.

4.5 Legitimate Interest

Volunteers, Including Trustees

To operate efficiently, effectively, and economically, it is in the legitimate interests of the Charity to hold such personal information on its volunteers and Trustees as will enable the Charity to communicate with them on matters relating to the operation of the Charity, e.g.:

- The holding of meetings.
- Providing information about the Charity's activities, particularly those relevant to individual volunteers/Trustees.
- Seeking help, support, and advice from volunteers/Trustees, particularly where they have specific knowledge and experience, including in supporting care leavers.
- Ensuring that any needs of volunteers/Trustees are appropriately and sensitively accommodated when organizing meetings and other activities of the Charity.

4.6 Enhanced DBS Checks

For employees and volunteers working with 16-17 year old care leavers, the Charity will collect and process data related to enhanced Disclosure and Barring Service (DBS) checks to comply with safeguarding requirements.

5. Individual Rights

Note: The following clauses are based on guidance from the Information Commissioner's Office (ICO): <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/>.

5.1 The Right to be Informed (Arts 12-14)

When collecting personal information, the Charity will provide to the data subject, free of charge, a Privacy Notice written in clear, plain, and age-appropriate language (especially for 16-17 year old care leavers), which is concise, transparent, intelligible, and easily accessible (e.g., easy-read, audio formats). The Privacy Notice will contain:

- Identity and contact details of the controller, controller's representative, and/or data protection officer, where applicable.
- Purpose of the processing and the lawful basis for the processing.
- The legitimate interests of the controller or third party, where applicable.
- Categories of personal data (not applicable if obtained directly from the data subject).
- Any recipient or categories of recipients of the personal data, including local authorities or social services for care leaver support.
- Details of transfers to third countries and safeguards.
- Retention period or criteria used to determine the retention period.
- The existence of each of the data subject's rights.
- The right to withdraw consent at any time, where relevant.
- The right to lodge a complaint with a supervisory authority.
- The source of the personal data and whether it came from publicly accessible sources (not applicable if obtained directly from the data subject).
- Whether the provision of personal data is a statutory or contractual requirement or obligation and consequences of failing to provide the personal data (not applicable if not obtained directly from the data subject).
- The existence of automated decision-making, including profiling, and information about how decisions are made, their significance, and consequences.

For 16-17 year old care leavers, Privacy Notices will be tailored to their needs, using simplified language and accessible formats, and explained by trained staff or advocates if needed.

In the case of data obtained directly from the data subject, the information will be provided at the time the data are obtained.

In the case that the data are not obtained directly from the data subject, the information will be provided within a reasonable period of the Charity having obtained the data (within one month), or when the first communication takes place, or before disclosure to another recipient.

5.2 The Right of Access (Art:15)

The data subject shall have the right to obtain from the controller confirmation as to whether personal data concerning them are being processed, and, where applicable, access to their personal data and the information detailed in the Charity's relevant Privacy Notice.

5.3 The Right to Rectification (Art:16)

The data subject shall have the right to require the controller to rectify any inaccurate or incomplete personal data concerning them without undue delay.

5.4 The Right to Erase (The Right to be Forgotten) (Art:17)

Except where the data are held for purposes of legal obligation (e.g., care records under the Children Act) or public task (3.3 or 3.4), the data subject shall have the right to require the controller to erase any personal data concerning them without undue delay.

5.5 The Right to Restrict Processing (Art:18)

Where there is a dispute between the data subject and the controller about the accuracy, validity, or legality of data held by the Charity, the data subject shall have the right to require the controller to cease processing the data for a reasonable period to allow the dispute to be resolved.

5.6 The Right to Data Portability (Art:20)

Where data are held for purposes of consent or contract (3.1 or 3.2), the data subject shall have the right to require the controller to provide them with a copy in a structured, commonly used, and machine-readable format of the data they have provided, and to transmit those data to another controller (e.g., social services for care leaver support) without hindrance.

5.7 The Right to Object (Art:21)

a. The data subject shall have the right to object, on grounds relating to their situation, at any time to processing of personal data concerning them based on Public Task or Legitimate Interest (3.4 or 4.5), including profiling. The controller shall no longer process the personal data unless compelling legitimate grounds override the interests, rights, and freedoms of the data subject or for legal claims.

b. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to such processing, including profiling.

c. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

d. The right to object shall be explicitly brought to the attention of the data subject at the latest at the time of the first communication, clearly and separately from other information.

5.8 Rights in Relation to Automated Decision Making and Profiling (Art:22)

Except where it is based on explicit consent or necessary for a contract, the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or similarly significantly affects them.

6. Operational Policies & Procedures – The Context

Roots South West is a small charity holding personal data, including sensitive data on 16-17 year old care leavers. The Trustees understand and accept their responsibility under the UK GDPR, Data Protection Act 2018, and EU GDPR to hold all personal data securely and use it only for legitimate purposes with the knowledge and approval of data subjects, particularly vulnerable young people. These policies are proportionate to the nature of the data held, with enhanced safeguards for care leaver data due to its sensitivity and safeguarding implications.

7. Personnel

7.1 Data Protection Officer

In the considered opinion of the Trustees, the scope and nature of the personal data held by the Charity, including care leaver data, do not warrant the appointment of a Data Protection Officer. Accordingly, no Data Protection Officer is appointed.

7.2 Data Controller

The Board of Trustees is the Data Controller for the Charity.

7.3 Data Processor

The Board of Trustees will appoint at least 2 and not more than 5 of its number, or other appropriate persons trained in safeguarding protocols, to be the Data Processors for the Charity. The Charity will not knowingly outsource data processing to any third party except as provided for in Section 12.

7.4 Access to Data

Only Data Processors shall have access to personal data held by the Charity, except where necessary to pursue legitimate purposes, such as safeguarding or supporting care leavers.

7.5 Training

The Board of Trustees and Data Processors will undergo regular training on GDPR compliance, handling sensitive data of vulnerable youth, recognizing safeguarding risks, and age-appropriate communication, commensurate with the scale and nature of the personal data held.

8. Collecting & Processing Personal Data

The Charity collects personal data, including special category data from 16-17 year old care leavers, using trauma-informed approaches to ensure sensitivity to their care experiences. All personal data will be collected, held, and processed in accordance with the relevant Data Privacy Notice provided to data subjects at the time of collection.

A Data Privacy Notice will be provided in accessible formats (e.g., simplified language, visual aids, audio) to all persons, particularly care leavers, on whom the Charity collects, holds, and processes data covered by the GDPR. The Notice will detail the nature of the data, purpose(s) for collection, subjects' rights, and compliance with GDPR requirements.

9. Information Technology

9.1 Data Protection by Design/Default

The Trustees will seek professional advice, including from safeguarding experts, when planning significant changes to data processing involving care leaver data or in response to new risks (e.g., cyber-attacks). Personal data will never be transmitted electronically unless securely encrypted.

9.2 Data Processing Equipment

The Charity will purchase and own at least 2 and not more than 5 removable storage devices to store personal data, including care leaver data. These devices will act as backups and will not store unrelated data. No personal data will be stored on computers/laptops used for processing; interim working data will be deleted after processing. Devices will be kept in a secure location when not in use, protected against damage, loss, or theft. A register will track device locations and access.

9.3 Data Processing Location

Data Processors shall only process personal data in a secure location, not in public places where data could be overlooked or devices lost/stolen. Computers/laptops will not be left unattended during processing.

9.4 Data Backups

All personal data, especially care leaver data, shall be backed up periodically and after significant changes, using encryption for special category data. Backup copies will be held in separate secure locations not susceptible to common risks (e.g., fire, flood, theft).

9.5 Obsolete or Dysfunctional Equipment (Disposal of Removable Storage Media)

Equipment containing personal data, particularly care leaver data, shall be stored securely until expert advice on data cleansing and disposal is obtained and implemented, ensuring compliance with ICO standards for sensitive data destruction.

10. Data Subjects

The Charity will give data subjects the following rights, clearly outlined in the relevant Data Privacy Notice:

- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erasure (subject to legal obligations, e.g., care records).
- The right to restrict processing.
- The right to data portability.
- The right to object.
- The right not to be subjected to automated decision-making, including profiling.

10.1 Rights of Access, Rectification, and Erasure

Data subjects, including 16-17 year olds (with advocate support if needed), will be informed of their right to access their data and request corrections or erasure. Requests will be free unless unreasonable or vexatious. Requests must be made in writing, signed, and dated, identifying the data in question. Delays will be communicated in age-appropriate language, particularly to care leavers. Rectifications or erasures will be applied to all copies, including those held by third parties.

10.2 Right of Portability

The Charity will provide portable copies of personal data, including care plans for care leavers, on written request, unless requests are unreasonable or vexatious. A reasonable charge may be applied for excessive requests.

10.3 Data Retention Policy

Personal data shall not be retained for longer than:

a. For consent-based data: the period of consent. b. For legitimate interest: the period the interest applies (e.g., identifying former volunteers). c. For legal obligation: the period required (e.g., care records retained until the individual reaches age 75 under the Children Act, or until age 25 for care leaver support continuity).

The Charity shall review personal data every 6 months and remove data no longer justified within 20 working days.

11. Privacy Impact Assessment

11.1 Trustees' Data

Volume: Extremely low (<15 individuals).

Sensitivity: Low-moderate (e.g., date of birth, previous names, addresses).

Risk of Breach: Small, as data are rarely used.

Overall Impact: LOW.

11.2 Volunteers'/Members' Data

Volume: Low (<100 individuals).

Sensitivity: Low (e.g., names, email addresses).

Risk of Breach: Small (e.g., accidental disclosure).

Overall Impact: LOW.

11.3 Supporters' & Enquirers' Data

Volume: Low-moderate.

Sensitivity: Low (e.g., names, email addresses).

Risk of Breach: Small (e.g., accidental disclosure).

Overall Impact: LOW.

11.4 Care Leaver Data

Volume: Moderate (50-200 individuals, depending on service user numbers).

Sensitivity: High (includes special category data like health, care history, ethnicity, or criminal records).

Risk of Breach: Moderate to high (due to vulnerability and potential harm from unauthorized disclosure).

Overall Impact: MODERATE-HIGH, requiring enhanced safeguards (e.g., encryption, restricted access, regular audits).

12. Third Party Access to Data

The Charity will only share personal data with third parties (e.g., local authorities, social services, health providers) where necessary for safeguarding or supporting 16-17 year old care leavers. Data subjects, or their advocates, will be informed in advance using accessible language. Third parties must sign contracts specifying:

- The Charity owns the data.
- The third party will process data only as instructed, complying with GDPR Art. 9 and safeguarding laws.
- The third party will not use data for its own purposes.
- Industry-standard best practices will be adopted to protect data.

- The third party is responsible for any breach, loss, or corruption unless caused by the Charity's instructions.
- Data will be deleted securely once processing is complete.
- No data will be transferred outside the UK/EU.

13. Data Breach

In the event of a data breach, the Trustees will notify the ICO immediately and, for care leaver data, conduct a safeguarding review to assess risks to vulnerable young people. Relevant authorities (e.g., safeguarding teams) will be notified if required. Full details will be provided to the ICO as soon as available.

14. Privacy Policy & Privacy Notices

The Charity will provide Privacy Notices in age-appropriate, accessible formats (e.g., simplified language, audio) to all data subjects, particularly care leavers, explaining data use, sharing (e.g., for safeguarding), and rights. Notices will be provided at the time of collection or within one month for indirectly obtained data, or before third-party disclosure.

Appendix 1: Extracts of Relevant Articles from the GDPR

Article-4: Definitions

For the purposes of this Regulation:

1. **‘personal data’** means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
2. **‘processing’** means any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.
3. **‘restriction of processing’** means the marking of stored personal data with the aim of limiting their processing in the future.
4. **‘profiling’** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location, or movements.
5. **‘pseudonymisation’** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
6. **‘filing system’** means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.
7. **‘controller’** means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
8. **‘processor’** means a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.
9. **‘recipient’** means a natural or legal person, public authority, agency, or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member

State law shall not be regarded as recipients; the processing of those data by those public authorities shall follow the applicable data protection rules according to the purposes of the processing.

10. **‘third party’** means a natural or legal person, public authority, agency, or body other than the data subject, controller, processor, and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

11. **‘consent’** of the data subject means any freely given, specific, informed, and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

12. **‘personal data breach’** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

13. **‘genetic data’** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result from an analysis of a biological sample from the natural person in question.

14. **‘biometric data’** means personal data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopy data.

15. **‘data concerning health’** means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

16. **‘main establishment’** means:

a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be the main establishment.

b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation.

17. **‘representative’** means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor regarding their respective obligations under this Regulation.

18. **‘enterprise’** means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity.

19. **‘group of undertakings’** means a controlling undertaking and its controlled undertakings.

20. **‘binding corporate rules’** means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.

21. **‘supervisory authority’** means an independent public authority which is established by a Member State pursuant to Article 51.

22. **‘supervisory authority concerned’** means a supervisory authority which is concerned by the processing of personal data because:

- a) the controller or processor is established on the territory of the Member State of that supervisory authority.
- b) data subjects residing in the Member State of that supervisory authority are affected or likely to be affected by the processing; or
- c) a complaint has been lodged with that supervisory authority.

23. **‘cross-border processing’** means either:

- a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State: or
- b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union, but which affects or is likely to affect data subjects in more than one Member State.

24. **‘relevant and reasoned objection’** means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union.

25. **‘information society service’** means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council ⁽¹⁾.

26. **‘international organisation’** means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or based on, an agreement between two or more countries.

¹ Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1).

Article 6: Lawfulness of processing

Processing shall be lawful only if and to the extent that at least one of the following applies:

- a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes.
- b) processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering a contract.
- c) processing is necessary for compliance with a legal obligation to which the controller is subject.
- d) processing is necessary to protect the vital interests of the data subject or of another natural person.
- e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

1. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation regarding processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

2. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

- a) Union law; or
- b) Member State law to which the controller is subject.

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

- a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing.
- b) the context in which the personal data have been collected, regarding the relationship between data subjects and the controller.
- c) the nature of the personal data, whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10.
- d) the possible consequences of the intended further processing for data subjects.
- e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Article 8: Conditions Applicable to Child's Consent

1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.
2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, considering available technology.
3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation, or effect of a contract in relation to a child.

Article 9: Processing of Special Categories of Personal Data

1. Processing of personal data revealing racial or ethnic origins, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data, data concerning health or a natural person's sex life or sexual orientation shall be prohibited.
2. Paragraph 1 shall not apply if one of the following applies:

- a) The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be applied.
- b) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment, social security and social protection law in so far as it is authorised by Union or Member State law providing for appropriate safeguards for the fundamental rights and freedoms of the data subject.
- c) Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.
- d) Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or not-for-profit body with a political, philosophical, religious or trade union aim, provided that the processing relates solely to the members or former members of the body or to persons who have regular contact with it in connection with its purposes and that no personal data are disclosed to a third party without the consent of the data subject.
- e) Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and freedoms of the data subject.
- f) Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
- g) Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.
- h) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and freedoms of the data subject.
- i) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- j) Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except 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.

Article 12: Transparent information, communication, and modalities for the exercise of the rights of the data subject

1. The controller shall act appropriately to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible, and easily accessible form, using clear and plain language, for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.
2. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not able to identify the data subject.
3. The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, considering the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.
4. If the controller does not act on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not acting and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.
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, the controller may either:
 - a) charge a reasonable fee considering the administrative costs of providing the information or communication or taking the action requested; or
 - b) refuse to act on the request.
6. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.
7. Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.
8. The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons to give in an easily visible, intelligible, and clearly legible

manner a meaningful overview of the intended processing. Where the icons are presented electronically, they shall be machine-readable.

9. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.

Article 13: Information to be provided where personal data are collected from the data subject

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all the following information:

- a) the identity and the contact details of the controller and, where applicable, of the controller's representative.
- b) the contact details of the data protection officer, where applicable.
- c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing.
- d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party.
- e) the recipients or categories of recipients of the personal data, if any.
- f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and how to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

- a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.
- b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability.
- c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.
- d) the right to lodge a complaint with a supervisory authority.
- e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data.
- f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

4. Paragraphs 1, 2 and 3 shall not apply where and as far as the data subject already has the information.

Article 24: Responsibility of the Controller

Considering 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.

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.

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. 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.