



Data Protection (GDPR) Policy and Procedure

Contents

1.0	Scope of Data Protection Policy	1
2.0	Data Protection Policy Statement	1
3.0	Legal Framework.....	2
4.0	Background	2
5.0	Data Protection Key Principles	2
6.0	Lawful, Fair and Transparent processing.....	3
7.0	Users' Rights as Data Subject	4
8.0	Accuracy.	5
9.0	Archiving/Removal	5
10.0	Security.....	5
11.0	Sharing of Personal Data	5
12.0	Breach	6
13.0	Contacts.....	6

1.0 Scope of Data Protection (GDPR) Policy

1.1 This policy, accompanying procedure, guidance for staff and guidance for volunteer's outline Room4's approach data protection.

1.2 The intended outcome of this document is to ensure that all data is kept lawfully, fairly and in a transparent manner; is collected for specific explicit and legitimate purposes; is limited to what is relevant to the purpose it is being collected; the data is accurate and up to

date; kept for no longer than is necessary and all data is processed in a secure manner safe from accidental loss or destruction.

- This policy applies to all personal data processed by Room4.
- The Responsible Person shall take responsibility for Room4's ongoing compliance with this policy.
- This policy shall be reviewed at least annually.
- Room4 shall register with the Information Commissioner's Office as an organisation that processes personal data.

2.0 Data Protection (GDPR) Policy Statement

2.1 The Data Protection Act 2018 controls how personal information is used by organisations, businesses, or the government. Everyone responsible for using personal **data** must follow strict rules called '**data protection principles**'. They must make sure the information is: used fairly, lawfully, and transparently.

Room4 is committed to high standards of information security, privacy, and transparency. We place a high priority on protecting and managing data in accordance with accepted standards. Room4 will comply with **Data Protection Act 2018** including as a data processor, while also working closely with our service users and partners to meet contractual obligations for our procedures, products, and services.

This policy applies to all staff, the Board of Directors, volunteers and sessional workers, agency staff, students or anyone working on behalf of Room4. GDPR is mandatory training for all staff at Room4 and training will be arranged as part of staff induction either online or face to face. New staff who have previously attended training will be required to supply evidence.

3.0 Legal Framework

Room4 is committed to comply with:

- Data Protection Act 2018

4.0 Background

All those working on behalf of Room4 have a responsibility to keep the data of staff, volunteers, service users and professionals secure, to gather only data which is necessary and to use it for its specific purpose.

Room4 is committed to processing data in accordance with its responsibilities under Data Protection Act 2018 (General Data Protection Regulations (GDPR). ICO Registration no ZB094997

5.0 Data protection key principles.

Room4 is committed to processing data in accordance with its responsibilities under the Data Protection Act. Article 5 of the Act requires that personal data shall be:

- Lawfulness, fairness and transparency: processed lawfully, fairly and in a transparent manner in relation to individuals.
- Purpose Limitation: collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Data minimisation: adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accuracy: 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.
- Storage limitation: 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 GDPR in order to safeguard the rights and freedoms of individuals.
- Integrity: 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.

6.0 Lawful, fair and transparent processing

6.1 To ensure its processing of data is lawful, fair and transparent, Room4 maintains a Register of Systems.

6.2 The Register of Systems shall be reviewed at least annually.

6.3 Individuals have the right to access their personal data and any such requests made to Room4 shall be dealt with in a timely manner.

6.4 Lawful purposes All data processed by Room4 must be done on one of the following lawful bases: The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

- (a) Consent: the individual has given clear consent for processing their personal data for a specific purpose.
- (b) Contract: the processing is necessary for a contract with the individual, or because they have asked for specific steps to be taken before entering into a contract.

- (c) Legal obligation: the processing is necessary to comply with the law (not including contractual obligations).
- (d) Vital interests: the processing is necessary to protect someone's life.
- (e) Public task: the processing is necessary to perform a task in the public interest or for official functions and the task or function has a clear basis in law. (not including contractual obligations).
- (d) Vital interests: the processing is necessary to protect someone's life.
- (e) Public task: the processing is necessary to perform a task in the public interest or for official functions and the task or function has a clear basis in law.
- (f) Legitimate interests: the processing is necessary for legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.
(see ICO guidance for more information).

6.5 Room4 shall note the appropriate lawful basis in the Register of Systems.

6.6 Where consent is relied upon as a lawful basis for processing data, in consent shall be kept with the personal data.

6.7 Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems are in place to ensure such revocation is reflected accurately in Room4's systems.

7.0 Users' rights as a data subject

Users' have rights as a data subject. These rights are:

7.1 The right to be informed – this means we must inform you how we are going to use personal data. We do this through this privacy policy and by informing Users' how data will be used each time we collect it.

7.2 The right of access – you have the right to access your personal data (e.g. data that is about you) that we hold. This is called a subject access request. We must respond to your request within one month. To request access to your data, please email info@room4.org It is very helpful if you tell us what personal data you are seeking.

7.3 The right to rectification – if you think the data we hold on you is incorrect, tell us so we can put it right. You can do this by emailing: info@room4.org

7.4 The right to erasure – you have the right to request that we delete your data. We will do so, provided that we do not have a compelling reason for keeping it. To request this, please e-mail: info@room4.org

7.5 The right to restrict processing – you can change your communication preferences (therefore restricting how we communicate with you) by contacting, info@room4.org

There are also certain other circumstances in which you can suppress the processing of your personal data. To request this, please email info@room4.org

7.6 The right to data portability – It allows data subjects to obtain data that a data controller holds on them and to reuse it for their own purposes. Individuals are free to either store the data for personal use or to transmit it to another data controller.

info@room4.org

7.7 The right to object – you have the right to object to Direct Marketing. This is not something we do at Room4. If that ever changes, this policy will be updated accordingly.

7.8 Rights in relation to automated decision making and profiling – this is not something we do at Room4. If that ever changes, this policy will be updated accordingly.

8.0 Accuracy

8.1 Room4 shall take reasonable steps to ensure personal data is accurate.

8.2 Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

9.0 Archiving/Removal

9.1 To ensure that personal data is kept for no longer than necessary, Room4 shall put in place a Retention Policy for each area in which personal data is processed and review this process annually.

9.2 The Retention Policy shall consider what data should/must be retained, for how long, and why.

10.0 Security

10.1 Room4 shall ensure that personal data is stored securely using a secured filing system.

10.2 Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.

10.3 When personal data is deleted this should be done safely such that the data is irrecoverable.

10.4 Appropriate back-up and disaster recovery solutions shall be in place.

11.0 Sharing of Personal Data

Who does Room4 share information with?

11.1 Unidentifiable information is shared for monitoring purposes. Information may be shared with partner agencies to access support for the service user via referral – consent is sought from the service user.

11.2 Data will be shared in the event to safeguard a vulnerable adult or child. For example, individuals who are referred for support will have their details added to a case management system or donors' details will be recorded for the purposes of collecting Gift Aid.

11.3 When Room4 shares personal information with another organisation it will always have an agreement in place to ensure that we comply with all data protection law.

11.4 In the course of providing support to clients, Room4 may also ask for consent to share personal data with other organisations so that we can provide the best support to our clients. For example, this could include social care and health agencies, education or any other relevant agencies. This will be explained at the start of support and consent can be given or withdrawn to share data with other agencies at any time.

11.5 On a rare occasion it may be necessary for us to share personal information without consent if we are required to do so by a court order or if there are other valid reasons, such as to protect a child or adult who is thought to be at risk or to stop a crime. If this happens, then we will record our reasons for doing so. We will also advise the client what we have done, if it is safe to do so.

11.6 We never sell personal information to anyone else or transfer personal data to a third country or international organisation.

12.0 Breach

12.1 In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, Room4 shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO (more information on the ICO website).

13.0 Contacts

Room4 does not meet the criteria for a mandatory Data Protection Officer.

Policy Reference Information

Approved by Board of Directors: 27.2.2020

Last Review Date: 27.2.2021

Next Review Date: 27.2.2022