

PRIVACY STATEMENT

GENERAL

This policy is for Coventya (UK) Ltd.

The Data Protection Officer is Nicola Parker.

We are registered with the Information Commissioner's Office, under registration number Z3243703. You can access our notified use of personal data on the Information Commissioner's Office website (www.ico.co.uk).

SIX DATA PROTECTION PRINCIPLES

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy and relevancy
5. Storage limitation
6. Integrity and confidentiality

WHOSE DATA DO WE HOLD?

We hold personal data in respect of the following:

- Our employees
- Our former employees
- Prospective employees
- Customers
- Former customers
- Suppliers
- Former suppliers
- Professionals
- Work experience students

WHAT DATA DO WE HOLD?

Employees, Former Employees

- Name
- Address
- Date of Birth
- National Insurance Number
- Tax code
- Telephone number
- Email address
- Gender
- Marital status
- Bank Details
- Pension provider details
- Next of kin
- Emergency contact details
- Employment contract
- Training records
- CV
- Proof of eligibility to work in the UK

We may hold this information in respect of work experience students and prospective employees.

Customers, Suppliers and Other Third Parties

- Name
- Address
- Telephone number
- Email address
- Orders, invoices, etc.

WHAT SENSITIVE DATA DO WE HOLD?

Staff

- Health details

WHERE DO WE GET DATA FROM?

Employees, Former Employees, Prospective Employees, Work Experience Students

- Employees
- Third parties (eg. reference requests)
- Colleges
- Training providers
- HM Revenue & Customs
- Pension providers

Customers, Suppliers and Other Third Parties

- Business cards
- Emails
- Quotes
- Letters

HOW AND WHERE WE HOLD DATA?

We hold personal data in a variety of ways, both manually and electronically.

Manual data (which might include printed electronic data) is held as follows:

- Employee information (which includes CV's, personal details, employment contracts, etc.)
- Business cards
- Agreements
- Address books
- Letters
- Quotes

These are held within the office at Enterprise Drive, Station Road, Four Ashes, Wolverhampton, WV10 7DF.

Employee details are held in a locked fireproof filing cabinet and the room is locked, when the office is closed.

We maintain physical security with a code lock on the internal entry point into the office in office hours and five lever mortice locks at night, with a regularly maintained burglar alarm set. We do not permit third parties to access areas of the office, other than the reception area, without legitimate cause.

Electronic data

Electronic data is held on our networked IT infrastructure and individual laptops/PCs. The majority of the data is held on our server, which is held in a locked cabinet and the room is locked, when the office is closed.

We use passwords, user controls and access rights to limit access to data, to employees with a legitimate need to access the data.

We back up our file server daily, the backup is held on a separate server. This is held in a locked cabinet and the room is locked, when the office is closed. An additional backup of the backup server is done daily, via an encrypted external HDD and kept off site at an employee's home.

Coventya Holding SAS IT department in Paris hosts our email. They secure this, along with VPN access, firewalls and a secure router.

Some data is held on PC's and laptops, this data is backed up daily to an encrypted NAS server, which is held in a locked cabinet and the room is locked when the office is closed. All PC's and laptops are protected by Symantec antivirus software.

External access to the server from outside the office is by Global Protect VPN and our laptops are encrypted.

Our IT support provider (Severn Business Solutions Ltd, The Ironbridge Business Centre, Wesley Rooms, Jockey Bank, Ironbridge, Telford, TF8 7PD) undertake a review of our IT infrastructure on a regular basis, which includes consideration of the security data.

Certain members of staff have access to their emails on mobile phones. When an employee leaves the company, we take all reasonable steps to prevent continued access to our IT infrastructure and data and we require data held on mobile phones to be removed and act to prevent future access to it.

HOW DO WE MAINTAIN THE ACCURACY OF DATA?

It is important to us that the data we hold is accurate. Employees notify changes to personal data to our Finance & HR Manager, who updates all the relevant software.

Changes to customer and supplier details are amended on our ERP software, when they notify us.

WHAT DO WE DO WITH THE DATA WE HOLD?

We process data within our company to:

- Maintain our own accounting records
- Prepare VAT returns
- Operate our payroll
- Manage pensions
- Administer Training
- Send and receive third party references

HOW LONG DO WE HOLD DATA FOR AND WHAT WE DO AFTERWARDS?

The length of time for which we retain data depends on the nature of the data as follows:

- Employees – records for HMRC are kept for 7 years and personnel files are kept for 6 months after an employee leaves
- Customer and Supplier details – these are kept until business ceases. Data is kept on ERP software for 12 months and then deleted. The Business cards of any customers and suppliers, who we are no longer trading with, are disposed of through confidential waste collections.

We use a third party confidential waste disposal company, to destroy all manual data containing personal data.

YOUR RIGHTS

If we hold personal data relating to you, you have a right under Data Protection Act 2018 and GDPR to find out what information we hold, that relates to you. If you wish to exercise this right, please complete the Subject Access Request Form, found on our website at www.molclear.com and send it to n.parker@coventya.com.