

## Privacy Notice

### 1. Information About Us

We are a sign manufacturer and installer.

Our address is Unit 6/7 Fairlawn Enterprise Park, Bonehurst Road, Redhill, Surrey, RH1 5GH

Company registration number: 4257931

We have identified that we do not satisfy the requirements under the GDPR and UK Data Protection Act (2018) where a Data Protection Officer is mandated. However, we have identified a single contact (the Information Officer) for all queries, complaints and correspondence relating to data protection. They are responsible for controlling and assessing the risk to personal data within our company, and for ensuring that we comply with the relevant legislation.

Information Officer: David Klein

Email address: [info@signsandsafety.co.uk](mailto:info@signsandsafety.co.uk)

Telephone number: 01293 827 830

Postal Address: as above

### 2. What Does This Notice Cover?

This Privacy Information explains how we use your personal data: how it is collected, how it is held, and how it is processed. It also explains your rights under the law relating to your personal data.

### 3. What is Personal Data?

Personal data is defined by the General Data Protection Regulation (EU Regulation 2016/679) (the "GDPR") as 'any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier'.

Personal data is, in simpler terms, any information about you that enables you to be identified. Personal data covers obvious information such as your name and contact details, but it also covers less obvious information such as identification numbers, electronic location data, and other online identifiers.

The personal data that we use is set out in Part 5, below.

### 4. What Are My Rights?

Under the GDPR, you have the following rights, which we will always work to uphold:

a) The right to be informed about our collection and use of your personal data.

This Privacy Notice should tell you everything you need to know, but you can always contact us to find out more or to ask any questions using the details in Part 11.

- b) The right to access the personal data we hold about you. Part 10 will tell you how to do this.
- c) The right to have your personal data rectified if any of your personal data held by us is inaccurate or incomplete. Please contact us using the details in Part 11 to find out more.
- d) The right to be forgotten, i.e. the right to ask us to delete or otherwise dispose of any of your personal data that we have. Please contact us using the details in Part 11 to find out more.
- e) The right to restrict (i.e. prevent) the processing of your personal data.
- f) The right to object to us using your personal data for a particular purpose or purposes.
- g) The right to data portability. This means that, if you have provided personal data to us directly, we are using it with your consent or for the performance of a contract, and that data is processed using automated means, you can ask us for a copy of that personal data to re-use with another service or business in many cases.
- h) Rights relating to automated decision-making and profiling. We do not use your personal data in this way.

For more information about our use of your personal data or exercising your rights as outlined above, please contact us using the details provided in Part 11.

Further information about your rights can also be obtained from the Information Commissioner's Office or your local Citizens Advice Bureau.

If you have any cause for complaint about our use of your personal data, you have the right to lodge a complaint with the Information Commissioner's Office.

## 5. What Personal Data Do You Collect?

We may collect some or all of the following personal data (this may vary according to your relationship with us):

- Name;
- Date of birth;
- Gender;
- Address;
- Email address;
- Telephone number;
- Business name;
- Job title;
- Profession;

- Payment information (including but not limited to bank account number, sort code, receipts of credit card transactions);
- Information about your preferences and interests.

We may also collect and process the following personal data of prospective, current and past employees:

- National Insurance and tax details;
- Emergency contact details, and details of next-of-kin;
- Medical information, such as conditions, allergies, details of regular medication, GP contact details;
- Car details, copies of driving licence and proof of insurance;
- Proof of right to work (e.g. copies of passports);
- Personnel files, including (but not limited to): application form(s), CV, details of previous employment, records of references sought, attendance/absence/sickness records, records of meetings and disciplinary proceedings, training records;
- Details related to criminal records checks (DBS disclosure), if this is required for the position.

## 6. **How Do You Use My Personal Data?**

Under the GDPR, we must always have a lawful basis for using personal data. This may be because the data is necessary for our performance of a contract with you, because you have consented to our use of your personal data, or because it is in our legitimate business interests to use it. Your personal data may be used for one (or more) of the following purposes:

- Providing and managing your account with us;
- Supplying our products and/or services to you. Your personal details are required in order for us to enter into and fulfil our obligations under a contract with you;
- Personalising and tailoring our products and/or services for you;
- Communicating with you. This may include responding to emails or calls from you;
- Supplying you with information by email, telephone or post that you have either opted-in to (you may unsubscribe or opt-out at any time by contacting us) or we have a legitimate interest in sending you;
- Administration of our business (including the monitoring of our service, our employees and our financial performance);
- Ensuring that we comply with the law, and taking reasonable steps to ensure that staff, customers and 3<sup>rd</sup> parties are complying with the law (including the recording of CCTV images at our offices, the monitoring of Company email, telephone and internet usage, and the sharing of data with law enforcement and credit reference agencies, where allowed).

With your permission and/or where permitted by law, we may also use your personal data for marketing purposes, which may include contacting you by email, telephone and post with information, news, and offers on our products and services. You will not be sent any unlawful marketing or spam. We will always work to fully protect your rights and comply with our obligations under the GDPR and the Privacy and Electronic Communications (EC Directive) Regulations 2003, and you will always have the opportunity to opt-out and to object to us processing your data in this way.

## 7. **How Long Will You Keep My Personal Data?**

We will not keep your personal data for any longer than is necessary in light of the reason(s) for which it was first collected. A full data retention schedule is available on request. As an illustration, some of the purposes (and retention periods) for keeping personal data are listed below:

- For the purposes of legislative requirements (for instance, for VAT and other tax returns) – governed by the appropriate legislation, including but not limited to:
  - Details of invoices, goods supplied and purchased, company and employee tax returns, company accounts – 6 years from the end of the accounting/tax period (maximum 7 years);
  - Details of purchase of goods or services relating to the quotation, selection, negotiation and/or delivery of the goods and/or services, and any subsequent communications related to the provision of those goods and/or services – minimum 6 years (Limitation Act 1980);
  - Employee records (other than covered by financial and other legislation) – maximum 6 years from end of employment, except the following:
    - Special category data, including data related to medical information, next of kin and payment processing details – maximum 3 months from end of employment;
    - Except in the case of identification documents to prove an individual's right to work, in which case this is kept for 2 years from end of employment;
    - Details of any exposure to hazardous substances (e.g. asbestos dust) will be retained for a minimum of 40 years;
    - Details pertaining to incidents involving the welfare of a child during the course of work duties may be kept for a period of time and manner strictly in line with child protection legislation;
    - Name, start/finish date and job title, which are retained indefinitely);
  - Any records pertaining to health and safety incidents in the workplace will be kept for a minimum of 3 years from the date of the report;
- Where the processing of personal data is required to fulfil a contract (including a contract of sale), data will be retained during and for 6 years following the end of the contract (or longer if stated in the contract itself);
- Where Signs & Safety Ltd is processing data as a data processor, then personal data will be permanently removed (and, where applicable, returned

to the controller / processor) once any data processing contract/agreement has ended, except where legislation requires that we retain the data or part thereof. This includes personal data belonging to customers that may be processed by Signs & Safety Ltd as part of a service that we offer;

- Where, as identified by a Data Protection Impact Assessment, we believe that we have a legitimate interest to process personal data for the purposes of our business (for example, marketing), only the minimum amount of personal data for the purposes of this processing will be retained indefinitely unless the data subject requests that processing be suspended or stopped or their data erased;
- Images stored on CCTV are retained for the purposes of crime detection and prevention, and are retained for a maximum of 14 days;
- Records of subject access requests, erasure requests, data protection complaints, and any other record of an individual or business exercising their rights under data protection law, will be kept indefinitely for the purposes of demonstrating compliance to the appropriate supervisory authority.

## 8. How and Where Do You Store or Transfer My Personal Data?

Where possible, information will be stored and processed within the United Kingdom and if not, within the EEA.

However, we may need to store or transfer some or all of your personal data in countries that are not part of the European Economic Area (the “EEA” consists of all EU member states, plus Norway, Iceland, and Liechtenstein). These are known as “third countries” and may not have data protection laws that are as strong as those in the UK and/or the EEA. This means that we will take additional steps in order to ensure that your personal data is treated just as safely and securely as it would be within the UK and under the GDPR as follows:

We may share your data with external third parties, as detailed below in Part 9, that are based outside of the EEA. The following safeguards are applied to such transfers:

- We will only transfer your personal data to countries that the European Commission has deemed to provide an adequate level of personal data protection. More information is available from the [European Commission](#).
- Where we transfer your data to a third party based in the US, this may be protected if they are part of the EU-US Privacy Shield. This requires that third party to provide data protection to standards similar levels of data protection to those in Europe. More information is available from the [European Commission](#).

Please contact us using the details below in Part 11 for further information about the particular data protection mechanism used by us when transferring your personal data to a third country.

The security of your personal data is essential to us, and to protect your data, we take a number of important measures, including the following:

- Annual accreditation to the CyberEssentials and IASME standards in Information Security (see <http://www.iasme.co.uk>);

- Careful selection of 3<sup>rd</sup> party suppliers, and having contracts/agreements in place with them compliant with the GDPR (including ensuring that they implement adequate technical and organisational measures to protect personal data);
- Ensuring that data is always encrypted in transit, and stored securely according to industry standards;
- Regular security audits and internal training.

## 9. Do You Share My Personal Data?

We may sometimes contract with the following types of third parties in order to supply products and/or services to you and to operate our business. These may include payment processing, delivery, and marketing. In some cases, those third parties may require access to some or all of your personal data that we hold. These parties include:

- Suppliers of goods (for instance, manufacturers, distributors and other stockists);
- Professional advisers (e.g. lawyers, insurers and accountants);
- Marketing companies and distributors;
- Payment providers (e.g. SagePay);
- Cloud-based IT software providers (such as our email);
- Contractors providing a direct service to our customers on our behalf (e.g. installers, trainers and consultants);
- Government and regulatory authorities (such as HMRC, the police, or the Information Commissioner).

If any of your personal data is required by a third party, as described above, we will take steps to ensure that your personal data is handled safely, securely, and in accordance with your rights, our obligations, and the third party's obligations under the law, as described above in Part 8.

If any personal data is transferred outside of the EEA, we will take suitable steps in order to ensure that your personal data is treated just as safely and securely as it would be within the UK and under the GDPR, as explained above in Part 8.

In some limited circumstances, we may be legally required to share certain personal data, which might include yours, if we are involved in legal proceedings or complying with legal obligations, a court order, or the instructions of a government authority.

## 10. How Can I Access My Personal Data?

If you want to know what personal data we have about you, you can ask us for details of that personal data and for a copy of it (where any such personal data is held). This is known as a "subject access request".

All subject access requests should be made in writing and sent to the email or postal addresses shown in Part 11.

There is not normally any charge for a subject access request. If your request is 'manifestly unfounded or excessive' (for example, if you make repetitive requests) a fee may be charged to cover our administrative costs in responding.

We will respond to your subject access request within one month of receiving it. Normally, we aim to provide a complete response, including a copy of your personal data within that time. In some cases, however, particularly if your request is more complex, more time may be required up to a maximum of three months from the date we receive your request. You will be kept fully informed of our progress.

## 11. **How Do I Contact You?**

To contact us about anything to do with your personal data and data protection, including to make a subject access request, please use the following details (for the attention of David Klein – DATA PROTECTION):

Email address: [info@signsandsafety.co.uk](mailto:info@signsandsafety.co.uk)

Telephone number: 01293 827830

Postal Address: Unit 6/7 Fairlawn Enterprise Park, Bonehurst Road, Redhill, Surrey, RH1 5GH.

## 12. **Changes to this Privacy Notice**

We may change this Privacy Notice from time to time. This may be necessary, for example, if the law changes, or if we change our business in a way that affects personal data protection.

Any changes will be made available on our websites.

Last Updated: 1<sup>st</sup> March 2019