

## **STC PAYROLL GIVING EMPLOYER PRIVACY NOTICE**

**Data controller: StC Payroll Giving**, Unit 97C+D, Harvey Drive, John Wilson Estate, Whitstable, Kent, CT5 3QZ

**Data Protection Officer:** Alice Wright  
t: 01227 376993  
e: [compliance@stcpayrollgiving.co.uk](mailto:compliance@stcpayrollgiving.co.uk)

### **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) the Electronic Communications Data Protection Directive (2002/58/EC), the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 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.

### **Information that StC Payroll Giving collects**

StC Payroll Giving collects and processes a range of information about your employees. It collects:

- Their name and address
- Other contact details, including their email address and telephone number
- Date of birth
- Their charity(s) of choice and the amounts of their chosen donation(s)
- The identity of their employer, their National insurance number, payroll details and chosen HMRC registered Payroll Giving Agent (PGA)

StC Payroll Giving collects this personal data in a variety of ways. Personal data may be collected from employees via:

- Giving forms completed by employees or on their behalf
- Online forms completed by employees
- Your flexible benefits or other portals (if you have them)

Their personal data will be stored securely within StC Payroll Giving's donor systems and in other IT systems, predominantly using Citrix Sharefile for any data transfers.

### **Why does StC Payroll Giving process personal data?**

StC Payroll Giving processes their personal data in line with our "legitimate interests" in ensuring that all of your employees' charitable giving wishes and instructions are respected and fulfilled.

In order for their donation to be processed, StC Payroll Giving must always share their name, address, employee and/or national insurance number, choice of charity(s) and donation amount with your Payroll Department and with the chosen HMRC registered Payroll Giving Agent (PGA). You have a contract with the PGA, who is in turn responsible for passing the money that employees donate to their chosen charity(s). If you have an existing relationship with a different named organisation (e.g. a payroll provider or flexible benefits provider), we may need to share their details with that organisation in order to process their donation in accordance with their wishes.

We must also always pass their name, address, employer details, charity choice and donation amount to their chosen charity(s) so that they can match their actual financial donation with the personal data about employees, which we supply to them. Unless employees have given us their consent, we will inform their chosen charity(s) that employees have not consented to their personal data being used for secondary marketing or other donation solicitation purposes. If employees have given us their consent to share their personal data with their chosen charity(s) for secondary marketing or other donation solicitation purposes, we will do so but only to the extent that employees have given consent for this to happen.

### **Who has access to data?**

Their personal data may be shared internally by employees and officers of StC Payroll Giving, if access to that information is necessary for the proper performance of their roles.

Their personal data will always be shared with you (and, where appropriate, your payroll provider and/or flexible benefits provider), and the relevant PGA; but only to the extent necessary to facilitate the making of their charitable donations in accordance with their wishes; or, where appropriate, to facilitate reimbursement credits from StC Payroll Giving to their chosen charity(s). We always share their personal data with chosen charity(s) for the purposes of ensuring the matching of their details with the income that their chosen charity(s) receives through the relevant PGA; but only to the extent required to achieve that purpose.

We may share address, telephone and email contact information with their chosen charity(s) who may use it for secondary marketing or donation solicitation purposes; but only to the limited extent that employees have consented to the sharing of their personal data for that purpose.

### **How does StC Payroll Giving protect data?**

StC Payroll Giving takes the security of their data seriously. StC Payroll Giving has internal policies and controls in place to minimise the risk of their personal data being lost, accidentally destroyed, misused or disclosed, and is not accessed or shared except a) by its officers or employees in the performance of their duties; or b) as otherwise explained in this privacy notice.

Where StC Payroll Giving engages third parties to process personal data on its behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

### **For how long does StC Payroll Giving keep data?**

StC Payroll Giving holds their personal data for 3 years in order to address administrative queries from their employer or chosen charity(s).

### **Their rights**

As a data subject, employees have a number of rights. Employees can:

- Access and obtain a copy of their data on request
- Require StC Payroll Giving to change incorrect or incomplete data
- Require StC Payroll Giving to delete or stop processing their data, for example where the data is no longer necessary for the purposes of processing
- Object to the processing of their data where StC Payroll Giving is relying on its legitimate interests as the legal ground for processing

If employees would like to exercise any of these rights, they should contact our Data Protection Officer (contact details as above).

If employees believe that StC Payroll Giving has not complied with their data protection rights, employees have the right to complain to the Information Commissioner's Office.

**Automated Decision-Making**

StC Payroll Giving does not use their personal data for automated decision-making.

Issue Date: 19th February 2018