



Data Protection Policy

The company is committed to being transparent about how it collects and uses the personal data of its employees and customers, and to meeting its data protection obligations. This policy sets out the company's commitment to data protection, and person's rights and obligations in relation to personal data.

This policy applies to the personal data of job applicants, employees, contractors, former employees, suppliers, consultants, potential customers and customers.

The company has appointed the Managing Director as Data Processor who has responsibility for data protection. Contact information is below.

Definitions

1. **"Personal data"** is any information that relates to a person who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.
2. **"Special categories of personal data"** means information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.
3. **"Criminal records data"** means information about a person's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Data protection principles

The company processes all personal data in accordance with the following data protection principles:

1. The company processes personal data lawfully, fairly and in a transparent manner.
2. The company collects personal data only for specified, explicit and legitimate purposes.
3. The company processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
4. The company keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
5. The company keeps personal data only for the period necessary for processing.
6. The company adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

The company tells employees the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of employees for other reasons.

THE PROTECTOR GROUP
Protector House, Station Approach, Team Valley Trading Estate, Gateshead, Tyne & Wear NE11 0ZF
Tel: 0191 4958 240 Fax: 0191 4874 141
Web: www.protectorsecurity.co.uk

Company Registration No: 03448690



Data Protection Policy

The company will update all personal data promptly if an employee advises that his/her information has changed or is inaccurate.

Personal data gathered during the employment is held in the employee's personnel file in hard copy or electronic format, or both, and on HR systems. Personal data gathered during the supplier or client business relationship is held on our central records management system. The periods for which the company holds all personal data are contained in its privacy notices to persons.

The company keeps a record of its processing activities in respect of all personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

Persons rights

As a data subject, person's have a number of rights in relation to their personal data.

Subject access requests

Persons have the right to make a subject access request. If an person makes a subject access request, the company will tell him/her:

1. whether or not his/her data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the person;
2. to whom his/her data is or may be disclosed;
3. for how long his/her personal data is stored;
4. his/her rights to rectification or erasure of data, or to restrict or object to processing;
5. his/her right to complain to the Information Commissioner if he/she thinks the company has failed to comply with his/her data protection rights; and
6. whether or not the company carries out automated decision-making and the logic involved in any such decision-making.

The company will also provide the person with a copy of the personal data undergoing processing. This will normally be in electronic form if the person has made a request electronically, unless he/she agrees otherwise.

If the person wants additional copies, the company will charge a fee, which will be based on the administrative cost to the company of providing the additional copies.

To make a subject access request, the person should send the request to the Data Controller listed below. In some cases, the company may need to ask for proof of identification before

The Protector Group
Protector House, Station Approach, Team Valley Trading Estate, Gateshead, Tyne & Wear NE11 0ZF
Tel: 0191 4958 240 Fax: 0191 4874 141
Web: www.protectorsecurity.co.uk

Company Registration No: 03448690



Data Protection Policy

the request can be processed. The company will inform the person if it needs to verify his/her identity and the documents it requires.

The company will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the company processes large amounts of the person's data, it may respond within three months of the date the request is received. The company will write to the person within one month of receiving the original request to tell him/her if this is the case.

If a subject access request is manifestly unfounded or excessive, the company is not obliged to comply with it. Alternatively, the company can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the company has already responded. If an person submits a request that is unfounded or excessive, the company will notify him/her that this is the case and whether it will respond to it.

Other rights

Persons have a number of other rights in relation to their personal data. They can require the company to:

1. rectify inaccurate data;
2. stop processing or erase data that is no longer necessary for the purposes of processing;
3. stop processing or erase data if the person's interests override the company's legitimate grounds for processing data;
4. stop processing or erase data if processing is unlawful; and
5. stop processing data for a period if data is inaccurate or if there is a dispute about whether the person's interests override the company's legitimate grounds for processing data.

To do this please contact the Data Controller below.

Data security

The company takes the security of all personal data seriously. The company has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties. (See our Security Statement Policy and relevant Privacy Notices for further details).

The Protector Group
Protector House, Station Approach, Team Valley Trading Estate, Gateshead, Tyne & Wear NE11 0ZF
Tel: 0191 4958 240 Fax: 0191 4874 141
Web: www.protectorsecurity.co.uk

Company Registration No: 03448690



Data Protection Policy

Where the company engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and company measures to ensure the security of data.

Data breaches

If the company discovers that there has been a breach of any personal data that poses a risk to the rights and freedoms of persons, it will report it to the Information Commissioner within 72 hours of discovery. The company will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of persons, it will tell affected persons that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken. (Please see our Data Protection Breach Procedure for further details).

Person responsibilities (Employees and customers)

Persons are responsible for helping the company keep their personal data up to date. Persons should let the company know if data provided to the company changes, for example if an person moves to a new house or changes his/her bank details.

Persons may have access to the personal data of other persons and of our customers and clients in the course of their employment, contract, volunteer period, internship or apprenticeship. Where this is the case, the company relies on persons to help meet its data protection obligations to staff and to customers and clients.

Persons who have access to personal data are required:

1. to access only data that they have authority to access and only for authorised purposes;
2. not to disclose data except to persons (whether inside or outside the company) who have appropriate authorisation;
3. to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
4. not to remove personal data, or devices containing or that can be used to access personal data, from the company's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and



Data Protection Policy

5. not to store personal data on local drives or on personal devices that are used for work purposes.

Further details about the company's security procedures can be found in its Security statement policy.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the company's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Training

The company will provide training to all persons about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

Persons whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

Data Controller

Phil Thwaites

phil.thwaites@protectorsecurity.co.uk