GDPR Data Protection Policy

Date Agreed: 24 May 2018
Review: Annually in May

Introduction
Banana Link needs to gather and retain certain information about individuals for various purposes and has written this data protection policy to comply with GDPR regulations introduced in 2018.

Personal data collected and retained by Banana Link includes, but is not limited to: employee, director and partner information, volunteer contact details, donor and trade union contact details, subscribers to our various publications and any information relating to contacts the organisation has a relationship with.

This policy outlines how this personal data will be collected, handled and stored to comply with the law and has been written following Information Commissioner's Office (ICO) guidelines.

GDPR places emphasis on consent, accountability and transparency with regards to the collection, management and storage of personal data and Banana Link endeavours to comply fully.

Definitions

Personal data is viewed as any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people. (www.ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/)

Key Principles
Under the GDPR, the data protection principles set out the main responsibilities for organisations and Banana Link will ensure 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.

- 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.
- The controller shall be responsible for, and be able to demonstrate, compliance with the principles.

Consent

The GDPR is clearer that an indication of consent must be unambiguous and involve a clear affirmative action (an opt-in) - It specifically bans pre-ticked opt-in boxes.

It also requires distinct ('granular') consent options for distinct processing operations. Consent should be separate from other terms and conditions and should not generally be a precondition of signing up to a service.

The GDPR gives a specific right to withdraw consent. You need to tell people about their right to withdraw, and offer them easy ways to withdraw consent at any time.

A contract is also a lawful basis to collect/store personal data because either they have asked you to do something before entering into a contact or to fulfil your contractual obligations to them (e.g provide a quote).

You must keep records to evidence consent identifying: who consented, when, how and what they were told.

In order to comply with these regulations, Banana Link will be using Mailchimp to store contact lists and send out communications. Anyone on our lists currently has been sent an email asking them to consent to their details being stored and to continue receiving Banana Link literature. There is also always an opportunity to unsubscribe at any time. All these actions are recorded and evidenced by Mailchimp and the deletion process instantaneous.

Individual Rights

The GDPR provides the following rights for individuals:

1. The right to be informed – individuals must be informed about the collection and use of their personal data as well as the purpose for processing, retention period and who is will be shared with.

2. The right of access - individuals has the right to obtain confirmation that their data is being processed and access to their personal data (information is to be provided free of charge and within one month unless requests are found to be unfounded, excessive or repetitive).

3. The right to rectification – individuals have the right to request inaccurate data to be corrected either verbally or in writing. This must be done within one month.

4. The right to erasure – Individuals have 'the right to be forgotten' unless data must be kept for legal reasons. Requests can be made verbally or in written and organisations have one month to respond and react.

5. The right to restrict processing – individuals have the right to request the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances.

6. The right to data portability – allows individuals to obtain and reuse their personal data for their own purposes across difference services. It allows them to move, copy or transfer personal data.

7. The right to object – individuals have the right to object to process based on legitimate interest, direct marketing and processing for purposes of scientific/historical research and statistics.

8. Rights in relation to automated decision making and profiling – individuals must explicitly consent to have their data used for automated decision making and profiling.

Accountability and Governance
Banana Link agrees, in accordance with GDPR regulations, to demonstrate and evidence its compliance to the above principles and recognises our responsibility and accountability.

Banana Link will demonstrate compliance by:

- Implementing appropriate measures and will ensure all staff, directors and volunteers comply with our internal Data Protection Policy.
- Regular reviews of the data we hold and record yearly data destruction cycles. Completion of this audit will be evidenced on the attached sheet which is to be kept in the master policy folder.

Storage of Data
Any lists or databases will stored on mailchimp wherever possible. Subscribers can remove themselves from lists at any time and this process is managed by Mailchimp.

All Banana Link files will be stored on Google Drive with password only access and access permissions will be given only to those for whom it is appropriate.

Paperwork containing personal data and sensitive information is to be kept in locked filing cabinets with restricted access.

Data Breaches
As per ICO instruction, Banana Link will report any data breaches within 72 hours to ICO.