Connexin Group Data Protection Policy

Document Reference: CXNPOL 008

Version Number: 2.2

Date Created: 10/01/2022

1 INTRODUCTION

This policy sets out how Connexin Limited and all subsidiaries within the Connexin group of companies ("**we**", "**our**", "**us**", "**Connexin**") handle the Personal Data of our customers, suppliers, employees, workers and other third parties that we have a relationship with or may need to contact.

We adopt safeguards to ensure information about you is kept confidential and is accessed only by authorised personnel and used for proper purposes. This policy describes the principles and standards that Connexin applies when collecting, processing and storing this personal data to meet our obligations under applicable data protection laws.
This policy applies to all personal data we process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users, or any other data subject.
A summary of the capitalised expressions used in this policy can be found in Annex A.

2 PURPOSE OF THE POLICY

Connexin is committed to complying with the UK General Data Protection Regulation and all other data protection and privacy laws in force from time to time which are applicable to Connexin and its business operations ("**Data Protection Laws**"). The purpose of this policy is to provide an overview as to how Connexin intends to achieve compliance with Data Protection Law and to ensure an appropriate and consistent approach to protecting personal data used within Connexin.
Everyone who works for Connexin has a duty to respect the confidentiality and integrity of any information and data that they access and is personally accountable for safeguarding assets in line with this policy. This policy sets out the behaviours that are expected of employees and third parties in relation to the collection, use, retention, transfer, disclosure, and destruction of any personal data.

3 SCOPE OF THE POLICY

This policy applies to all Employees and Third Parties ("**you**", "**your**") with access to personal data used by or for Connexin.

Headquarters: K3 Business Park, 200 Clough Road, Hull, HU5 1SN
Registered Office Address: 9th Floor 107 Cheapside, London, EC2V 6DN
: +44 1482 363738
: www.connexin.co.uk

All employees and third parties have a personal responsibility to comply with the Data Protection Laws and have a duty to familiarise themselves with the relevant policies and procedures to ensure that no individual or corporate breach can occur.

Failure to comply with Data Protection Laws could result in huge fines to Connexin of up to £17.5 million or 4% of the total annual worldwide turnover in the preceding financial year, whichever is higher. In addition, we could face claims from people affected by a breach and significant reputational damage.

Any breach of this policy and/or related policies may result in disciplinary action.

The Head of SHEQ and Compliance is responsible for overseeing this policy.

This policy must be read in conjunction with any other related data and/or security policies, all of which are internal documents and cannot be shared with third parties, clients or regulators without prior authorisation from the Head of SHEQ & Compliance.
We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated before being adopted.
The scope of this policy applies to all personal data of employees, customers and other data subjects created or processed by or for Connexin to deliver services and conduct business, including information received from or exchanged with external partners. The policy includes information held in electronic or hard-copy/paper formats and may also determine what can be communicated verbally to third parties.

Personal Data can take many forms including, but not limited to, the following:

- Hard copy data held on paper,
- Data stored electronically in computer systems and mobile devices (e.g., smart phones).
- Communications sent by physical post or using email,
- Data stored using electronic media such as USB drives, disks and tapes
- Data stored in the cloud (e.g., file sharing sites) and social media.

Headquarters: K3 Business Park, 200 Clough Road, Hull, HU5 1SN
Registered Office Address: 9th Floor 107 Cheapside, London, EC2V 6DN
: +44 1482 363738
: www.connexin.co.uk

4 DATA PROTECTION PRINCIPLES

This policy is underpinned by a number of data protection principles which drive compliance. You must ensure compliance with these principles at all times. These are summarised in the table below.

Principle	Definition
Fairness and transparency	Connexin must tell the customer or employee what we intend to do with their personal data (transparency) and must process that data in accordance with the description given to the customer or employee (fairness) contained within a fair processing notice or privacy policy, and one of the lawful grounds set out in the Data Protection Laws must apply (lawfulness).
Purpose limitation	Connexin must specify exactly what the personal data collected will be used for and limit the processing of that personal data to only what is necessary to meet the specified purpose.
Data minimisation	Connexin must not collect or store any personal data beyond what is strictly required.
Accuracy	Connexin must have in place processes for identifying and addressing out-of-date, incorrect, incomplete, and redundant personal data.
Storage limitation	Connexin must, wherever possible, store personal data in a way that limits or prevents identification of a customer or employee. Personal data should not be retained for longer than necessary in relation to the purposes for which they were collected.
Security, Integrity, and Confidentiality	Connexin must use appropriate technical and organisational measures to ensure the integrity and confidentiality of personal data is maintained at all times.
Transfer limitation	Connexin must not transfer personal data to another country without appropriate safeguards being in place.
Data Subject's Rights and Requests	Connexin must make personal data available to data subjects and data subjects are allowed to exercise certain rights in relation to their personal data.
Accountability	Connexin and all employees are responsible for and must be able to demonstrate compliance with the data protection principles listed above.

Headquarters: K3 Business Park, 200 Clough Road, Hull, HU5 1SN
Registered Office Address: 9th Floor 107 Cheapside, London, EC2V 6DN
: +44 1482 363738
: www.connexin.co.uk

5 ACCOUNTABILITY

Connexin must demonstrate that all of the data protection principles (outlined above) are met for all personal data for which we are responsible. We have implemented measures to reduce the risk of breaching the applicable data protection laws and to demonstrate that we take governance seriously. Connexin has put in place a number of processes to achieve accountability.

These include:

- operation of a data privacy governance structure through the appointment of a Head of SHEQ & Compliance Manager;
- maintaining an inventory of data processing activities;
- implementing appropriate privacy notices;
- obtaining and recording appropriate consents, ensuring consents can be easily withdrawn, and managing consents and marketing preferences (and all Employees must adhere to the rules on Consent when relying on this legal ground to Process Personal Data);
- applying appropriate organisational and technical measures to ensure compliance with the data protection principles;
- carrying out Data Protection Impact Assessments ("**DPIAs**") on any "high risk" processing activity for all new and/or revised systems or processes before it starts including security of how this data is handled and a process implemented to ensure that DPIAs are carried out where required; and
- creating a breach reporting mechanism.

6 DATA PROTECTION TRAINING

All employees will receive training on this policy. New joiners will receive information security and data protection training as part of the induction process. Training for all employees must be refreshed annually or whenever there is a substantial change in the law or our policy and procedures. Training may also be required at more frequent intervals where a data or security breach occurs or if Connexin identifies non-compliances with this policy.

Completion of training is compulsory for all Employees.

Headquarters: K3 Business Park, 200 Clough Road, Hull, HU5 1SN
Registered Office Address: 9th Floor 107 Cheapside, London, EC2V 6DN
: +44 1482 363738
: www.connexin.co.uk

7 DATA PROCESSING

Connexin uses the personal data of employees, customers and other data subjects for the following broad purposes:

- the general running and business administration of Connexin;
- to provide goods and/or services to its customers; and
- the ongoing administration and management of its business and the services provided.

The use of employees, customers and other data subject's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object. For example, it would clearly be within a customer's expectations that their details will be used by Connexin to respond to a customer's request for information about the products and services on offer. However, it might not be within their reasonable expectations that Connexin would then provide their details to third parties for marketing purposes without their consent.

Connexin will process personal data (included special category data) in accordance with all applicable laws and any applicable contractual obligations. More specifically, Connexin will not process personal data (including special category data) unless at least one of the legal bases under the Data Protection Laws apply.

In most cases where we process special category data, we will require the Data Subject's explicit consent to do this unless exceptional circumstances apply, or we are required to do this by law (e.g., to comply with legal obligations to ensure health and safety at work).
Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed. Connexin will only process special category data in accordance with Data Protection Laws.
Where special category data is being processed, Connexin will adopt additional measures to protect the data (e.g., encryption).

Headquarters: K3 Business Park, 200 Clough Road, Hull, HU5 1SN
Registered Office Address: 9th Floor 107 Cheapside, London, EC2V 6DN
: +44 1482 363738
: www.connexin.co.uk

8 DATA QUALITY

You must ensure that the personal data you collect is complete and accurate in the first instance and is updated to reflect the current situation of the data subject. You must take care when entering a data subjects' details onto a Connexin system. Personal data (e.g., contact details) should be validated and/or updated wherever possible.

Personal data known to be incorrect, inaccurate, incomplete, ambiguous, misleading, or outdated, even if provided by the customer or employee (or known by them to be inaccurate) must be corrected.

9 DATA RETENTION

Connexin will ensure that personal data relating to all data subjects is deleted or destroyed where there is no longer a reason to retain it. The length of time for which Connexin needs to retain personal data is set out in our Data Retention Policy. This takes into account the legal and contractual requirements that influence the retention periods set forth in the schedule to that policy

10 PROTECTION OF PERSONAL DATA

Connexin is required to make adequate technical and organisational security arrangements to protect personal data in its possession or under its control in order to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

You must ensure you have read and understood the Information Security Policies which are available on Connexin's HR management platform (HiBob). All employees must comply with these Information Security Policies.

A summary of the personal data related security measures is provided below:

- Hard copies of personal data should be kept in a secure place where unauthorised personnel cannot access it (e.g., locked cabinet or restricted rooms). Keys to such cabinets used to store such data must also be kept secure when not in use (e.g., key safe).
- Printed data containing personal data should be shredded or disposed of in a confidential waste bin or destroyed using an office shredder when it is no longer needed.
- Data stored on a computer should be protected by strong complex passwords that are changed regularly. Passwords must not be shared.

Headquarters: K3 Business Park, 200 Clough Road, Hull, HU5 1SN
Registered Office Address: 9th Floor 107 Cheapside, London, EC2V 6DN
: +44 1482 363738
: www.connexin.co.uk

- Employees must always lock their PC or workstation when it is left unattended and mobile devices must always be locked when not in use.
- Data must be accessed only by those employees authorised to do so. You must only access personal data on a strict need to know basis in the course of your normal business duties. Inappropriately accessing personal data will not be tolerated and may result in disciplinary action.
- Data stored on CDs or memory sticks/cards must be locked away securely when they are not being used.
- Where Connexin has taken possession of a customer device such as a mobile phone or laptop (e.g., repairs), the device must be kept secure at all times. The device must be locked away for safekeeping when not in use.
- Employees must accept all legitimate software and app updates on their computer, phone or tablet. Installing updates as soon as they are available will help keep your devices secure. Where an employee believes their anti-virus is not up to date then they must promptly notify the IT Department.
- Employees must not open email attachments or click on web links embedded in suspicious emails or emails from senders who they are unfamiliar with. Ensure that the email address is checked correctly Please check the email address. For example, if you receive an e-mail from Apple and the sender's address is AppleSupport765@hotmail.com, this is clearly not from Apple.
  If you do click on a suspicious attachment then you must disconnect your device from the internet by switching off Wi-Fi and/or removing the ethernet cable and report the incident immediately to the IT Department.
- Any data relating to or owned by Connexin (including personal data) must not be stored on a personal device unless expressly permitted to do so.
- Servers containing personal data must be kept in a secure location, away from general office space.
- The Infrastructure and Security Manager at Connexin must approve any cloud used to store any personal data.
- Encrypting data whilst it is being stored (e.g., on a laptop, mobile, USB or back-up media, databases and file servers) provides effective protection against unauthorised or unlawful processing. Personal data should never be saved to mobile devices such as laptops, tablets or smartphones unless these devices are encrypted. Encryption should be enabled by default. Where possible, Connexin data (including any personal data) should only be stored temporarily on these devices and transferred to Connexin network as soon as possible. This is to ensure the on-going availability of information in the event of damage or loss of a laptop.

Headquarters: K3 Business Park, 200 Clough Road, Hull, HU5 1SN
Registered Office Address: 9th Floor 107 Cheapside, London, EC2V 6DN
: +44 1482 363738
: www.connexin.co.uk

- Employees must use appropriate measures (e.g., encryption) when sending emails containing personal data outside Connexin. Any email containing special category data (either in the title, body or within an attachment) sent outside Connexin should be sent encrypted. Employees must exercise care when sending emails containing personal data. Employees must promptly report incidents when an email containing personal data is sent to an incorrect recipient in error.

11 BREACH REPORTING

Connexin has established incident response processes in place to deal with security breaches including those involving personal data. It has a separate security incident reporting policy relating to data security and breaches that must be followed by all employees.
All employees have an obligation to promptly report actual or potential data protection breaches or compliance failures. Any individual who suspects that a personal data breach has occurred must **immediately** notify the Head of SHEQ and Compliance.

Notification can be made by e-mail to dpo@connexin.co.uk

The Head of SHEQ & Compliance will then consider the incident, ensure that any consequences of the incident can be appropriately managed, comply with any notification requirements to the ICO and/or the data subjects affected by a data breach, and remedy and/or mitigate against the underlying causes of the incident. All data security breaches will be recorded in an internal breach log, including pertinent facts relating to the incident, effects and remedial actions taken.

This includes any actual or suspected leakage of personal data. A personal data breach ***could*** be caused by a number of events, by way of example only:

- theft of a laptop;
- loss of a USB containing customer records;
- emailing records containing personal data to the wrong email address or cc to unauthorised recipients;
- sending a spreadsheet containing customer or employee information to print, and failing to collect it straight away;
- phishing or vishing attack allowing a third party to access company systems or records;

Headquarters: K3 Business Park, 200 Clough Road, Hull, HU5 1SN
Registered Office Address: 9th Floor 107 Cheapside, London, EC2V 6DN
: +44 1482 363738
: www.connexin.co.uk

- malicious hacking;
- an employee or consultant accessing HR records without having the authority to do so.

Connexin has established incident response teams and processes in place to deal with security breaches including those involving personal data. See the Security Incident Reporting Policy for further information.

12 RIGHTS OF DATA SUBJECTS

In relation to employees, details of your rights and how to exercise them can be found in the employee handbook In relation to other Data Subjects, details of your rights are set out in Annex B.

13 OUTSOURCING SUPPLIERS

13.1 SUPPLIERS

Third Parties (i.e., Connexin suppliers) with access to personal data, must guarantee in writing that they comply with the applicable Data Protection Laws. Connexin will only transfer personal data to, or allow access by, third parties when it is assured that any such personal data will be processed legitimately and protected appropriately by the third party recipient.

13.2 CONTRACTS

Connexin will enter into an appropriate agreement with a third party to clarify each party's responsibilities in respect to the personal data transferred and/or otherwise processed.

The agreement must require the third party to protect the personal data, promptly report data breaches to Connexin and to only process personal data in compliance with Connexin's instructions. Third Parties will be required to complete a supplier questionnaire during procurement/contract negotiations.

Please consult your line manager and/or the Head of SHEQ & Compliance who may engage Connexin's external lawyers to assist you with putting together your contract

13.3 TRANSFERS OF DATA

Employees must not allow personal data to be transferred to any individual or company located outside the UK and/or the European Economic Area (EEA) without the prior written approval of the senior management team.

Headquarters: K3 Business Park, 200 Clough Road, Hull, HU5 1SN
Registered Office Address: 9th Floor 107 Cheapside, London, EC2V 6DN
: +44 1482 363738
: www.connexin.co.uk

This also applies where a company uses equipment, resources or a subcontractor located outside the UK to process personal data. This is because certain conditions need be met and/or safeguards be in place before any personal data can be transferred outside of the UK or EEA in order to comply with applicable Data Protection Laws.

13.4 AUDITS

Connexin may conduct audits of Third Parties handling Connexin data (including any personal data), especially in respect of information security measures they have in place. Any major deficiencies identified will be reported to and monitored by Connexin's senior management team.

14 COMPLAINTS HANDLING

Data Subjects with a complaint about the processing of their personal data should put their complaint in writing to Connexin. An investigation of the complaint will be carried out by Connexin in consultation with the relevant business owner to the extent that is appropriate based on the merits of the specific case. Connexin will inform the complainant of the progress and the outcome of the complaint within a reasonable period.

If the issue cannot be resolved through consultation with the complainant, then the complainant should be advised that they may, at their discretion, complain to the relevant data protection authority, which in the UK is the Information Commissioner's Office (ICO).

15 CONTACT

Please contact your line manager or the Head of SHEQ and Compliance, with any questions about the operation of this policy or Data Protection Laws or if you have any concerns with this policy not being followed or has not been followed.

Any exceptions or deviations from the requirements of this policy shall require prior written approval from the Head of SHEQ & Compliance.

Headquarters: K3 Business Park, 200 Clough Road, Hull, HU5 1SN
Registered Office Address: 9th Floor 107 Cheapside, London, EC2V 6DN
: +44 1482 363738
: www.connexin.co.uk