

Better Purpose Data Protection Policy

1. Policy Statement

All individuals have rights in relation to how their personal information is handled. During the course of our business we will collect, store and process personal information and we recognise the need to treat it in an appropriate and lawful manner.

The types of information we may be required to handle include details of current, past and prospective directors and employees; contractors; suppliers; clients; and others we communicate with. The information is subject to certain legal safeguards primarily those which are specified in the Data Protection Act 2018 (*the Act*) and other regulations including the UK GDPR. The Act imposes restrictions on how we may use that information.

This policy together with our privacy policy sets out our policy on data protection. We will continue to monitor and review the effectiveness of the policy. Anyone who handles personal data in any way on behalf of the company must ensure that they comply with this policy. Any breach of this policy will be taken seriously and may result in disciplinary action or more serious sanctions.

2. Data Protection Officer

Alice Cornish (Director) is the company's Data Protection Officer and is responsible for ensuring compliance with the Act and with this policy.

3. Definitions

Data is information which is stored electronically or in certain paper-based filing systems.

Data subjects for the purpose of this policy include all living individuals about whom we hold personal data. All data subjects have legal rights in relation to their personal data.

Personal data means data relating to a living individual who can be identified from that data, alone or when it is combined with data in our possession. Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).

Data controllers determine the purposes for which and the manner in which any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. Better Purpose Ltd is the data controller of all personal data used in our business.

Data users include directors and employees (including contractors) whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection policy at all times.

Data processors include anyone who processes personal data on behalf of a data controller. This could include suppliers who handle personal data on our behalf such as outsourced providers of finance services.

Processing is any activity that involves use of personal data. It includes obtaining, recording or holding the data or carrying out any operation on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Sensitive personal data includes information about a person's racial or ethnic origins; political opinions; religious or similar beliefs; trade union memberships; physical or mental health; sex life or orientation; or criminal charges or records (including any allegation that they have committed an offence). Sensitive personal data can only be

processed under strict conditions and will usually require the express consent of the person concerned. Purely financial data does not fall within the definition of sensitive personal data, but particular care should be taken when processing such data as any breach relating to it will be treated very seriously.

4. Data Protection Principles

Anyone processing personal data must comply with the eight data protection principles which are set out in the Act. These provide that personal data must be:

1. Processed fairly and lawfully;
2. Processed for purposes which the individual has been told about, and not in a way that is incompatible with those purposes;
3. Adequate, relevant and not excessive in relation to those purposes;
4. Accurate and up-to-date;
5. Not kept longer than necessary;
6. Processed in line with data subjects' rights; S
7. Secure; and,
8. Not transferred to people or organisations situated in countries outside the European Economic Area (EEA) without adequate data protection.

Better Purpose Ltd is committed to complying with these principles.

5. Processing of Data

The Act is not intended to prevent the processing of personal data but to ensure that it is done fairly.

The data subject must be told who the data controller is (i.e. Better Purpose Ltd), the purpose for which the data is to be processed by us (e.g. for employees, to facilitate their employment or to provide updates), and the identities of anyone to whom the data may be disclosed or transferred.

For personal data to be processed lawfully, one of a number of conditions has to be met. One such condition is that the data subject has consented to the processing. An alternative condition is that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed provided it is not unwarranted because of its prejudicial effect on the rights and freedoms, or legitimate interests, of the individual.

We should not collect personal data for one purpose and then use it for another incompatible purpose. If it becomes necessary to process a person's information for a new purpose, that individual should be informed of the new purpose beforehand. For example, if we collect a contact email address in order to provide an individual with updates it should not then be used for a new purpose such as to share it with other organisations for marketing purposes, without first getting the individual's consent.

6. Accuracy of Data

Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps will therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals thereafter. Inaccurate or out of date data will not be retained.

Better Purpose Ltd maintains an employee database detailing all the information we need to know about our employees (including contractors and consultants). You must ensure that you notify us of any change to your circumstances so that this information is kept up to date.

7. Retention of Data

Personal data that we hold should be destroyed or erased from our systems when it is no longer needed. For guidance on how long particular types of personal data should be kept before being destroyed or erased, please contact the Directors of Better Purpose Ltd or seek legal advice.

8. Data Subjects' Rights

Data must be processed in line with data subjects' rights. Data subjects have a right to (amongst other things): request a copy of any data held about them and a description of the type of information we are processing, the uses made of their data and details of anyone to whom their data has been disclosed; prevent the processing of their data for direct marketing purposes; ask to have inaccurate data amended; and prevent processing that is likely to cause damage or distress to themselves or anyone else.

9. Data Security

We will ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data and against the accidental loss of or damage to personal data.

The Act requires us to put in place procedures to maintain the security of all personal data. Personal data will only be transferred to a third-party data processor if that processor contractually agrees to comply with those procedures.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of personal data. Our security procedures include entry controls; secure lockable desks and cupboards; secure methods of disposal; and IT security including the use of passwords and logging off when away from the desk. Particular care must be taken with security when homeworking.

When we are dealing with sensitive personal data, more rigorous security measures are likely to be needed, for instance, if sensitive personal data is held on a memory stick or other portable device it should always be encrypted.

10. Marketing materials

Email and SMS marketing must only be sent to individuals who have given their consent. This includes newsletters and other information promoting our work. Consent is not mandatory for marketing sent by post, but it is good practice to obtain it.

11. Subject Access Requests

A formal request from a data subject for information held about them must be made in writing to the Data Protection Officer with evidence of the identity of the data subject. A fee of £10 is payable for provision of this information. Any subject access requests will be dealt with in accordance with the statutory time limit.

Last updated: 13 January 2023

Next review date: 13 January 2024