

# GDPR Policy

**Version:** 1.1

**Effective Date:** January 2025

**Approved By:** Board of Trustees

**Date of Approval:** January 2025

**Review Date:** January 2026

**Amendments:** SAR Procedure Update, 05/07/24

---

## Purpose

The goal of this data protection policy is to depict the legal data protection aspects in one summarising document. This is not only to ensure compliance with the European General Data Protection Regulation (GDPR) and Data Protection Act (DPA) 2018 but also to provide proof of compliance.

At Bridge to Unity we are committed to processing data in accordance with our responsibilities under the GDPR. 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
- 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.

## General Provisions

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

## What data do we collect?

In order to enable us to carry out the work that we do, we often need to collect personal details from our service users and other members of the community. This might be, as an example, to enable us to support a service user in finding employment, to process a fundraising donation, or to ensure you receive information that you have requested.

As well as this, our marketing team uses data collected in the form of statistics to analyse how for example our website and social media profiles are connecting with people.

We use Google Analytics which records data which does not personally identify you but looks at things like geographical location. You can find more information about how Google Analytics records your data via Googles own policies and procedures page:

<https://support.google.com/analytics/answer/4597324?hl=en>

We may collect data via our online fundraising systems for example; if you have a regular direct debit we will need to store name, address and bank details, as well as things like phone numbers and email addresses. If you book tickets for one of our events we may hold your personal information to provide you with essential updates about relevant arrangements.

Our service users and others are able to voluntarily register for our newsletter which is delivered via email. In order to sign up to this newsletter we will record your name and email address. You can unsubscribe from this at any time. As well as our newsletter there are a number of other forms on our website such as: application forms, referral forms, expenses forms. These forms will collect information such as name, address, email, phone number. This information is stored securely in our CRM and website systems and will be automatically deleted after 18 months.

## How do we keep your data safe?

At Bridge to Unity we are committed to ensuring we take appropriate measures to ensure your personal information is kept safe.

Personal information is stored electronically on our secure CRM system. Only members of staff, usually exclusively senior management, that require access to this data will have access, and only when necessary to carry out our day-to-day work.

As part of our commitment to data security, we ensure that all members of staff that have access to personal data have received data protection training.

We are committed to ensuring that personal data is stored securely using modern software that is kept-up-to-date. As and when we delete personal data we shall ensure that it is irrecoverable. As well as this, appropriate back-up and disaster recovery solutions shall be in place.

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, Bridge to Unity 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).

## Legal Framework

- All data processed by Bridge to Unity 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).

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

As defined and set out in the General Data Protection Regulation (GDPR) and UK data protection legislation, we are required to ensure we have a 'legal basis' for collecting personal information.

We require consent from yourself to use your information for a specific purpose, eg for donations or newsletters, and legally you are able to withdraw this consent at any time.

Occasionally we are legally required to collect personal data to comply with our regulatory requirements. As well as this, if for example you work for us or are applying to work with us, or you are registering as a service user for support, we will be required to collect information needed to enable us to carry out our contract with you.

The legal framework of the GDPR allows us to collect and process your information if it is necessary to carry out our legal and legitimate activities, assuming of course that this does not impact your rights. This could be for example by: providing support to service users, organising events and processing donations, or for example if you have contacted us for information.

We will not ever sell your personal information to other organisations or share it with other organisations, unless we have your explicit consent, or if for example it is required by law, for example in safeguarding situations.

You have a right to request, at any time, information about the personal data we hold about you, as well as this if you feel we hold inaccurate information you have a right to have this corrected.

If you require further information about any of the contents of this policy please contact us on: [info@bridgetounity.co.uk](mailto:info@bridgetounity.co.uk)

# Subject Access Requests (SARs)

<b>1. Submission and Acknowledgment</b>	<p><b>Method:</b> Requests can be submitted via email, postal mail, or our online portal</p> <p><b>Email:</b> <a href="mailto:info@bridgetounity.co.uk">info@bridgetounity.co.uk</a></p> <p><b>Postal Address:</b> The Pallant Centre, Havant, PO9 1BE</p>
<b>2. Identity Verification</b>	<p><b>Acknowledgment:</b> We will acknowledge the request within 3 business days.</p> <p><b>Proof Required:</b> Government-issued ID and a utility bill or bank statement.</p> <p><b>Additional Info:</b> We may request further information if needed.</p>
<b>3. Logging and Tracking</b>	<p><b>Log Entry:</b> All SARs will be logged with a unique reference number.</p> <p><b>Tracking:</b> Progress will be tracked until completion.</p>
<b>4. Data Collection</b>	<p><b>Notification:</b> We will coordinate and collect the relevant data.</p> <p><b>Review:</b> Data will be reviewed to include only the requester's personal data.</p>
<b>5. Response Timeframe</b>	<p><b>Standard Deadline:</b> One month from receipt.</p> <p><b>Extensions:</b> Up to two additional months for complex requests, with notification to the requester.</p>
<b>6. Providing Information</b>	<p><b>Format:</b> Electronic format unless otherwise requested.</p> <p><b>Contents:</b></p> <ul style="list-style-type: none"> <li>• Confirmation of data processing</li> <li>• Copy of personal data</li> <li>• Processing purposes, data categories, and recipients</li> <li>• Storage duration</li> <li>• Rights to rectification, erasure, and restriction</li> <li>• Right to complain to a supervisory authority</li> <li>• Data source (if not from the data subject)</li> <li>• Details of automated decision-making, if applicable</li> </ul>

<b>7. Handling Rectification, Erasure, or Restriction Requests</b>	<p><b>Rectification:</b> Correct inaccurate data and inform the requester.</p> <p><b>Erasure:</b> Assess and act on erasure requests as per GDPR criteria.</p> <p><b>Restriction:</b> Comply with requests to restrict processing and inform the requester.</p>
<b>8. Refusal of Requests</b>	<p><b>Grounds for Refusal:</b> Requests that are manifestly unfounded, excessive, or infringe on others' rights.</p> <p><b>Notification:</b> Inform the requester of the refusal within one month, including reasons and the right to complain.</p>
<b>9. Training and Policy Review</b>	<p><b>Staff Training:</b> Regular training on handling SARs and GDPR compliance.</p> <p><b>Policy Review:</b> Annual review and updates to ensure compliance.</p> <p><b>Data Protection Lead:</b> Matt Simmons, Bridge to Unity   <a href="mailto:info@bridgetounity.co.uk">info@bridgetounity.co.uk</a>   Phone - 01329 600414</p> <p><b>By adhering to this procedure, Bridge to Unity ensures efficient and GDPR compliant handling of Subject Access Requests.</b></p>