Securus Group Policy Document

Document Title:	Privacy Policy (Customers)
Owner:	Data Protection Officer
Further Information:	For queries, please contact the Data Protection Officer (Contact details contained within policy)
Version No:	1.0
Issue Date:	May 2018
Review Date:	April 2019

Purpose

To outline the Securus Group's policy in relation to personal data governance and security. This policy will be regularly reviewed and details why we collect personal data, what information we collect, what we do with this, how to request access to your personal data, the measures we take to protect data as well as other information you may find useful. This privacy policy sets out our responsibilities under The General Data Protection Regulation 2016 (GDPR) and other applicable laws in England and Wales relating to the processing and security of personal information.

Scope

This policy applies to all customers of the Securus Group. For the avoidance of doubt, where this policy refers to 'Securus Group' we refer to all companies within the Group as follows: Securus Group Limited, Rodgers Securus Limited, Goldshield Securus Limited, CEL Securus Limited, Deetronic Fire Systems Limited, AIS Securus Limited, Lyrico Securus Limited, TFS Securus Limited, Suffolk Electrical Services Limited, Security Centres Securus Limited, Diverse Securus Limited.

Head Office

The Head Office for 'Securus Group Limited' is a company registered in England and Wales under registration number 10489886. Our registered office is at Suite 506 Chadwick House Warrington Road, Birchwood Park, Birchwood, Warrington, WA3 6AE. Our Head Office is at Century House, Chapelhall Industrial Estate, Chapelhall, Airdrie, ML6 8QH.

Our Data Protection Officer (DPO) is Pete Holland. If you have any queries relating to personal data, please direct your enquiry to data@securusgroup.co.uk

Changes to this privacy policy

We review our policy periodically ensuring that a detailed review is done at least every 12 months. We will however update this policy sooner if regulations change, if we change our data handling processes or see areas we can enhance governance or security. We are committed to ensuring that your privacy is protected and to developing suitable technology or processes to protect your data.

Why do we collect Personal Information?

We collect personal data for the purpose of fulfilling our contractual obligations for our customers. The range of services that we provide includes but is not limited to: system design, specification, installation, commissioning, servicing, maintenance and around the clock monitoring (intruder alarms, warden / nurse call systems and CCTV monitoring).

The systems that we support our customers with include but are not limited to: fire detection and suppression (portable fire extinguishers, fixed extinguishing systems), PA/VA (public address and voice alarms) security (including intruder, access control, CCTV and door entry), warden / nurse call systems as well as allied technologies.

What Personal data do we collect?

Given the diversity of our UK wide customer base, the personal data that we collect will vary. Some of our customers have a contract with us for their own home. Other customers may take the form of a local authority, housing association, private business or consortium who contract us to attend a portfolio of sites to provide a range of services.

The information we collect in order to meet our contractual obligations will therefore include but not be limited to the following (where appropriate):

- Name
- Address
- Mobile telephone number(s)
- Landline telephone number(s)
- Facsimile number(s)
- Email address
- Access codes required to gain entry to the site
- Bank details
- Company registration number (Business customers only)
- Legal ownership (Business customers only)
- Trading address (Business customers only)
- Job Title (Business customers only)

Our operational database holds information about customer sites in order for us to perform our contractual obligations. An example of this information may include the engineering disciplines we cover in the contract e.g. fire detection or CCTV or the results of testing a system following a routine planned maintenance visit.

When you visit our website:

When someone visits www.thesecurusgroup.co.uk we use a third-party service, Google Analytics, to collect standard internet log information and details of visitor behaviour patterns. We do this to find out things such as the number of visitors to the various parts of the site. This information is only processed in a way which does not identify anyone. We do not make, and do not allow Google to make, any attempt to find out the identities of those visiting our website.

If we do want to collect personally identifiable information through our website, we will be up front about this. We will make it clear when we collect personal information and will explain what we intend to do with it.

If you use our contact form, we will collect your name, email address and any personal data that you may choose to include in your message such as a telephone number so we can respond to your request for information.

When you telephone our offices or field-based employees:

If you ring us we will collect your name and contact number so we can respond to your enquiry.

Who will we share your Personal Information with and why?

We will only share your personal data with a third party if we have your consent to do so, if it is necessary to fulfil contractual obligations to you, or if we are obliged to do so by law (e.g. a Police investigation).

Any personal data that is shared with a third party (e.g. a call centre that operates 24 hours a day, 365 days of the year to monitor an intruder alarm or to coordinate our engineers to attend a service call) will be restricted to the basic information required to perform the task in which they have been engaged.

Below are primary data processors that we use:

Name of data processor:	Call Miss Jones
Link to data processor's website:	www.callmissjones.co.uk
Why they may process personal data:	Call handling 24 hours a day, 365 days of the year to coordinate engineers to respond to customer sites outside of normal office hours.

Name of data processor:	Custodian
Link to data processor's website:	www.custodianmonitoring.com
Why they may process personal data:	Emergency monitoring 24 hours a day, 365 days of the year to respond to warden / nurse call systems.

If you would like any further information regarding the data processors we use, please do not hesitate to contact us.

Our Regulators

National Security Inspectorate (NSI)
We are regulated by the NSI and during audit inspections they are given access to our files to ensure that we are carrying out activities in accordance with ISO 9001.
Here is a link to their Privacy Notice.
www.nsi.org.uk/privacy-statement/

National Inspection Council for Electrical Installation Contracting (NICEIC)
We hold an accreditation with the NICEIC who audit our activity against their approved standards.
Here is a link to their Privacy Notice.
www.niceic.com/privacy-policy

British Approvals for Fire Equipment (BAFE)
We hold an accreditation with the BAFE who audit our activity against their approved standards.
Here is a link to their website.
www.bafe.org.uk

Marketing and the use of your Personal Information

We will only market services and products to you if we have your consent and at any time you can contact us and withdraw that consent and we will update our records accordingly.

Accuracy of your Personal Information

We work hard to make sure the data we hold is accurate, if you believe that the data we hold may be inaccurate then please contact us and we will correct any inaccuracies.

Your rights

Under the General Data Protection Regulations 2016, you have rights as an individual which you can exercise in relation to the information we hold about you.

You can read more about these rights here – www.ico.org.uk/for-the-public/is-my-information-being-handled-correctly/

Complaints or queries

We try to meet the highest standards when collecting and using personal information. For this reason, we take any complaints we receive about this very seriously. We encourage people to bring it to our attention if they think that our collection or use of information is unfair, misleading or inappropriate. We would also welcome any suggestions for improving our procedures.

This privacy policy was drafted with brevity and clarity in mind. It does not provide exhaustive detail of all aspects of our collection and use of personal information. However, we are happy to provide any additional information or explanation needed. Any requests for this should be sent to the address below.

If you want to make a complaint about the way we have processed your personal information, you can contact the ICO, the statutory body which oversees data protection law – www.ico.org.uk/concerns.

Access to Personal Information

We try to be as open as we can be in terms of giving people access to their personal information. Individuals can find out if we hold any personal information by making a 'subject access request' under the General Data Protection Regulations 2016. If we do hold information about you we will:

Give you a description of it; tell you why we are holding it; tell you who it could be disclosed to; and let you have a copy of the information in an intelligible form.

To make a request for any personal information please see the 'How to contact us' section at the base of this policy.

If you agree, we will try to deal with your request informally, for example by providing you with the specific information you need over the telephone.

Security of your Personal Information

In addition to any personal data that is securely held within our UK wide offices, we take the protection of personal data in an electronic format very seriously. We therefore continually review a range of measures in order to enhance the protection of this data including:

Firewalls:

Our Firewalls are used to protect the internal network from potentially malicious activity. This is achieved through a set of rules and access-lists, used to control the connections that can be made between Securus Group's corporate network and the Internet.

Group I.T governance and policy

All Securus Group servers / PC's that are available to users are overlaid by a security GPO (Group Policy Object). These polices are applied from the top level DOMAIN forest to workstations enforcing 'Windows' updates & Installation of applications etc. to complete system lockdown within the RDS session host environment.

Anti-Virus

Several AV systems are in use to protect against e-mail and Internet-borne threats. These systems are updated on a daily basis to counter the latest Viruses, Trojans, Worms etc.

Securus Group runs Sophos EndPoint Protection which helps deploy our Anti-Virus software and updates automatically to PC's on the corporate network from a centrally managed location. This gives us the ability to manage the group's Anti-Virus protection more effectively.

Our Microsoft Exchange Email Solution is protected by Sophos PureMessage. Sophos PureMessage for Microsoft Exchange guards against email-borne threats such as spam, phishing, viruses and spyware. It also controls the information sent and received both internally and externally and can protect our company against the loss of confidential information or inappropriate use of the email system.

Encryption

We encrypt all information that is stored on our servers. We continually assess the expansion of encryption to all relevant hardware and software that is used throughout our operations.

How to contact us

If you want to request information about our privacy policy or to request further information, please see below:

Method of communication	Contact details
Email	Please direct your enquiry to data@securusgroup.co.uk
Telephone	Please call 01236 541282 and ask for our Data Protection Officer
Letter	Please address to: Data Protection Officer, Head Office, Century House, Chapelhall Industrial Estate, Chapelhall, Airdrie, ML6 8QH