Secure-All Security

General Privacy Policy

POL006

Document Review Sheet

The signatures below certify that this process has been reviewed and accepted.

	Name
Authored By	 Christine Moran IT/Quality Manager 22/06/2018
Approved By	 Alan Moran Managing Director 22/06/2018

Revision History

Rev	Author	Description of Change	Effective Date
001	Christine Moran	First release of document	26/04/2018
002	Christine Moran	Update company registered address	22/06/2018

1. Introduction

Protecting our customers' and employees' personal data is important to Secure-All Security. The Company gathers and processes your personal information in accordance with this privacy notice and in compliance with the relevant data protection Regulation and laws. This notice provides you with the necessary information regarding your rights and our obligations, and explains how, why and when we process your personal data.

2. Company Information

We are Secure-All Security which is a trading name of Cairbourne Trading Ltd. Cairbourne Trading Ltd. is a company limited by shares with a registered office is at 19A Briarhill Business Park, Ballybrit, Galway H91X2E2 and company number 240777.

We provide security services to customers including mobile security, manned-guarding and commercial and domestic key holding services.

Our designated Privacy Protection Officer is Alan Moran, who can be contacted by writing to him at the address above or at **dataprotection@secureall.ie** or by phoning our head office at +353-91-384922

We are regulated and licensed by the Private Security Authority and our license number is 00036

Further information about our company can be found at www.secureall.ie .

3. Scope of this Policy

This policy explains how we use your personal data. This includes 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. This policy is intended for customers and those seeking employment with Secure-All Security. A separate privacy policy is in place for employees of the company which addresses special categories of data which we may hold about you.

4. 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'.

In simpler terms, it is 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. Protecting your Information.

We are committed to protecting your personal data and to implementing appropriate technical and organisational security measures to protect it against any unauthorised or unlawful processing and against any accidental loss, destruction, or damage.

5. Data we Collect

In order to provide security services, provide you with information on these products and services, or respond to queries regarding employment with the company, we may need to collect a number of categories of personal data from you. Depending on your relationship with us, these personal data categories may include Name, address, contact details such as telephone number, mobile phone number, email address, property details, access codes, bank details, credit and debit information, records of payments, telephone recordings.

In certain circumstances, we may collect special categories of personal data such as country of origin to ensure we meet with our regulatory requirements (e.g. employment law).

We would ask that you do not send us sensitive personal information (e.g. health data, data concerning racial or ethnic origin, religion) when initially making contact with the company. If this information is required, we will ask you for it at a later time and explain to you why we need it and how it will be used.

6. How we use your Information

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.

We will use your personal data to provide you with security services and to allow us to manage your customer account and/or manage your employment. In particular we may use your personal data for the following purposes:

Service Provision In particular, we will use premises access information and alarm codes to access your premises and carry out any duties you have requested of us. Where key holder contact information is provided, we will use these details to contact key holders in the event of an emergency or other circumstances as directed by you. It is your responsibility to ensure that those whose details you have provided agree to be contacted by us on your behalf.

Legal Basis: The processing is necessary for the performance of the contract to which you are party.

Account Management. This involves processing personal data for the purpose of account set up, monitoring, identity verification and processing payments.

Legal Basis: The processing is necessary for the performance of the contract which you are party to or in order to take specific steps prior to you entering into a contract.

Legal Basis: The processing is necessary to comply with our legal obligations

Customer Support. In order to respond to queries and manage and investigate any complaints we are required to process your personal data. If you contact our security team or if we contact you we will use personal data such as account information and contact history. We may monitor and record such communications, email and other electronic communication to help investigate any complaints and for training purposes.

Legal Basis: The processing is necessary for the performance of the contract twhich you are party to or in order to take specific steps prior to you entering into a contract.

Legal Basis: The processing is necessary to comply with our legal obligations

Legal Basis: The processing is necessary for our legitimate interests to ensure the accuracy of instructions and investigate any complaints or queries regarding our service.

Debt Management. In order to allow Secure-All Security to appropriately manage any debt issues if they were to occur.

Legal Basis: The processing is necessary for the performance of the contract which you are party to or in order to take specific steps prior to you entering into a contract.

Legal Basis: The processing is necessary for our legitimate interests to manage a debt issue

Regulatory & Licence. In order to meet our regulatory and licence requirements Secure-All Security is required to process personal data and provide information to the Regulatory Authorities and government departments

Legal Basis: The processing is necessary to comply with our legal obligations

Recruitment. If you submit a job application via email, by post or by hand delivery to our offices, we will use your personal data for recruitment-related purposes only, which may include contacting you via email, telephone, SMS or post.

Legal Basis: The processing is necessary for our legitimate interests to to recruit employees.

We do not use automated decision making or automated profiling in the processing of your personal data

7. Sharing your Information

We may share your information with our selected business associates, suppliers and contractors to provide you with our services. For example, these business partners may include our web hosting provider and our IT service providers. Where we disclose your information to third parties, it will always be in compliance with the terms of the GDPR and Irish Data Protection Law.

- At the time you enter into a contract for security services with us or at a later date, we may enter into an arrangement for that service to be provided by one of our selected business partners. If this happens, you will be given the opportunity to consent to the transfer of information necessary to provide the service to such service providers.
- In the event that we sell or buy any business or assets, in which case we will disclose your personal data to the prospective seller or buyer of such business or assets.
- If we or substantially all of our assets are acquired by a third party, in which case information held by us about our customers will be one of the transferred assets.
- If we are under a duty to disclose or share your information in order to comply with any legal obligation, or in order to enforce or apply our terms of use and other agreements; or to protect our rights, property, or safety, our customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.
- In order to ensure the safety and security of your personal data e.g. with our backup providers, IT support providers.

8. Retention of your information

We will retain your personal data only for as long as is necessary for the purposes for which it was collected and in order to meet the legal and business requirements of managing your customer account and experience with us. In particular:

- We will retain personal data that is necessary for us to provide you with a requested service (e.g. building access codes) for as long as it takes us to provide that product or service. This data will be removed from our systems and destroyed within two weeks of the service contract ceasing.
- We will retain records of any transactions you enter into with us for services you receive for up to seven years after the year of the transaction. This is so that we can respond to any complaints or disputes that arise in that period.
- We will retain any financial transaction information for seven years after the year of transactions.
- We will retain other personal data necessary for as long as is necessary to comply with our regulatory and legal requirements.
- We will retain information connected with an unsuccessful quotation for 2 years after the year of quotation/
- We will retain recruitment related data for unsuccessful candidates for 1 year from after the year of receipt.

9. Your Rights Regarding Personal Data

Under the GDPR you have a number of important rights regarding the way we process your personal data. These rights are outlined below.

Right of access. 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 (subject to applicable exemptions). This is known as a "subject access request" (SAR). All subject access requests should be made in writing and sent to the email or postal addresses shown in Part 2 of this policy. To help us better deal with your request please provide us with the information necessary to identify you and to identify the personal data you require. To make this as easy as possible for you, a Subject Access Request Form is available for you to use. You do not have to use this form, but it is the easiest way to tell us everything we need to know to respond to your request as quickly as possible. This form can be downloaded from www.secureall.ie/privacy.

There is normally no 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.

Right to rectification. If the personal data we hold on you is inaccurate or incomplete you have the right to rectify such personal data and we would encourage you to ensure the personal data we hold on you is kept as up to date and accurate as possible. If at any time there is a change to your personal data, please adviseus by contacting our office using the details provided in part 2 of this policy of this document.

Right to Erasure. In certain circumstances you have the right to request the deletion of your personal data where there is no compelling reason (e.g. a regulatory requirement for us to retain it) for us to continue processing it.

Right to restrict processing. In certain circumstances you can request the restriction of the processing of your personal data where you contest the accuracy of the information; where you object to processing which is based on legitimate interests; where the processing is unlawful and you wish to restrict the processing rather than seek erasure; or where we no longer require to retain your personal data but you wish the personal data to be held while you establish, exercise or defend a legal claim.

Right to data portability. You can request to receive your personal data, which you provided to us,

in a structured, commonly used and machine readable format and have the right to transmit this data to another controller.

Right to withdraw consent. If we are processing your personal data on the legal basis of consent you have the right to withdraw your consent at any time. If you withdraw your consent we will no longer be able to carry out processing based on your consent. However by withdrawing your consent it does not invalidate any processing which was undertaken prior to the withdrawal of your consent.

Right to object to processing. You have the right to object to processing based on legitimate interests. Where we have indicated that we are processing your personal data based on legitimate interest you are entitled to object to such processing on grounds relating to your particular situation. We will stop processing your personal data unless we can demonstrate compelling legitimate grounds for the processing which overrides your interests, rights and freedoms or where the processing is necessary for the establishment, exercise or defence of legal claims.

Note that when you become our customer the processing of your information, and/or that of your team who you nominate to liaise with us, will become a condition of the contract between us as we require certain information in order to be able to provide you with our services (e.g. contact information). In those circumstances, if you do not wish us to process your information we may be unable to provide our services to you.

Right to lodge a complaint with Data Protection Commissioner. If you are not happy with the way that we deal with and process your data would encourage you to contact our privacy officer by using one of the methods detailed in part 2 of this policy. However, you also have the right to lodge a complaint with the Data Protection Commissioner by emailing info@dataprotection.ie or writing to the Data Protection Commissioner, Canal House, Station Road, Portarlington, R32 AP23 Co. Laois.

10 Changes to this policy notice.

This Statement will be regularly reviewed as part of our Management Review Process to ensure we continue to meet our obligations in processing your personal data and protecting your privacy. In order to do so we reserve the right to update, modify and amend this Statement at any time as required. We would recommend that you check back regularly to keep informed of any updates. We will not make any significant changes to this policy without informing you. The data and issue of this Privacy Policy is detailed on page 3 of this document. You can view the latest version of this document at any time on www.secureall.ie/privacy