

King Vehicle Engineering Limited
Riverside, Market Harborough
Leicestershire, LE16 7PX
T: +44 (0) 1858 467361
F: +44 (0) 1858 467161

DATA PROTECTION POLICY

Introduction

The King Group of Companies is committed to protecting the rights and freedoms of data subjects by safely and securely processing their data in accordance with all our legal obligations. We hold personal data about our employees, clients, customers, suppliers and other individuals for a variety of business purposes. This policy sets out how we seek to protect personal data and ensure that our staff understand the rules governing their use of the personal data to which they have access during their work. In particular, this policy requires staff to ensure that appropriate planning and consultation is undertaken before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed. This policy is applicable to everyone and must be observed by all employees. The board will keep this policy under review and update, amend or re-issue it as required.

Definitions

Business purposes	<p>The purposes for which personal data may be used by The King Group include the following:</p> <ul style="list-style-type: none">• Performing the functions and operations required for the successful and efficient day-to-day running of our businesses, operating companies, contracts and projects• Compliance with our legal, regulatory and corporate governance obligations and good practice• Ensuring business policies are adhered to (such as those covering the use of email and the internet)• Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests• The investigation of complaints• Operational functions such as the recording of transactions, managing training, quality control, safeguarding the confidentiality of commercially sensitive information, security vetting, reference checking and credit scoring / checking• Ensuring safe working practices, monitoring and managing staff access to systems / facilities, managing staff absences and conduct, disciplinary matters and administration• Marketing and business development• Improving the services we offer and expansion into new markets
Personal data	<p>Personal data means any information relating to an identified or identifiable person ("data subject"). An identifiable person is anyone who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. We gather personal data in relation to the business purposes outlined above. Examples of personal data we gather include (but are not limited to) the following:</p> <ul style="list-style-type: none">• contact information (such as address, phone, email)• details of education, employment history, training, qualifications, certifications and curriculum vitae• nationality and evidence of an individual's right to work in the UK• payroll information (such as bank details, NI number, tax coding)

	<ul style="list-style-type: none">• information related to the driving of vehicles on company business (such as driving licences, records of driving hours and tachographs)• information relating to medical or occupational health assessments, drugs and alcohol testing, illness and absences from work• information relating to work-related accidents and incidents• information about third parties (non-employees) for the purposes of undertaking our legal, regulatory or contractual obligations
Special categories of personal data	Special categories of data include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences (or related proceedings) and genetic and biometric information. Any use of personal data covered by these special categories will be strictly controlled in accordance with this policy.
Data controller	Data controller means the person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means by which personal data is processed, where the purposes and means of such processing are determined by law.
Data processor	Data processor means a person, public authority, agency or other body that processes personal data on behalf of a data controller.
Processing	Processing means any operation(s) performed on personal data by manual or automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Supervisory authority	The national body responsible for data protection and supervisory authority for our organisation is the Information Commissioners Office.

Scope

This policy applies to all staff, who must be familiar with and comply with its content. This policy supplements our other policies relating to the use of CCTV and Information and Communications Technology. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff prior to implementation.

Responsibilities

The Group Strategic Development Manager has overall responsibility for the content and implementation of this policy. They are also responsible for:

- Keeping the board updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all staff members and those included in this Policy
- Answering questions on data protection from staff, board members and other stakeholders
- Responding to individuals such as clients and employees who wish to know what data is being held on them by us
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing

Data Controllers are responsible for the following:

- The analysis and documentation of the type of personal data we gather and process
- Checking procedures to ensure all rights of individuals and data subjects are appropriately covered
- Ensuring data is stored in a safe and secure manner
- Identifying the lawful basis for processing and gathering data
- Ensuring procedures for obtaining consent are suitable, sufficient and lawful
- Implementing and reviewing procedures to detect, report and investigate personal data breaches
- Assessing the potential risks posed to individual rights and freedoms should any breaches of personal data occur

Data Processors are responsible for the following:

- Ensuring they fully understand their data protection obligations
- Checking that any data processing activities they are dealing with comply with this policy
- Ensuring that data is not used in any unlawful way or in a manner that breaches this policy
- Ensuring data is stored correctly and processed carefully and accurately
- Raising any concerns, notifying any breaches or errors and reporting anything suspicious or contradictory to this policy or our legal obligations without delay to the appropriate Data Controller

The ICT Manager is responsible for:

- Ensuring all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party services, such as cloud services the company is considering using to store or process data

Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the relevant Data Controller (usually a Senior Manager or Director).

Data Security and Storage

We will ensure we keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the relevant Data Controller will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

- When data is stored on printed paper, it will be kept in a secure place where unauthorised personnel cannot access it
- Printed data will be shredded when it is no longer needed
- Data stored on a computer will be protected by strong passwords
- The ICT Manager must approve any cloud-based services used for the storage of data
- Data will be regularly backed up in line with the Group ICT department's procedures
- All servers containing sensitive data will be protected by security software
- All reasonably practicable technical measures will be put in place to keep data secure

Data Retention

We will retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

International Data Transfers

There are restrictions on international transfers of personal data. You must not transfer personal data abroad, or anywhere else outside of normal rules and procedures without express permission from the relevant Data Controller.

The principles of the General Data Protection Regulation

The King Group will comply with the six principles of data protection as set out in the General Data Protection Regulation. These six principles are:

1. Lawful, fair and transparent

Data collection will be fair, for a legal purpose and we will be open and transparent as to how the data will be used.

2. *Limited for its purpose*

Data will only be collected for a specific purpose.

3. *Data minimisation*

All data collected will be strictly necessary and not excessive for its purpose.

4. *Accurate*

The data we hold will be accurate and kept up-to-date.

5. *Retention*

We will not store data for any longer than necessary.

6. *Integrity and confidentiality*

We will ensure data we hold is kept safe and secure.

Procedures

The procedures contained within each operating company's Management System will ensure we act with accountability and transparency in all our use of personal data and demonstrate how we will comply with each of the principles set out above. Data Controllers and processors will work together to generate Data Protection Impact Assessments for high-risk areas and maintain written records of how our data processing activities are lawful and compliant. Our Group Register contains details of the data we collect, how it is collected, how it is used and who by and how it is stored and secured. It identifies the high-risk areas that require Data Protection Impact Assessments to be generated. The Group Data Register will be reviewed and updated annually with this policy, and as required due to changes in legislation or the activities being undertaken by any of the Group companies.

Special Categories

Special categories of personal data cover subjects that are more sensitive and therefore require additional protection. This type of data could create significant risks to an individual's fundamental rights and freedoms, for example by placing them at risk of unlawful discrimination. The special categories include information about an individual's:

- race
- ethnic origin
- political beliefs
- religion
- trade union membership (or non-membership)
- genetics
- biometrics (where used for ID purposes)
- health
- sexual orientation

We will seek each individual's explicit consent to process data that falls into these special categories, unless exceptional circumstances apply, or we are required to do so in order to comply with the law (e.g. to ensure compliance with the Health and Safety at Work Act). Such consent will clearly identify what the relevant personal data is, why it is being processed and to whom it will be disclosed. Any processing of special categories of personal data that takes place without this consent will be stopped immediately and reported as a breach.

Criminal Offence Data

We will only undertake criminal record checks where they can be lawfully justified. Checks will not be undertaken based only on the consent of the data subject. We will not keep registers of criminal offence data. All data relating to criminal offences will be treated as a special category of personal data.

Rights of Individuals and Data Subjects

Individuals have rights to their data which we must respect and comply with to the best of our ability. We will ensure individuals can exercise their rights in the following ways:

1. *Right to be informed*

- We will provide privacy notices that are concise, transparent, intelligible, easily accessible, free of charge and written in clear and plain language.
- We will keep records of how we use personal data to demonstrate compliance with the need for accountability and transparency.

2. *Right of access*

- We will enable individuals to access their personal data and supplementary information.
- We will allow individuals to be aware of and verify the lawfulness of the processing activities.

3. *Right to rectification*

- We will rectify or amend the personal data of any individual if requested because it is inaccurate or incomplete.
- This will be done without delay and always within one month of a request being received.

4. *Right to erasure*

- We will delete or remove an individual's data if requested and there is no compelling reason for its continued processing.

5. *Right to restrict processing*

- We will comply with any request to restrict, block, or otherwise suppress the processing of personal data.
- We will continue to store personal data if it has been restricted, but not process it further. We will retain enough data to ensure the right to restriction is respected in the future.

6. *Right to data portability*

- We will provide individuals with their data so that they can reuse it for their own purposes or across different services.
- We will provide it in commonly used, machine-readable formats, and send it directly to another controller if requested.

7. *Right to object*

- We will respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.
- We will respect the right of an individual to object to direct marketing, including profiling.
- We will respect the right of an individual to object to processing their data for scientific and historical research and statistics.

8. *Rights in relation to automated decision making and profiling*

- We will respect the rights of individuals in relation to automated decision making and profiling.
- Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

Privacy Notices

Privacy notices will be supplied at the time we obtain personal data, if the data is being obtained directly from the individual. If the data is not obtained directly from the individual, then we will provide a privacy notice within one month of the data being obtained. Where we envisage data being disclosed to another recipient, we will provide a privacy notice prior to the data being disclosed.

Our privacy notices will be concise, transparent, intelligible and easily accessible. They will be provided free of charge and written in clear, plain language. We will include the following information in privacy notices to all data subjects:

- The identity and contact details of the employer;
- A description of the personal data that is collected;
- The purposes for processing the data;
- The legal basis on which the processing will take place;
- Who the personal data is shared with;
- Whether personal data is transferred outside of the EEA and if so, details of the safeguards that are in place to protect the security of the data;
- How long the personal data will be kept for; and
- Details about the rights that employees have in relation to that personal data, for example the right to request that the employer rectify any incorrect information

Subject Access Requests

An individual has the right to receive confirmation that their data is being processed, access to their personal data and any supplementary information. We will provide an individual with a copy of the information they request, free of charge. This will occur without delay, and within one month of their request being received. We will provide data subjects with access to their information in commonly used electronic formats. If complying with a request is complex or multifaceted, the timescale for responding may be extended to three months with approval from the relevant Data Controller. The individual must be informed of this extension within one month of their original request being received. Following the receipt of a subject access request, we will ensure that the data requested is not altered or amended in any way.

We retain the right to refuse to respond to certain requests and may choose, in circumstances of the request being manifestly unfounded or excessive, to charge a fee. If the request is for a large quantity of data, we will request that the individual specify precisely the information they are requesting.

Right to Erasure

Individuals have a right to have their data erased and for processing to cease in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and / or processed
- Where consent is withdrawn
- Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed or otherwise breached data protection laws
- To comply with a legal obligation
- The processing relates to a child

We will only refuse to comply with a right to erasure in the following circumstances:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

If personal data that needs to be erased has been passed onto other parties or recipients, they will be contacted and informed of their obligation to erase the data. We will inform the individual of those recipients upon request.

Right to Object

Individuals have the right to object to their data being used on grounds relating to their particular situation. We will inform individuals of their right to object in our privacy notices. We will cease processing unless:

- We have legitimate grounds for processing which override the interests, rights and freedoms of the individual.
- The processing relates to the establishment, exercise or defence of legal claims.

Right to restrict automated profiling or decision making

We will only carry out automated profiling or decision making that has a legal or similarly significant effect on an individual in the following circumstances:

- It is necessary for the entry into or performance of a contract.
- Based on the individual's explicit consent.
- Otherwise authorised by law.

In these circumstances, we will:

- Give individuals detailed information about the automated processing.
- Offer simple ways for them to request human intervention or challenge any decision about them.
- Carry out regular checks and user testing to ensure our systems are working as intended.

Third Parties

We will have written contracts in place with any third-party data controllers and / or processors that we use or have need to interact with. This includes the transfer of personal data to our clients and potential clients for the purposes of demonstrating our competence and ability to discharge our contractual obligations. The contracts will contain specific clauses that set out the liabilities, obligations and responsibilities of each party. As a data controller, we will only appoint processors who can provide sufficient guarantees under GDPR and that the rights of data subjects will be respected and protected. As a data processor, we will only act on the documented instructions of a controller. We acknowledge our responsibilities as a data processor under GDPR and we will protect and respect the rights of data subjects.

Our contracts will comply with the standards set out by the Information Commissioners Office and, where possible, follow the standard contractual clauses which are available. Our contracts with other data controllers and / or data processors will set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller.

As a minimum, our contracts will include terms that specify:

- Acting only on written instructions
- Those involved in processing the data are subject to a duty of confidence
- Appropriate measures will be taken to ensure the security of the processing
- Processors will only be engaged with the consent of the controller and under a written contract
- The controller will assist the processor in dealing with subject access requests and allowing data subjects to exercise their rights under GDPR
- The processor will assist the controller in meeting its GDPR obligations in relation to the security of processing, notification of data breaches and implementation of Data Protection Impact Assessments
- Delete or return all personal data at the end of the contract
- Submit to regular audits and inspections and provide whatever information necessary for the controller and processor to meet their legal obligations
- Nothing will be done by either the controller or processor to infringe on GDPR.

Audits, Monitoring and Training

Regular audits to manage and mitigate risks related to data protection will ensure the data register is maintained to include accurate, relevant data. The register contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant. Data Controllers and Processors will conduct regular data audits as defined by the procedures contained in our Integrated Management Systems.

Employees will receive suitable training on data protection law specific to their role. This will include training on what constitutes a breach, how to identify a breach and how breaches should be reported. Employees must complete all training they are nominated to undertake. Employees who change roles or take on new responsibilities are responsible for requesting new data protection training relevant to their new role or responsibilities.

Reporting Breaches


The King Group has a legal obligation to report any data breaches to the Information Commissioners Office within 72 hours. Any breaches of this policy, our procedures or data protection laws must be reported to the appropriate Data Controller and the Group Strategic Development Manager as soon as any employee becomes aware of a breach. The prompt reporting of actual or potential data protection compliance failures is vital to ensure we can:

- Investigate the non-compliance and take remedial action where necessary
- Maintain a register of compliance failures



- Notify the Information Commissioners Office of any compliance failures that are material either in their own right or as part of a pattern of failures

The King Group takes compliance with this policy very seriously. Failure to comply places the Group and individuals at risk. Employees who fail to notify a breach or are found to have known or suspected a breach has occurred but not followed the correct reporting procedures may be subject to disciplinary proceedings.

Approved By	Position	Signature	Date
Harold W Martin	Chairman		January 2020