Privacy Notice

Data Controller:	GSL Dardan Limited t/a Dardan Security Suite 2, McClintock Building Granta Park Great Abington Cambridge CB21 6GP
Data Protection Officer:	Andrew Barnard ESG and Compliance Manager T: 0800 3899 517 E: andrew.barnard@dardansecurity.co.uk

Notice statement

The organisation collects and processes personal data relating to its employees, customers, potential customers, subcontractors, suppliers and members of the public to manage its employee and customer relationship, discuss and tender for business and to manage complaints and reports raised to the organisation.

Information organisation collects - staff

The organisation collects and processes a range of information about you. This includes:

- your name, address and contact details, including email address and telephone number, date of birth and gender;
- the terms and conditions of your employment;
- details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the organisation;
- information about your remuneration, including entitlement to benefits such as pensions or insurance cover;
- details of your bank account and national insurance number;
- information about your marital status, next of kin, dependants and emergency contacts;
- information about your nationality and entitlement to work in the UK;
- information about your criminal record;
- details of your schedule (days of work and working hours) and attendance at work;
- details of periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave;
- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence;
- assessments of your performance, including appraisals, performance reviews and ratings, training you have participated in, performance improvement plans and related correspondence;
- information about medical or health conditions, including whether or not you have a disability for which the organisation needs to make reasonable adjustments;
- details of trade union membership; and
- equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief.
- Recording (video and / or audio), transcripts from meetings, incident reports or H&S systems (vehicle cameras).

The organisation collects this information in a variety of ways. For example, data is collected through application forms, CVs; obtained from your passport or other identity documents such as your driving licence; from forms completed by you at the start of or during employment (such as return to work forms); from correspondence with you; or through interviews, meetings or other assessments.

In some cases, the organisation collects personal data about you from third parties, such as references supplied by former employers, information from employment background check providers, information from credit reference agencies and information from criminal records checks permitted by law.

Personal data is also shared with third party providers to complete screening and vetting, creating your digital profile (for example; the Employee HR System Engage, TeamTailor, TrackTik, our Resource and Scheduling system)

Data is stored in a range of different places, including in your personnel file, in the organisation's HR management systems and in other IT systems (including the organisation's email, MS Teams and Employee HR System).

Why does the organisation process personal data – staff?

The organisation needs to process data to enter into an employment contract with you and to meet its obligations under your employment contract. For example, it needs to process your data to provide you with an employment contract, to pay you in accordance with your employment contract and to administer benefit, pension and insurance entitlements.

In some cases, the organisation needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check an employee's entitlement to work in the UK, to deduct tax, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled and for certain positions, it is necessary to carry out criminal records checks to ensure that individuals are permitted to undertake the role in question.

In other cases, the organisation has a legitimate interest in processing personal data before, during and after the end of the employment relationship. Processing employee data allows the organisation to:

- run recruitment and promotion processes;
- maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights;
- operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace;
- operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes;
- operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled;
- obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled;
- operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that the organisation complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled;
- ensure effective general HR and business administration;
- provide references on request for current or former employees;
- respond to and defend against legal claims; and
- maintain and promote equality, diversity and inclusion in the workplace.

Where the organisation relies on legitimate interests as a reason for processing data, it has considered whether or not those interests are overridden by the rights and freedoms of employees or workers and has concluded that they are not.

Some special categories of personal data, such as information about health or medical conditions, is processed to carry out employment law obligations (such as those in relation to employees with disabilities and for health and safety purposes).

Where the organisation processes other special categories of personal data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is done for the purposes of equal opportunities and diversity monitoring.

Information organisation collects – customers, potential customers, subcontractors and members of the public

The organisation collects and processes a range of information about your business, premises and systems. This includes:

- corresponding with us by phone, e-mail or otherwise. We ask you to disclose only as much information as is necessary to provide you with our services or to submit a question / suggestion / comment in relation to our site or our services.
- filling in forms on www.dardansecurity.co.uk (our site) such as the contact us form.
- hiring Dardan. Customers supply us with information which may include employee's contact details; a contact name; email; business address; telephone number and billing payment details.
- information to complete the contracted service which could include access and alarm codes, keyholder details, electronic system passwords, contract numbers and plans.
- Using security systems (body cameras, CCTV) for capturing of information relating to incident or observation.

Why does the organisation process personal data – customers, potential customers, subcontractors and members of the public?

We collect the information in order to provide you with our services and to market our services.

We will use this information:

- to set your company up as a client on our systems;
- to liaise with you about projects that we are undertaking with you;
- to administer and improve our site and for internal operations, including troubleshooting, data analysis, testing, research, statistical and survey purposes;
- as part of our efforts to keep our site safe and secure;
- to deliver information about our products and services, where you have subscribed to receive same.

The legal bases for the processing of your data are:

- processing necessary for the performance of a contract which you have entered into with us or to take steps at your request prior to entering into a contract
- processing necessary for compliance with a legal obligation to which we are subject.
- processing necessary for the purposes of the legitimate interests which we pursue in providing you with quotes and proposals about our services prior to contract where such interests are not overridden by your interests or fundamental rights or freedoms which require the protection of your information.

Who has access and who we might share this information with?

Your information will be shared internally, including with accounts for payroll and invoicing, HR and the recruitment team, your line manager, managers in the business area for your employment or service and IT staff if access to the data is necessary for the role or service.

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, screening services to obtain pre-employment references from other employers, obtain employment background checks from third-party providers and obtain necessary criminal records checks from the Disclosure and Barring Service.

In addition, we may disclose your personal information to third parties:

- 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 TUPE, fraud protection and credit risk reduction.

The organisation transfers your data to countries outside the UK and has completed a data risk assessment to confirm the companies comply to the UK GDPR and the UK Data Protection Act

Disclosure of your information

- We may share your Personal Data with any member of Dardan Security.
- We may also share your information with selected third parties including: Business partners, suppliers and sub-contractors for the performance of any contract we enter into with them or you.

Set out below a list of third parties with whom we share your data and the reason for such sharing:

No	Third party description	Purpose
1	Sub-contractors	To help us to run our business effectively and to provide you with the services under the terms of our contract with you
2	Cloud Service Providers	To store information held by the company for our legitimate business purposes
3	IT Back-up Providers	To hold information, for our legitimate business purposes
4	Archive/shredding companies	To help us to run our business effectively, for our legitimate business purposes
5	IT Service Providers	To store data, for IT security and service issues and for our legitimate business purposes
6	Email Service Providers	To help us to run our business effectively, for our legitimate business purposes

7	Internal customer database	To run our internal database, to provide the service under the terms of the contract with you and for our legitimate business purposes
8	CCTV and forward-facing camera technology used on company security vans	To help us to run our business effectively, for our legitimate business purposes
9	Third party security consultancy	To help us run our business in the screening and vetting of staff and security intelligence gathering for high risk contracts and services
10	Third party training companies	To help run our business for specific staff training requirements for high risk contracts and services
11	Any UK Customs, Revenue, Security Industry Authority including other UK and Security Statutory bodies	To comply with our legal obligations.

How long do we keep hold of your information

The time periods for which we retain your information depends on the type of information and the purposes for which we use it. We will keep information for no longer than is required or permitted. Please see our data retention policy for more detail.

Your rights with respect to your information

You have the following rights:

- The right to access the information we hold about you.
- The right to require us to rectify any inaccurate information about you without undue delay.
- The right to have us erase any information we hold about you in circumstances such as where it is no longer necessary for us to hold the information for your use of our services or if you have withdrawn your consent to the processing.
- The right to object to us processing information about you such as processing for profiling or direct marketing.
- The right to ask us to provide your information to you in a portable format or, where technically feasible, for us to port that information to another provider provided it does not result in a disclosure of information relating to other people.
- The right to request a restriction of the processing of your information.

Where our processing of your information is based on your consent to that processing, you have the right to withdraw that consent at any time but any processing that we have carried out before you withdrew your consent remains lawful.

You may exercise any of the above rights by contacting the Data Protection Officer by email.

If you believe that the organisation has not complied with your data protection rights, you may lodge a complaint with the Information Commissioner's Office (ICO) in respect to our processing of your information.

When you become our customer or employee, 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) or employment. In those circumstances, if you do not wish us to process your information we may be unable to provide our services or will

hinder the organisation's ability to administer the rights and obligations arising as a result of the employment relationship efficiently, to enable to the organisation to enter into a contract of employment with you.

Changes to notice

This notice may change from time to time, and any changes will be posted on our website and will be effective when posted.

Please review this notice each time you use our site or our services.

This notice was last updated on 13th January 2026

Paul Beard

Chief Commercial Officer

13th January 2026