GROUP HUG

Data Protection (GDPR 2018) & Privacy Policy

Reference:	Data Protection (GDPR 2018) & Privacy Policy
Date Approved:	16th May 2021
Approving By:	Jonathan Andrew Greenwood
Implementation Date:	16th May 2021
Version:	V2
Supersedes:	V1
Consultation Undertaken:	Internal
Target Audience:	Staff and Volunteers
Review Date:	16th may 2022
Lead	Jonathan Andrew Greenwood
Author/Lead:	Denise Read

GROUP HUG

Contents

GROUP HUG

Data Protection (GDPR 2018) & Privacy Policy

1. Data protection principles

Group Hug are committed to processing data in accordance with its responsibilities under GDPR (General Data Protection Regulations 2018).

Article 5 of the GDPR requires that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- 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;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- 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;
- 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; and
- 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.

2. Individual Data Protection Rights

Every user/ individual is entitled to the following:

- **The right to access** – You have the right to request Group Hug for copies of your personal data. We may charge you a small fee for this service.
- **The right to rectification** – You have the right to request Group Hug correct any information you believe is inaccurate. You also have the right to request Group Hug to complete the information you believe is incomplete.

- **The right to erasure** – You have the right to request that Group Hug erase your personal data, under certain conditions.
- **The right to restrict processing** – You have the right to request Group Hug restrict the processing of your personal data, under certain conditions.
- **The right to object to processing** – You have the right to object to Group Hug's processing of your personal data, under certain conditions.
- **The right to data portability** – You have the right to request Group Hug transfer the data that we have collected to another organisation, or directly to you, under certain conditions.

3. General provisions

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

4. Lawful, fair and transparent processing

- To ensure its processing of data is lawful, fair and transparent, Group Hug shall maintain a Register of Systems.
- The Register of Systems shall be reviewed at least annually.
- Individuals have the right to access their personal data and any such requests made to Group Hug shall be dealt with in a timely manner.

5. Lawful purposes

- All data processed by Group Hug must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests (see ICO guidance for more information).
- Group Hug shall note the appropriate lawful basis in the Group Hug - Controller documentation spreadsheet and in section 11 Personal data collected, held and processed.
- Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
- 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 should be in place to ensure such revocation is reflected accurately in Group Hug's systems.

6. Data minimisation

- Group Hug shall ensure personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

7. Accuracy

- Group Hug shall take reasonable steps to ensure personal data is accurate.
- Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure personal data is kept up to date.

8. Archiving / removal

- To ensure personal data is kept for no longer than necessary, Group Hug shall put in place an archiving policy for each area in which personal data is processed and review this process annually.
- The archiving policy shall consider what data should/must be retained, for how long, and why.

9. Security

- Group Hug shall ensure personal data is stored securely using modern software that is kept-up-to-date.
- 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.
- When personal data is deleted this should be done safely as such that the data is irrecoverable.
- Appropriate back-up and disaster recovery solutions shall be in place.

10. Breach

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, Group Hug 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).

11. Personal Data Collected, Held, and Processed

The following personal data is collected, held, and processed by Group Hug (for details of data retention,

please refer to the Data Handling Policy):

Data Ref.	Type of Data	Purpose of Data
1	Title	Regular email communications
2	First Name	Regular email communications
3	Surname	Regular email communications
4	Company Email Address	Regular email communications
5	Personal Email Address	
6	Home Address	
7	Home Telephone Number	
8	Company Name	
9	Company Address	
10	Company Telephone Number	
11	Minutes	
12	Presentations	
13	Emails	Emails sent to and from Group Hug from 2021 onwards

12. Data Retention

- Group Hug shall not keep personal data for any longer than is necessary considering the purpose or purposes for which that personal data was originally collected, held, and processed.
- When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.
- For full details of Group Hug's approach to data retention, including retention periods for specific personal data types held by Group Hug, please refer to our Data Handling Policy.

13. Data Security – Storage

Group Hug shall ensure the following measures are taken with respect to the storage of personal data:

- All electronic copies of personal data should be stored securely using passwords.
- All personal data stored electronically should be backed up immediately on a cloud storage platform.
- No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to Group Hug or otherwise without the formal written approval of Data Protection Officer or General Manager and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary.
- No personal data should be transferred to any device personally belonging to any volunteer, agent, contractor, or other party working on behalf of Group Hug and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of Group Hug where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the GDPR.

14. Data Breach Notification

- All personal data breaches must be reported immediately to Group Hug's Data Protection Officer.
- If any volunteer, agent, contractor, or other party working on behalf of Group Hug becomes aware of or suspects that a personal data breach has occurred, they must not attempt to investigate it themselves. All evidence relating to the personal data breach in question should be carefully retained.
- If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g., financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.
- In the event a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.
- Data breach notifications shall include the following information:
    - The categories and approximate number of data subjects concerned.

- The categories and approximate number of personal data records concerned.
- The name and contact details of Group Hug's data protection officer (or other contact point where more information can be obtained).
- The likely consequences of the breach.
- Details of the measures taken, or proposed to be taken, by Group Hug to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

15. Implementation of Policy

This Policy shall be deemed effective as of 16th May 2021. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.