

Uncontrolled copy when printed

Title	Privacy Policy & Data Processing Statement
Document Number	SoVIT – Privacy Policy & Data Processing Statement
Author	Alex Wellings
Owner	Operations Director
Email	Alex.wellings@sovisionit.com
Version Date	24 May 2018
Amendment Record	Issue 3

Overview

Personal data is data which by itself or with other data available can be used to identify individuals. We are soVision IT Ltd, your data processor. This data protection statement sets out what we do with the information we collect and hold about you, how we keep it secure and your rights. You can contact our Head of Health & Safety Services at soVision IT, Avon House, Avon Mill Lane, Keynsham, Bristol, BS31 2UG if you have any questions.

The types of personal data soVision IT collect and use

soVision IT will use your personal data for the reasons set out below and if you become or are an existing customer we will use it to manage your account, and the service we provide to you. We will collect most of the personal data we require **directly** during service onboarding or registration, however other data may be **indirectly** collected over the life of any service, contract or course. The personal data we collect may include:

- Full name and personal details including contact information (e.g. email address, home and mobile telephone numbers);
- Financial details (e.g. bank details);
- Records of products and services used and how they have been used;
- Information from credit reference or fraud prevention agencies, court records of debt judgements and bankruptcies and other publicly available sources;

Providing your personal data

soVision IT will inform you if providing some personal data is optional, however we generally do not collect extraneous information. In all other cases you must provide personal data so that soVision IT can fulfil our contractual obligations to you (unless you're already our customer and we legitimately hold your details on record).

Using your personal data: the legal basis and purposes

soVision IT will process your personal data:

1. As necessary to **perform our contract with you** for relevant services:
 - a. To decide whether to enter into it;
 - b. To manage and perform that contract; and
 - c. To update our records.
2. As necessary **for our own legitimate interests**, e.g.:
 - a. To send you marketing communications.
3. As necessary **to comply with a legal obligation**, e.g.:
 - a. When you exercise your rights under data protection law and make requests;
 - b. For compliance with legal and regulatory requirements and related disclosures;
 - c. For establishment and defence of legal rights;
 - d. For activities relating to the prevention, detection and investigation of crime;
4. Based on **your consent**, e.g.:
 - a. When you request us to disclose your personal data to other people or organisations such as a company handling another service you use, or otherwise agree to disclosure;
 - b. To send you marketing communications where we have asked for your consent to do so.

You are free at any time to change your mind and withdraw your consent. The consequence of this may be that we cannot perform certain contractual functions, or do certain things for you.

Sharing of your personal data

Subject to applicable data protection law, we may share your personal data with:

- Sub-contractors, sub-processors and other persons who help provide our products and services;
- Government bodies and agencies in the UK where the law requires;



Uncontrolled copy when printed

- Courts, to comply with legal requirements, and for the administration of justice;
- In an emergency, or to otherwise protect your vital interests;
- To protect the security or integrity of our business operations;
- When we restructure or sell our business or its assets, or have a merger or re-organisation;
- Market research organisations who help improve our products or services; and
- Anyone else where we have your consent, or as required by law.

International transfers

Wherever possible soVision IT select service providers and sub-processors who hold data within the UK and the European Economic Area (EEA) to ensure data protection compliance to the highest standards.

If data is transferred outside of the UK or EEA during processing activities for any reason, we will take steps to ensure any sub-processors are compliant with our high data protection standards. These steps include imposing contractual obligations of adequacy, or requiring the certification of compliance with the UK data protection framework.

soVision IT website

You can access parts of soVision IT's website without using any registration process or providing any personal information. For parts that do require registration, during the user registration process, we will collect certain information that we need to provide you with services.

The mandatory information we require at this stage will be your name, a telephone number and an email address. We may ask for other details, such as your organisation's name and address, but registration can be completed without providing these details. We will also collect personal information from you if you complete any other forms featured on this site or if you contact us requesting specific information or provide us with feedback. Financial information that is collected is used to verify, identity and to bill either you or your company for products and services, as applicable.

When you use soVision IT's website we automatically collect certain technical and routing information about your visit so we can continuously improve what and how the site delivers. For example, we may log the Internet Protocol (IP) address of your computer and measure your browsing patterns when on this site. This information is held in aggregate form and is not matched with your personal information so no individual user is identified.

Use of cookies

We use cookies to identify you when you visit soVision IT's website to build up a demographic profile. A cookie is a small piece of information sent to your web browser by a web server and can only be read by the server that gave it to you. It cannot be executed as code or used to deliver viruses to your computer.

Most browsers are initially set to accept cookies. You can set your browser to notify you when you receive a cookie, giving you the chance to decide whether to accept it.

Links

Our website contains articles with links to other sites. We are not responsible for the privacy policies or the content of such web sites.

If you have a question about the privacy policy of those web sites, please contact them directly.



Uncontrolled copy when printed

Public forums

You are advised that any information disclosed via discussion forums, message boards and/or news groups available on or via this site becomes public information and you should exercise caution when deciding to disclose your personal information.

What we do to protect your personal data

soVision IT ensures that, in respect of all personal data it receives from you or processes on your behalf, we maintain security measures to a standard appropriate to:

- The harm that might result from unlawful or unauthorised processing or accidental loss, damage, or destruction of the personal data; and
- The nature of the personal data.

soVision IT will:

- Ensure that appropriate security safeguards and virus protection are in place to protect the hardware and software which is used in processing the personal data in accordance with best industry practice;
- Prevent unauthorised access to personal data;
- Protect the personal data using pseudonymisation, where it is practical to do so;
- Ensure that its storage of personal data conforms with best industry practice such that the media on which personal data is recorded (including paper records and records stored electronically) are stored in secure locations and access by personnel to personal data is strictly monitored and controlled;
- Have secure methods in place for the transfer of personal data whether in physical form (for example, by using couriers rather than post) or electronic form (for example, by using encryption);
- Password protect all computers and other devices on which personal data is stored, ensuring that all passwords are secure, and that passwords are not shared under any circumstances;
- Take reasonable steps to ensure the reliability of personnel who have access to the personal data;
- Have a secure procedure for backing up all electronic personal data and storing back-ups separately from originals; and
- Have a secure method of disposal of unwanted personal data including for back-ups, disks, print-outs, and redundant equipment;

Criteria used to determine retention periods

The following criteria are used by soVision IT to determine data retention periods for your personal data:

- **Retention in case of queries about your account.** We will retain your personal data as long as necessary to deal with any queries - this period is usually two years after service termination;
- **Retention for contacting previous customers for marketing purposes.** We will retain some personal data after a contract or service with us has expired or been terminated. We use this information for marketing, and for contacting you to ensure things are going well with your new supplier - this period is two years after service termination;
- **Retention in case of claims or complaints.** We will retain your personal data if necessary to deal with any claims or complaints - this period is usually two years after service termination;
- **Retention in accordance with legal and regulatory requirements:** We will retain some personal data after your account or contract has been closed or has otherwise come to an end based on legal and regulatory requirements.

Your rights under UK data protection law

Your rights are as follows (noting that that these rights don't apply in all circumstances):

- The **right to be informed** about the processing of your personal data;



Uncontrolled copy when printed

- The right to **request access** to your personal data and details of how we process it;
- The right to have your personal data **corrected if it's inaccurate** and to have **incomplete personal data completed**;
- The right to **object** to processing of your personal data;
- The right to **restrict processing** of your personal data;
- The right to **have your personal data erased** (the “right to be forgotten”);
- The right to **move, copy or transfer your personal data** (“data portability”); and
- Rights in relation to **automated decision making** including profiling.

The right to be informed & the right to request access

You have the right to see what information we hold about you and/or how we process this information, subject to certain conditions.

If you want to exercise these rights, you should make an application to us in writing. We may ask you to provide us with sufficient information so that we can be sure of your identity. We also reserve the right to make a charge of a reasonable fee for providing you with the information you are requesting if a request is excessive or repetitive.

If you would like to proceed with a request to see what data we hold about you and/or how it is processed, please write to us at the address within the contact us section of this policy.

The right of rectification

You have a right to request the rectification of information we hold about you if it is inaccurate, subject to certain conditions.

If you want to exercise this right, you should make an application to us in writing. We may ask you to provide us with sufficient information so that we can be sure of your identity. This request will be actioned within one month, or up to two months if the request is complex in nature.

If action is not taken in response to a request for rectification, soVision IT will explain why this is the case. If you are unsatisfied with our response, you then have the right to complain to the supervisory authority and to a judicial remedy.

The right to object

Wherever possible, soVision IT will inform their customers and prospective customers of the right to object at the point of first communication. You have a right to object to the processing of some or all information we hold about you, subject to certain conditions, listed below.

Individuals have the right to object to:

- Processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority - including profiling
- Direct marketing - including profiling
- Processing for purposes of scientific/historical research and statistics.

soVision IT will stop processing personal information with immediate effect if the right to object is invoked unless:

- soVision IT can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.
- The processing is for the establishment, exercise or defence of legal claims.



Uncontrolled copy when printed

The right to restrict processing

You have a right to request the restriction of processing of some or all information we hold about you, subject to certain conditions, listed below:

- When an individual contests the accuracy of the personal data, the processing will be restricted until the accuracy of the personal data has been verified.
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and soVision IT is considering if legitimate grounds exist to override the request of the individual.
- When processing is unlawful and the individual opposes erasure and requests restriction instead.
- If soVision IT no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

If soVision IT have disclosed the personal data in question to third parties, we will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

The right of erasure

You have a right to request the erasure of some or all information we hold about you, subject to certain conditions, listed below:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (ie otherwise in breach of the GDPR).
- The personal data must be erased to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

If you would like to proceed with a request for the erasure of some or all of your data, please write to us at the address within the contact us section of this policy. In some circumstances, soVision IT may refuse to comply with the erasure request. This may be due to one or more of the following reasons:

- To exercise the right of freedom of expression and information;
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- For public health purposes in the public interest;
- Archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- The exercise or defence of legal claims.

The right to move, copy or transfer your personal data

You have a right to request the movement, copying or transfer of information we hold about you, subject to certain conditions.



Uncontrolled copy when printed

soVision IT will move, copy or transfer the data in a format reasonably requested. If the data requires hardware to be moved, copied or transferred, this must be provided.

If you want to exercise this right, you should make an application to us in writing. We may ask you to provide us with sufficient information so that we can be sure of your identity. This request will be actioned within one month, or up to two months if the request is complex in nature.

Automated decision making and processing

Automated decision making involves processing your personal data without human intervention. soVision IT do not undertake any automated decision making with our personal data.

Breach Management Identification and Classification

soVision IT have put in place procedures that will allow any staff member to report any information/data security breach.

- We ensure that all staff are aware to whom they should report such a breach.
- Having such a procedure in place will allow for early recognition of the breach so that it can be dealt with in the most appropriate manner.
- Details of the breach will be recorded accurately according to procedure, including the date and time the breach occurred, the date and time it was detected, who/what reported the breach, description of the breach, details of any ICT systems involved, corroborating material such as error messages, log files, etc.
- In this respect, staff are made fully aware as to what constitutes a breach. In respect of this policy a breach maybe defined as the unintentional release of customer confidential or personal information/data to unauthorised persons, either through the accidental disclosure, loss or theft of the information/data.

Containment and Recovery

Containment involves limiting the scope and impact of the breach of data/information. If a breach occurs, soVision IT will:

- Decide on who would take the lead in investigating the breach and ensure that the appropriate resources are made available for the investigation.
- Establish who in the affected organisation/s need to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise.
- Establish whether there is anything that can be done to recover losses and limit the damage the breach can cause.

Risk Assessment

In assessing the risk arising from any security breach, soVision IT will consider what would be the potential adverse consequences for individuals, i.e. how likely it is that adverse consequences will materialise and, in the event of materialising, how serious or substantial are they likely to be. In assessing the risk, the following points will be considered:

- What type of Information/data is involved?
- How sensitive is the information/data?
- Are there any security mechanism's in place (e.g. password, protected, encryption)?



Uncontrolled copy when printed

- What could the information/data tell a third party about the individual/s?
- How many individuals are affected by the breach?

Notification of Breaches

- All information/data breaches are reported to soVision IT's Operations Director.
- Where it is deemed the breach is likely to result in a high risk to individual's rights and freedoms, soVision IT will notify the Information Commissioners Office within 72 hours.
- Where it is deemed the breach is likely to result in a high risk to individual's rights and freedoms, soVision IT will notify the affected customer/s within 96 hours. This will include a copy of the completed security incident report if requested by the affected individuals.
- soVision IT document all breaches of information security, even if they don't all need to be reported.

Evaluation and Response

- After any information/data security breach a thorough internal review of the incident will occur. The purpose of this review is to ensure that the steps taken during the incident were appropriate and to identify areas that may need to be improved.
- Any recommended changes to policies and/or procedures will be documented and implemented as soon as possible thereafter.

Data anonymisation and aggregation

Your personal data may be converted into statistical or aggregated data which can't be used to identify you, and then used to produce statistical research and reports. This aggregated data may be shared and used in all the ways listed above in the document.

Email messages

We send regular updates by email to customers, website registered users and subscribers telling them about new products and services available from soVision IT.

If you do not wish to receive information about our products and services or the products and services offered by our affiliated organisations, please tick the appropriate box on the registration form or use the unsubscribe link we provide with all such communications at any time.

Contact Us

If you have any queries concerning this Privacy Policy, your personal information or any questions on our use of the information, please contact us:

Data Compliance,
soVision IT Ltd,
Avon House,
Avon Mill Lane,
Keynsham,
Bristol,
BS31 2UG
United Kingdom.

Complaints

You have the right to complain to the Information Commissioner's Office if you believe there has been misuse of your personal data. It has enforcement powers and can investigate compliance with data protection law: ico.org.uk.



Uncontrolled copy when printed

Policy Review

The Policy will be subject to review whenever any relevant technological or regulatory changes occur and will, as a minimum, be formally reviewed on an annual basis.

