Privacy Policy for Employees

Scope of the Business

This policy covers the scope of all Group Solutions Limited 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

This privacy notice explains why we collect your personal information, what we collect, what we do with it and the conditions in which we may disclose it to others. The notice applies to all employees of Kings, including labour only subcontractors.

In order to fulfil our contractual requirements to you we may share your data between any of our companies: Kings Security Systems Limited, Kings Guarding Solutions Ltd, Quidvis Limited, Cougar Monitoring Limited, East Fire Extinguishers & Alarms UK Limited and Silver UK Limited.

Kings are the Data Controller in the relationship between Kings and the employee, you, the employee, are the Data Subject.

This policy may be updated from time to time and is freely available to all stakeholders of Kings in the Compliance Document Store and on the company website.

Kings are committed to the security of data at all times and to this end are externally audited to ISO 27001, the international standard of approval for Information Security Management Systems. More about this can be found in our security policy, CPL04.

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.

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 General Data Protection Regulation (GDPR) 2018.

Data controllers are the people or organizations who determine the purposes for which, and the way, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act.

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

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.

How we use your 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

Privacy Policy for Employees

In the course of your employment and for a period after we may process the following information. This information will be collected at the start of your employment throughout the application and employment process. This information is only available to HR unless otherwise stated.

If any of the information changes at any time you can update your records on your ADP Self Service Portal or by contacting the HR department.

- **Name, address, telephone number** – this information is used to contact you during the course of your employment to fulfil our employment contract. This information is also shared with Sodexo, our insurance companies (currently AIB Insurance) and Health Shield to allow them to process any agreed benefits, more information about this is available in the Recipient of data section of this policy.
- **Next of kin** – this information is collected in compliance with employment law, so we have a point of contact in the unlikely event you are involved in an accident at work, or we have concerns and are unable to contact you following an extended period of unauthorised absence. This information will be shared internally with line managers in your business areas for those who work out of hours.
- **Criminal history (sensitive personal data)** – we carry out two levels of criminal record checks dependent on your level of employment:
    1. We conduct a basic ACPO check with West Yorkshire Police on commencement of employment as part of our screening process, which is a requirement of BS 7858, the British Standard for security screening which all security companies must adhere to. The legal basis for processing is the legitimate interests of Kings to allow us to meet our customer's contractual requirements.
    2. We may require additional screening dependent on the customer data you process which is called SC Clearance. This is conducted by Warwickshire Police, and you can find out more about them in the Recipient of data section of this policy.
- **Financial History (sensitive personal data)** – As part of your initial screening our approved screening companies submit the following information to TransUnion to do a financial health check of you: Full name, title, Address history for 5 years, DOB. TransUnion look at: if you are known at that address, if you are on the electoral roll, notices of undeclared addresses and any adverse information (adverse information is any County Court Judgement over £10,000 or bankruptcy, should this be highlighted on the report a director must accept the risk of hire). This is in the legitimate interest of Kings to ensure you are fit for the role and is a requirement of BS7858 as detailed above.
- **Performance Achievement Reviews and any associated Improvement Plans** – this is available to your line manager and HR and is processed for the legitimate of interests of Kings to ensure you are suitable and competent for your role, and to ensure you have all the support you need to complete your tasks.
- **Records of discipline and grievance** – these are processed in line with employment law requirements and are retained for the duration of any sanctions. Where no further action has been deemed necessary, these will be immediately removed unless otherwise stated in the investigatory meetings or closures.
- **Race & Ethnic origin (sensitive personal data)** – to meet the requirements of discrimination laws, companies must process their employment statistics and publish them internally (at Board level) for monitoring. These are anonymised and never shared.
- **Contract information including salary** – these are processed to meet our contractual obligations to you, such as fulfil holiday entitlement requests and process salary payments. Salary information will be shared with payroll and your line manager. Your contract of employment may be shared with your line manager on request.
- **CCTV footage** – CCTV is processed in the legitimate interest of Kings. For the purpose of workplace safety, security and to prevent theft and other misconduct we have installed video surveillance cameras in work areas. The companies' legitimate purpose for the monitoring of footage is to;
    - To keep employees safe and secure by preventing violence or theft.
    - To prevent pilfering and deliberate damage or other misconduct.
    - To ensure health and safety procedures are being followed.
    - To monitor and improve productivity.

If there is any reported incident of theft, trespass, workplace misconduct such footage will be used.

Kings reserves the right to use covert surveillance inside or outside the workplace in cases where there are sufficient grounds for suspecting dishonesty, suspicious activity, some form of criminal activity or other malpractice is taking place either in relation to the activities of employee(s) or third parties or in cases where there may be suspected breach of contract, e.g. breach of a restrictive covenant or breach of confidential information, such as would be likely you damage the business or reputation of the Company. Where there are sufficient grounds, any covert surveillance would be authorised by the Senior Leadership Team, and will always be within legal parameters.

- **Access cards** – access and photos for the pass are kept for the duration of your employment, this is in the legitimate interest of Kings to provide you with an identity card and access pass to allow you to fulfil your terms and conditions in your contract. For security purposes access to all areas in Head Office is monitored and recorded on the Winpak database. This information may be used in the proceedings of an investigation.

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

- **Email** – all company email is monitored in line with our IT and Acceptable Use policies. This processing is in the legitimate interests of Kings to ensure the reputation of the business is upheld at all times. Emails are kept for two years in mailboxes and available for seven years in the archive.
- **SIA licence** – a record of SIA licence details is kept (where applicable) which consists of a copy of the card and a log of licence numbers and expiry dates. This information may be shared with customers to fulfil contractual requirements. In the event of TUPE this may be shared with the receiving company, however you will be notified of this in writing prior to the exchange of information and given an opportunity to object to the sharing of data.
- **Driving licence** – for employees who have access to a company vehicle a copy of your driving licence will be kept on file and checks will be carried out for penalty points. These checks are completed by a third party – Licence Bureau. You will be asked to complete an authorisation form before any such checks take place. This is to ensure you are covered at all times under the company insurance policies.
- **Personal health information** – we may be required to ask you to complete a health questionnaire, for example (but not limited to) where any shift work is involved. Kings may share this information with our Occupational Health provider from time to time. We will always ask for your permission before we do this.
- **Other forms of identification** – as part of the screening process we are required to check your identification, to do this we may take a copy of your passport, driving licence or birth certificate. These are kept for the duration of your employment plus seven years with your personnel file.
- **Training records and cards** – From time to time these may be shared with certification bodies to evidence compliance with legislation and regulatory requirements. Where Kings customers require this information, it will be shared in order to enable us to carry out the company's contractual obligations and to allow you to fulfil your terms and conditions in your contract.

Unless otherwise stated above your data will be kept for seven years following the end of your employment as required by employment law.

Our website

You can use our website to contact us or to sign up to our newsletter. We restrict the information gathered on our website. We use this information to improve our products and services and to respond to your contact form.

How we use cookies

A cookie is a small file which asks permission to be placed on your computer's hard drive. Once you agree, the file is added, and the cookie helps analyse web traffic or lets you know when you visit a particular site. Cookies allow web applications to respond to you as an individual. The web application can tailor its operations to your needs, likes and dislikes by gathering and remembering information about your preferences.

We use traffic log cookies to identify which pages are being used. This helps us analyse data about webpage traffic and improve our website in order to tailor it to customer needs. We only use this information for statistical analysis purposes and then the data is removed from the system.

Overall, cookies help us provide you with a better website by enabling us to monitor which pages you find useful and which you do not. A cookie in no way gives us access to your computer or any information about you, other than the data you choose to share with us.

You can choose to accept or decline cookies. Most web browsers automatically accept cookies, but you can usually modify your browser setting to decline cookies if you prefer. This may prevent you from taking full advantage of the website.

Links to other websites

Our website may contain links to other websites. However, once you have used these links to leave our site, you should note that we may not have any control over that other website. Therefore, we cannot be responsible for the protection and privacy of any information which you provide whilst visiting such sites and such sites are not governed by this privacy statement. You should exercise caution and look at the privacy statement applicable to the website in question.

Recipients of data

In order to fulfil our contractual and legal obligations to you, we share your data with the following people. We have contracts including privacy clauses in place with each recipient:

National Vetting Solutions (NVS) / National Security Screening Agency (NSSA)
We use NVS and NSSA to conduct screening for new employees. They receive the data included in your application form (name, address, DOB, employment history, references). These companies also conduct the financial checks. Your

authorisation to pass this information is sought in the application process. This is in the legitimate interest of Kings as we do not conduct screening in house and must screen employees as part of our scope of approvals.

Sodexo
Sodexo provide childcare vouchers and our Lifestyle Benefit scheme. We pass Sodexo your name and work email to allow them to include you in the scheme. This is in the legitimate interest of Kings and employees to provide employment benefits as part of your contract of employment.

Health Shield
Health Shield provide your health insurance. Upon passing probation we pass them your name, address, DOB and personal email to enable them to create your Health Shield account. This is in the legitimate interest of Kings and employees to provide employment benefits as part of your contract of employment.

Aviva
Receive names, addresses and dates of birth for employees who qualify for private medical insurance. This is in the legitimate interest of Kings and employees to provide employment benefits as part of your contract of employment.

Reference Hub
Reference Hub process past employee's data including name, start date, end date, National Insurance number and reason for leaving. We pass this information for the legitimate interest of Kings to ensure an efficient and accurate service is proved on request of a reference. All information is verified by Kings as correct at the point of request. Reference Hub retain data for seven years from cessation of employment as required by employment law.

West Yorkshire Police
In some roles additional Security Clearance is required, which is called SC Clearance. This is based on role and contractual requirements. The reason for processing is to fulfil our contractual requirements with the customer. If your role requires you to have this clearance level, you will be passed an application form which is provided by the police to complete. We then pass the application form to the police with payment, and they contact you for further confidential information which we do not have access to at any point.

Training Providers
Through the duration of your employment at Kings you may be required to attend externally provided training courses. To fulfil the requirements of these courses your personal data may be shared with them such as name, email address and contact telephone number. You can request what data has been shared with each training provider through HR or the Learning and Development Team.

Licence Bureau
For employees who have access to company vehicles your driving licence will be checked by Licence Bureau on a regular basis for penalty points. This is detailed further in the Fleet Handbook. Guarding Solutions employees specifically will have their licence checked six monthly – a requirement of the British Standard BS 7984, all other personnel will have their licence checked annually unless our risk assessment based on any recorded offences deems an increased frequency is required.

Wagestream
Wagestream provide you with financial wellbeing benefits. Upon passing probation we pass them your name, and personal email to enable them to contact you regarding their benefits. This is in the legitimate interest of Kings and employees to provide employment benefits as part of your contract of employment.

Timegate / Innovise
For employees working for the Guarding Solutions Team we share data with the Timegate platform. This data is used to ensure you can complete your contractual requirements and also to allow us to monitor your welfare under Health & Safety legislation when working remotely.

Zoho
Data may be shared with Zoho as part of our HR processes and Training requirements. We will only share the minimal required data to allow efficient use of the Zoho platforms and access to this will be restricted internally to ensure privacy is maintained.

Other Third Parties
From time to time we may be required to share your data with other third parties, for example (but not limited to) local authorities, insurance companies and solicitors, to fulfil our legal and contractual requirements.

Kings Commitment

Privacy Policy for Employees

In line with the requirements of the European General Data Protection Regulation 2018 (GDPR) Kings commit to the following:

- Your data will only be used as you intended it, to deliver your contractual requirements and any additional requests which come from you.
- Your data will never be bartered or sold.
- Your data will only be given to law enforcement when legal process has been followed.
- Your data will never be given to advertisers.

Your rights

Under the GDPR, you have the following rights, which we will honour at all times:

- The right to be informed – this privacy policy outlines how and why we process your data.
- The right of access – you may request a copy of all your personal data held by Kings at any time.
- Right to rectification – if you believe any data, we hold is incorrect you may request we update it.
- Right to erasure – you have the right to request your information be removed from our systems at any time. We will fulfil this request as long as it does not conflict with legal or contractual requirements.
- Right to restrict processing – you may limit what data of yours we process and how, at any time, as long as it does not conflict with legal or contractual requirements.
- Right to data portability – we are obliged to make your information available in a legible format to your chosen company if you choose to leave us.
- Right to object – at any time you may object to the processing of your data, details how are below in section 8
- Rights related to automated decision making – we do not use automated decision-making platforms.

Contact Us

Any questions concerning this policy should be sent to compliance@kstl.co.uk, or our registered Head Office address: 4 St Dunstans Technology Park, Bradford, BD4 7HH, alternatively call 0330 678 0635 and ask to speak to the Compliance Team.

If you would like to make a complaint or request access to your data, you can use these contact details also. Our complaints and subject access request policies are available on our website or on request.

Complaints

If you are unsatisfied with how we've handled a complaint in regard to your personal data, you can contact the Information Commissioner's Office https://ico.org.uk/

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