

Data protection policy

Introduction

The Data Protection Act (DPA) 1998 (the Act) regulates the way in which all personal data is held and processed. This is a statement of the data protection policy adopted by Coverguard Security. It applies to all Coverguard Security contractors and employees. In May 2018, the Data Protection Act will be changing to GDPR, which means that all companies need to become more aware of how they store personal data.

In order to operate efficiently Coverguard Security needs to collect and use information about the people with whom we work. This includes current, past and prospective employees, reviewers, professional experts, stakeholders, delegates and others with whom we communicate.

Coverguard Security regards the lawful and correct treatment of personal information as integral to our successful operation, and to maintaining the confidence of the people we work with. To this end we fully endorse and adhere to the principles of the Act.

Coverguard Security is registered as a data controller on the register kept by the Information Commissioner.

Purpose

The purpose of this policy is to ensure that everyone handling personal information at Coverguard Security is fully aware of the requirements of the Act and complies with data protection procedures and that data subjects are aware of their rights under the Act.

Scope: information covered by the Act

'Personal data' covered by the Act is essentially any recorded information which identifies a living individual. Personal data held by Coverguard Security will include contact information for a variety of stakeholders and other personal details.

Responsibility for Coverguard Security's compliance with the Act

The Assistant Director reports on any data protection matters to the Managing Director.

The MD has overall responsibility for compliance with the Act but individual members of staff are responsible for the proper use of the data they process

Policy statement



The principles of the Act require that personal information must:

- be processed fairly and lawfully
- not be used for a purpose for which it was not collected
- be adequate, relevant and not excessive for the purpose
- be accurate and up-to-date
- not be kept longer than necessary
- be processed in accordance with the data subject's rights
- be kept secure and protected from unauthorised processing, loss or destruction
- be transferred only to those countries outside the European Economic Area that provide adequate protection for personal information.

In order to meet the requirements of the principles Coverguard Security will:

- fully observe conditions regarding the fair collection and use of information
- meet its legal obligations to specify the purposes for which information is used
- collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements
- ensure the quality of the information used
- hold personal information on Coverguard Security's systems for as long as is necessary for the relevant purpose, or as long as is set out in any relevant contract held with Coverguard Security or Coverguard Security's Records Retention Schedule (this is a policy that defines which documents should be kept and for how long).
- ensure that the rights of people about whom information is held can be fully exercised under the Act (these include: the right to be informed that processing is being undertaken; the data subject's right of access to their personal information; the right to prevent processing in certain circumstances; the right to correct, rectify, block or erase information which is regarded as wrong information)
- provide data requests to individuals and companies within 72 hours
- provide assurances that a person / company's "right to be forgotten" will be implemented within 72 hours
- take appropriate technical and organisational security measures to safeguard personal information
- ensure that personal information is not transferred outside the EEA without suitable safeguards
- ensure that personal / company information is not shared with external agencies
- ensure that reference requests are only accepted in writing, will only confirm if the person has worked for us, in what capacity and the dates of their employment
- ensure that the ICO is made aware of any data breaches within 72 hours of discovery and
- ensure that we comply with GDPR at all times.



Coverguard Security's responsibilities for data protection and confidential information

Coverguard Security will ensure that there is someone with specific responsibility for data protection in the organisation. The nominated person is currently the Assistant Director. The Assistant Director may be contacted at:

Coverguard Security
8/9 The Arcade
High Street
Stony Stratford
MK11 1AY
paulam@coverguardsecurity.co.uk

Coverguard Security will ensure that:

- everyone managing and handling personal information understands that they are responsible for following good data protection practice
- this policy is available to each member of staff
- everyone managing and handling personal information is appropriately trained and supervised
- queries about handling personal information are promptly and courteously dealt with and clear information is available to all staff

Staff responsibilities for data protection and confidential information

- All staff should be aware of the requirements of the Act and how the rules apply to them.
- All staff must complete data protection induction and annual training.
- All staff have a responsibility to ensure that they respect confidential information in their possession and maintain information security. Disclosure of confidential information gained as part of your employment to a third party, or assisting others in disclosure, will be viewed by Coverguard Security with the utmost seriousness.
- All staff are responsible for ensuring personal information is kept no longer than is necessary.

For further advice, please contact the Assistant Director.

Privacy statement

Coverguard Security respects your privacy. The information that you provide us with, or that is gathered automatically, helps us to monitor our services and provide you with the most relevant information.

Subject Access Requests



COVERGUARD

PD021

Under the Act individuals have the right to access personal information Coverguard Security may hold about them.

If you wish to request such information please email paulam@coverguardsecurity.co.uk

Data Protection Complaints Procedure

Coverguard Security aims to comply fully with its obligations under the Act. If you have any questions or concerns regarding Coverguard Security's management of personal data, including your right to access data about yourself, or if you feel Coverguard Security holds inaccurate information about you, please contact Coverguard Security's Assistant Director (details above).

If you feel that your questions or concerns have not been dealt with adequately or that a subject access request you have made to Coverguard Security has not been fulfilled you can use Coverguard Security's complaints procedure: www.coverguardsecurity.co.uk

If you are still dissatisfied, you have the right to contact the office of the Information Commissioner, the independent body overseeing compliance with the Act: <http://ico.org.uk/>.