General Data Protection Regulation (GDPR) Policy

This Policy sets out how Lifeafterhummus Community Benefit Society Limited will comply with the requirements of GDPR.

Background

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

As a provider of services directly to the public and for private, public and voluntary sector organisations it is necessary for Lifeafterhummus Community Benefit Society to collect and process personal data. As our services generate health and wellbeing outcomes for individuals, it is also necessary for us to process sensitive personal data which helps us demonstrate the impact of our services. This is a legitimate interest as it is both crucial to our commercial viability (demonstrating capability and impact) and the achievement of our objects as a Community Benefit Society.

General

1. Lifeafterhummus Community Benefit Society is the Data Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes.
2. We will appoint a Data Protection Officer, who is responsible for monitoring and implementing compliance with GDPR. The Data Protection Officer is responsible for reporting to the Directors any relevant breaches or concerns about data collection and processing within the Society.
3. Data protection will be a standard agenda item at Directors meetings.
4. We will publish a Privacy Policy on our website.
5. We will maintain a data protection compliance folder on our society file system. This will form the basis of our proof of compliance.
6. In addition to Directors meetings, we will keep minutes of internal meetings on GDPR, and decisions made on GDPR.
7. The Data Protection Officer and Directors will ensure that we map our data, i.e. establish what data our society collects and where, separate the data into categories and identify the lawful basis for processing each category of data.
8. Where there is no lawful basis for processing or retaining personal data, we will erase that data.
9. All data subject access requests will be sent to the Data Protection Officer for approval, who may delegate processing of such requests.
10. All requests to erase or correct data will be sent to the Data Protection Officer for approval, who may delegate processing of such requests.

Sharing data with third parties

11. We will only share Personal Data we hold with third parties, such as our service providers if:
    (a) they have a need to know the information for the purposes of providing the contracted services;
    (b) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;
    (c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
    (d) the transfer complies with any applicable cross border transfer restrictions; and

(e) we have an agreement or contract in writing that details compliance with GDPR for third party processing of data .

12. We may be required to provide data to statutory bodies in discharge of our legal obligations
13. We will maintain records of third-party recipients of Personal Data

Retention of data

14. In order to ensure that personal data is not retained for longer than is necessary, the Directors will approve a retention schedule for different categories and sub-categories of data. When personal data has reached the end of its retention period Directors will ensure it is securely erased or anonymised unless there is a lawful basis for retaining it for a further period. Any decision to retain data longer than the period outlined in the schedule must be approved by the Directors.

Non compliance and breaches

15. In the event of any data breach, the Data Protection Officer must be informed immediately. The Data Protection Officer will decide what immediate action should be taken and will inform the Directors.
16. All data breaches must be recorded in a Data Breach Log to record events such as "Stacey emailed the client list to Tim Smith in the finance team not Tom Smith in the sales team".
17. We will document any potential non-compliance issues in our data protection compliance folder to show awareness of compliance omissions and actions being taken towards total compliance or risk mitigation.
18. We will provide training to all staff so they understand what constitutes personal data, how to identify a personal data breach or any other potential non-compliance with data protection principles, and how to notify the Data Protection Officer.
19. Any volunteer processing data will also be provided with training to ensure they understand what constitutes personal data, how to identify a personal data breach or any other potential non-compliance with data protection principles, and how to notify the Data Protection Officer.

Data security

20. All staff, volunteers, Directors and Members must ensure they store personal data securely.
21. All personal data will be kept on secure password protected servers, on password protected computers which are stored in locked premises, or in filing systems which can be secured (i.e. lock on filing cabinet or stored in locked premises).
22. The Directors will ensure the Society's asset register details the serial numbers of all computers or other devices used to store or process personal data.
23. Managers or the Data Protection Officer must carefully consider which individuals should have access to the data on each device and take appropriate measures such as password protection to ensure data can only be accessed by authorised individuals.

Approved by Directors on November 2018