



Secure-All Security

Employee Privacy Policy

POL007

Document Review Sheet

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

Name	
Authored By	 <hr/> Christine Moran IT/Quality Manager 16/02/2022
Approved By	 <hr/> Alan Moran Managing Director 16/02/2022

Revision History

Rev	Author	Description of Change	Effective Date
001	Christine Moran	First release of document	23/05/2018
002	Christine Moran	Update Company Address	22/06/2018
003	Christine Moran	Add information on TMS Time & Attendance System	10/08/2020
004	Christine Moran	Remove reference to TMS system as no longer used & add reference to SAG system.	16/02/2022

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 Cairborne Trading Ltd. Cairborne 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 employees of Secure-All Security. A separate privacy policy is in place for customers and those seeking employment with Secure-All Security

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.

5. Our Commitment

The GDPR applies to the processing of personal data. We are committed to complying with its legal obligations in this regard. The organisation collects and processes personal data relating to its

employees in the course of business in a variety of circumstances, e.g., recruitment, training, payment, performance reviews, and to protect the legitimate interests of the company. For further information regarding the processing of employee data, please see the organisation's data protection notice which can be obtained by contacting the office.

This policy covers any employee about whom this organisation processes data. This may include current and former employees. Processing of data includes: collecting; recording; storing; altering; disclosing; destroying; and blocking.

Personal data kept by this organisation shall normally be stored on the employee's personnel file or electronic database on the company server. We ensure that only authorised personnel have access to an employee data.

We have appropriate security measures in place to protect against unauthorised access. These security measures include: user access restrictions, encryption, and physical safeguards.

6. Collection and storage of data – What information to we hold?

The sort of information we hold about you includes your application form and references, your contract of employment and any amendments to it; correspondence with or about you, for example letters to you regarding your employment or, at your request, a letter to your mortgage company confirming your salary; information needed for payroll, benefits and expenses purposes; contact and emergency contact details; records of holiday, sickness and other absence information needed for equal opportunities monitoring policy; and records relating to your career history, such as training records, appraisals, other performance measures and, where appropriate, disciplinary and grievance records.

You will, of course, inevitably be referred to in many company documents and records that are produced by you and your colleagues in the course of carrying out your duties and the business of the company.

We process such data to comply with relevant legal obligations, to perform the employment contract and, where necessary, to protect our legitimate business interests and the rights and entitlements of employees. We will ensure that personal data will be processed in accordance with the principles of data protection, as described in the GDPR and Data Protection Acts.

Personal data is normally obtained directly from the employee concerned. In certain circumstances, it will, however, be necessary to obtain data from third parties, e.g., references from previous employers. We will always obtain your consent to approach third parties about you.

Personal data we collect is used for ordinary Operations, HR management purposes, payroll, and administration purposes. Where there is a need to collect data for another purpose, the we will inform you of this. In cases where it is appropriate to get your consent to such processing, the organisation will do so.

Employees are responsible for ensuring that they inform us of any changes in their personal details, e.g. change of address. We endeavour to ensure personal data held by the organisation is up to date and accurate.

Medical data

Occasionally, it may be necessary to refer employees to the company doctor for a medical opinion and all employees are required by their contract of employment to attend in this case. The organisation may receive certain medical information e.g. a doctor's note regarding an absence which will be stored in a secure manner with the utmost regard for the confidentiality of the document.

Email

Where the organisation provides e-mail facilities and access to the internet employees should note that these are not personal mail accounts and should not be used for personal correspondence of any kind. We reserve the right to access all company email accounts to protect our legitimate interests or where there is a legitimate work reason to do so.

Recording of Telephone Calls

Calls to and from Company phones are recorded and employees are advised not to discuss personal matters on company phones. Recording is necessary to protect our legitimate business interests and for training and quality control purposes. The company reserves the right to use these recordings for disciplinary purposes where appropriate.

Closed circuit monitoring

The organisation has closed circuit television cameras located in public areas of the office. This is necessary in order to protect against theft or pilferage, for the security of staff and for the security of customer and company property. Access to the recorded material will be strictly limited to authorised personnel. CCTV footage recorded by the company is not used to manage employee discipline.

GPS Tracking

The organisation uses a Global Positioning System (GPS) to automatically track the location vehicles in the fleet. The use of such tracking equipment is a commercial necessity. The purpose of this tracking system is to monitor the whereabouts of company vehicles at all times to better manage response to alarms and to plan patrol routes and to protect against theft. The company reserves the right to use GPS information for disciplinary purposes. Personal use of company vehicles is not permitted.

Attendance at work , Well-being Check

The organisation uses a 2 way notification/response system to confirm employees' attendance at work and to check on employees' health and well-being while they are at work. This is a legal requirement for those operating in the security industry and forms part of our duty of care to our employees. This system consists of a backend database which holds details of employees' names, phone numbers and rostered shifts. Employees are also required to load an application (SAG) on their personal phones. The backend database sends notifications to employees to confirm their attendance at work and their well-being. Details of live shifts appear on a dashboard in the control room and if employees do not respond to notifications these are escalated to the control room. Personal data (name, phone number) are stored in a database managed by GRIP Communications who are GDPR compliant. The phone app does not have any permissions to access data on the host device (phone).

7. Retention of Data

The organisation is under a legal obligation to keep certain data for a specified period of time. In addition, the organisation will need to keep personal data for a period of time in order to protect its legitimate interests. Below are details of data retained with their retention periods.

Type of Data	Elements of Personal Data	Retention Period
Recruitment Related Data	e.g. contact details , date of birth, cv, work history, referee notes etc	Length of employment plus 7 years
Terms and Conditions of employment, Employee payroll and tax records, Employment permit records.	This may include personal data contained in contracts of employment and all related documentation.	Length of employment plus 7 years
Working Time Records, payslips	e.g. This will include details regarding weekly working hours, annual leave and public holidays, etc., it also includes records of attendance and well-being checks	3 years from the year of creation
Employee payroll and tax records		Length of employment plus 7 years
Medical Records	May include sick leave certificates, occupational health assessments and other records relating to sick leave	Length of employment plus 7 years
CCTV data		4 months from date of recording
Telephone Recordings		4 months from date of recording

The retention periods set out above may be extended in exceptional circumstances including where records are required by the company to defend any legal claims against it on receipt of appropriate advice.

8. Security of Data

We will take all reasonable steps to ensure that appropriate security measures are in place to protect the confidentiality of both electronic and manual data. Security measures will be reviewed from time to time, having regard to the technology available, the cost and the risk of unauthorised access. Employees must implement all organisational security policies and procedures, e.g. protection of user passwords, locking filing cabinets, ensuring that buildings and offices are locked and alarmed according to procedures.

Employee Responsibilities

All employees will have access to a certain amount of personal data relating to colleagues, customers and other third parties. Employees must play their part in ensuring its confidentiality.

Employees must not disclose personal data, except where necessary in the course of their employment, or in accordance with law. They must not remove or destroy personal data except for lawful reasons and with the permission of the organisation.

Any breach of the data protection principles is a serious matter and may lead to disciplinary action up to and including dismissal. If employees are in any doubt regarding their obligations, they should contact their supervisor or the privacy protection officer.

9. Disclosure of Data

We will not share your personal data with anyone except in the following circumstances:

- In order to fulfil client contracts and provide security services, it may be necessary on occasion to share some of your personal details with our clients. Information which may be shared may include Name, Telephone Number and details and/or copies of certificates and licenses held by you and required by the client for a particular job. (e.g. PSA License, Safe Pass, First Aid course etc.).
- In order to fulfil client contracts, and protect our legitimate interests it may be necessary to provide timesheet data to customers .
- If we are under a duty to disclose or share your information in order to comply with any legal obligation.
- In order to enforce the terms of our contract , to protect our rights, property, or the safety of our employees, customers or others.
- In order to ensure the safety and security of your personal data e.g. with our backup providers, IT support providers.

We will never share your data outside the European Union and then only under the conditions set out in the GDPR.

10. Disclosure of 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 (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 or requested from the office.

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 advise us by contacting the office.

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 employee the processing of your information will become a condition of the contract between us. If you do not wish us to process your information we may be unable to continue with your employment.

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, we would encourage you to contact your supervisor, or 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, Portarlinton, R32 AP23 Co. Laois.

11. 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 date 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