Recorra Ltd – DATA PROTECTION POLICY

Introduction
We receive, use and store personal information about our customers, business partners and employees. This personal information is handled and dealt with properly, however it is collected, recorded, and used, whether it's on paper, in computer records or recorded by any other means.

We regard the lawful and correct treatment of personal information as very important to our successful operation and to maintaining confidence between us and those with whom we carry out business.

We will ensure that we treat personal information lawfully and correctly. To this end we fully endorse and adhere to the principles of the General Data Protection Regulation (GDPR).

This policy applies to the processing of personal data in paper based and electronic records kept by us in connection with:

a) our human resources function
b) the provision of our recycling/data destruction/office supplies service
c) communication with our customers, business partners and suppliers
d) achieving our business goals

It also covers our response to any data breach and other rights under the GDPR.

This policy applies to the personal data of our customers, suppliers, job applicants, existing and former employees, apprentices, workers and self-employed contractors. These are referred to in this policy as relevant individuals.

Definitions

Personal data is information that relates to a living individual who can be identified directly or indirectly from that information, for example, a person's name, identification number, location or online identifier. It can also include pseudonymised data.

Special categories of personal data is sensitive personal data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes). It can also include data about criminal offences or convictions. Sensitive personal data can only be processed under strict conditions, including with the consent of the individual.

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

Data Protection Principles

Under the GDPR, all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:

a) processing will be fair, lawful and transparent

b) data be collected for specific, explicit, and legitimate purposes
c) data collected will be adequate, relevant and limited to what is necessary for the purposes of processing
d) data will be kept accurate and up to date. Data which is found to be inaccurate will be rectified or erased without delay
e) data is not kept for longer than is necessary for its given purpose
f) data will be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
g) data will not be transferred to people or organisations situated in countries without adequate protection and without firstly having advised the individual

Fair and Lawful Processing

We acknowledge that processing of personal data may only be carried out where a lawful basis for that processing exists and we have assigned a lawful basis against each processing activity.

The lawful bases include (amongst others): whether the individual has given their consent, the processing is necessary for performing a contract, for compliance with a legal obligation, or for the legitimate interest of the business. When sensitive personal data is being processed, additional conditions must be met.

Where consent is given, we understand that it must be freely given, specific, informed and unambiguous. Where consent is to be sought, we will do so on a specific and individual basis where appropriate.

Notifying Individuals

If we collect personal data directly from an individual, we will inform them about:

a) the purpose or purposes for which we intend to process that personal data, as well as the legal basis for the processing
b) where we rely upon the legitimate interests of the business to process personal data, the legitimate interests pursued
c) the types of third parties, if any, with which we will share or disclose that personal data
d) the fact that the business intends to transfer personal data to a non-EEA country or international organisation and the appropriate and suitable safeguards in place
e) how individuals can limit our use and disclosure of their personal data
f) information about the period that their information will be stored or the criteria used to determine that period
g) their right to request from us as the controller access to and rectification or erasure of personal data or restriction of processing
h) their right to object to processing and their right to data portability
i) their right to withdraw their consent at any time (if consent was given) without affecting the lawfulness of the processing before the consent was withdrawn
j) the right to lodge a complaint with the Information Commissioners Office
k) other sources where personal data regarding the individual originated from and whether it came from publicly accessible sources
l) whether the provision of the personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the individual is obliged to provide the personal data and any consequences of failure to provide the data

m) the existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the individual

If we receive personal data about an individual from other sources, we will provide them with this information as soon as possible (in addition to telling them about the categories of personal data concerned) but at the latest within one month.

We will also inform individuals whose personal data we process that we are the data controller with regard to that data, our contact details and the name of the member of staff responsible for compliance in respect of our Data Protection Activities.

Types of Data Held

In carrying out our business activities, we may collect and process data from our clients, business partners and suppliers for the legitimate purpose of providing a recycling/data destruction/ office supplies service, or to provide relevant information about the benefits of our services and waste, recycling and sustainability.

Personal data collected from our clients, business partners and suppliers is limited to the following:

a) contact name
b) work email address
c) work phone number
d) job title

In addition, we keep several categories of personal data on our employees in order to carry out effective and efficient HR processes. For example:

a) personal details such as name, address, phone numbers
b) information gathered via the recruitment process
c) details relating to pay
d) medical or health information
e) information relating to employment with us, including:

    i) job title and job descriptions
    ii) salary
    iii) terms and conditions of employment
    iv) details of formal and informal proceedings, annual leave records and performance information
    v) training undertaken

All of the above information is required for our processing activities.

Rights of Individuals

All personal data will be processed in line with the individual's rights. These are:

a) the right to be informed about the data we hold about them and what we do with it
b) the right of access to the data we hold. More information on this can be found in the section headed "Access to Data" below
c) the right for any inaccuracies in the data we hold about them, however they come to light, to be corrected. This is also known as 'rectification'

d) the right to have data deleted in certain circumstances. This is also known as 'erasure'
e) the right to restrict the processing of the data
f) the right to transfer the data we hold about them to another party. This is also known as 'portability'
    i. the right to object to the inclusion of any information
    ii. the right to regulate any automated decision-making and profiling of personal data

Responsibilities

In order to protect the personal data of relevant individuals, those within our business who must process data as part of their role have been made aware of our policies on data protection.

We have also appointed employees with responsibility for reviewing and auditing our data protection systems.

Access to Data

As stated above, individuals have a right to access the personal data that we hold on them. To exercise this right, individuals should make a **Subject Access Request**. We will comply with the request without delay, and within one month unless, in accordance with legislation, we decide that an extension is required. Those who make a request will be kept fully informed of any decision to extend the time limit.

No charge will be made for complying with a request unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the individual making the request. In these circumstances, a reasonable charge will be applied.

When receiving telephone enquiries about a Subject Access Request, 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

Disclosure and Sharing of Personal Data

We may share personal data we hold with other Recorra companies (this means our subsidiaries, as defined in section 1159 of the UK Companies Act 2006). In addition, we may be required to disclose certain data/information to any person. The circumstances leading to such disclosures include:

a. providing customer contact details to sub-contractors in order to perform the service
b. any employee benefits operated by third parties
c. disabled individuals - whether any reasonable adjustments are required to assist them at work
d. individuals' health data - to comply with health and safety or occupational health obligations towards the employee
e. for Statutory Sick Pay purposes

f. HR management and administration - to consider how an individual's health affects his or her ability to do their job
g. the smooth operation of any employee insurance policies or pension plans
h. to assist law enforcement or a relevant authority to prevent or detect crime or prosecute offenders or to assess or collect any tax or duty

These kinds of disclosures will only be made when strictly necessary for the purpose.

Data Security

We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental or unlawful destruction, damage, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.

We will maintain data security by protecting the confidentiality, integrity and availability of personal data and will put in place procedures and technologies to maintain the security of all personal data from the point of the determination of the means for processing and point of data collection to the point of destruction. Employees are trained to follow the Company's rules on data security.

All our employees are aware that hard copy personal information should be kept in a locked filing cabinet, drawer, or safe.

Employees are aware of their roles and responsibilities when their role involves the processing of data. All employees are instructed to store files or written information of a confidential nature in a secure manner so that are only accessed by people who have a need and a right to access them and to ensure that screen locks are implemented on all PCs, laptops etc when unattended. No files or written information of a confidential nature are to be left where they can be read by unauthorised people.

Where data is computerised, it should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

Employees must always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them.

Personal data should not be kept or transported on laptops, USB sticks, or similar devices, unless prior authorisation has been received. Where personal data is recorded on any such device it should be protected by:

a) ensuring that data is recorded on such devices only where absolutely necessary.
b) using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted.
c) ensuring that laptops or USB drives are not left where they can be stolen.

Third Party Processing

Where we engage third parties to process data on our behalf, we will ensure, via a data processing agreement with the third party, that the third party takes such measures in order to maintain the Company's commitment to protecting data.

International Data Transfers

The Company does not transfer personal data to any recipients outside of the EEA.

Requirement to Notify Breaches

All data breaches will be recorded on our Data Breach Register. Where legally required, we will report a breach to the Information Commissioner within 72 hours of discovery. In addition, where legally required, we will inform the individual whose data was subject to breach.

More information on breach notification is available in the Company's Breach Notification policy.

Training

All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.

The nominated data controller/auditors/staff responsible for data protection compliance for the Company are trained appropriately in their roles under the GDPR.

All employees who need to use the Company's computer systems are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and the Company of any potential lapses and breaches of the Company's policies and procedures.

Records

The Company keeps records of its processing activities including the purpose for the processing and retention periods in its Data Register. The Register will be kept up to date so that it reflects current processing activities.

Data Protection Compliance

Our appointed compliance officer in respect of our data protection activities is:

Lyndsay Edwards – **Compliance Director**

Telephone – 020 7407 9100
Email – Lyndsay.edwards@recorra.co.uk
Address – 52 Lant Street, London, SE1 1RB

This policy will be reviewed on an annual basis.

Signed:  Date: 01/04/2024

MANAGING DIRECTOR

Recorra includes Recorra Ltd and its subsidiaries. Recorra was formerly known as BPR Group which included Paper Round, Secure Paper, Brighton Paper Round Ltd and Reef Environmental Solutions Ltd.