STC Payroll Giving Ltd
Data Protection Policy

Introduction

The directors and staff of StC Payroll Giving Ltd understand the data security needs and expectations of its interested parties both within the organisation and from external parties including, amongst others, clients, suppliers, regulatory and governmental departments. The company has recognised that the disciplines of confidentiality, integrity and availability of information in data security management are integral parts of its management function and views these as their primary responsibility and fundamental to best business practice. We ensure that the company:

Complies to all applicable laws and regulations and contractual obligations
Implements data security objectives that consider data security requirements following the results of applicable risk assessments
Communicates these objectives and performance against them, to all interested parties
Adopts a data security management system comprising a security manual and procedures which provides direction and guidance on data security matters relating to employees, customers, suppliers and other interested parties who come into contact with its work
Works closely with customers, business partners and suppliers in seeking to establish appropriate data security standards
Adopts a forward-thinking approach on future business decisions, including the continual review of risk evaluation criteria, which may impact on data security
Instructs all members of staff in the needs and responsibilities of data security management
Constantly strives to meet and, where possible, exceed its customer's expectations
Implements continual improvement initiatives, including risk assessment and risk treatment strategies, while making best use of its management resources to better meet data security requirements

Responsibility for upholding this policy is truly company-wide under the authority of the directors who encourage the personal commitment of all staff to address data security as part of their skills. The purpose of this policy is to demonstrate our commitment to the Data Protection Act 1998 (the DPA), the Data Protection Directive (95/46/EC)l the Electronic Communications Data Protection Directive (2002/58/EC), the Privacy and Electronic Communications (EC Directive) Regulations 2003 (Sl 2426/2003) (as amended) and General Data Protection Regulation (GDPR) and all applicable laws and regulations relating to the processing of the Personal Data and privacy, including where applicable the guidance and codes of practice issued by the Information Commissioner or any other national data protection authority, and the equivalent of any of the foregoing in any relevant jurisdiction. We ensure that the 5 principles of GDPR are followed to the letter and that data is:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) 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;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) 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;

e) 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; and

f) 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.

Background

StC is a professional fundraising organisation specialising in Payroll Giving Fundraising. Payroll Giving is a way of giving money to charity without paying tax on it. I It must be paid through the donor's employer's PAYE or from a pension (see the Taxes Act 1988, s.2020 and SI no 2211/1986 the Charitable Deductions (Approved Schemes) Regulations and SI no 759/2000 the Charitable Deductions (Approved Schemes) (Amendment) Regulations 2000).

1. Policy Statement

1.1 Everyone has rights with regard to the way in which their personal data in handled. During the course of our activities we will collect, store and process personal data about charity donors, our customers, suppliers and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

1.2 Data users are obliged to comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary action.

2. About this policy

2.1 The types of personal data that we may be required to handle include information about charity donors, current, past and prospective suppliers, customers, employers and others that we communicate with. The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Act and equivalent EU regulations.

2.2 This policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

2.3 This policy may be amended at any time and posted on our website www.stcpayrollgiving.co.uk

2.4 This policy sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

2.5 Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to Helen Von Trotsenburg, hvont@stcpayrollgiving.co.uk

3. Definition of data security terms

3.1 **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems.

3.2 **Data subjects** for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

3.3 **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

3.4 **Data controllers** are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Act. We are the data controller of all personal data used in our business for our own commercial purposes.

3.5 **Data users** are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.
3.**6 Data processors** include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on our behalf.

3.7 **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties
.
3.8 **Sensitive personal data** includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

4. Fair and Lawful Processing

5.1 The Act is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

5.2 For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in the Act. These include, among other things, the data subject's consent to the processing, or that the processing is necessary for the performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, additional conditions must be met. When processing personal data as data controllers in the course of our business, we will ensure that those requirements are met.

5. Processing for Limited Purposes

6.1 In the course of processing the Payroll Giving Scheme, we collect and process personal data. This may include data we receive directly from the data subject (for example, by their completing forms or from their communications with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, their employers, the charity partners, sub-contractors in technical, payment and delivery services and others).

6.2 We will only process personal data for the specific purposes disclosed to the data subject, for which activities we will have their express consent, or for any other purposes specifically permitted by the Act. We will disclose those purposes to each data subject when we first collect the data or as soon as possible thereafter.

6.3 There may be times when making the data anonymous (where the recipient will not be able to associate information about your donation with your identity) will be more appropriate, or possible (at their request), and we will take all reasonable steps to ensure that this is done.

6. Notifying Data Subjects

7.1 If we collect personal data directly from data subjects, we will inform them about: (a) The purpose or purposes for which we intend to process that personal data. (b) The types of third parties, if any, with which we will share or to which we will disclose that personal data. (c) The means, if any, with which data subjects can limit our use and disclosure of their personal data.

7.2 If we receive personal data about a data subject from other sources, we will provide the data subject with this information as soon as possible thereafter.

7.3 We take every reasonable measure to ensure that you are not mislead about the collection and use of personal data and that no pressure or improper inducements are applied to or offered to data subjects when collecting data.

7.4 We will also inform data subjects whose personal data we process that we are the data controller with regard to that data and how to contact us.

7.5 Any breach of our policy or other loss or disclosure of personal data will be reported to the Information Commissioner and to data subjects as soon as reasonably practical after discovery of the incident.

7. Adequate, Relevant and Non-Excessive Processing

We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject. This means that your data will only be used to ensure and enable your donation to reach your chosen charities. Data will be passed to the appropriate government registered agencies (with whom their employers have contracted) to enable the donations to reach the chosen charities and for those charities to process the donation. This processing ensures that the payment achieves the criteria for Payroll Giving.

8. Accurate Data

We will only collect and process sufficient information to enable the Payroll Giving process to be achieved. We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

9. Timely Processing

We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data that is no longer required or at the latest 7 years from collection. We use one of the UK's leading data destruction service suppliers.

10. Processing in Line With Data Subject's Rights

11.1 We will process all personal data in line with data subjects' rights, in particular their right to:
(a) Request access to any data held about them by a data controller (see also clause 15).
(b) Prevent the processing of their data for direct-marketing purposes.
(c) Ask to have inaccurate data amended (see also clause 9).
(d) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

11. Data Security

12.1 We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

12.2 We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processing company if they are approved by us and agree to comply with these procedures and policies, or if they put in place adequate security measures.

12.3 We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:
(a) Confidentiality means that only people who are authorised to use the data can access it; our employees have robust confidentiality obligations in their contracts of employment.
(b) Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.
(c) Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our, or our approved supplier's, central computer system instead of individual PCs.

12.4 Security procedures include:
(a) Employee controls. All of our employees and the employees of any subcontractors who process data on our behalf are obliged to comply with our strict data security procedures.
(b) Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
(c) Methods of disposal. Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.
(d) Equipment. Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.
(e) Training, our employees are regularly updated in privacy procedures.

12.5 We monitor and take all reasonable steps to prevent malicious internet attacks, such as hacking or a distributed denial of service attack.

12. Transferring Personal Data to A Country Outside The EEA

13.1 We may transfer any personal data we hold to a country outside the European Economic Area ("EEA"), provided that one of the following conditions applies:
(a) The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms.
(b) The data subject has given his consent.
(c) The transfer is necessary for one of the reasons set out in the Act, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.
(d) The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.
(e) The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

13. Disclosure and Sharing of Personal Information

13.1. We may share personal data we hold with third parties, subject to the data subjects consent, or any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries, as defined in section 1159 of the UK Companies Act 2006.

13.2. We may also disclose personal data we hold to third parties: (a) In the event that we sell or buy any business or assets, in which case we may disclose personal data we hold to the prospective seller or buyer of such business or assets. (b) If we or substantially all of our assets are acquired by a third party, in which case personal data we hold will be one of the transferred assets.

If we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

14.4 We may also share personal data we hold with our data processing company Bell Donor Management Ltd (BDM). We have a written agreement in place with this supplier, which obliges them to meet rigorous international standards of data privacy. BDM have been accredited ISO 27001:2013 by an independent auditor.

14. Dealing with Subject Access Requests

1. Data subjects must make a formal request for information we hold about them. This must be made in writing.
2. When receiving telephone inquiries, we will only disclose personal data we hold on our systems if the following conditions are met: (a) We will check the caller's identity to make sure that information is only given to a person who is entitled to it. (b) We will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.
3. Our employees will refer a request to their line manager for assistance in difficult situations. Employees should not be bullied into disclosing personal information.

4. Changes to this Policy

We reserve the right to change this policy at any time. Where appropriate, we will notify data subjects of those changes by mail or email.