

Data Protection Policy

This data protection policy ensures Paul Bragman Community and Economic Regen:

- Complies with data protection law and follow good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

In undertaking our work with communities Paul Bragman Community and Economic Regen needs to gather and use certain information about individuals.

These can include community members, clients, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law.

Policy statement

Paul Bragman Community and Economic Regen is committed to a policy of protecting the rights and privacy of individuals, voluntary and community group members, volunteers staff and others in accordance with The Data Protection Act 1998 and the General Data Protection Regulation 2018 (GDPR). Any breach of legislation or the Data Protection Policy is considered to be an offence and in that event, disciplinary procedures apply.

As a matter of good practice, other organisations and individuals working with the organisation, and who have access to personal information, will be expected to have read and comply with this policy. It is expected that any staff, or associates, who deal with external organisations will take responsibility for ensuring that such organisations sign a contract agreeing to abide by this policy where they have access to data we have collected.

Legal Requirements

Data are protected by the Data Protection Act 1998, which came into effect on 1 March 2000. Its purpose is to protect the rights and privacy of individuals and to ensure that personal data are not processed without their knowledge, and, wherever possible, is processed without their consent.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

Purpose of data held by Paul Bragman Community and Economic Regen

Data may be held by us for the following purposes:

1. Staff Administration
2. Accounts & Records
3. Evaluations
4. Research
5. Working with Volunteers

6. Community development programmes
7. Advertising, Marketing & Public Relations
8. Information and Databank Administration
9. Journalism and Media

Data Protection Principles

In terms of the GDPR, we are the 'data controller', and as such determine the purpose for which, and the manner in which, any personal data are, or are to be, processed. We must ensure that we have:

1. Fairly and lawfully processed personal data

will always state our intentions on processing the data and state if, and to whom, we intend to give the personal data. Also provide an indication of the duration the data will be kept.

2. Processed for limited purpose

We will not use data for a purpose other than those agreed by data subjects. If the data held by us are requested by external organisations for any reason, this will only be passed if data subjects agree. Also external organisations must state the purpose of processing, agree not to copy the data for further use and sign a contract agreeing to abide by the GDPR and Paul Bragman Community and Economic Regen Data Protection Policy.

3. Adequate, relevant and not excessive

Paul Bragman Community and Economic Regen will monitor the data held for our purposes, ensuring we hold neither too much nor too little data in respect of the individuals about whom the data are held. If data given or obtained are excessive for such purpose, they will be immediately deleted or destroyed.

4. Accurate and up-to-date

We will ensure that all who give Paul Bragman Community and Economic Regen their data are able to access this to see what information is held and amend this if needed. All amendments will be made immediately and data no longer required will be deleted or destroyed. It is the responsibility of individuals and organisations to ensure the data held by us are accurate and up-to-date. To support this data will be held in as few places as necessary and staff should not create any unnecessary additional data sets.

5. Not kept longer than necessary

We discourage the retention of data for longer than it is required.

6. Processed in accordance with the individual's rights

All individuals that Paul Bragman Community and Economic Regen hold data on have the right to:

- Be informed upon the request of all the information held about them within 40 days.
- Prevent the processing of their data for the purpose of direct marketing.

- Compensation if they can show that they have been caused damage by any contravention of the Act.
- The removal and correction of any inaccurate data about them.

7. **Secure**

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of data.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media, these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All Paul Bragman Community and Economic Regen computers have a log in system

- Our Contact Database is password protected, which allow only authorised staff to access personal data.
- When staff members are using the laptop computers out of the office care should always be taken to ensure that personal data on screen is not visible to strangers.