Data Protection Policy

Scope of the Business

This policy covers the scope of all Kings Solutions Group Companies (Kings) including:

- Kings Security Systems Ltd T/A Kings Secure Technologies
- Kings Guarding Solutions Ltd
- East Fire Extinguishers & Alarms UK Ltd T/A E-fire
- Silver UK Ltd T/A Silver Group
- Cougar Monitoring Ltd
- Quidvis Ltd

Introduction

As individuals, we want to know that personal information about ourselves is handled properly, and we and others have specific rights in this regard. In the course of its activities the company will collect, store and process personal data, and it recognizes that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

The types of personal data that the company may be required to handle include information about current, past and prospective employees, suppliers, customers, and others with whom it communicates, including CCTV footage. A table of all data processed is maintained in accordance with Article 30 of the General Data Protection Regulation 2016 (GDPR). The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the GDPR and other regulations including the Data Protection Act (2018) (hereto referenced as “the Acts”). The GDPR imposes restrictions on how the company may process personal data, and a breach could give rise to criminal sanctions, fines and bad publicity. Kings are always committed to meeting the legal and regulatory requirements imposed by the GDPR and all relevant Acts.

The purpose for processing of CCTV footage is specified in CPL52 CCTV Policy.
If your personal or bank details change, please inform the company straight away so that accurate records may be maintained.
For monitoring purposes all monitoring is carried out by companies which are part of the Kings Solutions Group Limited.

Status of this Policy

This policy sets out the company’s rules on data protection and the six data protection principles contained in it. These principles specify the legal conditions that must be satisfied in relation to the obtaining, handling, processing, transportation and storage of personal data.

The Compliance Team are responsible for ensuring compliance with the Acts and with this policy. Any questions or concerns about the interpretation or operation of this policy should be taken up in the first instance with the Compliance Team.
This policy is not part of the contract of employment and the company may amend it at any time. However, it is a condition of employment that employees and others who obtain, handle, process, transport and store personal data will adhere to the rules of the policy. Any breach of the policy will be taken seriously and may result in disciplinary action.
Any employee who considers that the policy has not been followed in respect of personal data about themselves or others should raise the matter with their Line Manager and/or the company’s Compliance Team in the first instance.

Definition of Data Protection Terms

Data is recorded information whether stored electronically, on a computer, or in certain paper-based filing systems.

Data subjects for the purpose of this policy include all living individuals about whom Kings holds personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

Group Solutions Limited & Subsidiaries,
4 St Dunstans Technology Park, Bradford, West Yorkshire, BD4 7HH
Tel: 0330 678 0635 Email: info@kingsltd.co.uk Web: www.kingsltd.co.uk
Company Registration No: 07706703

Data Protection Policy

Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in possession of the company). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal). It can even include a simple e-mail address. It is important that the information has the data subject as its focus and affects the individual's privacy in some way. Mere mention of someone's name in a document does not constitute personal data, but personal details such as someone's contact details or salary would still fall within the scope of the Acts.

Data controllers are the people or organizations who determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the GDPR. The contracted customer is the data controller in the relationship between Kings and the customer. Where any processing is sub-contracted, Kings assume the role of data controller.

Data Users include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following the company's data protection and security policies at all times.

Data Processors include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on the company's behalf.

Processing is any activity that involves use of the data. It includes obtaining, recording, or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Sensitive Personal Data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

Data Protection Principles

Anyone processing personal data must comply with the six enforceable principles of good practice. These provide that personal data must be:-

- Processed fairly and lawfully and in a transparent manner
- Collected for specific, explicit and legitimate purposes
- Adequate, relevant and not excessive for the purpose
- Accurate, and where necessary, kept up to date
- Not kept longer than necessary for the purpose
- Processed in an appropriate manner to maintain security

Fair and Lawful Processing

The Acts are not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is, the purpose for which the data is to be processed and the identities of anyone to whom the data may be disclosed or transferred. This is outlined in Kings Privacy policies which are available in Entropy and on the company website.

For personal data to be processed lawfully, certain specific conditions must be met. These are detailed in Article 6 of the GDPR for personal data and Article 9 for sensitive personal data. These include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, additional conditions must be met. In most cases the data subject's explicit consent to the processing of such data will be required.

Group Solutions Limited & Subsidiaries,
4 St Dunstans Technology Park, Bradford, West Yorkshire, BD4 7HH
Tel: 0330 678 0635 Email: info@kingsltd.co.uk Web: www.kingsltd.co.uk
Company Registration No: 07706703

Data Protection Policy

Processing for Limited Purposes
Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Acts. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

Adequate Relevant and Non-Excessive Processing
Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

Accurate Data
Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

Timely Processing
Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from the company's systems when it is no longer required. Kings retention policies are detailed in CPL19 Retention and Destruction Policy.

Data Security
The company will ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

The Acts require the company to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:-

- Confidentiality means that only people who are authorised to use the data can access it
- Integrity means that personal data should be accurate and suitable for the purpose for which it is processed
- Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on the company's central computer system instead of individual PCs.

Security procedures include:-

- Entry controls. Any stranger seen in entry-controlled areas should be reported
- Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential)
- Methods of disposal. Paper documents should be shredded. USBs and CD-ROMs should be physically destroyed when they are no longer required
- Equipment. Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended
- Encryption. Data is encrypted in transit and at rest using the AES 256 specification where it is technically possible to do so. Email is secured using TLS if supported by the recipient. Confidential data sent to third parties must be secured as per the 'Sending Encrypted Data Externally' work instruction.
- Robust screening processes for all employees and subcontractors

Group Solutions Limited & Subsidiaries,
4 St Dunstans Technology Park, Bradford, West Yorkshire, BD4 7HH
Tel: 0330 678 0635 Email: info@kingsltd.co.uk Web: www.kingsltd.co.uk
Company Registration No: 07706703

- A rigorous approval procedure for all suppliers and subcontractors including reviews of their information security
- Contractual agreements in place with all suppliers and subcontractors with relevant data protection schedules, recently updated to meet the requirements of the Acts

Kings evidence commitment to data security with the ongoing certification to ISO 27001, which has been in place since 2012 and is externally audited by an independent, IRCA approved company annually. The certificate is available on request.

Dealing With Subject Access Requests

Kings have a documented procedure for handling subject access requests which is available on request (CR05). A formal request from a data subject for information the company holds about them may be made verbally or in writing, either by post or email.

Employees who receive a written request should forward it to the Compliance Team immediately. When receiving telephone enquiries, employees should be careful about disclosing any personal information held on the company's systems. In particular they should:-

- Check the caller's identity to make sure that information is only given to a person who is entitled to it
- Suggest that the caller put their request in writing where the employee is not sure about the caller's identity and where their identity cannot be checked.
- Refer to the Compliance Team for assistance in difficult situations. Employees should not be bullied into disclosing personal information.

Bob Forsyth
Chief Executive Officer

Group Solutions Limited & Subsidiaries,
4 St Dunstans Technology Park, Bradford, West Yorkshire, BD4 7HH
Tel: 0330 678 0635 Email: info@kingsltd.co.uk Web: www.kingsltd.co.uk
Company Registration No: 07706703