UK-GDPR
(General Data Protection Regulations)
Policy

A. Introduction

Ventol Maintenance is committed to the security and privacy of your data. We collect and use personal information from individuals we work with, and we ensure this data is handled properly, whether in paper or digital format. Our successful operation and the trust of our business contacts depend on the lawful and correct treatment of personal information.

We fully adhere to the principles of the Data Protection Act 2018 and the UK General Data Protection Regulation (UK-GDPR). This policy covers the processing of personal data in our human resources function, including how we handle data breaches and other UK-GDPR rights.

This policy applies to the personal data of job applicants, current and former employees, apprentices, volunteers, placement students, workers, self-employed contractors, and consultants, collectively referred to as "relevant individuals".

B. Definitions

- **Personal data**: Information that identifies a person directly or indirectly, such as name, ID number, location, or online identifier. This can include pseudonymised data.
- **Special categories of personal data**: Data related to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, trade union membership, and genetic or biometric data used for ID purposes.
- **Criminal offence data**: Data concerning an individual's criminal convictions and offences.
- **Data processing**: Any operation performed on personal data, automated or not, including collection, recording, storage, alteration, retrieval, use, disclosure, or destruction.

C. Data Protection Principles

All personal data we obtain and hold is processed according to core UK-GDPR principles. We ensure that:

- Processing is fair, lawful, and transparent.
- Data is collected for specific, explicit, and legitimate purposes.
- Collected data is adequate, relevant, and limited to what is necessary for processing.
- Data is accurate and kept up to date; inaccurate data will be rectified or erased promptly.
- Data is not kept longer than necessary for its purpose.
- Data is processed securely, protecting against unauthorised or unlawful processing, accidental loss, destruction, or damage through appropriate technical or organisational measures.
- We comply with UK-GDPR procedures for international data transfers.

D. Types of Data Held

We maintain various categories of personal data for our employees to ensure effective processes. This data is kept in personnel files and on computer systems (e.g., holiday booking system).

Specific types of data we hold include:

- Personal details (name, address, phone numbers).
- Recruitment information (CV details, references, education, employment history).
- Pay administration details (National Insurance numbers, bank account details, tax codes).
- Medical or health information.
- Employment-related information:
  - Job title and descriptions.
  - Salary.
  - Terms and conditions of employment.
  - Details of formal and informal proceedings (e.g., disciplinary actions, leave records, appraisals).
  - Internal and external training undertaken.

All this information is necessary for our processing activities, and more details are available in our employee privacy notice from your manager.

E. Employee Rights

You have the following rights regarding your personal data:

- To be informed about your data and its use.
- To access your data (further details in "Access to Data" section and Subject Access Requests policy).
- To have inaccuracies corrected (rectification).
- To have data deleted in certain situations (erasure).
- To restrict data processing.
- To transfer your data to another party (portability).
- To object to any information's inclusion.
- To regulate automated decision-making and profiling of personal data.

More information on these rights is in our separate policy on employee rights under UK-GDPR.

F. Responsibilities

Employees involved in data processing are trained on our data protection policies. We have also appointed employees responsible for reviewing and auditing our data protection systems.

G. Lawful Basis of Processing

We only process data when a lawful basis exists and have assigned a basis to each activity. If no other basis applies, we may seek employee consent, understanding that consent must be freely given, specific, informed, and unambiguous. When seeking consent, we will provide clear instructions on the processing activity, its consequences, and the right to withdraw consent at any time.

H. Access to Data

Employees can access their personal data by making a Subject Access Request. We will respond without delay, within one month, unless an extension is legally required, in which case you will be informed. No charge applies unless the request is clearly unfounded, excessive, repetitive, or for duplicate copies for other parties, in which case a reasonable charge may apply. More details are in our Subject Access Request policy.

I. Data Disclosures

We may disclose data in specific circumstances, including:

- For employee benefits operated by third parties.
- To determine if reasonable adjustments are needed for disabled individuals at work.
- For individuals' health data to meet health and safety or occupational health obligations.
- For Statutory Sick Pay purposes.
- For HR management and administration, to assess how health affects job ability.
- For the smooth operation of employee insurance policies or pension plans.
- To assist law enforcement or relevant authorities in preventing/detecting crime, prosecuting offenders, or assessing/collecting tax/duty.

These disclosures are made only when strictly necessary.

J. Data Security

All employees are aware that hard copy personal information must be kept in locked cabinets, drawers, or safes. Employees know their data processing roles and responsibilities. Confidential files or written information should be stored securely, accessible only by authorised personnel, and screen locks should be used on unattended devices.

Computerised data should be coded, encrypted, or password protected on local and regularly backed-up network drives. Removable storage media with data must be kept in a locked cabinet, drawer, or safe. Employees must use provided passwords and not share them.

Personal data should not be kept or transported on laptops, USB sticks, or similar devices without prior authorisation. If used, such devices must:

- Record data only when absolutely necessary.
- Use an encrypted system where a dedicated folder encrypts all files.
- Be secured to prevent theft.

Failure to follow data security rules may result in disciplinary action, including dismissal.

K. Third-Party Processing

When engaging third parties to process data, we will use data processing agreements to ensure they uphold our commitment to data protection.

L. International Data Transfers

We do not currently send personal data outside the European Economic Area (EEA). If this changes, you will be notified, and protective measures explained.

M. Requirement to Notify Breaches

All data breaches are recorded in our Data Breach Register. Where legally required, we report breaches to the Information Commissioner within 72 hours of discovery and inform affected individuals. More information is in our Breach Notification policy.

N. Training

New employees must read and understand data protection policies during induction. All employees receive training on confidentiality, data protection, and breach identification. Nominated data controllers/auditors/protection officers are appropriately trained in their UK-GDPR roles. Employees using computer systems are trained to protect private data, ensure security, and understand the consequences of lapses.

O. Records

We maintain an HR Data Record of processing activities, including purposes and retention periods, keeping it up to date.

P. Data Protection Compliance

For questions or comments about this policy, contact our Data Protection Officer: Mrs. Victoria Franks Email: dpo@ventol.co.uk

Or

by mail: Data Protection Officer Ventol Maintenance Limited Unit 1 & 2, Landsberg, Lichfield Road Industrial Estate Tamworth, Staffordshire B79 7XB

Mr. Elliott Mordue
Managing Director

Date: 28 February 2025
Next review: 28 February 2026