



Veriflo
Water Asset Management

POLICY 005: Data Protection Policy

Issue: 23/08/2023

v2.1

Contents

1	Introduction.....	3
1.1	Purpose.....	3
1.2	Application.....	3
2	Statement	3
3	Scope	4
4	Definitions.....	4
5	Data protection principles.....	4
6	Types of Data Held	5
7	Data Collection activity	6
8	The Need for Data Handling	7
9	Individual rights.....	8
9.1	Subject access requests.....	8
9.2	Other rights.....	9
10	Security of personnel data.....	9
11	Data breaches	10
12	International data transfers	10
13	Individual responsibilities.....	10
14	Staff access to sensitive data	10
15	Training.....	11
16	Responsibility for Information Security.....	11
17	Associated Documents	12

DATA PROTECTION POLICY

1 Introduction

1.1 Purpose

The Company is committed to being transparent about how it collects and uses the personal data of its employees, and to meeting its data protection obligations in alignment with the General Data Protection Regulations (GDPR), the current Data Protection Act and any other appended or subsequent legislation. This policy sets out the Company's commitment to data protection, and individual rights and obligations in relation to personal data.

1.2 Application

Veriflo Limited, ("Veriflo", "the Company") as a 'data controller', collects and processes personal data relating to its own personnel and contractors to manage the employer-employee/contractor relationship. We minimise our data handling to compliance and legitimate business use only.

This policy applies to the personal data of job applicants, employees, workers, contractors, volunteers, interns, apprentices and former employees, referred to as HR-related personal data. Additional personal data of clients and other parties may be held for a limited time for strictly business purposes; contact details, address and asset location data, vehicle and insurance information, dashcam and driver footage.

The Company has accordingly registered with the Information Commissioner's Office (ICO).

The Company has appointed Kelly Grayland as its Data Protection Officer. Their role is to inform and advise the Company on its data protection obligations. They can be contacted at kgrayland@veriflo.co.uk. Questions about this policy, or requests for further information, should be directed to the Data Protection Officer.

2 Statement

Through application of this policy and the systems and processes to which it relates, Veriflo undertakes to limit and control personal information as far as practicable, which is collected, handled and stored on the basis of legitimate business needs.

All requests for data are accompanied by notice of the reasons for collection, handling and storage, and requested entities are informed of their rights to review what is held at any time.

All personal data requests are limited to information necessary to enable the functions of the employer role including the facilitation of payment and training, and in the interests of equal opportunities and anti-discrimination. Additional data including limited medical information and recorded vehicle and driver footage is retained for the use of Health and Safety provision and planning, including employee safeguarding and the provision of emergency plans.

Business data is collected and stored for commercial reasons and is limited to individuals directly involved with the execution of our duties under contract. Financial data is limited to the Directors and the Finance Officer.

At all stages data access is limited to persons with a legitimate need, and all access requests are reviewed and analysed by Management before being granted. All forms and data stores are audited to remove unnecessary information and limit duplication on a continuous basis.

Server access is granted only after review, and personnel are only given access they need, after consideration of data sources located therein. Folder structures are organised to limit access to personnel to only that which they need. Hard copy is controlled, only printing when necessary and no sensitive data is left unsecured at any time. All sensitive or personal data is kept in locked filing systems.

Where possible, electronic copies of data are made and kept in secure server areas for access by only specified personnel and hard copy is destroyed. All hardcopy containing any personal or sensitive data is shredded before disposal. Personnel who leave employment take no data sources with them, and laptops, phones and other devices are data wiped by I.T. service providers.

Stored data is held for limited time periods based upon data type, and only retained as far as necessary. Data which must be preserved for the long term for Health, Safety and Compliance reasons is held in a dedicated locked archive area with access limited to Director level personnel only.

It is our commitment that we:

- Protect the confidentiality, integrity and availability of all personally identifiable information and confidential data
- Comply with all relevant legislation and contractual obligations including GDPR and relevant legislation.
- Take a risk-based approach to our business activities to ensure team member and other data is securely processed and protected from system vulnerabilities and internal & external threats
- Breaches of personal data arising through misdeed of negligence will be treated with appropriate disciplinary and/or legal action.

3 Scope

This policy relates to all use of sensitive or private data or personal information which is collected, stored and processed by Veriflo Limited in the course of our legitimate business practices. All persons employed by, working on behalf of or in association with Veriflo are expected to comply with the terms of this policy.

4 Definitions

- "**Personal data**" is any information that relates to a living individual who can be identified from that information.
- "**Processing**" is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.
- "**Special categories of personal data**" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic and biometric data.
- "**Criminal records data**" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

5 Data protection principles

The company processes HR-related personal data in accordance with the following data protection principles:

- The company processes personal data lawfully, fairly and in a transparent manner.
- The company collects personal data only for specified, explicit and legitimate purposes.
- The company processes personal data only where it is adequate, relevant and limited to what is necessary

for the purposes of processing.

- The company keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- The company keeps personal data only for the period necessary for processing.
- The company adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

The company tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. HR-related data will not be shared with third parties, except as set out in privacy notices. Where the company relies on its legitimate business need as the basis for processing data, it will carry out an assessment to ensure that those interests are not overridden by the rights and freedoms of individuals.

Personal data gathered during the employment, worker, contractor or volunteer relationship, or apprenticeship or internship is held in the individual's personnel file (in hard copy or electronic format, or both), and on HR systems. The company will update HR-related personal data promptly if an individual advises that their information has changed or is inaccurate.

The periods for which the company holds HR-related personal data are contained in its privacy notices to individuals. The company keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

6 Types of Data Held

In the interests of managing the employer-employee relationship, Veriflo collects, processes and stores the following types of personal information about their personnel;

- name, address and contact details, including email address and telephone number, date of birth and gender
- job title, job descriptions and pay grade
- training records including competencies, qualifications, certificates and accreditations
- driving license details and where applicable, penalty points and/or disqualifications
- recordings made from vehicle dashcams of driving and driver behaviour
- CV's and associated details: qualifications, skills, experience and employment history, including start and end dates, with previous employers and with Veriflo
- references from former employers
- information about remuneration, including entitlement to benefits such as pensions or insurance cover and other flexible benefits as appropriate
- details of bank accounts and national insurance numbers, payroll records and tax status information including information received from HMRC
- information about marital status, next of kin, dependents and emergency contacts including their personal data such as home address, employer's address, contact details, birth certificates, passports etc.
- information about nationality and entitlement to work in the UK including information received from the UK Border Agency and/or the Home Office
- details of schedules (days of work and working hours), location of workplace and attendance at work including CCTV / dashcam footage
- employment records (including job titles, work history, working hours, holidays, training records and professional memberships)

- staff photographs
- information about access and use of our I.T. and communications systems
- details of periods of leave taken, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave
- details of any disciplinary or grievance procedures, including any warnings issued and related correspondence
- assessments of performance, including appraisals, performance reviews and ratings, performance improvement plans and related correspondence

Special Categories of Personal Data:

- trade union membership information
- information about medical or health conditions, including potential disability for which the company needs to make reasonable adjustments
- occupational health records including details relating to Occupational Medical Assessments, medical history, medical conditions – past & present, and details relating to your GP, and doctors or consultants that you may be/ have been in the care of
- equal opportunities monitoring information including information about ethnic origins, sexual orientation and religion or belief and any other personal data referring to protected characteristics

Criminal Records data:

- criminal convictions, cautions or offences

7 Data Collection activity

Veriflo may collect the categories of information listed above in a variety of ways. For example, data might be collected through employment agencies, application forms, CVs or resumes; obtained from your passport or other identity documents such as your driving license; from forms completed by you at the start of or during employment (such as benefit nomination forms); from correspondence with you; or through interviews, meetings or other assessments.

In some cases, Veriflo may collect personal data about you from third parties, such as references supplied by former employers, applicant information from recruitment agencies, information from employment background check providers, information from credit reference agencies and information from criminal records checks permitted by law.

Data will be stored in a number of locations, including in your personnel file and I.T. systems (including email system).

8 Recruitment Data

The Company collects data from individuals during recruitment, including from persons who will not ultimately be employed by the Company. All personal data and information which is collected, processed or held shall be controlled as far as practicable to minimum limited personnel. Where such data is stored, it is held for use under legitimate business interest for the fair and effective recruitment of personnel. No personal data will be held or proliferated any more than is absolutely necessary in pursuit of this end.

Applicant data will be held on file for a maximum 6 months after completion of the probationary period of the relevant position, thereby to ensure that standby or second-choice personnel can be assessed and contacted in case of recruitment changes or failure to pass probation. Applicants will need to resubmit applications for subsequent positions beyond this timescale.

When personnel leave the business, personal recruitment data will be stored securely and out of the active personnel registers for a period not exceeding two years, and shall be completely removed from Veriflo personnel records after this time, where such information does not need to be retained for insurance, Health and Safety or incident investigation needs. Limited records relating to the individual's employment; performance of duty, Incident and Health and Safety information will be retained beyond this time but such will be limited according to information type.

Right-to work documents regarding personnel shall be held on file for no less than two years after the employment has ended in line with Home Office guidelines. When personal data is removed it shall be removed from all stored locations; to include hardcopy and electronic documents, files and email records.

9 The Need for Data Handling

Veriflo needs to process all the categories of data in the list above primarily to enter into an employment contract with employees and meet its obligations under the employment contract. (e.g. to provide an employment contract, to pay wages in accordance with contract and to administer benefit, pension and insurance entitlements.)

In some cases, the company needs to process data to ensure that it is complying with its legal obligations. (e.g. to check personnel entitlement to work in the UK, to deduct tax, to comply with health and safety laws and to enable personnel to take periods of leave to which they are entitled.)

In other cases, Veriflo has a legitimate interest in processing personal data before, during and after the end of the employment relationship. Supplemental processing of personnel data allows the company to:

- Demonstrate compliance with right-to-work regulations
- Run recruitment and promotion processes
- Maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of team member contractual and statutory rights
- To pay wages, deduct tax and National Insurance contributions (NICs) and prepare P45 documents
- Operate and keep oversight of disciplinary and grievance processes, to ensure acceptable conduct within the workplace
- Oversight of driving behaviour in the interests of road safety and employee conduct
- Operate and keep a record of personnel performance and related processes, to plan for career development, and for succession planning and workforce management purposes
- Enrolment in pension schemes in accordance with statutory automatic enrolment duties
- Making decisions about salary reviews and compensation
- Education, training and development requirements
- Record of absence and absence management procedures, to allow effective workforce management and ensure that team members are receiving the pay or other benefits to which they are entitled
- Obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities and ensuring the Company makes provisions where necessary for reasonable adjustment, meet

its obligations under health and safety law, ensures you are able to carry out the duties of your role, and ensure that team members are receiving the pay or other benefits to which they are entitled

- Operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that the Company complies with duties in relation to leave entitlement, and to ensure that team members are receiving the pay or other benefits to which they are entitled
- Ensure effective general HR and business administration
- To monitor use of our information and communication systems to ensure compliance with our I.T. policies
- Perform high-level equal opportunities monitoring
- Provide references on request for current or former personnel
- Respond to, and defend against legal claims
- Monitor staff locations & whereabouts in order to meet fire safety regulations, Health & Safety compliance, and to pay you accurately for the work you do.

Some of the above grounds for processing will overlap and there may be several grounds which justify the company's use of your personal information.

- We will not use personal information for purposes other than that for which it was collected, unless we reasonably consider that this is required, and the reason is compatible with the original purpose.
- If the company needs to use data for an unrelated purpose, we will notify the subject and explain the legal basis which allows us to do so. The company may process personal information without knowledge or consent, in compliance with the above, where it is required or permitted by law.
- The legal basis on which we will process personal information is to carry out our obligations under employment law, equality laws, health & safety laws and to protect vital interests of personnel.

10 Individual rights

As a data subject, individuals have a number of rights in relation to their personal data.

10.1 Subject access requests

Individuals have the right to make a subject access request. If an individual makes a subject access request, the company will tell them:

- Whether or not their data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- To whom their data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- For how long their personal data is stored (or how that period is decided);
- Their rights to rectification or erasure of data, or to restrict or object to processing;
- Their right to complain to the Information Commissioner if they think the company has failed to comply with their data protection rights; and
- Whether or not the company carries out automated decision-making and the logic involved in any such decision-making.

The company will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless they agree otherwise. If the individual wants additional copies, the company will charge a fee, which will be based on the administrative cost to the company of providing the additional copies.

To make a subject access request, the individual should send the request to kgrayland@veriflo.co.uk or use the company's form for making a subject access request. In some cases, the company may need to ask for proof of identification before the request can be processed.

The company will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the company processes large amounts of the individual's data, it may respond within three months of the date the request is received. The company will write to the individual within one month of receiving the original request to tell them if this is the case.

If a subject access request is manifestly unfounded or excessive, the company is not obliged to comply with it. Alternatively, the company can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the company has already responded. If an individual submits a request that is unfounded or excessive, the company will notify them that this is the case and whether or not it will respond to it.

10.2 Other rights

Individuals have a number of other rights in relation to their personal data. They can require the company to:

- Rectify inaccurate data;
- Stop processing or erase data that is no longer necessary for the purposes of processing;
- Stop processing or erase data if the individual's interests override the company's legitimate grounds for processing data (where the company relies on its legitimate interests as a reason for processing data);
- Stop processing or erase data if processing is unlawful; and
- Stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the company's legitimate grounds for processing data.

To ask the company to take any of these steps, the individual should send the request to kgrayland@veriflo.co.uk.

11 Security of employee data

The company takes the security of HR-related personal data seriously. The company has internal controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties. All systems that are used to store HR-related personal data are kept password protected and can only be accessed by those who require access for the performance of their duties as an employer. These systems include, online HR Management systems, such as BreatheHR as well as Dropbox.

Where the company engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

12 Data breaches

If the company discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The company will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

13 International data transfers

The company will not transfer HR-related personal data to countries outside the EEA.

14 Individual responsibilities

Individuals are responsible for helping the company keep their personal data up to date. Individuals should let the company know if data provided to the company changes, for example if an individual moves to a new house or changes bank details.

Individuals may have access to the personal data of other individuals and of our customers and clients in the course of their employment, contract, volunteer period, internship or apprenticeship. Where this is the case, the company relies on individuals to help meet its data protection obligations to staff and to customers and clients. Individuals who have access to personal data are required:

- To access only data that they have authority to access and only for authorised purposes;
- Not to disclose data except to individuals (whether inside or outside the company) who have appropriate authorisation;
- To keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- Not to remove personal data, or devices containing or that can be used to access personal data, from the company's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
- Not to store personal data on local drives or on personal devices that are used for work purposes; and
- To report data breaches of which they become aware to the data protection officer immediately.

15 Staff access to sensitive data

Staff with privileged access to personal and sensitive data, deemed to have the “need to know” shall be given extra information, orientation and training to ensure they are aware of the significance of the data being held and the repercussions of disclosing it to those who have been granted access.

Access to sensitive data will be closely controlled and applied through the Principle of Least Privilege, where users will only be allowed to access data that is required for their job role and to which they have a legitimate purpose to see.

16 Training

The Company will provide training to all new starters about their data protection responsibilities as part of the induction process. All policies and guides relating to data protection are available for employees via BreatheHR.

17 Responsibility for Information Security

Within the company, the Directors are ultimately responsible for matters relating to Information Security and has ultimate responsibility for:

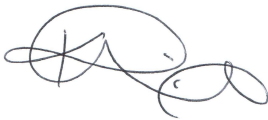
- Ensuring Data & Information Security considerations are integrated into business strategy
- Origination, Development and maintenance of Data Protection & Information Security Policies and Procedures
- Communication and review of Data & Information Security Policies
- Undertaking data risk assessments and authorising risk treatment plans
- Communicating externally with clients and the ICO on information security matters

18 Associated Documents

Other documents associated to this policy include:

- Privacy Notice

Approved and implemented.



Kirsty Scott, Business Director, Veriflo Ltd.

23/08/2023 Review: annual