



# Ribbex UK Ltd General Data Protection Policy

## Context and overview

<b>System Document Ref:</b>	55
<b>Title:</b>	Data Protection Policy
<b>Revision:</b>	2
<b>Date</b>	July 2018

### Introduction

Ribbex UK Ltd needs to gather and use certain information about individuals, known as 'data'. These can include information from customers, 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 policy standards and to comply with the law.

### Why this policy exists

This data protection policy exists to ensure that Ribbex UK Ltd:

- Complies with the Data Protection Act 2018 (DPA 2018), which incorporates the General Data Protection Regulations 2018 (GDPR 2018) and follows good practice
- Protects the rights and information of staff, customers and all other stakeholders
- Is open about how it stores and processes individuals' or company's data
- Protects itself from the risks of a data breach

### Data Protection Law

The Data Protection Act 2018 and the General Data Protection Regulations 2018, describe how organisations such as Ribbex, must collect, handle, store and protect personal data and information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials or formats. To comply with the regulations, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The DPA and GDPR are underpinned by important principles for compliance. These require Ribbex to be accountable for managing data held, to honour the rights of those with whom we hold data about and to comply with the law.



### Accountability

Principally that we should identify;

- What data we hold about individuals or organisations
- Why we are holding data
- How we obtained the data
- Why it was initially gathered
- How long we will retain it
- How secure we believe our storage methods are
- How or if we share data with 3<sup>rd</sup> parties

### Personal Privacy Rights

Principally that individuals or organisations have the right to;

- Be informed of any data held
- Have any errors rectified
- Have part or all of the data erased
- Restrict data processing
- Data portability
- Object about any data held
- Have access to any data held

### Lawful Grounds for Processing Data

Ribbex has a duty to comply with the law and certain rights to access & process data.

Principally that Ribbex has a duty or right to;

- Comply with the law
- Process or use data if there is a vital interest
- For the purpose of a public task
- Has a contract with an individual
- Access data for a legitimate interest

Complete Waste Management Solutions

Ribbex (UK) Limited. Registered in England No. 1852357. VAT Reg No. 396 6426 07.  
Registered office: 34 Burrowfields, Welwyn Garden City, Hertfordshire AL7 4SR  
T: 01707 375 891 | E: customerservices@ribbex.co.uk | www.ribbex.co.uk

# People, Risks and Responsibilities Policy scope

## This policy applies to:

- The head office of Ribbex UK Ltd
- All branches of Ribbex UK Ltd
- All staff, volunteers, contactors, sub contactors, consultants and 3<sup>rd</sup> parties working for or on behalf of Ribbex UK Ltd

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside the scope of DPA and/or GDPR. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- ...plus any other information relating to individuals

## Data protection risks

This policy helps to protect Ribbex UK Ltd from some very real data security risks, including:

- Breaches of confidentiality, for instance, information being given out inappropriately.
- Failing to offer choice, for instance, all individuals should be free to choose how the company uses data relating to them.
- Reputational damage, for instance, the company could suffer if hackers successfully gained access to sensitive data.

## Responsibilities

Everyone who works for, with or on behalf of Ribbex UK Ltd has a responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The board of directors is ultimately responsible for ensuring that Ribbex UK Ltd meets its legal obligations.
- The data protection officer, Alasdair Coulson, is responsible for:
  - › Keeping the board updated about data protection responsibilities, risks and issues.
  - › Reviewing all data protection procedures and related policies, in line with an agreed schedule.
  - › Arranging data protection training and advice for the people covered by this policy.
  - › Handling data protection questions from staff and anyone else covered by this policy.
  - › Dealing with requests from individuals to see the data Ribbex UK Ltd holds about them (also called 'subject access requests').
  - › Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- The IT manager, CSUK LTD, is responsible for:
  - › Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
  - › Performing regular checks and scans to ensure security hardware and software is functioning properly.
  - › Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

- The Commercial Director, Dave Tyson, is responsible for:
  - › Approving any data protection statements attached to communications such as emails and letters.
  - › Addressing any data protection queries from journalists or media outlets like newspapers.
  - › Where necessary, working with other staff to ensure marketing initiatives abide by the DPA and /or the GDPR principles.

## General staff guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- Ribbex UK Ltd will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

## Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data controller.

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 or destroyed by secure means.
- 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 (like a CD or DVD), 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 servers and computers containing data should be protected by approved security software and a firewall.



## Data use

Personal data is of no value to Ribbex UK Ltd unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorised external contacts.
- Personal data should never be transferred outside of the European Economic Area.
- Employees should not save copies of personal data to their own computers.
- Always access and update the central copy of any data.

## Data accuracy

The law requires Ribbex UK Ltd to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Ribbex UK Ltd should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- Ribbex UK Ltd will make it easy for data subjects to update the information Ribbex UK Ltd holds about them. For instance, via the company website.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the marketing manager's responsibility to ensure marketing databases are checked against industry suppression files every six months.

## Subject access requests

All individuals who are the subject of personal data held by Ribbex UK Ltd are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it, amend or delete it, providing it does not conflict with any legal obligations the company has.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its GDPR obligations.

If an individual contacts the company requesting this information, this is called a '*subject access request*'.

Subject access requests from individuals should be made by telephone to Kim McCready, the data controller on 01707 375891, or via email to [Kim@ribbex.co.uk](mailto:Kim@ribbex.co.uk). The data controller can supply a standard request form, although individuals do not have to use this.

Complete Waste Management Solutions

Ribbex (UK) Limited. Registered in England No. 1852357. VAT Reg No. 396 6426 07.  
Registered office: 34 Burrowfields, Welwyn Garden City, Hertfordshire AL7 4SR  
T: 01707 375 891 | E: [customerservices@ribbex.co.uk](mailto:customerservices@ribbex.co.uk) | [www.ribbex.co.uk](http://www.ribbex.co.uk)



The data controller will aim to provide the relevant data within a reasonably practicable time. The data controller will always verify the identity of anyone making a subject access request through a due diligence process before handing over any information.

Although not mandatory for individuals to complete a subject access request form, for auditing and due diligence purposes, Ribbex employees must complete a form for each 'subject access request' made. This should be filed either electronically or on paper in a file pertinent to the data being requested.

## Disclosing data for other reasons

In certain circumstances, DPA & GDPR permits personal data to be disclosed to law enforcement agencies without the consent of the data subject. In such circumstances and were Ribbex are required by law to disclose data, we would do so only to those legitimate enforcement agencies making the request.

Under these circumstances, Ribbex UK Ltd will disclose the requested data. However, the data controller will be required to ensure the request is legitimate, seeking advice and confirmation from the board and the company's legal advisers where necessary.

## Providing information

Ribbex UK Ltd aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To this end, the company has a privacy statement, setting out how data relating to individuals is used by the company. This is an appendices to this document and is also available on the companies website.

Alasdair Coulson, Managing Director

24<sup>th</sup> May 2018

Complete Waste Management Solutions

Ribbex (UK) Limited. Registered in England No. 1852357. VAT Reg No. 396 6426 07.  
Registered office: 34 Burrowfields, Welwyn Garden City, Hertfordshire AL7 4SR  
T: 01707 375 891 | E: customerservices@ribbex.co.uk | www.ribbex.co.uk