National Survivor User Network

Policy name	**Data Protection Policy**
Operational from	05/03/2021
Next review date	05/03/2022
Responsible staff member(s)	Mandy Crandale (Chief Executive Officer) mandy.crandale@nsun.org.uk Chair of the Board
Associated policies	Privacy Policy Safeguarding Policy
Privacy	External

Contents

Data Protection Policy

1. Introduction

The Data Protection Act 2018 (DPA) sets out the framework for data protection law in the UK and was amended on 01 January 2021 by regulations under the European Union (Withdrawal) Act 2018, to reflect the UK's status outside the EU. It works alongside the UK General Data Protection Regulation (GDPR) which came into effect on 01 January 2021 (the original EU GDPR came into effect in May 2018). NSUN is required to comply with these laws and undertakes to do so.

The purpose of the DPA and the GDPR is to protect the rights of individuals about whom data (information) is obtained, stored, processed and disclosed. Data protection is the area of the law that governs what may, and what may not, be done with personal information. Such personal information may be in electronic (e.g. stored on computer hard drive) or manual form (in a manual filing system). All staff (paid and unpaid) undertake to uphold the good name of NSUN, including its relations with the public, its members and supporters.

Security of data is concerned with the preservation of:

- **Confidentiality.** Only persons who are authorised should have access to data or other data for supporting functions.
- **Integrity.** It should be possible to trust the information generated by a system. It must be certain, for instance, that data relating to members is not only present, but is accurate and fit for purpose in every detail.
- **Availability.** The system should be able to provide data when and where it is needed.

Throughout this policy document, numbers prefixed by "Art:" in brackets *(eg: {Art:5})* refer to the relevant Article(s) in the GDPR – to note: currently the only legislation available to view and refer to is the EU GDPR which will largely be adopted by the UK with some small amendments. When the UK GDPR legislation becomes available, this policy will be amended to reflect any necessary changes.

For ease of access, extracts of relevant GDPR Articles are contained in the Appendix to this Policy.

This Data Protection policy sets out NSUN's responsibilities in law in some detail. The accompanying Privacy Policy is more of a public-facing, easy read as to what data we collect, how, when and why we collect it, and how we protect it in simpler terms.

2. Definitions *{Art:4}*

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

Data Subject

A data subject is an identifiable individual person about whom NSUN holds personal data.

Contact Information

For the purposes of this Policy, "Contact Information" means any or all of the data subject's:

- full name (including any preferences about how they like to be called);
- full postal address
- telephone and/or mobile number(s); email

address(es);
- social media IDs/UserNames (*eg:* Facebook, Twitter, WhatsApp)

Special category data

Special category data is some types of personal data that the UK GDPR singles out as likely to be more sensitive, and gives them extra protection. From the Information Commissioner's Office (ICO):

- personal data revealing **racial or ethnic origin**;
- personal data revealing **political opinions**;
- personal data revealing **religious or philosophical beliefs**;
- personal data revealing **trade union membership**;
- **genetic data**;
- **biometric data** (where used for identification purposes);
- data concerning **health**;
- data concerning a person's **sex life**; and
- data concerning a person's **sexual orientation**.

NSUN also adds **gender** and **accessibility needs** data in this list.

3. Principles of the GDPR *{Art:5}*

NSUN will ensure that all personal data that it holds will be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) 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 or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

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 which permits identification of data subjects for no longer than is 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 or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4. Lawful Basis for Processing

NSUN 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 2 above).

4.1 By Consent

a) People who are interested in, and wish to be kept informed of, the activities of NSUN.

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

b) Volunteers who may wish to work for NSUN.

The information provided will be held and processed solely for the purpose of enabling the volunteer to carry out the work specified by NSUN.

4.2 By Contract

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

The information collected will additionally contain details of:

a) The goods/services being sold to, or purchased from NSUN;

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 NSUN.

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

Employees (Human Resources)

For the purpose of managing Human Resources records, NSUN will collect contact information and in addition:

a) Date of birth
b) Emergency contact information of next of kin or similar

4.3 By Legal Obligation

Taxation (HM Revenue & Customs)

For the purpose of 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.

Pensions

For the purpose of managing an employee's statutory pension rights the information collected will additionally contain details, as required by NSUN'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.

Trustees

So that NSUN can fulfil its statutory obligations regarding charity governance, it holds personal information on its Trustees including:

a) Date of birth
b) Home address
c) Telephone numbers
d) Email addresses

4.4 By Vital Interest

If NSUN is in contact with a member whose life we believe may be at risk or is at risk of harm, we reserve the right to share their data with appropriate organisations to try to mitigate this risk. Please see Safeguarding policy.

5. Individual Rights

Note: Please see this guidance provided by the Office of the Information Commissioner for more information.
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/

5.1 The right to be informed {Arts 12-14}

When collecting personal information NSUN will provide to the data subject free of charge, a Privacy Policy written in clear and plain language which is concise, transparent, intelligible and easily accessible containing the following information:

a) Identity and contact details of the controller
b) Purpose of the processing and the lawful basis for the processing
c) The legitimate interests of the controller or third party, where applicable
d) Any recipient or categories of recipients of the personal data
e) Details of transfers to third country and safeguards, if applicable
f) Retention period or criteria used to determine the retention period
g) The existence of each of data subject's rights
h) The right to withdraw consent at any time, where relevant
i) The right to lodge a complaint with a supervisory authority
j) The source the personal data originates from and whether it came from publicly accessible sources

Not applicable if the data are obtained directly from the data subject

k) Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data

Not applicable if the data are obtained directly from the data subject

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 NSUN having obtained the data (within one month), ***or,*** if the data are used to communicate with the data subject, at the latest, when the first communication takes place*; **or***
if disclosure to another recipient is envisaged, at the latest, before the data are disclosed.

5.2 The right of access {Art:15}

The data subject shall have the right to obtain from the Controller confirmation as to whether or not personal data concerning them are being processed, and, where that is the case, access to their personal data and the information detailed in NSUN's relevant Privacy Policy:

5.3 The right to rectification {Art:16}

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

5.4 The right to erase {The right to be forgotten} {Art:17}

The data subject shall have the right to require the controller without undue delay to erase any personal data concerning them.

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 NSUN the data subject shall have the right to require the

controlled to cease processing the data for a reasonable period of time 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 (4.1 or 4.2) 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, and have the right to transmit those data to another controller without hindrance.

5.7 The right to object {Art:21}

The data subject shall have the right to object, on grounds relating to their particular situation, at any time to processing of personal data concerning them, including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

Operational Policies and Procedures

6. Operational Policies & Procedures – The Context

NSUN is a small charity holding personal information on its members, staff, trustees, associates and volunteers.

NSUN understands and accepts its responsibility under the UK General Data Protection Regulation (GDPR) to hold all personal data securely and use it only for legitimate purposes with the knowledge and approval of the data subjects.

By the following operational policies and procedures NSUN undertakes to uphold the principles and requirements of the GDPR in a manner which is proportionate to the nature of the personal data being held by NSUN. The policies are based on NSUN's assessment, in good faith, of the potential impacts on both NSUN and its data subjects of the personal data held by NSUN being stolen, abused, corrupted or lost.

7. Personnel

7.1 Data Protection Officer

In the considered opinion of NSUN the scope and nature of the personal data held by NSUN is not sufficient to warrant the appointment of a Data Protection Officer.

Accordingly, no Data Protection Officer is appointed.

7.2 Data Controller

NSUN is the Data Controller.

7.3 Data Processor

NSUN will not knowingly outsource its data processing to any third party (*eg:* Google G- Suite, Microsoft OneDrive) except as provided for in the section "Third Party Access to Data".

7.4 Access to Data

Except where necessary to pursue a vital interest, only NSUN will have access to the personal data held by NSUN, and those specified in the section "Third Party Access to Data".

7.5 Training

NSUN staff, trustees, associates, and volunteers will periodically undergo appropriate training commensurate with the scale and nature of the personal data that NSUN holds and processes under the GDPR.

8. Collecting & Processing Personal Data

NSUN collects a variety of personal data commensurate with the variety of purposes for which the data are required in the pursuit of our charitable objects.

All personal data will be collected, held and processed in accordance with the relevant Privacy Policy provided to data subjects as part of the process of collecting the data.

A Privacy Policy will be provided, or otherwise made accessible, to all persons on whom NSUN collects, holds and processes data covered by the GDPR. The Privacy Policy provided to data subjects will detail the nature of the data being collected, the purpose(s) for which the data are being collected and the subjects rights in relation to NSUN's use of the data and other relevant information in compliance with the prevailing GDPR requirements.

9. Information Technology

Personal data is mainly processed by NSUN staff, however on occasion, it may be processed by trustees, volunteers and NSUN associates. The following section and its processes and safeguards relates to all of these parties where reasonably possible.

9.1 Data Protection by Design/Default

Inasmuch as:

a) none of NSUN's staff or trustees are data protection professionals;

b) it would be a disproportionate use of charitable funds to employ a data protection professional, given the scale and nature of the personal data held by NSUN;

NSUN will seek appropriate professional advice commensurate with its data protection requirement whenever:

c) they are planning to make significant changes to the ways in which they process personal data;

d) there is any national publicity about new risks (*e.g.* cyber attacks)

which might adversely compromise NSUN's legitimate processing of personal data covered by the GDPR.

All personal data sent outside of NSUN's secure systems will be password-protected.

9.2 Data Processing Equipment

NSUN staff use laptops or personal computers to facilitate their work which are usually located at their home environment unless the equipment needs to be taken to a face-to-face meeting.

When not in use, the computers/laptops will be kept in a secure location and reasonably protected against accidental damage, loss, avoidable theft or other misuse by persons other than NSUN staff.

The Data Controller will keep a register of:

a) the location of all such devices used for the processing of personal data;

b) each occasion when the data on each device were accessed or modified and by whom (usually facilitated by the respective software used).

9.3 Data Processing

In normal working use, the data processed using staff equipment is processed within NSUN's

secure password-protected cloud-based systems e.g. membership database.
Should any data need to be extracted to be worked on temporarily, it will be stored on NSUN's secure password-protected cloud-based document storage systems i.e. SharePoint or OneDrive, and then deleted after the purpose for which it has been extracted has been accomplished. If this is not possible and the data has to be stored on the local hard drive, all staff local hard drives are encrypted and can only be accessed by a security key.

9.4 Data Processing Location

NSUN staff shall only process NSUN's personal data in a secure location, and not in any public place, e.g. locations where the data could be overlooked by others, or the equipment could be susceptible to loss or theft.

Computers/laptops in use for data processing will not be left unattended at any time.

9.5 Data Backups

The vast majority of personal data held by NSUN is held within secure, password-protected, cloud-based software. As such the data is backed up by the respective software providers.

Should interim working data need to be downloaded onto computers/laptops, to protect against the loss of data by accidental corruption of the data or malfunction of said IT equipment (including by physical damage), all NSUN's personal data shall be backed up periodically to a secure, local drive separate to the laptop/computer, or to a secure cloud location e.g. OneDrive, and whenever any significant changes (additions, amendments, deletions) are made to the data.

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

Equipment used to hold personal data, whether permanently or as interim working copies, which come to the end of their useful working life, or become dysfunctional, shall be disposed of in a manner which ensures that any residual personal data held on the equipment cannot be recovered by unauthorised persons.

Inasmuch as:

a) this will be a relatively infrequent occurrence;

b) techniques for data recovery and destruction are constantly evolving;

c) none of NSUN staff have relevant up-to-date expert knowledge of data cleansing;

Equipment which becomes obsolete or dysfunctional shall not be disposed of immediately. Instead it will be stored securely while up-to-date expert advice on the most appropriate methods for its data cleansing and disposal can be sought and implemented.

10. Data Subjects

10.1 The Rights of Data Subjects

In compliance with the GDPR NSUN will give data subjects the following rights.
These rights will be made clear in the relevant Privacy Policy provided to data subjects:

a) the right to be informed;

b) the right of access;

c) the right to rectification;

d) the right of erasure *Also referred to as "The right to be forgotten"*

e) the right to restrict processing

f) the right to data portability

g) the right to object

h) the right not to be subjected to automated decision making, including profiling.

Exemptions may apply as per Schedules 2-4 of the DPA 2018 and UK GDPR. Any exemption will be looked at on a case-by-case basis.

10.2 Rights of Access, Rectification and Erasure

Data subjects will be clearly informed of their right to access their personal data and to request that any errors or omissions be corrected expeditely.

Such access shall be given and the correction of errors or omissions shall be made free of charge provided that such requests are reasonable and not trivial or vexatious.
The request must be made in writing, either:

a) via email using the same email address that NSUN has on record; or

b) via hard copy to the NSUN postal address, signed and dated by the data subject (or their legal representative);

and,

c) the communication must clearly and unambiguously identify the data claimed to be in error or missing

The data will be corrected and the action will be communicated to the subject.

It will be explained to subjects who make a request to access their data and/or to have errors or omissions corrected, or that their data be erased, that, while their requests will be actioned as soon as is practical there may be delays where the appropriate NSUN staff who deal with the request may not work on every normal weekday.

Where a data subject requests that their data be rectified or erased the Data Controller and Data Processor will ensure that the rectifications or erasure will be applied to all copies of the subject's personal data including those copies which are in the hands of a Third Party for authorised data processing, where applicable.

10.3 Right of Portability

NSUN will only provide copies of personal data to the subject (or the subject's legal representative) on written request.

NSUN reserves the right either:

a) to decline requests for portable copies of the subject's personal data when such requests are unreasonable (ie: excessively frequent) or vexatious;
or

b) to make a reasonable charge for providing the copy, should it involve very onerous work.

10.4 Data Retention Policy

Personal data shall not be retained for longer than:

a) In the case of data held by subject consent:
the period for which the subject consented to NSUN holding their data;

b) in the case of data held by legitimate interest of the charity:
the period for which that legitimate interest applies. For example: in the case of data subjects who held a role, such as a volunteer, with NSUN the retention period is that for which NSUN reasonably has a legitimate interest in being able to identify that individual's role in the event of any retrospective query about it;

c) in the case of data held by legal obligation:
the period for which NSUN is legally obliged to retain those data.

NSUN shall regularly, and not less than every 6 months, review the personal data which it holds and remove any data where retention is no longer justified. Such removal shall be made as soon as is reasonably practical, and in any case no longer than 20 working days after retention of the data was identified as no longer justified.

11. Privacy Impact Assessment

11.1 Members' and Supporters' Data

The volume of personal data is high – around 4000 individuals
The sensitivity of the data is high: data includes email addresses, some postal addresses, and some special category data.
The risk of data breach is small – Membership data is held securely on the membership database. Should any data need to be worked on outside of this software it is held on password-protected IT equipment and within password-protected files. Any special category data worked on outside of the database environment is anonymised.

Overall impact: LOW

11.2 Employees' Data

The volume of personal data is very low – less than 6 individuals
The sensitivity of the data is moderate: the most sensitive data being date of birth and addresses.
The risk of data breach is low as the data is held within our secure, password-protected, cloud-based BrightHR software system.

Overall impact: LOW

11.3 Trustees' Data

The volume of personal data is very low – less than 15 individuals
The sensitivity of the data is moderate: the most sensitive data being date of birth and addresses.
The risk of data breach is low as the data is held within the secure Microsoft Office SharePoint storage environment.

Overall impact: LOW

11.4 Enquirers' Data

The volume of personal data is low-moderate.

The sensitivity of the data is low: the most sensitive data being an e-mail address;
The risk of data breach is low – primarily the accidental disclosure of names & e-mail addresses.

Overall impact: LOW

12. Third Party Access to Data

Under no circumstance will NSUN share with, sell or otherwise make available to Third Parties any personal data except where it is necessary and unavoidable to do so in pursuit of our charitable objects as authorised by the Data Controller.

Whenever possible, data subjects will be informed in advance of the necessity to share their personal data with a Third Party in pursuit of NSUN's objects.

Before sharing personal data with a Third Party, NSUN will take all reasonable steps to verify that the Third Party is, itself, compliant with the provisions of the GDPR and confirmed in a written contract. The contract will specify that:

a) NSUN is the owner of the data;
b) The Third Party will hold and process all data shared with it exclusively as specified by the instructions of the Data Controller;
c) The Third Party will not use the data for its own purposes;
d) The Third Party will adopt prevailing industry standard best practice to ensure that the

data are held securely and protected from theft, corruption or loss;

e) The Third Party will be responsible for the consequences of any theft, breach, corruption or loss of NSUN's data (including any fines or other penalties imposed by the Information Commissioner's Office) unless such theft, breach, corruption or loss was a direct and unavoidable consequence of the Third Party complying with the data processing instructions of the Data Controller

f) The Third Party will not share the data, or the results of any analysis or other processing of the data with any other party without the explicit written permission of the Data Controller;

g) The Third Party will securely delete all data that it holds on behalf of NSUN once the purpose of processing the data has been accomplished.

h) NSUN does not, and will not, transfer personal data out of the EEA.

13. Data Breach

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

In the event of any data breach coming to the attention of the Data Controller, NSUN will without undue delay and not later than 72 hours notify the Information Commissioner's Office.

In the event that full details of the nature and consequences of the data breach are not immediately accessible (*e.g:* because relevant staff do not work on every normal weekday) NSUN will bring that to the attention of the Information Commissioner's Office and undertake to forward the relevant information as soon as it becomes available.

14. Privacy Policy

NSUN will have a Privacy Policy which it will make available to everyone on whom it holds and processes personal data, in accordance with 5.1.

In the case of data obtained directly from the data subject, the Privacy Policy 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 Privacy Policy will be provided within a reasonable period of NSUN having obtained the data (within one month), ***or,***
if the data are used to communicate with the data subject, at the latest, when the first communication takes place*; **or***
if disclosure to another recipient is envisaged, at the latest, before the data are disclosed.

Appendix
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, in particular 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 or not 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, in particular 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 be in compliance with 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, in particular, 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 dactyloscopic 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 considered 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 with regard to 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 substantially affected or likely to be substantially 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 substantially affects or is likely to substantially 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 on the basis of, 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

1. 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 in order to take steps at the request of the data subject prior to entering into a contract;
   c) processing is necessary for compliance with a legal obligation to which the controller is subject;
   d) processing is necessary in order 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, in particular 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.
2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to 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.
3. 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.

4. 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, in particular regarding the relationship between data subjects and the controller;
   c) the nature of the personal data, in particular 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 12: Transparent information, communication and modalities for the exercise of the rights of the data subject

1. The controller shall take appropriate measures 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, in particular 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 in a position 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, taking into account 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 take action 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 taking action 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 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.

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 in order to give in an easily visible, intelligible and clearly elegible 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 of 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 the means by which 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 into 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 insofar as the data subject already has the information.

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.