DATA PROTECTION

AssetWorks
Policy To:

Data Protection Policy

Date: 01 May 2023
Point of Contact - Tamzin Wright, UK Bid Coordinator
Tel: 0161 927 3680| tamzin.wright@assetworks.com

DATA PROTECTION POLICY

Contents

© May 2, 2023 AssetWorks Inc. | All Rights Reserved | www.assetworks.co.uk
© May 2, 2023 Trapeze Software ULC. | All Rights Reserved | www.trapezegroup.com

© May 2, 2023 AssetWorks Inc. | All Rights Reserved | www.assetworks.co.uk
© May 2, 2023 Trapeze Software ULC. | All Rights Reserved | www.trapezegroup.com

Purpose and Applicability

We regard the lawful and correct treatment of personal information as very important to successful operations, and to maintaining confidence between those with whom we deal and ourselves. We ensure that our organisation treats personal information lawfully and correctly.

We fully endorse and adhere to Article 5 of the EU General Data Protection Regulations (2016/679) and the Data Protection Act 2018 and subsequent legislation which specify that data must be:

- Fairly and lawfully processed
- Processed for specified and legitimate purposes
- Adequate, relevant, and limited to the minimum necessary in relation to the purpose
- Accurate and, where necessary, kept up to date
- Not kept for longer than is necessary
- Processed in line with the rights of data subjects
- Secure
- Not transferred to countries outside the relevant jurisdiction (EU for EU-related contracts and the UK for UK-related contracts) without adequate protection.

Scope

This access control policy applies to Trapeze Group (UK) trading as AssetWorks.

Introduction

This policy sets out how our organisation seeks to protect personal data and ensures that our staff understand the rules governing their use of the personal data to which they have access in the course of their work.

The main legislation governing data protection is the UK General Data Protection Regulations [GDPR] and the Data Protection Act 2018 (hereafter referred to as *the Legislation*).

Broadly, the Legislation covers any information that relates to living individuals [Data Subjects].

This Data Protection Policy details the way in which our organisation fulfils its responsibilities towards people in both the spirit and the letter of the law. The Board of Directors are committed to ensuring that the Data Protection Policy not only complies with the Legislation but also demonstrates the concern for its employees, its customers, its suppliers and contractors and all other persons including members of the general public with whom it has contact.

© May 2, 2023 AssetWorks Inc. | All Rights Reserved | www.assetworks.co.uk
© May 2, 2023 Trapeze Software ULC. | All Rights Reserved | www.trapezegroup.com

In writing this policy, the organisation acknowledges that our business sometimes requires us to hold and process Personal Data associated with individuals.

There are categories of Personal Data referred to as Special Categories of Personal Data under the Legislation whose unauthorised disclosure could cause significant harm to the Data Subject. The definition of Special Categories of Personal Data can be found in section 2.1. The Legislation places a higher duty of care on data users in respect of Special Categories of Personal Data versus Personal Data. A number of systems that our organisation supplies handle Special Categories of Personal Data.

The Policy indicates the management structure, processes, and security measures that allow achievement and demonstration of our sound data protection performance.

This Policy will also apply where Personal Data (including Special Categories of Personal Data) is sent abroad for processing (including to North America for development purposes).

Note, as a member of the Volaris operating group within the CSI Group some systems are centrally provided and are outside the direct control of the organisation – for example, the HR and payroll systems.

Definitions

Term	Definition
Business purposes	The purposes for which personal data may be used by us: Personnel, administrative, financial, regulatory, payroll and business development purposes. Business purposes include the following: • Compliance with our legal, regulatory and corporate governance obligations and good practice • Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests • Ensuring business policies are adhered to (such as policies covering email and internet use) • Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking • Investigating complaints • Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and

© May 2, 2023 AssetWorks Inc. | All Rights Reserved | www.assetworks.co.uk
© May 2, 2023 Trapeze Software ULC. | All Rights Reserved | www.trapezegroup.com

	assessments • Monitoring staff conduct, disciplinary matters • Marketing our business • Improving services
Personal data	'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal data we gather may include: individuals' phone number, email address, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.
Special categories of personal data	Special categories of data include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings, and genetic and biometric information — any use of special categories of personal data should be strictly controlled in accordance with this policy
Data controller	'Data controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law
Data processor	'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Processing	'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Data Privacy Impact Assessment	An assessment that evaluates risks to the rights and freedoms of data subjects that result from data processing.
Supervisory Authority	This is the national body responsible for data protection. The supervisory authority for our organisation is the Information Commissioners Office.

© May 2, 2023 AssetWorks Inc. | All Rights Reserved | www.assetworks.co.uk
© May 2, 2023 Trapeze Software ULC. | All Rights Reserved | www.trapezegroup.com

Subject Access Request	The process by which an individual requests to receive confirmation that their data is being processed, access to their personal data and any supplementary information

Aims

The aim of this Policy is to ensure that

- Both as a company and as employees we completely adhere to the principles as stated in the Legislation
- All employees are aware of the Legislation
- We understand how the organisation complies with its obligations under the Legislation
- Employees are given suitable guidance on how Personal Data should be handled to comply with the Legislation, and
- Employees and customers are aware of their rights and obligations under the Legislation.

Principles

The Principles are:

1. **Lawful, fair and transparent** – Data collection must be fair, for a legal purpose and we must be open and transparent as to how the data will be used.
2. **Limited for its purpose** – Data can only be collected for a specific purpose.
3. **Data minimisation** –Any data collected must be necessary and not excessive for its purpose.
4. **Accurate** – The data we hold must be accurate and kept up to date.
5. **Retention** – We cannot store data longer than necessary.
6. **Integrity and confidentiality** – The data we hold must be kept safe and secure.

Equally, we want to help our customers to comply with GDPR. It is also the objective to this policy, and subsequent procedures, to ensure that all personal data transferred out of Live / Production environments for further testing or development, is anonymised as far as reasonably practical before any transfer can take place thereby taking the data outside GDPR.

Scope

The scope of the Data Protection Policy includes:

- Office locations throughout the UK
- Hosting centre environments for Live / Production services
- Employees working from home

© May 2, 2023 AssetWorks Inc. | All Rights Reserved | www.assetworks.co.uk
© May 2, 2023 Trapeze Software ULC. | All Rights Reserved | www.trapezegroup.com

Only environments that host Personal Data will be subject to the requirements set out within this policy.

A brief list of Dos and Don'ts

This is by no means comprehensive. The important thing is to be aware that your personal data and that of clients and colleagues must be safeguarded.

DOS	DON'TS
Hardware & systems	
Do ensure you use work laptops solely for work purposes.	Don't leave hard copies or data drives around.
Do make sure devices have the latest security updates.	Don't use USB storage devices, any exceptions must be approved by ICT
Do make full use of VPNs.	Don't use public Wi-Fi networks, if possible, where you do make sure it is genuine and don't take any risks
Do verify who is calling on the phone before you give any information out.	Don't leave devices unattended. Keep all mobile devices, such as laptops and mobile phones physically secured. If a device is lost or stolen, report it immediately to your line manager and IT staff.
Do look after your IT equipment including housekeeping (e.g., wipe screens and keyboards, clear out temp files, empty recycle bin).	Don't change or disable any of your device's security settings (e.g. bitlocker, anti-virus, screen saver time outs)
Ways of working	
Do keep up your guard – be aware whenever you are handling Personal Data.	Don't share passwords and don't use the same password to access different applications not on single sign-on.
Do use encryption methods – Bitlocker is mandatory, Office applications enforce multi- factor authentication to access. Make sure your password protect sensitive data.	Don't use Personal Data for anything other than what it was collected for.
Do use Blind Carbon Copy (BCC) where appropriate to avoid giving a list of all addressees and their email addresses to each addressee OR use the DDG groups for mass internal emails.	Don't keep data longer than necessary.
Do ask yourself "What would I do if it were my own Personal Data?"	Don't click on links in emails or open attachments unless you're absolutely sure they are safe.

© May 2, 2023 AssetWorks Inc. | All Rights Reserved | www.assetworks.co.uk
© May 2, 2023 Trapeze Software ULC. | All Rights Reserved | www.trapezegroup.com

Do register any Personal Data you get or hold on the appropriate company register. We must have a complete record of all Personal Data Processing.	Don't put Personal Data into emails if you can avoid it – emails are kept forever.
Do lock your machine whenever you leave it, even for a quick break.	Don't be unsure – keep up with Data Protection and Security Awareness training.
Do keep data accurate.	Don't hesitate – if you suspect a Data Breach or you think someone is making a Data Subject Access Request, tell the Data Protection Officer.

Management and Responsibilities

Our organisation comes into contact with Personal Data in four ways:

- In some cases, we host software holding Personal Data on behalf of our clients. In this case, we are the Data Processor.
- In some cases, we simply supply the software to our clients who either host the software themselves or contract its hosting with a 3rd party. In such cases, we are neither a Data Processor nor a Data Controller. However, we need to support our customers in complying with the Legislation.
- Occasionally, in order to investigate issues arising with our software we need to bring databases into our IT environment for a support engineer or developer to work on. If these databases have not been anonymised, then we are the Data Processor.
- We have a number of internal systems that we use to manage our business (Finance, HR, Payroll). Some of these systems are maintained by our parent company, Volaris, others by our organisation directly. We are always the Data Controller in such systems but may also be the Data Processor.

Ultimately, the relevant Portfolio Leader is responsible for implementation of this policy and the implementation of security controls in accordance with the Legislation.

Portfolio Leaders

The Portfolio Leaders have responsibility for implementing the Data Protection policy. The Portfolio Leader sets the overall policy framework within which our organisation complies with the principles of the Legislation. Specifically, the Portfolio Leader will:

- Appoint a Data Protection Officer (DPO) with specific responsibility for data protection issues.
- Ensure that an overall Data Protection Policy exists and is implemented for each Portfolio that is consistent with the Legislation.
- Act as an escalation point when the DPO finds that Business Units (see also section 0) are not taking effective corrective action to remedy any

© May 2, 2023 AssetWorks Inc. | All Rights Reserved | www.assetworks.co.uk
© May 2, 2023 Trapeze Software ULC. | All Rights Reserved | www.trapezegroup.com

deficiencies in compliance.
- Ensure that the Policy is reviewed at intervals not exceeding 12 months.

Data Protection Officer

The Portfolio Leader delegates the implementation and operational management of the Data Protection policy to the Data Protection Officer (DPO). For questions of data protection, the DPO reports directly to the Portfolio Leader and informs the IT Manager who covers line management and security responsibilities.

The DPO role includes the following responsibilities defined within the Legislation:

- To inform and advise employees about their obligations to comply with the Legislation;
- To monitor compliance with the Legislation and other appropriate laws, and with this data protection policy, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits;
- To advise on, and to monitor, Data Protection Impact Assessments;
- To cooperate with the supervisory authority (specifically the ICO); and
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.).

Specifically, the DPO will:

- Ensure that the Data Protection Audit System is established, implemented and maintained.
- Perform the necessary registration of our organisation with the Information Commissioner as a processor of Personal Data
- Audit the Register of Processing Activities (RoPA) to ensure all Personal Data and Special Category Data processed by the organisation is done so in compliance with the Legislation. Note, that the RoPA is also referred to as the Data Protection Register.
- Identify the legislative requirements that are applicable to the data protection aspects of the business activities, products or services.
- Report to the Portfolio Leader and ICT Manager on compliance.
- Coordinate Data Subject Access Requests in line with the Legislation.

Business Unit Directors

Our organisation is divided into a number of Volaris/Vertical Business Units (VBUs) with specific market focus (for example, commercial bus operators). All clients and products have a ‘home’ VBU. The Business Unit Director is responsible for ensuring that all activities associated with the VBU’s clients fully comply with this policy, and that the VBU’s products are implemented in a way so that the organisation and its clients can comply with the Legislation when using the product. Specifically, the Business Unit Director will:

- Ensure that the VBU’s products are managed in a way that ensures their usage can be compliant with the Legislation.

© May 2, 2023 AssetWorks Inc. | All Rights Reserved | www.assetworks.co.uk
© May 2, 2023 Trapeze Software ULC. | All Rights Reserved | www.trapezegroup.com

- Ensure that when acting as a data processor, VBU staff fully comply with this policy.
- Ensure that the data protection principles are regularly enforced, and management awareness levels remain high.
- If issues are reported by the DPO or ICT Manager to the Business Unit Director, ensure these are dealt with in a timely and efficient manner.
- Acknowledge compliance with this policy or raise any non-compliances – to be minuted at the quarterly Governance Meetings
- Lead by example.

Inform the Portfolio Leader, Data Protection Officer and ICT Manager of any reported breach of the Policy in line with the Major Incident Procedure.

Project Managers / System Owners

Personal Data may be held within a system as part of normal operation (e.g. personnel files or sales contact databases). In this case, a System Owner needs to be identified by the Business Unit Director who takes responsibility for ensuring compliance with this policy.

Alternatively, the organisation may need to process Personal Data on systems as part of fulfilling a client delivery contract. In this case, the Project Manager takes responsibility for ensuring that the organisation complies with this policy. The Project Manager may, in some cases be, for example, the Service Desk Analyst, Account Manager or another employee.

In both cases this includes:

- Informing the Data Protection Officer that they are processing Personal Data via the Data Protection Register for example https://jet.trapezegroup.co.uk/users/sign_in.
- Ensuring that data is deleted once no longer required (wherever hard copy documents are involved, the term ‘delete’ or similar in this document shall mean shred).
- Ensuring that ICT is made aware of hardware that has held Personal Data and is no longer required.
- Flagging any issues arising from implementing this policy to the Data Protection Officer.
- Communicating any relevant information to customers, suppliers and sub- contractors.
- Agreeing with the client how they will supply Personal Data of a Special Category to our organisation – see Appendix 3a
- Subcontractors ‘processing/handling’ Personal Data are deemed Sub- Processors under the Legislation. We have an obligation to obtain the consent of the Data Controller if we use a Sub-Processor, and a written contract allowing this needs to be in place.
- Ensuring that all team members are fully aware of the agreed methods of data supply.
- Leading by example.

© May 2, 2023 AssetWorks Inc. | All Rights Reserved | www.assetworks.co.uk
© May 2, 2023 Trapeze Software ULC. | All Rights Reserved | www.trapezegroup.com

Employees

All Employees are responsible for operating in line with this policy, specifically;

- They must ensure that all Personal Data provided to the organisation is accurate and updated where appropriate.
- Inform the Data Protection Officer that they are processing clients' Personal Data via the Data Protection Register, for both soft and hard copy.
- If they intend to store Personal Data for the first time, they must inform their Business Unit Director and obtain authorisation to do so.
- Datasets that may contain any Special Categories of Personal Data should only be stored on a laptop as a last resort. The laptop must be compliant with the rules of the Red Group (see section 7.1.1 Classification of Devices into Groups). Holding such data requires the written permission of the VBU Director.
- If the role requires working with customer data, then any employee shall only store a maximum of two customer datasets that include Special Categories of Personal Data on their laptop at any one time. If there is an urgent operational need to store more than two, then they must request authorisation from their Business Unit Director and the Data Protection Officer must be informed.
- If you intend to pass some Personal Data to another employee, you must state that this is Personal Data and must be stored and handled in accordance with this Policy.
- All Employees must ensure that they are familiar with the procedure for maintaining the relevant Data Protection Register [DP 1] – see Appendix 1.
- All Employees must ensure that any files containing Personal Data, including those relating to staff, are deleted as soon as they are no longer needed, for example, any screenshots held in the Call Logging system that contain client personal data should be deleted as soon as the case is closed. Unless strictly necessary, any screenshots should have personal data blanked before upload.
- Any employee who comes into possession of Personal Data unintentionally must inform their Line Manager.
- Any employee who becomes aware of any client, other employee or another party who is behaving in contravention of this policy, must inform their Line Manager. This would include, for example, receiving unencrypted Personal Data from a client – see Appendix 3d.
- In the event of a breach of this Policy, or if the security of any Personal Data is breached, an employee must inform their respective Line Manager, Business Unit Director & ICT immediately, even if out of hours. Failing that, they should attempt to contact the Portfolio Director or Data Protection Officer by phone or Teams app.
- In the event of receiving a supply of Personal Data in a format that does not comply with our protocols, to notify the client as per Notification to Client on receipt of Personal Data without adequate protection – see Appendix 3

© May 2, 2023 AssetWorks Inc. | All Rights Reserved | www.assetworks.co.uk
© May 2, 2023 Trapeze Software ULC. | All Rights Reserved | www.trapezegroup.com

In order to ensure that staff are familiar with their responsibilities under GDPR and ISO27001 the company has created an on-line training tool, which includes a test. Staff are required to undertake on-line training at least once per half year.

Compliance will be monitored by the DPO. Any non-compliance will be reported by the DPO to the appropriate Business Unit Director.

Information Classification

In order to ensure data is adequately protected, it is important that the sensitivity of the data is understood. To this end, the organisation operates a three-level information classification:

- Unmarked – this is the lowest level of Information Classification. Any information not explicitly identified as a higher level is considered unmarked. Any data that is, or will end up, in the public domain is unmarked.

- Sensitive – any data that is either Personal Data or is Commercially Sensitive (i.e., the release would cause harm or embarrassment to a customer or to the organisation) is in this category. Such data to be recorded in the Data Protection Register if it is client related.

- Special Category – any data that is defined as Special Category within the definition of the Act.

DATA PROTECTION PROCESSES & PRIVACY NOTICE

Management Process

Planning and Implementation

The Legislation requires that the risk associated with unlawful disclosure of personal information is assessed. Therefore, the 'Planning and Implementation' process is centred on ensuring that these risk assessments happen at least annually. Our preferred mechanism for these risk assessments is the Data Privacy Impact Assessment (PIA).

The Data Protection Officer will ensure:

- That a PIA is completed for all new developments that process personal information.
- That for all products and systems that process Personal Data the PIA is reviewed at least annually. Where relevant, the DPO will coordinate actions required to mitigate new risks identified through the PIA process. The DPO will provide a report at the quarterly Executive Meeting on progress of actions raised through PIAs.
- That suitable training mechanisms are in place to ensure that all staff refresh their knowledge on the Legislation and this policy at least once every half year.

© May 2, 2023 AssetWorks Inc. | All Rights Reserved | www.assetworks.co.uk
© May 2, 2023 Trapeze Software ULC. | All Rights Reserved | www.trapezegroup.com

- Ensure that this policy is reviewed at least annually and kept in line with evolving case law and best practice for the Legislation.

Reviews and Audits

The DPO will undertake the following audits:

- Monthly audit to confirm that the data protection register is being updated in a timely fashion, and that databases are not held longer than required. Any identified issues are to be escalated to the relevant Business Unit Director. If then not followed up, they are to be escalated to the IT Manager and Portfolio Leader.
- Quarterly audit to confirm that actions from PIAs are being followed up. Any identified issues to be escalated to the relevant Business Unit Director. If then not followed up, to be escalated to the IT Manager and relevant Portfolio Leader.
- Audit to confirm that staff are remaining familiar with this policy. Escalate any identified issues to the relevant Business Unit Director.
- The product leads will audit product developments to ensure that new software is complying with 'secure-by-design'.

Reports

The Data Protection Officer will produce a report at least quarterly to the Executive Team on the effectiveness of this policy.

Subject Access Requests

The Data Protection Officer will coordinate any Subject Access Requests to be carried out in line with the SAR procedure.

Employee involvement

Suitable training will be provided to all staff on this policy and their responsibilities at ensuring that our organisation complies with the Legislation.

Data Privacy Impact Assessments

The results of any PIAs are formally presented to the senior management team and the resulting actions agreed.

All PIAs are located on the relevant business document management system.

Client Projects

Note that the following procedure only applies if the client project involves processing Personal Data.

The Project Manager may in some cases be, for example, the Service Desk Team Lead, Account Manager or another employee.

© May 2, 2023 AssetWorks Inc. | All Rights Reserved | www.assetworks.co.uk
© May 2, 2023 Trapeze Software ULC. | All Rights Reserved | www.trapezegroup.com

Project Initiation

During project initiation the Project Manager is responsible for:

- Discussing with the client any special requirements the client organisation may have regarding data security and document management. These need to be agreed in writing between the client and the project manager.
- Agreeing with the client how they will supply Personal Data to our organisation – see Appendix 3
- Ensuring the client has been sent a copy of the Data Protection Policy along with the covering note – see Appendix 3
- Ensuring that the team are aware of their responsibilities under this policy and any additional requirements agreed with the client. Any additional security requirements must be communicated to the team in writing. The Project Manager must ensure that a Project Data Protection Requirements Record is completed to show that the team has read and understood the requirements. (See Appendix 2). Until the additional security requirements are known, the Project Data Protection Requirements Record cannot be completed and therefore there should be no transfer of data.
- Ensuring that team members have adequate technical resources to fulfil their project responsibilities while complying with this policy (e.g. laptop has hard disk encryption, staff have been issued with a USB encrypting key, staff have access to secure server).

Project Delivery

During project delivery the Project Manager and the Project Team are responsible for:

- Ensuring that all Personal Data received from a client has been received in encrypted form.
- Ensuring that all Personal Data provided to clients by email, other file transfer over the internet, or transferred using media, is encrypted in line with current guidance provided by the ICT Department. ICT will provide the current company standard software for this purpose.
- All data being processed on either one of the organisation's secure servers or a laptop with encrypted hard drive.
- Ensuring that any new databases received from the client or created by the organisation for the project are registered on the Data Protection Register.
- Where another employee becomes involved with the Project part way through, the Project Manager must ensure that the Project Data Protection Requirements Record is completed to show that the team member has read and understood the requirements. (See Appendix 2)

© May 2, 2023 AssetWorks Inc. | All Rights Reserved | www.assetworks.co.uk
© May 2, 2023 Trapeze Software ULC. | All Rights Reserved | www.trapezegroup.com

Project Closedown

As part of project closedown, the Project Manager is responsible for:

- Ensuring that all Personal Data held on laptops or other means of storage, including printouts, during the project, has been removed and/or destroyed. This should take the form of a written instruction via email to the relevant team members. Team members will confirm that the relevant databases have been deleted and that the Data Protection Register has been updated accordingly by signing and dating the Project Data Protection Requirements Record. The Project Manager ensures all entries are completed before closing the project.
- Ensuring that once the data has been removed, they inform the Data Protection Officer that the respective entries in the Data Protection Register can now be archived as they have added a deletion date.

Employee Leaving Mid Project

As part of the staff leaving process, the HR Director is responsible for ensuring that the Line Manager has asked the employee to confirm that:

- All Personal Data of which they are the Controller has been deleted or has been transferred and accepted by another staff member.
- The employee has signed the Project Data Protection Requirements Record for each project in which they are involved, confirming deletion of all Personal Data for which they are the Data Controller.

Personal Data of Staff

We may collect, store, and use the following categories of personal information about you:

1. Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses
2. Date of birth
3. Gender
4. Marital status and dependents
5. Next of kin and emergency contact information
6. National Insurance number
7. Bank account details, payroll records and tax status information
8. Salary, annual leave, pension and benefits information
9. Start date
10. Location of employment or workplace
11. Copy of driving licence and / or other photographic ID such as a passport
12. Recruitment information (including copies of right to work documentation, references, interview notes and opinions taken during and following interviews and other information included in a CV or cover letter or as part of the application process)
13. Employment records (including job titles, work history, working

© May 2, 2023 AssetWorks Inc. | All Rights Reserved | www.assetworks.co.uk
© May 2, 2023 Trapeze Software ULC. | All Rights Reserved | www.trapezegroup.com

hours, training records and professional memberships)
14. Any test results, psychometric or other, included in the recruitment process
15. Compensation history
16. Performance information
17. Disciplinary and grievance information
18. Data about your use of our information and communications systems including internet access
19. CCTV footage and other information obtained through electronic means such as swipecard records
20. Photographs

We may also collect, store and use the following "special categories" of more sensitive personal information:

21. Information about your health, including any medical condition, health and sickness records.

How your Personal Information is collected

We typically collect personal information about employees, workers and contactors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies.

We will collect additional personal information in the course of job-related activities throughout the period of you working for us. This will usually be directly from you but may be from third parties such as medical practitioners.
Some data is automatically logged via various system and security tools, including but not limited to internet usage, access, and software changes.

How we will use the information about you

We need all the categories of information in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal and security obligations. In some cases, we may use your personal information to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests. The situations in which we will process your personal information are listed below:

1. Making a decision about your recruitment or appointment
2. Determining the terms on which you work for us
3. Checking you are legally entitled to work in the UK
4. Paying you and, if you are an employee, deducting tax and National Insurance contributions
5. Providing the following benefits to you:
6. Healthcare
7. Sick Pay

© May 2, 2023 AssetWorks Inc. | All Rights Reserved | www.assetworks.co.uk
© May 2, 2023 Trapeze Software ULC. | All Rights Reserved | www.trapezegroup.com

8. Death in service
9. Pension
10. Childcare vouchers
11. Liaising with your pension provider
12. Administering the contract we have entered into with you
13. Business management and planning, including accounting and auditing
14. Conducting performance reviews, managing performance and determining performance requirements
15. Making decisions about salary reviews and compensation
16. Assessing qualifications for a particular job or task, including decisions about promotions
17. Gathering evidence for possible grievance or disciplinary hearings
18. Making decisions about your continued employment or engagement
19. Making arrangements for the termination of our working relationship
20. Education, training and development requirements
21. Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work
22. Ascertaining your fitness to work
23. Managing sickness absence
24. Complying with health and safety obligations
25. To monitor your use of our information and communication systems to ensure compliance with our IT policies and security obligations to protect the business and yourself.

We run daily checks at a high level, but we don't monitor an individual's usage and internet access unless alerted by security tools or specifically asked to by HR and the individual's line manager. Any such access must be authorised by the ICT lead.

26. To ensure network and information security, including preventing unauthorised access to our computer and electronic communication systems and preventing malicious software distribution.
27. Contracts may require us to share anonymised details of ethnicity.

Please note this is not an exhaustive list and some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information. The majority of the above types of processing will be justified on the basis of being necessary to perform a contract and / or so that we comply with a legal obligation. A few will be justified on the basis of legitimate interests.

In terms of the legitimate interests of our organisation or of third parties, these legitimate interests will be:

- To enable us to deal with and defend and dispute or legal proceedings

We may also use your personal information in the following situations, which are likely to be rare:

- Where we need to protect your interests (or someone else's interests).
- Where it is needed in the public interest or for official purposes.

© May 2, 2023 AssetWorks Inc. | All Rights Reserved | www.assetworks.co.uk
© May 2, 2023 Trapeze Software ULC. | All Rights Reserved | www.trapezegroup.com

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

How we use particularly sensitive information

"Special categories" of particularly sensitive personal information require higher levels of protection.

We need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the following circumstances:

1. In limited circumstances, with your explicit written consent.
2. Where we need to carry out our legal obligations and in line with our data protection policy.
3. Where it is needed in the public interest, such as for equal opportunities monitoring, and in line with our data protection policy.
4. Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards;
5. Where it is necessary for establishing, exercising or defending legal claims;

Less commonly, we may process this type of information where it is to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We will use your particularly sensitive personal information in the following ways:

1. We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws.
2. We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits.
3. We may use information about ethnic origin, to ensure meaningful equal opportunity monitoring and reporting.
4. We may obtain your biometric data as part of our recruitment process so as to comply with right to work checks.
5. We may use all special categories of data to defend legal claims.

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations

© May 2, 2023 AssetWorks Inc. | All Rights Reserved | www.assetworks.co.uk
© May 2, 2023 Trapeze Software ULC. | All Rights Reserved | www.trapezegroup.com

or exercise specific rights in the field of employment law, for example, to ensure we provide you with a safe place of work or to consider making reasonable adjustments. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Information about criminal convictions

We do not envisage that we will hold information about criminal convictions.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so.

Automated decision-making

Automated decision-making takes place when an electronic system uses personal information to decide without human intervention.

We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

If we make an automated decision based on any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights.

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making unless we have a lawful basis for doing so and we have notified you.

Data sharing

Some of our systems are run by our parent company and store data outside the EEA, i.e., USA and Canada. The European Commission has ruled that Data Protection is adequate in these countries. As at March 2021, the countries with adequate data protection provision included:

- The European Economic Area (EEA) countries.
    - These are the EU member states and the EFTA States.
      The EU member states are Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden.
    - The EFTA states are Iceland, Norway and Liechtenstein.
    - EU or EEA institutions, bodies, offices or agencies
- Gibraltar.
- Countries, territories and sectors covered by the European Commission's adequacy decisions (in force at 31 December 2020)

© May 2, 2023 AssetWorks Inc. | All Rights Reserved | www.assetworks.co.uk
© May 2, 2023 Trapeze Software ULC. | All Rights Reserved | www.trapezegroup.com

- These include a full finding of adequacy about the following countries and territories:
  - Andorra, Argentina, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay.
- In addition, the partial findings of adequacy about:
  - Japan – only covers private sector organisations.
  - Canada - only covers data that is subject to Canada's Personal Information Protection and Electronic Documents Act (PIPEDA). Not all data is subject to PIPEDA. For more details please see the EU Commission's FAQs on the adequacy finding on the Canadian PIPEDA.

We may share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

"Third parties" includes third-party service providers (including contractors and designated agents) and other entities within our group. The following activities are carried out by third-party service providers: payroll, pension administration, benefits provision and administration.

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

We will share your personal information with other entities in our group as part of our regular reporting activities on company performance, in the context of a business reorganisation or group restructuring exercise, for system maintenance support and hosting of data.

We may share your personal information with other third parties, for example in the context of the possible sale or restructuring of the business. We may also need to share your personal information with a regulator or to otherwise comply with the law.

We will transfer the personal information we collect about you to the following countries outside the UK: Canada & The USA in order to perform our contract with you. There are adequate safeguards to your data protection in relation to Canada and the USA. This means that the countries to which we transfer your data are deemed to provide an adequate level of protection for your personal information.

However, to ensure that your personal information does receive an adequate level of protection we have put in place the following appropriate measures to ensure that your personal information is treated by those third parties in a way that is consistent with and which respects the EU and UK laws on data protection:

- Minimisation of information stored: not collecting more than necessary and deleting anything no longer needed

© May 2, 2023 AssetWorks Inc. | All Rights Reserved | www.assetworks.co.uk
© May 2, 2023 Trapeze Software ULC. | All Rights Reserved | www.trapezegroup.com

- Data held entirely within the Volaris Group
- Secure transfer of data
- Oversight by Volaris Data Security
- Regular audits of Personal Data held

If you require further information about these protective measures, you can request it from the Data Protection Officer.

Your Rights

As with all your Personal Data, wherever it is held, the Legislation provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- rights in relation to automated decision making and profiling.

See https://ico.org.uk/your-data-matters/ for further details.

Right to withdraw consent

In some circumstances you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose. You have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Data Protection Officer. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

If you have questions or complaints

The Data Protection Officer is responsible for overseeing our compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact the Data Protection Officer. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

© May 2, 2023 AssetWorks Inc. | All Rights Reserved | www.assetworks.co.uk
© May 2, 2023 Trapeze Software ULC. | All Rights Reserved | www.trapezegroup.com

SUPPORTING PROCESSES AND POLICIES

Holding of Personal Data on Laptops /PCs

Classification of Devices into Groups

Our organisation has simplified classification into one group whereby all staff laptops are protected by two-form factor encryption irrespective of whether they need to hold Special Categories of Personal Data and/or hold Personal Data. Details of how the laptops are protected can be found in the Information Security Policy.

Transmitting Personal Data

Staff must use secure, encrypted communications channels (e.g. Filecloud, Secure FTP, Azure Storage Explorer or a VPN connection) to send and receive any Personal Data, unless portable media is unavoidable.

The use of USB pen drives, CD-ROMs, etc. should be avoided unless absolutely necessary. If used, the data must be held in encrypted form on the media, and the files removed as soon as the transfer is complete.

Data Breaches

The Data Protection Officer will investigate any incidents should a breach occur and ensure lessons are learnt.

If a breach of Personal Data has occurred, the organisation then needs to consider whether this poses a risk to people. We need to consider the likelihood and
severity of any risk to people's rights and freedoms, following the breach. When we've made this assessment, if it's likely there will be a risk then we must notify the ICO. If it's unlikely then you don't have to report it. You do not need to report every breach to the ICO. However, if the incident is notifiable to the ICO, we will invoke the Major Incident Procedure.

Security Measures for Staff

Depending on the type of work carried out, it is important that employees are aware that they could be criminally liable if they knowingly or recklessly disclose personal information in breach of this policy and, as a minimum, serious breaches of the policy will be regarded as a disciplinary matter.

If employees are required as part of their job to process Personal Data about other staff, customers or customer data, they will receive specific training and guidance on the security of data to ensure that all data is processed fairly and lawfully. This will include any separate rules or guidelines governing, for example, the retention, storage and destruction of records.

During the recruitment process, if employees are to be working with client Personal Data, their references will be checked with previous employers. This

© May 2, 2023 AssetWorks Inc. | All Rights Reserved | www.assetworks.co.uk
© May 2, 2023 Trapeze Software ULC. | All Rights Reserved | www.trapezegroup.com

check will include confirmation that the employer is not aware of any criminal convictions not considered spent under the Rehabilitation of Offenders Act.

Confidentiality and security are both covered within the Staff Handbook supplied to all employees.

Retention Policy

There needs to be a balance between keeping data for as long as is useful and minimising our holding of Personal Data.

Retention periods for files should strike this balance. The following periods are to be used as guide to how long to retain some files:

Record Type	Retention Period	Storage Media / Location
Leavers' Personal Data	6 years after leave date	Secure server
Customers' data used for support purposes	Default 1 month	Secure server / Red Group
Financial Data on Staff	6 years after leave date	Secure server
Leave / Absence / Sickness Data on staff	6 years after leave date	Cascade / Workday
Accounting Data	No limit	Secure server
Customer Data	Default one month	Secure server
Customer Contracts	No limit	Secure server

Once the retention period has passed and there is no further need for the data, ensure permanent deletion, taking care not to retain in recycle bins, on external hard drives or other backup media.

In some instances, this Data Retention Policy may be suspended, specifically if an investigation, litigation, or audit is anticipated. In some instances, this policy's disposal schedule may conflict with the need to produce documents relevant to the legal or regulatory procedures. If this is the case, then the need to comply fully with the law and/or regulation will override this policy, causing this policy to be suspended until the matter in question is satisfactorily resolved. Suspension of this policy will take the form of no business documents being disposed of whatsoever for a period.

Violations of this policy will be treated like other allegations of wrongdoing at our organisation. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

- Disciplinary action according to applicable policies;
- Termination of employment; and/or
- Legal action according to applicable laws and contractual agreements.

© May 2, 2023 AssetWorks Inc. | All Rights Reserved | www.assetworks.co.uk
© May 2, 2023 Trapeze Software ULC. | All Rights Reserved | www.trapezegroup.com

APPENDIX 1: DP 1 - MAINTAINING THE DATA PROTECTION REGISTER

Scope & Objectives	To ensure that client and organisational Personal Data is handled in a responsible manner, adhering to the principles stated in this Data Protection Policy
Responsibility	Portfolio Leader
Owner	Data Protection Officer
References	EU General Data Protection Regulations (2016/679) This Data Protection Policy

Procedure

Broadly, the Legislation covers any information that relates to living individuals which is held on computer (or any "filing system"). For example, this may include information such as name, address, date of birth and opinions about the individual or any other information from which the individual can be identified.

Before accepting client Personal Data, members of staff have justified the need for having this information by being able to answer yes to the following questions:

- Do I really need this information about an individual?
- Do I know what I'm going to use it for?

Once an employee comes into possession of client Personal Data, it is recorded in the Data Register, for example https://jet.trapezegroup.co.uk/users/sign_in

The majority of data supplied is in electronic form. However, if hard copies have been supplied or produced from the data, this will also be recorded in the Data Protection Register.

If the data supplied has screen shots that include Personal Data, or the information is included within a video capture of a WebEx session, this should also be entered into the Data Protection Register and adequate protection applied i.e. encrypted.

The Data Protection Register provides a record of all client Personal Data that we have in the organisation at any point in time. Therefore, all efforts are made to keep the Data Protection Register up to date and accurate.

Each data supply has a "Data Owner", a member of staff who is responsible for care of this data. This person has been able to answer yes to the following questions:

- Am I satisfied the information is being held securely?
- Is the information accurate and up-to-date for the purpose?
- Do I know who will be able to see the personal information?

Each data supply has its own row, and clearly states where it has been stored, and what the information is to be used for. It also provides a record of expected

© May 2, 2023 AssetWorks Inc. | All Rights Reserved | www.assetworks.co.uk
© May 2, 2023 Trapeze Software ULC. | All Rights Reserved | www.trapezegroup.com

and actual deletion date. If an employee creates a copy of a file, this is a new data supply and that employee is responsible for recording it.

If there is a requirement to copy the data onto another location, then this data will be entered on a separate row.

If the data is to be used by another member of staff, then this is recorded as a separate entry by that staff member.

Where a subcontractor is provided with client Personal Data, it is the responsibility of the relevant manager to record any data they hold on behalf of our organisation in the Data Protection Register and verify and record its eventual deletion.

Subcontractors 'processing/handling' Personal Data are deemed Sub-Processors under the Legislation. We have an obligation under the Legislation to obtain the consent of the Controller if we use a Sub-Processor. This is the responsibility of the relevant Project Manager.

The Data Protection Register is reviewed by each Data Owner on a monthly basis to ensure that all records exist and are still required, and the review date is recorded
in "Reviewed".

In addition, the Data Protection Officer reviews the Data Protection Registers each quarter, highlighting the 'Expected Deletion Dates' which have passed, to the Data Owner and Functional Area Manager. The review date is recorded in the Data Protection Register.

The Data Protection Officer will flag all items that have an "Actual Deletion Date" entry with an "Archive" status. Any records over five years old can be deleted from the register.

APPENDIX 2: PROJECT DATA PROTECTION REQUIREMENTS

Project Name:			
Customer/Sponsor			
Customer authorisation	*Name of person who authorised the transfer of data on the client side.*		
Date of Project Initiation:		**Project Number:**	
Date of project closure notification.			

© May 2, 2023 AssetWorks Inc. | All Rights Reserved | www.assetworks.co.uk
© May 2, 2023 Trapeze Software ULC. | All Rights Reserved | www.trapezegroup.com

Overview	*[Summary of the project with details of the expected data that contains client personal information.* *This form records the fact that every member of the project team is aware of that policy and that it applies to this project as the handling of personal data is involved.* *This is not a record of agreement between Trapeze and the customer.* *If it is the case that no customer personal data is involved, then there is no need for this form.*
Additional data security requirements	*[We have our agreed company communication requirements as per our current DP Policy.* *However, in the circumstances whereby there has been an agreed "alternative" means of communication with the customer, detail any special requirements the client organisation may have regarding data security and document management and any specific actions taken by Trapeze to ensure that they are being met.* *If there are none then state "None specified"]*

When you receive this document by email at project initiation, please reply to the email with "**Read and Understood**" which will then be regarded as your dated signature.

When you are emailed the form again with notification of project closure, please reply to the email with "**Data deleted & Data Register amended**" once you have undertaken this action, which again will be regarded as your dated signature.

Name	**Job Title**	**Dated Signature** (To denote they have read and understood the above requirements)	**Dated Signature** (Confirming all project related data has been deleted and the appropriate entries removed from the Data Register).
	Project Manager	**Date:**	**Date:**
		Date:	**Date:**
		Date:	**Date:**

© May 2, 2023 AssetWorks Inc. | All Rights Reserved | www.assetworks.co.uk
© May 2, 2023 Trapeze Software ULC. | All Rights Reserved | www.trapezegroup.com

APPENDIX 3: CUSTOMER COMMUNICATION GUIDELINES

How to supply Personal Data to our Organisation

Whenever we begin working with a new client, there is a need to ensure that adequate data processing and transfer protocols are in place. This is normally part of the Data Processing Agreement that should be part of any client contract involving Personal Data processing.

Apart from agreeing in writing any special requirements the client may have regarding data security and document management, the following statement may be sent:

"Due to the requirement to be able to send data to our organisation that may contain personal information that is governed by the General Data Protection Regulations (GDPR), we would request that where data needs to be transferred, the data is anonymised before being sent. If this is not possible, then all transfer of data should have adequate protection applied.

Our organisation does not provide consultancy as to what constitutes adequate protection but are willing to provide our Data Protection Policy if requested, which provides information as to the measures we take.

We do not accept responsibility for any data provided to the company without adequate protection, but should we receive any information that is deemed not to be adequately protected, we shall notify the client by email for them to take appropriate measures. The data received by us will then have adequate protection applied.

Therefore, please notify us as to how you will be transferring data, what protection we can expect, and a contact email address should we wish to notify you."

The response to the above is added to Project Data Protection Requirements – Appendix 2 during project initiation.

At Project Initiation

Ensuring the client has been sent a copy of the Data Protection Policy, along with the following covering note:

"Please find our Data Protection Policy attached which documents the approach we will be taking to protect your data. Could you please confirm receipt of this policy? If you should have any special requirements beyond those listed in the document, could you please let me know."

When the client is unable to supply the personal data to our standards

There will be occasions when the client cannot supply the information to what we deem as adequate standards but in order to continue working, the following notification is to be sent at project initiation in order to minimise our responsibility:

© May 2, 2023 AssetWorks Inc. | All Rights Reserved | www.assetworks.co.uk
© May 2, 2023 Trapeze Software ULC. | All Rights Reserved | www.trapezegroup.com

"We do not believe that the protection afforded the data that you supply to us is adequate to comply with the Data Protection Act.

However, we shall continue to receive the data and apply adequate protection on receipt, but we bear no responsibility for the security of the data prior to taking receipt."

Notification to client on receipt of personal data without adequate protection

Whenever we are supplied with Personal Data that is not by the agreed method and does not have the adequate protection in place, we have a duty to notify the sender at the earliest opportunity.

The notification will always be by email, regardless as to whether the data was sent by email, FTP, Fax, post or hand delivered. The Data Protection Officer should also be informed.

The following message is to be completed and sent to the client to the agreed address:

"This is to notify you that our organisation has received information itemised below, that contains Personal Data which is governed by the Data Protection Act legislation, but has been deemed as not being transferred with adequate protection. The data held by us has now had adequate protection applied and/or has been deleted from mailboxes."

Description of data: (to complete)

Data received by: (email /FTP/Fax/CD/Other Hardware)*

Date received: (to complete)

** Delete as appropriate*

However, we shall continue to receive the data and apply adequate protection on receipt but bear no responsibility for the security of the data prior to taking receipt."

© May 2, 2023 AssetWorks Inc. | All Rights Reserved | www.assetworks.co.uk
© May 2, 2023 Trapeze Software ULC. | All Rights Reserved | www.trapezegroup.com