

Dated 11th January 2018



DATA PROTECTION POLICY (GDPR)

SCOPE

This policy applies to all areas of the business and all employees of the Group. Elite Security Group acknowledges its duty to take adequate steps to mitigate against risk pertaining to data, data breaches and other such unintended consequences resulting from the collection and retention of information.

GDPR EXPLAINED

The **General Data Protection Regulation (GDPR)** (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intended to strengthen and unify data protection for all individuals within the European Union (EU).

Fundamentally many of the concepts and principals are much the same as those in the previous Data Protection Act (DPA), so compliance does not necessarily start from scratch. The biggest change places a greater emphasis on the documentation that data controllers must keep to demonstrate their accountability.

GENERAL STATEMENT

Elite Security Group inherently collects data during the routine course of business and such data may be retained for future reference or some other defined purpose. Data collection is typically relevant to employees, potential recruits, customers and/or suppliers, but additional data may be held relevant to our business function.

Scott Huntley, Director of Support Services, is the nominated Data Controller and the Company is appropriately registered with the ICO. It is the intention of the Company to fully comply with best practice for the protection of data, whilst also employing reasonable and duly considered care and attention to the normal operations of the business.

LAWFUL BASIS FOR PROCESSING DATA

The Company only requests or holds data specific to the intended function made clear at the outset. The Company does not hold data for marketing purposes, or for purposes which are manifestly different from which the original data was provided.

Whilst some data will be retained for the proper performance of agreed contractual obligations, as defined by Article 6 (1) (b) of the Regulations, much of the data retained is in

compliance with some other parliamentary enactment or British Standards. For example; a) previous employment data may be retained to comply with the Screening and Vetting conditions of BS7858, a requirement of the Private Security Act 2001 b) pay information will be retained for the compliance of the Employment Rights Act 1996 and maintained for the ongoing performance of the business, and c) deductions from earnings will be recorded to comply with The Income Tax (Pay As You Earn) Regulations 2003.

The Company will only process data in compliance with the General Data Protection Regulation (GDPR). Where a potential risk or concern is identified, the Company will seek the advice of Legal Counsel before proceeding further.

PROTECTION OF INDIVIDUALS' RIGHTS

The Company fully complies with the rights of individuals in respect to the regulations and employs systems to adequately carry out the functions pertaining to an individual invoking such a right. Note: individuals have the following rights:

- The right to be informed;
- The right of access;
- The right of rectification;
- The right of erasure;
- The right to restrict processing;
- The right to data portability;
- The right to object; and
- The right not to be subject to automated decision making (profiling).

SUBJECT ACCESS REQUESTS

All subject access requests are dealt with by the Director of Support Services, Scott Huntley. Unless compelled by subpoena, court order, legislation or some other enactment, such requests will be dealt with in accordance with the GDPR and will not usually be subject to charge. In the unlikely event of a refusal to comply with a subject access request, usually in the event of a manifestly unfounded or egregious request, the Company will identify the cause of resistance – with individuals retaining their right to complain the ICO.

Please Note: The Company has engaged the services of SAGE for the production of 'online pay slips' rendering simple 'subject access requests' potentially dealt with by way of individuals maintaining their own access points to this information. Furthermore, the

Company will regularly review technologies and adapt accordingly to reduce any potential logistical implications of having to deal with regular requests.

DATA STORAGE

The Company employs a 'cloud' based system for data retention. With 2048-bit RSA, SSL/TLS data encryption, data is replicated across multiple SSAE 16 type 2 certified datacentre locations with SAS RAID storage, maintaining an automatic failover with a 99.9% or better uptime SLA.

The system maintains an audit trail of users including recording information on those who have accessed, amended, deleted or otherwise administrated any given document, whilst retaining versions and revisions - pre-amendments onwards. The system can also allow the administration of 'read only' sections where suitable, providing ultimate control over document storage and retention and dissemination.

DATA ACCURACY

The Company will make every effort to maintain the accuracy of any data retained. In the event that such data becomes incorrect, or is otherwise found to require amendment, the Company will ensure this is done in a timely fashion, with amendments being recorded where appropriate, and incorrect data archived or removed as necessary.

The Company believes that the accuracy of data held for business purposes is not only a fundamental requirement of GDPR, but has a wider benefit to the business as a whole. It is in everybody's interest to ensure the Company works to maintain accurate, current and relevant information where appropriate.

DATA BREACHES

All computer systems and IT equipment are password protected to limit access to those machines often able to access data. Anti-virus is installed on every piece of equipment and backups are maintained through our standard of infrastructure.

In the unlikely event of a data breach the Company will investigate to understand the potential outcome of such a loss; for example, could such a loss result in the discrimination, damage to reputation, financial loss or loss of confidentiality of an individual. The Company

would seek to address and remedy such a situation having sought Legal Counsel from the Company solicitors.

DISCLOSURE OF DATA WITHOUT CONSENT

There are limited justifications for the disclosure of data without the consent of the subject to which the data pertains. For example, Article 6 (1) (c) provides such a justification whereby a disclosure is necessary for compliance of a legal obligation to which the Company is subject. There are other permissible justifications, but these are unlikely to affect or be applied our business in the short term.

EXAMPLE OF DATA RETAINED

The following list, whilst limited, provides an overview to the types of data the Company looks to retain as part of normal business operations. As previously identified, some of this information is required by law and/or some other justifiable reason. The Company is therefore keen to comply with GDPR whilst acknowledging its wider obligations where relevant.

Please note, this list is not exhaustive.

- 1) Personal Information of Employees
- 2) Training Records
- 3) Next of Kin Information
- 4) Work History of Employees
- 5) Credit Score of Employees
- 6) Payroll History
- 7) Court Orders (Attachment of Earnings Orders)
- 8) Client Information
- 9) Client Payment History
- 10) Client Property Information

SUMMARY

Elite Security Group fully complies with the obligations set out in the **General Data Protection Regulations (GDPR)** and maintains records to that effect. Should you require further clarification as to the compliance of the organisation, please contact the Data Controller, Scott Huntley at our Head Office in Swindon.