PL05 Privacy Policy

This Privacy Policy explains how we collect, use and process personal data, and how, in doing so, we comply with our legal obligations. Privacy is important to us and we are committed to protecting and safeguarding data privacy rights.

This Privacy Policy applies to the personal data of our customers, suppliers and employees.

Under the GDPR (2016), if you hold and process personal information about your clients, employees or suppliers, you are legally obliged to protect that information. Under the Data Protection Act, you must:

- only collect information that you need for a specific purpose;
- keep it secure;
- ensure it is relevant and up to date;
- only hold as much as you need, and only for as long as you need it; and
- allow the subject of the information to see it on request.

1. Personal Data

Customer data: In order to be able to carry out our work, we collect the following data directly from our customers:

- Name;
- Contact details, including address, phone numbers and email address;
- Extra information that you choose to tell us (e.g. marital status, gender);
- The dates, times and frequency with which you access our services; and
- CCTV footage at our premises.

Portal Users: We collect a limited amount of data from our On-line Portal users which we use to help us to improve the experience when using our portal and to help us manage the services we provide. This includes information such as how you use our portal, the frequency with which you access our portal, and the features of our portal that are most popular.

A number of elements of the personal data we collect from you are required to enable us to fulfil our contractual duties to you or to others. Depending on the type of personal data in question and the grounds on which we may be processing it, should you decline to provide us with such data, we may not be able to fulfil our contractual requirements or, in extreme cases, may not be able to continue with our relationship.

Supplier data: We need a small amount of information from our Suppliers to maintain a successful business relationship. We need contact details of relevant individuals at your organisation so that we can communicate with you. We also need other information such as your bank details so that we can pay for the services you provide (if this is part of the contractual arrangements between us). We may also hold extra information that someone in your organisation has chosen to tell us. In certain circumstances, such as when you engage with our Finance and Debt Recovery teams, our calls with you may be recorded, depending on the applicable local laws and requirements.

Employees data: we collect the following data directly from our employees:

- Name;
- Contact details, including address, phone numbers and email address;
- Extra information that you choose to tell us (e.g. marital status, gender);
- Driving licence, Passport, bank details, National Insurance Number, date of birth; and
- CCTV footage at our premises.

2. How we collect Personal Data

Customer data: There are two main ways in which we collect your personal data:

1. Directly from you; and
2. From an intermediate such as the property management company.

Supplier data: We collect your personal data during the course of our work with you.

Employee data: There are two main ways in which we collect your personal data:

1. Directly from you; and
2. From a third party such as a referee, former employer or recruitment agent.

3. How we use Personal Data

Customer data: The main reason for collecting your personal details is to ensure that the contractual arrangements between us can properly be implemented i.e. *Legitimate Interest*.

Our main area of work is the installation and servicing of Intruder Alarms, Access Control, Automated gates and barriers and CCTV. We've listed below various ways in which we may use and process your personal data for this purpose, where appropriate and in accordance with any local laws and requirements. Please note that this list is not exhaustive.

- Storing your details (and updating them when necessary) on our database, so that we can contact you in relation to our contractual obligations;
- Carrying out our obligations arising from any contracts entered into between us;
- Carrying out our obligations arising from any contracts entered into between SCS and intermediate parties such as Management Companies in relation to your property;
- Facilitating our payroll and invoicing processes;
- Carrying out customer satisfaction surveys;

Supplier data: The main reasons for using your personal data are to ensure that the contractual arrangements between us can properly be implemented so that the relationship can run smoothly, and to comply with legal requirements. We will store (and update when necessary) your details on our database, so that we can contact you in relation to our agreements;

Employee data: We collect your personal data to ensure that the legal obligations of our employer/employee relationship can be met. We are committed to ensuring that our recruitment processes are aligned with our approach to equal opportunities.

Some of the data we may (in appropriate circumstances and in accordance with local law and requirements) collect about you comes under the umbrella of "diversity information". This could be information about your ethnic background, gender, disability, age, sexual orientation, religion or other similar beliefs, and/or social-economic background. Where appropriate and in accordance

with local laws and requirements, we'll use this information on an anonymised basis to monitor our compliance with our equal opportunities policy.

This information is what is called 'sensitive' personal information and slightly stricter data protection rules apply to it. We therefore need to obtain your explicit consent before we can use it. We'll ask for your consent by offering you an opt-in. This means that you have to explicitly and clearly tell us that you agree to us collecting and using this information.

As a condition of your employment, we will collect other sensitive personal data about you, such as details of any criminal convictions. We will require your explicit consent before we gather such information.

4. Who we share Personal Data with

Customer data: We may share your personal data with various parties, in line with our contractual obligations. Primarily, these parties will be third party service providers who perform functions on our behalf such as out-of-hours monitoring stations or third party outsourced IT providers where we have an appropriate processing agreement (or similar protections) in place;

Supplier Data: Unless you specify otherwise, we may share your information with any of our associated third parties such as our service providers and organisations to whom we provide services.

Employee data: Following your consent, we will share your data with our external security screening consultants.

5. How we safeguard Personal Data

We are committed to taking all reasonable and appropriate steps to protect the personal information that we hold from misuse, loss, or unauthorised access. We do this by having in place a range of appropriate technical and organisational measures. These include measures to deal with any suspected data breach.

All of our employees are security screened and understand the importance of confidentiality. All of our paper waste containing sensitive information is shredded and disposed of securely. Management consider information security and data protection when reviewing performance.

If you suspect any misuse or loss of or unauthorised access to your personal information please let us know immediately.

6. How long we store Personal Data

Customer data: We keep your details on our secure database unless otherwise instructed by yourselves to remove it.

Supplier data: We keep your details on our secure database unless otherwise instructed by yourselves to remove it.

Employee data: If we have not had meaningful contact with you (or, where appropriate, the company you are working for or with) for a period of seven years, we will remove your personal data from our systems unless we believe in good faith that the law or other regulation requires us to

preserve it (for example, because of our obligations to tax authorities or in connection with any anticipated litigation).

7. How you can access, amend or delete Personal Data

One of the GDPR's main objectives is to protect and clarify the rights of EU citizens and individuals in the EU with regards to data privacy. This means that you retain various rights in respect of your data, even once you have given it to us.

Right to Object: If we are using your data because we deem it necessary for our legitimate interests to do so, and you do not agree, you have the right to object. We will respond to your request within 30 days (although we may be allowed to extend this period in certain cases).

Data Subject Access Requests (DSAR): You have the right to ask us to confirm what information we hold about you at any time, and you may ask us to modify, update or delete such information. At this point we may comply with your request or, additionally we may ask you to verify your identity, or ask for more information about your request and where we are legally permitted to do so, we may decline your request, but we will explain why if we do so.

Right to Erasure: In certain situations (for example, the data are no longer necessary for the purpose for which it was originally collected), you have the right to request us to erase your personal data. We will respond to your request within 30 days (although we may be allowed to extend this period in certain cases) and will only disagree with you if certain limited conditions apply. If we do agree to your request, we will delete your data but will generally assume that you would prefer us to keep a note of your name as a record of your request of erasure. That way, we will minimise the chances of you being contacted in the future where your data are collected in unconnected circumstances. If you would prefer us not to do this, you are free to say so.

Right to Rectification: You also have the right to request that we rectify any inaccurate or incomplete personal data that we hold about you. If we have shared this personal data with third parties, we will notify them about the rectification unless this is impossible or involves disproportionate effort. Where appropriate, we will also tell you which third parties we have disclosed the inaccurate or incomplete personal data to. Where we think that it is reasonable for us not to comply with your request, we will explain our reasons for this decision.

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during the period for which we hold your data.

8. How we store and transfer Data internationally

SCS is a local organisation and does not share any data internationally

9. How we apply appropriate security measures to IT data

All of our data requires a password to access. Passwords are restricted to employees and access is removed in the event of an employee leaving the company. Engineers understand the importance of password protection on their PDA's so that in the event that a PDA is lost/stolen, access to the data can be removed immediately.

Our IT data is protected by a securely configured firewall for perimeter protection and anti-Virus software which is updated in realtime. Our out-sourced IT provider ensures a secure configuration of the computers with no local administration rights for users and patch management of all the computers on the network.

Website users: We use traffic log cookies to identify which pages are being used. This helps us analyse data about web page traffic and improve our website in order to tailor it to customer needs. We only use this information for statistical analysis purposes and then the data is removed from the system. A cookie in no way gives us access to your computer or any information about you, other than the data you choose to share with us.

You can choose to accept or decline cookies. Most web browsers automatically accept cookies, but you can usually modify your browser setting to decline cookies if you prefer. This may prevent you from taking full advantage of the website.

Our website may contain links to enable you to visit other websites of interest easily. However, once you have used these links to leave our site, you should note that we do not have any control over that other website. Therefore, we cannot be responsible for the protection and privacy of any information which you provide whilst visiting such sites and such sites are not governed by this privacy statement.

10. Our Legal Bases for processing your Data: *Legitimate Interests*

Article 6(1)(f) of the GDPR states that we can process your data where it "is necessary for the purposes of the legitimate interests pursued by [us] or by a third party, except where such interests are overridden by the interests or fundamental rights or freedoms of [you] which require protection of personal data."

Customer data: It is reasonable to expect that if you request us to carry out a survey or installation/maintenance/repair works pertinent to an Intruder Alarm, Access Control, Automation or CCTV system, you are happy for us to collect your personal contact details. We have to make sure our business runs smoothly, so that we can carry on providing services. We therefore also need to use your data for our internal administrative activities such as invoicing, where relevant.

To ensure that we provide you with the best service possible, we store your personal data and/or the personal data of individual contacts at your organisation as well as keeping records of our conversations, meetings, correspondence etc. From time to time, we may also ask you to undertake a customer satisfaction survey. We think this is reasonable – we deem these uses of your data to be necessary for our legitimate interests as an organisation providing various installation/maintenance/repair services to you.

We have our own obligations under the law. If we believe in good faith that it is necessary, we may therefore share your data in connection with crime detection, tax collection or actual or anticipated litigation.

Supplier data: We use and store the personal data of individuals within your organisation in order to facilitate the receipt of services from you as one of our suppliers. We also hold your financial details, so that we can pay you for your services. We deem all such activities to be necessary within the range of our legitimate interests as a recipient of your services.

Employee data: In order to fulfil our obligations as an employer, we need to double check any information you've given us or to confirm your references, qualifications and criminal record, to the extent that this is appropriate and in accordance with local laws. We need to do these things so that we can function as a profit-making business. We also need to use your data for our internal administrative activities such as payroll, where relevant.

11. Consent

In certain circumstances, we are required to obtain your consent to the processing of your personal data in relation to certain activities. Depending on exactly what we are doing with your information, this consent will be opt-in consent or soft opt-in consent.

Article 4(11) of the GDPR states that (opt-in) consent is "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her." In plain language, this means that:

- you have to give us your consent freely, without us putting you under any type of pressure;
- you know what you are consenting to;
- you should have control over which processing activities you consent to; and
- you need to take positive and affirmative action in giving us your consent.

There is an exception called the 'soft opt-in'. This means that specific consent is not required if we are sending marketing message about similar products and services to our existing customers/clients or those we have negotiated with to provide products or services, as long as:

- We give you the opportunity to opt-out when we receive your contact information; and
- We give you the opportunity to opt-out when we send you subsequent messages.

M. Smith
Managing Director
March 2018