

PRIVACY NOTICE – EMPLOYEES

Aim

VertaseFLI (referred to hereafter as the Company) takes your privacy seriously and will only use your personal information to manage the employment relationship and in pursuit of the Company's ambitions. This privacy policy explains how the Company uses any personal information we collect about you when you are employed by us.

Who is responsible for your data

The Company controls the ways your personal data is collected and the purposes for which your personal data is used, and we are the 'data controller' for the purposes of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Personal data we collect about you

When using the term 'personal data' in our Privacy Notice, we mean information that relates to you and allows us, and others, to identify you. We collect personal data from you when you become an employee with us. This may include but is not limited to the following information:

- Your personal details - name, surname, address, date of birth, national insurance number, telephone numbers, email addresses.
- Your emergency contact details, names and contact details.
- Your job information – job title, location.
- Bank Details – name, address, account name, account no, sort code.
- Information about your health – medical questionnaire, if you have a medical condition that may affect your work.
- Qualifications, skills and training.
- Interview and recruitment details, including CV's.
- References.
- Driving licence details.
- Absence details.
- Performance review details.
- Pension's information.
- IT system usage data, security access logs and CCTV footage (where applicable).
- The communications you exchange with us (for example, your emails, letters, calls).

Special Category Data

We may also collect information that could reveal your racial or ethnic origin, physical or mental health, religious beliefs or alleged commission or conviction of criminal offences. Such information is considered 'special category data' under the GDPR.

We only collect this information where a lawful basis under UK GDPR and Data Protection Act 2018 applies (e.g., for employment law obligations, assessment of working capacity, equality monitoring).

For example, we may collect this information in the following circumstances:

- Any medical condition – for health and safety purposes.
- Ethnic group and sex – for equal opportunities purposes.

PRIVACY NOTICE – EMPLOYEES

How and why we use your personal data

We use your personal data to manage your employment relationship with us, this may include, but is not limited to the following:

- To pay your salary/ wages.
- For travel purposes, for example, when booking accommodation or travel.
- In tenders/ bids, for example company CV's detailing skills and competence in winning work.
- To communicate with you
- To comply with legal obligations (e.g., tax, National Insurance, right-to-work checks, health and safety reporting).
- To manage performance, conduct and training needs.
- For security, IT administration and access control.
- For business continuity and internal management purposes.

Lawful bases for processing

We rely on the following lawful bases under UK GDPR:

- Contractual necessity – processing required to deliver your employment contract.
- Legal obligation – e.g., HMRC reporting, right-to-work checks, health & safety law.
- Legitimate interests – e.g., business operations, security monitoring, tender submissions.

For special category data, we rely on conditions including:

- Employment law obligations.
- Assessment of working capacity.
- Equality monitoring.

How long will we keep your personal data?

We will retain your personal data for as long as we need it in order to fulfil our purposes set out in this Privacy Notice, or in order to comply with the law. Please note that we are required to keep some of your personal data beyond your employment relationship, this may include, but is not limited to the following:

- Accident records / medical records/ H&S records.
- Wages/ salary records.
- Asbestos medicals and monitoring records.
- Pensions records.
- Tax / NI records.

Security of your personal data

We are committed to taking appropriate technical and organisational measures to protect your personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage.

This includes access controls, encryption where appropriate, secure storage, staff training, and subcontractor/ supplier due diligence.

PRIVACY NOTICE – EMPLOYEES

Sharing your personal data

Your personal data is kept by the HR Department and may be shared with relevant people and the Accounts department.

Your personal data may be shared with some external companies. This may include, but is not limited to the following:

- Pension advisor and provider - to process employee pensions.
- HMRC – for Tax and National insurance deductions.
- Healthcare providers - to provide healthcare benefits to employees.
- Medical professionals – to undertake medical checks where necessary.
- Training providers – to provide training courses.
- Payroll - To process salaries and wages.
- IT Support company – to provide necessary IT equipment to undertake job roles.
- Accommodation/ travel companies – in pursuit of Company business.
- Clients – requiring personal data for projects/ sites. Please note, special category data will only be shared where legally permitted and necessary for employment or health & safety purposes.

The Company has no intention of sharing data with third parties for marketing purposes, but may for tender purposes as required.

Your rights and your personal data

Unless subject to an exemption under the GDPR, you have the following rights with respect to your personal data:

- The right to be informed about the collection and use of your personal data.
- The right of access to your personal data.
- The right to have inaccurate personal data rectified.
- The right to have personal data erased.
- The right to restrict or suppress personal data.
- The right obtain and reuse data across different services.
- The right to object – for example, profiling.
- Rights in relation to automated decision making and profiling.
- The right to lodge a complaint with the Information Commissioner's Office (ICO).

Requesting access to your personal data

If you would like a copy of some or all of the information, please email Rebecca Weller, People & Culture Director at rweiler@vertasefli.co.uk.

Reporting breaches

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;

PRIVACY NOTICE – EMPLOYEES

- alteration of personal data without permission; and
- loss of availability of personal data.

If you believe a data breach has occurred you must inform the People & Culture Director with immediate effect. The Company will investigate all suspected breaches and report notifiable breaches to the ICO within statutory time limits.

Updates to our privacy policy

We will keep our privacy policy under regular review and we will communicate any updates.

Contact Information

Questions, comments and requests regarding this privacy policy are welcomed and should be addressed to the People & Culture Director.

Signed on behalf of VertaseFLI



Steve Edgar, Managing Director

Reviewed: February 2026

Employee Name:

Signed:.....

Date:.....