Street Storage UK GDPR Policy*

***To be used in conjunction with Street Storage's Privacy**

Policy Purpose

This policy explains clearly how Street Storage will collect, process and store the data relating to our staff, volunteers and people who use the service. The UK General Data Protection Regulation ("UK GDPR") and the UK Data Protection Act 2018 gives people more control over their data, and ensures organisations remain accountable for their storage and disposal of said data.

The UK GDPR seeks to ensure that organisations processing personal data, including charities:

- Comply with provisions
- Demonstrate compliance
- Ensure best practice in advance of receiving data
- Make sure all data subjects know exactly what's happening with their data.

Sensitive Data

Sensitive data (also known as 'special category personal data' under the UK GDPR) includes the following:

- Race or ethnic origin
- Political opinions
- Religious or similar beliefs
- Trade Union memberships
- Physical or mental health
- Info on sexual health
- Commission or alleged commission of an offence, or information thereof
- Biometric data (new addition)

Data Processors and Data Controllers

The UK GDPR and UK Data Protection Act 2018 details the following roles both internally and externally to an organisation.

Data Controller – Street Storage as an organisation is a controller as it makes decisions about how the personal data is processed. Street Storage manages the collection, storage and disposal of data.

Data Processor(s) – this refers to any third-party organisation that handles personal data on behalf of, and under the instructions of, the controller. This includes:

- Mailing houses
- Third-party fundraisers
- Data destruction organisations

Data Protection Officers – Personnel specifically appointed within the organization as a data protection officer who ensure the charity complies with regulations. The UK GDPR requires a data protection officer be appointed if:

- The organisation is a public authority or body
- The charity involves regular monitoring of lots of data
- Its core activities involve processing lots of data.

Reasons for Collecting Data

To collect personal data, Street Storage must have one of the following reasons (which are prescribed by the UK GDPR):

- Individual has consented
- The processing is necessary for the performance of a contract with the individual
- The processing is necessary for compliance with a legal obligation
- The processing is necessary to protect the vital interests of the individual
- Necessary for administering justice
- In accordance with 'legitimate' interests (of Street Storage or a third party)

Legitimate Interests

Charities are allowed to process data when it's in their legitimate interests or that of a third party. The UK GDPR does not prescribe what is a legitimate interest, but they include:

- Network security
- Fraud prevention
- Maintaining existing person relations
- Direct marketing

Consider the following when deciding if something can be used as a legal legitimate reason for processing data.

Data Subject Interest – the processing should not harm the data subject or cause risk of harm. Does the legitimate interest cause harm or risk harm?
Reasonable Processing – this reason will generally not be applicable when data subjects wouldn't expect further processing. Is it in the reasonable expectation of the data subject?
Right to be Informed – data subjects must be informed of the legitimate interest being relied upon. Does the Street Storage Privacy Policy cover this?

Defining Legitimate Interest

When relying on legitimate interests, Street Storage must usually perform a Legitimate Interests Analysis (LIA). There is no hard and fast rule on what this should look like, but broadly it should answer the following questions:
1, Does a legitimate interest exist? What is it?
2. Does Street Storage need to process the data?

If Street Storage is satisfied the data meets both requirements, it must then perform a Balancing Test. This test will decide if the legitimate interest of Street Storage or third-party is outweighed by the rights of the individual whose data is being processed.
1. This should be clearly defined. It should be clear who the beneficiaries are
2. Though unlikely, alternatives to the data processing should be considered
3. Nature of interest
i. Would the individual expect the processing?
ii. Is the legitimate interest a fundamental or public right?
iii. Is there any harm caused by processing the data?
iv. Would the individual share the same interest?

Street Storage: Procedure for Collecting and Storing Data
To be able to perform its essential functions, Street Storage is required to collect and store data from people who use the service, employees, volunteers and referral partners.

Collection of people who use the service' and Referral Agents' Data
Data is collected and stored in both hard and electronic copies. The hard copies are stored in locked boxes at the St Giles unit, and only specific staff have access to these.

Electronic data is stored on Street Storage's GDrive and our CRM, Salesforce - both of which are password protected and have 2FA. Only key members of staff have access to this. Certain data that is stored is collected through explicit consent of the relevant data subject (in this case, the person). Documents used by Street Storage include:

- Data Consent Forms
- Email and Phone Communication Forms
- Video and Photo Consent Forms

These require signatures and acknowledgement. These sections may be filled in by the Referral Agent prior to the person's initial appointment. Whether or not this is the case, Street Storage are required to ensure that all people who use the service understand what they are agreeing to and that it is the person providing consent.

There is no statutory limit to how long storage data can or should be stored. Street Storage - on market research of similar organisations and through seeking legal advice (plus practical reasons re: service delivery) - have decided that data will be kept for a period of 6 years and disposed of after 6 years of no contact. This is marked in the Google Calendar and should be updated if the person requires an extension to their storage period or re-stores at a later date.

If someone is referred to Street Storage but, for whatever reason, does not store their belongings, the same rules will apply.

If and when Street Storage creates case-studies, these will be anonymised or Street Storage will have explicit, freely-given consent from the relevant person.

Data Breaches
Data breaches don't just include losing data. It's any security breach that leads to destruction, loss, alteration, unauthorised disclosures or access to personal data.

<u>See Street Storage Data Breach Procedure</u>
Report a Data Breach to the ICO within the first 72 hours where this is likely to cause harm to the affected data subjects. This can be done online. Street Storage may also have to notify the individuals concerned if the breach is likely to cause them harm.

If it is a serious breach, staff must also report the breach to the Charities Commission. Serious breaches include:

- Data accessed by an unknown party; data accessed and deleted. This includes email accounts, donor names and addresses.
- Laptop with data is stolen/missing/reported to the police
- Funds lost to phishing or telephone scam when account details were given out

Street Storage

Fundraising and Data

Direct Marketing to Donors. There are also data protection laws related to direct marketing. Direct marketing covers all advertising or promotional material and is not confined to communications sent in a commercial context - it also includes promoting an organizational aims and objectives – and so covers charities.

Broadly, Street Storage needs **Consent** to send direct marketing messages to donors.

- This must be freely given, opt-in consent.
- For example, a donor ticks a tick box agreeing to receive fundraising communications.
- Donors must be informed about what giving their consent means. This means the charity must be open about fundraising plans and the consequences of 'ticking a box.'

Records of fundraising data should be kept for 6 years after use with the exception of legacy donors. The same rules and procedures apply for income, expenditure information and financial data held by the organisation.

Gift Aid

HMRC advises that donor data must be kept for 6 years if they are regular givers. Exceptions to this rule (and data that can be disposed of) includes:

- If the donor has only donated once
- If the donor has not donated in three years

Audits

Audits help the ICO to understand processes and can include a review of:

- Employee records, including salary, credit applications and pension records
- Volunteer records, including financial data and expenses
- Supporter and fundraising data, including donations; support provided; any financial-linked data, such as property
- Supplier information, including email addresses and contact information

The audit could take the form of:

- Introductory presentations to key members of staff
- Questionnaires sent to the business/operation units to check on data held
- Consideration on whether all data held remains relevant
- Inquiries into how the records have been stored and disposed of

During a data audit, Street Storage may be required to produce a clear and understandable policy and procedural framework. This includes organisation communication/agreements with 3rd-party processors and both electronic and hard copy data.

Individual Rights

The UK GDPR ensures various rights for the individuals whose data is stored. Individuals have:

- The right to be informed

- A right of access
- The right of rectification
- The right of erasure (this excludes Gift Aid HMRC data)
- The right to restrict processing
- The right to object
- The right not to be subjected to automated decision making, including profiling
- The ‘right to portability’. This applies to personal data provided to
- the controller; where processing is based on consent or for the
- performance of a contract; when processing is automated.

Subject Access Requests (SAR)
The UK GDPR gives any individual the right to find out about what information a controller holds about them. A Subject Access Request (SAR) is a means by which an individual finds out what personal data a controller holds about them, why it is held, and with whom it is shared. This right can be exercised against Street Storage.

Validity
A Subject Access Request (SAR) can be requested in writing (via any medium) or orally. So it is important that Street Storage recognize a SAR when received.
The data an individual has the right to obtain is as follows:

- Confirmation that their data is being processed;
- Access to their personal data;
- Other supplementary information – this largely corresponds to the information that should be provided in a privacy notice (detailed further below)

SARs should be dealt with free of charge, unless the request is an unusually large or complex request, if this is the case a reasonable fee may be charged.

Verification
When a SAR is submitted, an individual must provide verification of their identity using ‘reasonable means’. This will be required by Street Storage before any data is released to them.

Data Release:
As a Data Controller Street Storage will supply all information available to them, which an individual has requested and that individual is entitled to receive under the legislation.

Response Times
Under the UK GDPR, SARs should be dealt with within **one month of receipt,** unless the request is an unusually large or complex request. If this is the case, communication should be made to the individual to explain the delay. Street Storage can refuse excessive SARs if the organisation informs the person requesting that they have the right to supervisory authority and judicial remedy within a month.

Reporting Financial Data
Most reports should be anonymised, including payroll expenditure reporting. Street Storage limits the amount of people able to write financial reports which may include identifiable factors to the following people:

- The Bookkeeper
- The Director
- The Fundraiser

Reporting Beneficiary Data

If beneficiary data is reported, it must be anonymised or pseudonymised to prevent identification of the subject, unless prior consent is received. This means the production of reports should be carefully monitored and should only be undertaken by key members of the organisation.

Disposal of Beneficiary Data

As with all other types of data, disposal of beneficiary data should be in line with policy framework and monitored to ensure against poor practice. There is no legal time limit required to keep beneficiary data so Street Storage has deemed it necessary to keep data for up to two years after a beneficiary leaves the service. This is due to potential re-storing and the need for comparative yearly statistics and impact monitoring.

Data Sharing

Street Storage may share personal data with third parties. If these are other Data Controllers, then it will need a lawful basis to do so and should keep a record of all parties it shares personal data with:

- The processing is necessary: in relation to a contract which the individual has entered into; or because the individual has asked for something to be done so they can enter into a contract.
- The processing is necessary because of a legal obligation that applies to you (except an obligation imposed by a contract).
- The processing is necessary to protect the individual's "vital interests". This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident or to a GP service if contact is presenting as suicidal.
- The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions.

Understanding Data as an Employer

Employers also typically do not rely on consent to process employee data – because of the imbalance in power in the employment relationship, consent is not considered freely given – so this should not be included in any employment contract. Street Storage also has to provide to employees privacy information (this will be like the website privacy policy, but instead explaining how employee personal data is processed). This form should explain:

- Who Street Storage are
- The purpose for which data will be processed
- A consent statement if information will be sent by email or text message
- Information on who Street Storage may disclose information to
- Details of the Data Protection Officer
- Basis on which charity will rely to process data
- If data transferred outside of the United Kingdom
- How long the data will be retained
- Individuals' rights of access
- Detail of how the individual can complain

Street Storage

What Street Storage Must Do With Volunteer and Employee Data

Data must be stored safely for as long as it is required, but no longer. In a similar way to beneficiary data there is no legal time limit for this as stated by UK GDPR Regulations so Street Storage has deemed it necessary to keep data for the below time periods:

- Employees of Street Storage's data is kept for six years post exit. This is for tax, insurance, tribunal and financial reasons.
- Volunteer data will be kept for two years after their time volunteering has ended.
- For volunteer NDAs the norm is a valid period of two years.
- For interviewees who were not hired, the data retention time is six months.

Regulators

The UK data protection regulator is the Information Commissioner's Office (ICO).