0333 015 1920
office@survey7.co.uk

GDPR Policy

Contents

POLICY SCOPE

Survey 7 Ltd. (hereinafter referred to as "S7") need to obtain, process and store information about individuals and building projects. These include, but are not limited to, clients, suppliers, business contacts, employees and any project/person that the organisation has a working relationship with or may need to contact.

This policy details how personal data obtained by S7 must be collected, handled and stored to meet the company's data protection standards and to comply with law.

This policy applies to all offices, staff, contractors, suppliers and any persons working for S7. It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the General Data Protection Regulation or the Data Protection Act 1998. Identifiable information includes any online or offline data that makes a person identifiable such as names, addresses, usernames, references, digital footprints, photographs, financial data and social security numbers etc.

With this policy, we ensure that we gather, store and handle data lawfully, fairly, transparently and with respect towards individual rights. It also ensures that S7:

- Comply with data protection law and follow good practice
- Protects the rights of staff, customers and partners
- Is open about how it obtains, processes and stores individuals' and projects data
- Protects itself from the risk of a data breach.

S7 collects information in a transparent way and only with the full cooperation and knowledge of interested parties.

This policy helps to protect S7 from serious security risks.

S7 collects its data through company application forms, correspondence, and official documentation. The data that S7 will require is varied and depends on the project itself. Legislation will often dictate what and how detailed the information that we require will need to be. When requested, S7 will provide details on what data we hold on an individual. Personal data will not be shared with a third party unless it is required in order for the works to progress. S7 will, where applicable, share addresses and descriptions of work with Warranty Providers and project connected developers and design teams. Data is used solely for the purpose that it was provided to us for. S7 will never sell on personal data.

RESPONSIBILITIES

Everyone who works for or with S7 has some responsibility for ensuring data is collected, stored and handled appropriately. Each team that handles personal data must ensure that it is handles and processed in line with this policy as well as data protection principles.

However, the following people have key areas of responsibility:

- The **Board of Directors** are ultimately responsible for ensuring that S7meets its legal obligations. They support data protection legislation and promote a positive culture of data protection compliance across the business.
- The **Data Protection Lead** – (Legal Support Manager by Proxy), is responsible for
    - Keeping the board updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and advice for the people covered by this policy.
    - Handling data protection questions from staff and anyone else covered by this policy
    - Dealing with requests from individuals to see the data S7 holds about them (subject access requests)
    - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- The **Office Managers, Supported by Tech Wales** is responsible for:
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards

- Performing regular checks and scans to ensure security hardware and software is functioning properly
- Evaluating any third-party services that the company is considering using to store or process data. (i.e. Cloud computing services)

- The **HR/Accounts Technician –** is responsible for:
  - Approving any data protection statements attached to communications such as emails and letters
  - Addressing any data protection queries from journalists of media outlets like newspapers.
  - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

GENERAL STAFF GUIDELINES

- The only people able to access any data that is covered by this policy should be those who **need it for their work.**
- Data **should not be shared informally.** When access to confidential information is required, employees must request it from the persons listed above, with authorisation from their line manager.
- S7 will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- Strong passwords must be used, and they should never be shared with unauthorised personnel.
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated. If it is found to be out of date or no longer required, it should be deleted and disposed of correctly.
- Employees should request help form their line manager or the data protection officer if they are unsure about any aspect of data protection.
- If employees are working remotely on company devices, they shall not use hotspot outlets or public Wi-Fi.

DATA STORAGE

These rules detail how and where data should be safely stored. Questions about storing data safely can be directed to the Data Protection Officer or IT manager. When data is **stored on paper** i.e. in a project file, it should be stored in a secure place where unauthorised personnel cannot see or access it.

The following guidelines also apply to data that is securely stored electronically but has been printed out:

- When not in use, paper files should be kept in a locked draw, filing cabinet or archive system.

- Employees should make sure paper and printouts are not left where unauthorised personnel could see them (I.e. If you are printing a document containing personal data, you are responsible for ensuring document isn't left at the printer)
- Data printouts are to be placed in the confidential waste bin to be shredded and disposed of once no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by passwords that are never shared between unauthorised personnel.
- If data is stored on removable drives, these should be kept locked away securely when not being used.
- Servers containing personal data should be sited in a secure location, away from general office space
- Data should be backed up frequently. Those backups should be tested regularly.
- All servers and computers containing data should be protected by approved security software and firewall.

S7 employees must ensure that any electronic device that holds data has the screen lock activated when not in use. Laptops, files, or anything that contains data shall not be left in parked cars. If an officer is granted the right to work from home by management, they must take only what they require to carry out their job.

DATA USE

Personal data is of no value to S7 unless the business can make use of it. Personal data will never be sold on or passed on to a third party. It is when Personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended
- Personal data should not be shared informally.
- Personal data should never be transferred outside of the European Economic Area – Please speak to the Data Protection Officer if you have any queries about this.

DATA ACCURACY

Legislation requires S7 to take reasonable steps to ensure data is kept accurate and up to date. The more important it is that the personal data is accurate, the greater effort S7 should put into ensuring its accuracy. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

Data should be held in as few places as necessary. Staff should not create any unnecessary additional data sets. Staff should take every opportunity to ensure data is up to date. For instance, by confirming

a clients' details when they call. Data should be updated as inaccuracies are identified. For instance, if a customer can no longer be reached on their stored telephone number, it should be noted and/or removed from the database.

It is the marketing manager's responsibility to ensure marketing databases are checked against industry suppression files every six months.

DATA RETENTION

S7 shall not hold personal data for any longer than necessary and will not use it for any purpose other than what the data was originally collected, processed and stored for.

When the requirement to store personal data is no longer necessary, S7 will ensure reasonable steps are taken to erase or otherwise dispose of the data.

Any questions relating to data retention, including retention periods for S7, please refer to our Data Protection Officer. You can request that we remove your details from our database. We will remove data in accordance with your wishes excluding data we are required to keep by law.

SUBJECT ACCESS REQUESTS

Persons are entitled to be notified if any personal information is held about them and if it is, to be given:

- a copy of the information in permanent form;
- an explanation of any technical or complicated terms;
- any information the organisation has about where they got your information from;
- a description of the information, the purposes for processing the information and who the organisation is sharing the information with; and
- the logic involved in any automated decisions (if S7 have specifically been asked for this).

S7 will provide a copy of the requested information **free of charge**. However, S7 reserve the right to charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive. All fees will be based on the administrative cost of providing the information.

S7 will only accept written subject access requests (SAR). A request sent by email or fax is as valid as one sent in hard copy. For any persons who find it impossible or unreasonably difficult to make a request in writing, S7 will make a reasonable adjustment for you under the Equality Act 2010 (or Disability Discrimination Act 1995 in Northern Ireland).

S7 will aim to reply within one month, starting from received date of the information required to identify you and the information you require. If S7 require additional details to help them find your information or identify you. The SAR will be put on hold until they have all the necessary information as well as the fee (if required) before dealing with your request.

S7 will respond to SAR's in writing, but may need not to do this if it is not possible, if it takes 'disproportionate effort' or if the requestee agrees to some other form of response, such as seeing it on screen. The Act does not define what disproportionate effort means but S7 will take into account the following:

- the cost of giving you the information;
- the length of time it will take;
- how difficult it will be;
- the size of the organisation; and
- the effect on you of not having the information in permanent form.

The GDPR does not include an exemption for requests that relate to large amounts of data, this means that S7 may be able to consider whether the request is manifestly unfounded or excessive. Where requests are manifestly unfounded or excessive, S7 reserves the right to:

- charge a reasonable fee taking into account the administrative costs of providing the information; or
- refuse to respond.

Where S7 refuse to respond to a request, a full explanation will be provided, informing the relevant persons of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

S7 reserves the right to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, you must inform the individual within one month of the receipt of the request and explain why the extension is necessary. There are some circumstances where the information requested contains information that relates to another person. Unless the other person gives their permission, or it is reasonable in all the circumstances to provide the information without permission, the organisation is entitled to withhold this information.

The Act covers personal information that:

- is held, or going to be held on computers;
- is in, or going to be in, a manual filing system that is highly structured so that information about you can be easily retrieved;
- is in most health, educational, social service or housing records; or
- is other information held by a public authority.

S7 recognises that under equality law, an organisation has a duty to make sure that its services are accessible to all service users. Any persons can request a response in a format that is accessible to you, such as Braille, large print, email or audio format.

DISCLOSING DATA FOR OTHER REASONS

In certain circumstances, the act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, S7 will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

PROVIDING INFORMATION

S7 aims to ensure that individuals are aware that their data is being processed, and that they understand how their data is being used and how to exercise their rights. To these ends, the company has a data flow map setting out how data relating to individuals is used by the company. This is available on request.

LAWFUL BASES FOR PROCESSING PERSONAL DATA

The lawful bases for processing are set out in Article 6 of the GDPR. S7 have identified the below lawful bases for processing personal data that are applicable in line with the service that we provide.

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

STAFF AWARENESS

S7 will ensure that staff are fully aware of the General Data Protection Regulation and subsequently are trained to know the essential requirements of the regulation.

MONITORING AND ASSESSMENT

The Company will assess and review the effectiveness of this Policy and the impact of all other relevant policies and practices on all employers.

Signed on behalf of Survey 7 Ltd (Senior Management)

Date	Signature	Position
25.02.2022		Director