SAMR CENTRE

GDPR Policy

Approved by: Directors
Last Review Date: 14th July 2023
Next Review Date: 14th July 2025

Contents

1. Introduction to the UK-GDPR

Under the United Kingdom General Data Protection Regulations (UKGDPR) Samr Centre (herein after referred to as "The organisation") is required to comply with the UK-GDPR and undertakes to do so.

Throughout this policy document, numbers prefixed by "Art:" in brackets *(eg: {Art:5})* refer to the relevant Article(s) in the UK-GDPR, as modified by the Keeling Schedule.

2. Definitions

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

Data Subject

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

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 (*eg:* Facebook, Skype, Hangouts, WhatsApp)

3. Principles of the UK-GDPR

The organisation 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 only for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall 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 in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK-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 Processing

The organisation will obtain, hold and process all personal data in accordance with the UK-GDPR for the following lawful purposes. In all cases the information collected, held and processed will include Contact Information (as defined in 2 above).

By Consent

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

a) Subject to the person's consent, this may include information selected and forwarded by The organisation on activities by other organisations which are relevant to those of the organisation.
Note: this will not involve providing the person's personal data to another organisation.

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

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

By Contract

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

The information collected will additionally contain details of:

d) The goods/services being sold to, or purchased from the organisation;

e) 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 organisation.

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

By Legal Obligation

People where there is a legal obligation on the organisation to collect, process and share information with a third party – *eg:* the legal obligations to collect, process and share with HM Revenue & Customs payroll information on employees of the organisation.

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

Employees; Taxation; Pensions

Note: *Legal obligations to employees fall under the much broader "umbrella" of UK employment law, taxation law (HM Revenue & Customs) and pensions law.*
It is beyond the skill level of Samr Centre to provide guidance in this area. Charities which employ staff are therefore advised to consult an appropriately qualified professional advisor (ie: one having skills in ***BOTH*** *employment* ***AND*** *charity law).*

By Vital Interest

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

By Public Task

The organisation undertakes no public tasks which require the collection, holding and/or processing of personal information.

Legitimate Interest

Volunteers, Including Executive Committee

In order to be able to operate efficiently, effectively and economically, it is in the legitimate interests of the organisation to hold such personal information on its volunteers and Executive Committee as will enable the organisation to communicate with its volunteers on matters relating to the operation of the organisation, *eg:*

- ☑ the holding of meetings;
- ☑ providing information about the organisation's activities – particularly those activities which, by their nature, are likely to be of particular interest to individual volunteers/Executive Committee;
- ☑ seeking help, support and advice from volunteers/Executive Committee, particularly where they have specific knowledge and experience;
- ☑ ensuring that any particular needs of the volunteer/trustee are appropriately and sensitively accommodated when organising meetings and other activities of the organisation.

Closed Circuit TV (CCTV) Recording

The organisation collects video CCTV images of people entering and moving around its premises in order to safeguard its collection from theft and vandalism, as required by its insurers.

The information collected is only processed and, where appropriate, shared with other authorities (eg: the Police) where it is necessary to investigate a potential crime.

5. Individual Rights

The right to be informed

When collecting personal information the organisation 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:

- Identity and contact details of the controller
  Note: *where the organisation has a controller's representative and/or a data protection officer, their contact details should also be included*.
- 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 the data are obtained directly from the data subject
- Any recipient or categories of recipients of the personal data
- Details of transfers to third country and safeguards
- Retention period or criteria used to determine the retention period
- The existence of each of 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 existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences.

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 organisation 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.

The right of access

The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him/her are being processed, and, where that is the case, access to his/her personal data and the information detailed in the organisation's relevant Privacy Policy:

The right to rectification

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

The right to erase {The right to be forgotten}

Except where the data are held for purposes of legal obligation or public task (0 or 0) the data subject shall have the right to require the controller without undue delay to erase any personal data concerning him/her.
Note: *This provision is also known as "The right to be forgotten".*

The right to restrict processing

Where there is a dispute between the data subject and the Controller about the accuracy, validity or legality of data held by the organisation 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.

The right to data portability

Where data are held for purposes of consent or contract (0 or 4.c)) the data subject shall have the right to require the controller to provide him/her with a copy in a structured, commonly used and machine-readable format of the data which he/she has provided to the controller, and have the right to transmit those data to another controller without hindrance.

The right to object

a) The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him/her which is based Public Task or Legitimate Interest (0 or 0), 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.

b) Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him/her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

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

d) At the latest at the time of the first communication with the data subject, the right referred to in paragraphs a) and d) shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

Rights in relation to automated decision making and profiling

{Except where it is: a) based on the data subject's explicit consent, *or b)* necessary for entering into, or performance of, a contract between the data subject and a data controller; 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 concerning him/her or similarly significantly affects him/her.

Operational Policies and Procedures

6. Operational Policies & Procedures – The Context

Samr Centre (The organisation) is a small non profit organisation holding just a small amount of non-sensitive data on a small number of people.

The Executive Committee understand and accept their responsibility under the UK General Data Protection Regulation (UK-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 the Executive Committee undertake to uphold the principles and requirements of the UK-GDPR in a manner which is proportionate to the nature of the personal data being held by the organisation. The policies are based on the Executive Committee' assessment, in good faith, of the potential impacts on both the organisation and its data subjects of the personal data held by the organisation being stolen, abused, corrupted or lost.

7. Personnel

Data Protection Officer

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

Accordingly, no Data Protection Officer is appointed.

Data Controller

The Board of Executive Committee is the Data Controller for the organisation.

Data Processor

The Board of Executive Committee will appoint at least 2 and not more than 5 of its number, or other appropriate persons, to be the Data Processors for the organisation.

The organisation 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".

Access to Data

Except where necessary to pursue the legitimate purposes of the organisation, only the Data Processors shall have access to the personal data held by the organisation.

Training

The Executive Committee and Data Processors will periodically undergo appropriate training commensurate with the scale and nature of the personal data that the organisation holds and processes under the UK-GDPR.

8. Collecting & Processing Personal Data

The organisation collects a variety of personal data commensurate with the variety of purposes for which the data are required in the pursuit of its charitable objects.

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

A Data Privacy Notice will be provided, or otherwise made accessible, to all persons on whom The organisation collects, holds and processes data covered by the UK-GDPR. The Data Privacy Notice 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 The

organisation's use of the data and other relevant information in compliance with the prevailing UK-GDPR requirements.

9. Information Technology

Data Protection by Design/Default

Inasmuch as:

a) none of the organisation's volunteer Executive Committee 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 the organisation;

The Executive Committee 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 (*eg:* cyber attacks);

e) any material changes to the UK-GDPR are proposed or have been made;

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

Personal data will never be transmitted electronically (*eg:* by e-mail) unless securely encrypted.

Data Processing Equipment

The scale and nature of the personal data held by the organisation is not sufficient to justify the organisation purchasing dedicated computers for the processing of personal data.

Instead The organisation will purchase and own at least 2 and not more than 5 removable storage devices to store the personal data that it holds and processes.
The removable storage devices will also act as backup devices.

Whilst the data will be processed on the computers/laptops to which the Data Processors have access, no personal data covered by the UK-GDPR will be stored on those computers/laptops. All interim working data transferred to such computers/laptops for processing will be deleted once processing has been completed.

When not in use the removable storage devices will be kept in a secure location and reasonably protected against accidental damage, loss, avoidable theft or other misuse by persons other than the Data Processors.

The Data Controller & Data Processors will keep a register of

f) the location of all removable devices used for the storage and processing of personal data;

g) each occasion when the data on each device were accessed or modified and by whom.

The organisation's removable storage devices shall not be used for the storage of any data which are unrelated to The organisation's processing of personal data.

Data Processing Location

Data Processors shall only process the organisation's personal data in a secure location, and not in any public place, *eg:* locations whether the data could be overlooked by others, or the removable data storage devices would be susceptible to loss or theft.

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

Data Backups

To protect against loss of data by accidental corruption of the data or malfunction of a removable data storage device (including by physical damage), all the organisation's personal data shall be backed up periodically and whenever any significant changes (additions, amendments, deletions) are made to the data.

Backup copies of the data shall be held in separate secure locations which are not susceptible to common risks (*eg:* fire, flood, theft).

As far as is reasonably practical, all files containing personal data covered by the UK-GDPR will be encrypted by the use of NCH-Meo, Kaspersky Vault or other comparable software.
The encryption keys will be held securely in a location which is separate from the data storage media.

Obsolete or Dysfunctional Equipment

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:

h) this will be a relatively infrequent occurrence;

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

j) none of the Executive Committee have relevant up-to-date expert knowledge of data cleansing;

equipment which becomes obsolete or dysfunctional shall not be disposed 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

The Rights of Data Subjects

In compliance with the UK-GDPR the organisation will give data subjects the following rights. These rights will be made clear in the relevant Data Privacy Notice provided to data subjects:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right of erasure *Also referred to as "The right to be forgotten"*
- the right to restrict processing;
- the right to data portability; *{LO} {LI}*

- the right to object; *{SC} {Co} {LO}*
- the right not to be subjected to automated decision making, including profiling.

The above rights are not available to data subjects when the legal basis on which the organisation is holding & processing their data are:*{SC}* Subject Consent; *{Co}* Contractual obligation*{LO}* Legal Obligation*{LI}* Legitimate Interest

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 promptly.

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.
There is no prescribed format for making such requests provided that:

a) the request is made in writing, signed & dated by the data subject (or their legal representative);

b) the data claimed to be in error or missing are clearly and unambiguously identified;

c) the corrected or added data are clear and declared by the subject to be complete and accurate.

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 volunteers or staff to deal with the request do 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.

Right of Portability

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

The organisation reserves the right either:

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

e) to make a reasonable charge for providing the copy.

Data Retention Policy

Personal data shall not be retained for longer than:

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

g) in the case of data held by legitimate interest of the organisation:
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 the organisation the retention period is

that for which the organisation reasonably has a legitimate interest in being able to identify that individual's role in the event of any retrospective query about it;

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

The organisation shall regularly – 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 (of the relevant Data Processor) after retention of the data was identified as no longer justified.

11.Privacy Impact Assessment

Executive Committee' Data

The volume of personal data is very low – less than 15 individuals
The sensitivity of the data is low-moderate: the most sensitive data being date of birth, previous names and previous addresses;
The risk of data breach is small as the data are rarely used, with the majority of the data being held for a combination of legal obligation and legitimate interest.

Overall impact: LOW

Volunteers'/Members' Data

The volume of personal data is low – less than 100 individuals
The sensitivity of the data is low: the most sensitive data being an e-mail address;
The risk of data breach is small – primarily the accidental disclosure of names & e-mail addresses.

Overall impact: LOW

Supporters' & 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 small – primarily the accidental disclosure of names & e-mail addresses.

Overall impact: LOW

12. Third Party Access to Data

Under no circumstance will the organisation 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 its 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 the organisation's objects.

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

- The organisation is the owner of the data;

- The Third Party will hold and process all data shared with it exclusively as specified by the instructions of the Data Controller;
- The Third Party will not use the data for its own purposes;
- 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;
- The Third Party will be responsible for the consequences of any theft, breach, corruption or loss of The organisation'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
- 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;
- The Third Party will securely delete all data that it holds on behalf of The organisation once the purpose of processing the data has been accomplished.
- The organisation does not, and will not, transfer personal data out of the UK.

13. Data Breach

In the event of any data breach coming to the attention of the Data Controller the Executive Committee will immediately notify the Information Commission's Office.

In the event that full details of the nature and consequences of the data breach are not immediately accessible (*eg:* because Data Processors do not work on every normal weekday) the Executive Committee 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 & Privacy Notices

The organisation will have a Privacy Policy and appropriate Privacy Notices which it will make available to everyone on whom it holds and processes personal data, in accordance with 0.

In the case of data obtained directly from the data subject, the Privacy Notice 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 Notice will be provided within a reasonable period of The organisation 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.