**KMS PRIVACY NOTICE**

This privacy notice applies between you and Ken Mallinson and Sons (KMS) Limited. KMS takes the privacy of your information very seriously. This privacy notice applies to our use of all Data collected by us or provided by you in relation to your association with KMS. **Please read this privacy notice carefully.**

**DEFINITIONS AND INTERPRETATION**

In this policy, the following definitions are used:

**DATA**

Collectively all information that you submit to KMS. Personal data we gather may include: individuals' phone number, email address,

educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality,

job title and CV. This list in not exhaustive, it will however, only be limited to data required legally and in accordance with contracultural

agreements.

**SPECIAL CATERGORIES 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 special categories of personal data should be strictly controlled in accordance with this policy.

**DATA CONTROLLER**

‘Data controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law.

**DATA PROCESSOR**

‘Data Processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

**PROCESSING**

‘Processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by 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.

**SCOPE**

This policy applies to all staff, who must be familiar with this policy and comply with its terms. This policy supplements our other policies relating to personal data. 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 before being adopted. Eddie Harris; the Data Security Manager (DSM); has overall responsibility for the day-to-day implementation of this policy. You should contact him for further information about this policy if necessary.

**PRINCIPLES**

KMS shall comply with the principles of data protection (the Principles) enumerated in the EU General Data Protection Regulation. We will make every effort possible in everything we do to comply with these principles. The Principles are: Lawful, fair and transparent. Data collection must be fair, for a legal purpose and we must be open and transparent as to how the data will be used. Limited for its purpose. Data can only be collected for a specific purpose. Data minimisation. Any data collected must be necessary and not excessive for its purpose. Accurate. The data we hold must be accurate and kept up to date. Retention. We cannot store data longer than necessary.

Integrity and confidentiality. The data we hold must be kept safe and secure.

**ACCOUNTABILITY AND TRANSPARENCY**

KMS will ensure accountability and transparency in all our use of personal data. KMS will keep a written record of how all the data processing activities comply with each of the Principles. This will be kept up to date and will be approved by the DSM. KMS will also comply with data protection laws and the accountability and transparency Principle of GDPR. KMS understands their responsibilities to ensure data protection obligations are met and this will be ensured by carrying out the following: Fully implement all appropriate technical and organisational measures. Maintain up to date and relevant documentation on all processing activities. Conducting Data Protection Impact Assessments. Implement measures to ensure privacy by design and default, including: Data minimisation, pseudonymisation, transparency, allow individuals to monitor processing, creating and improving security and enhanced privacy procedures on an ongoing basis.

**FAIR AND LAWFUL PROCESSING**

KMS will process personal data fairly and lawfully in accordance with individuals’ rights under the first Principle. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening. If we cannot apply a lawful basis (explained below), our processing does not conform to the first principle and will be unlawful. Data subjects have the right to have any data unlawfully processed erased. KMS is classified as a data controller and data processor. We must maintain our appropriate registration with the Information Commissioners Office to continue lawfully controlling and processing data. We will comply with our contractual obligations and act only on the documented instructions of the data controller. If we at any point determine the purpose and means of processing with the instructions of the controller, we shall be considered a data controller and therefore breach our contract with the controller and have the same liability as the controller. As a data processor, we must: Not use a sub-processor without written authorisation of the data controller, co-operate fully with the ICO or other supervisory authority, ensure the security of the processing, keep accurate records of processing activities and notify the controller of any personal data breaches. If you are in any doubt about how we handle data, contact the DSM for clarification.

**LAWFUL BASIS FOR PROCESSING DATA**

KMS will establish a lawful basis for processing data. Ensure that any data you are responsible for managing has a written lawful basis approved by the DSM. It is your responsibility to check the lawful basis for any data you are working with and ensure all of your actions comply the lawful basis. At least one of the following conditions must apply whenever we process personal data: Consent. Hold recent, clear, explicit, and defined consent for the individual’s data to be processed for a specific purpose. Contract, the processing is necessary to fulfil or prepare a contract for the individual. Legal obligation, there is a legal obligation to process the data (excluding a contract). Vital interests. Processing the data is necessary to protect a person’s life or in a medical situation. Public function. Processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law. Legitimate interest. The processing is necessary for our legitimate interests. This condition does not apply if there is a good reason to protect the individual’s personal data which overrides the legitimate interest.

**RESPONSIBILITIES – OURS**

Analysing and documenting the type of personal data we hold. Checking procedures to ensure they cover all the rights of the individual. Identify the lawful basis for processing data. Ensuring consent procedures are lawful. Implementing and reviewing procedures to detect, report and investigate personal data breaches. Store data in safe and secure ways. Assess the risk that could be posed to individual rights and freedoms should data be compromised.

**RESPONSIBILITIES - YOURS**

Fully understand your data protection obligations. Check that any data processing activities you are dealing with comply with our policy and are justified. Do not use data in any unlawful way. Do not store data incorrectly, be careless with it or otherwise cause us to breach data protection laws and our policies through your actions. Comply with this policy at all times. Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay.

**RESPONSIBILITIES - DATA SECURITY MANAGER (DSM)**

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 which 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. Appointed DSM is Eddie Harris eh@kmstransport.com

**RESPONSIBILITIES - IT**

Ensure 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.

* **Where data is stored; Servers** (Exchange, Proofpoint), Mobile Devices, Laptops, Printers, USB Sticks – cannot be taken off site after 25 May 2018, NAS, Telephone call recording system and Website portal for customer job entry.
* **How data is destroyed**; Data will be marked as deleted and only accessible by management/ data security manager. Paper waste is destroyed outside premises by 707 waste services.
* **Processes in place to stop a cyber-attack;** Firewalls installed on servers and PC’s, Hardware firewall with all unnecessary ports closed, McAfee installed on servers and PC’s, shadow copies are deployed on servers and back up at 0700 and 1200hrs,

off-site backup at end of working day, 3/2/1 Back up rule applied, laptops to be encrypted in case of loss/theft, penetration testing on firewall.

* **IT Policy;** Password to be changed every 30 days, Password must contain upper case, lower case and symbol and number and at least 8 characters, PC’s must be locked when not in use, user accounts auto locked after 3 incorrect password attempts and can only be unlocked by IT and no USB to be taken off site.
* **How we access devices with data stored and is accessible;** Username/Password access on PC’s/Laptops, passwords on mobile devices (all apple devices are linked to i-cloud to delete data if lost).

**RESPONSIBILITES- MARKETING**

Approving data protection statements attached to emails and other marketing copy. Addressing data protection queries from clients, target audiences or media outlets. Coordinating with the DSM to ensure all marketing initiatives adhere to data protection laws and the company’s Data Protection Policy. The Customer Relationship Management (CRM) system is a consent and subscription system and data will be kept as long as there is a legitimate interest and explicit consent must be given (documented) when dealing with B2C. All data shall be secured safely and within the safe parameters of IT responsibilities.

**ACCURACY AND RELEVANCE**

KMS 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 DSM.

**DATA COLLECTION**

KMS will obtain information from you in various methods, i.e. verbally, emails, telephone and data capture forms. Consent must be ‘opted in’ and shall be as easy to withdraw as it is to agree. The data collected will be email addresses, personal (work) addresses, qualifications, education and skills, CVs, health surveillance and any relevant health issues, driving licence details, national insurance number, bank details, next of kin details, marital details and when B2B all relevant details to ensure legal compliance (insurances, trade associations etc). This list in not exhaustive, it will however, only be limited to data required legally and in accordance with contractual

agreements. (See paragraph regarding Lawful Basis for Processing Data). We do not collect data from children under 16.

**DATA SECURITY**

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

**STORING DATA SECURELY**

In cases 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 that are changed regularly. We encourage all staff to use a password manager to create and store their passwords. Data stored on CDs or memory sticks will be encrypted or password protected and locked away securely when they are not being used. The DSM will approve any cloud used to store data. Servers containing personal data will be kept in a secure location, away from general office space. Data swill be regularly backed up in line with the company’s backup procedures. Data will not be saved directly to mobile devices such as laptops, tablets or smartphones. All servers containing sensitive data will be approved and protected by security software. All possible technical measures will be put in place to keep data secure. All data controllers and processors shall operate a clear desk policy with all sensitive data stored securely to prevent unauthorised access.

**ACCEPTABLE USAGE POLICY**

KMS Acceptable Usage Policy covers the security and use of all KMS information and IT equipment. It also includes the use of email, internet, voice and mobile IT equipment. This policy applies to all KMS employees, contractors, agents and third parties.

**DATA RETENTION**

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

**DISCLOSURE OF PERSONAL DATA**

KMS will never share your personal data with any Third-Party (i.e., a party other than an entity within the KMS Group) business organisation that intends to use it for their own purposes, other than as required by law i.e. DVLA, DVSA. KMS, as part of a group, may transfer or disclose your personal data to another data controller in the KMS Group to be used for similar purposes, at its discretion, and you hereby consent to such transfer or disclosure. If your personal data is transferred or disclosed to another data controller within the KMS Group, that other data controller shall have the same rights and obligations regarding your personal data as KMS. With your consent, KMS may share your personal data with Third-Parties (i.e. parties other than entities within the KMS Group) such as those who assist us in providing the products and services and who perform operations, but only in the strictly limited circumstances: Our “Third-Party Data Processors” (service providers such as our fulfilment and activation partners, and digital agencies, hosting providers, data storage providers and other technical partners) who help us administer contracts, or process the data submitted to it, may have access to your data.

**TRANSFERRING DATA INTERNATIONALLY**

There are restrictions on international transfers of personal data. We will not transfer personal data abroad, or anywhere else outside of normal rules and procedures without express permission from the DSM.

**RIGHTS OF INDIVIDUALS**

Individuals have rights to their data which we will respect and comply with to the best of our ability. We will ensure individuals can exercise their rights in the following ways: Right to be informed. Providing privacy notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language. Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency. Right of access. Enabling individuals to access their personal data and supplementary information. Allowing individuals to be aware of and verify the lawfulness of the processing activities. Right to rectification. We will rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete. This will be done without delay, and no later than one month. This can be extended to two months with permission from the DSM. Right to erasure. We will delete or remove an individual’s data if requested and there is no compelling reason for its continued processing. Right to restrict processing. We will comply with any request to restrict, block, or otherwise suppress the processing of personal data. We are permitted 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. 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 a commonly used, machine-readable format, and send it directly to another controller if requested. 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. 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.

**SUBJECT ACCESS REQUESTS**

An individual has the right to receive confirmation that their data is being processed, access to their personal data and supplementary information which means the information which should be provided in a privacy notice. 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 receipt. We endeavour to provide data subjects access to their information in commonly used electronic formats, and where possible, provide direct access to the information through a remote accessed secure system. If complying with the request is complex or numerous, the deadline can be extended by two months, but the individual must be informed within one month. The DSM must approve any extension of the deadline. We can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, we can request the individual specify the information they are requesting. This can only be done with express permission from the DSM. Once a subject access request has been made, we will change or amend any of the data that has been requested. Doing so is a criminal offence.

**DATA PORTABILITY REQUESTS**

We will provide the data requested in a structured, commonly used and machine-readable format. This would normally be a CSV file, although other formats are acceptable. We must provide this data either to the individual who has requested it, or to the data controller they have requested it be sent to. This must be done free of charge and without delay, and no later than one month. This can be extended to two months for complex or numerous requests, but the individual must be informed of the extension within one month and you must receive express permission from the DPO first.

**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.

**HOW WE DEAL WITH THE RIGHT TO ERASURE**

We can 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. In the interests of Health and Safety. If personal data that needs to be erased has been passed onto other parties or recipients, they must be contacted and informed of their obligation to erase the data. If the individual asks, we must inform them of those recipients.

**THE RIGHT TO OBJECT**

Individuals have the right to object to their data being used on grounds relating to their situation. We shall 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. We shall always inform the individual of their right to object at the first point of communication, i.e. in the privacy notice. We will offer a way for individuals to object.

**THE RIGHT TO RESTRICT AUTOMATED PROFILING OR DECISION MAKING**

We may 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 shall: 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.

**USING THIRD PARTY CONTROLLERS AND PROCESSORS**

As a data controller and data processor, we have written contracts in place with any third party [data controllers (and/or) data processors] that we use. The contract must contain specific clauses which set out our and their liabilities, obligations and responsibilities.

As a data controller, we must 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 must 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.

**CONTRACTS**

Our contracts comply with the standards set out by the ICO and, where possible, follow the standard contractual clauses which are available. Our contracts with [data controllers (and/or) data processors] 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 shall 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.

Sub-processors will only be engaged with the prior 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.

**CRIMINAL OFFENCE DATA -CRIMINAL RECORD CHECKS**

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject. We cannot keep a comprehensive register of criminal offence data. All data relating to criminal offences is a special category of personal data and must be treated as such. KMS will obtain approval from the DSM prior to carrying out a criminal record check.

**DATA AUDITS**

Regular data audits to manage and mitigate risks will inform the data register. This 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. You must conduct a regular data audit as defined by the DSM and normal procedures.

**MONITORING**

Everyone must observe this policy. The DSM has overall responsibility for this policy. KMS will keep this policy under review and amend or change it as required. You must notify the DSM of any breaches of this policy. You must comply with this policy fully and always.

**TRAINING**

You will receive adequate training on provisions of data protection law specific for your role. You must complete all training as requested. If you move role or responsibilities, you are responsible for requesting new data protection training relevant to your new role or responsibilities. If you require additional training on data protection matters, contact the DSM. GAP analysis shall be carried out by the DSM to identify any areas and/or individuals that require additional training/addressing.

**REPORTING BREACHES**

Any breach of this policy or of data protection laws must be reported as soon as practically possible. This means as soon as you have become aware of a breach. KMS has a legal obligation to report any data breaches to ICO within 72 hours. All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to: Investigate the failure and take remedial steps if necessary. Maintain a register of compliance failures. Notify the ICO of any compliance failures that are material either in their own right or as part of a pattern of failures. Any member of staff who fails to notify of a breach or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action. Please refer to our reporting system for our reporting procedure. Potential fines for any breach of this Policy is a maximum of 4% of annual turnover.

**FAILURE TO COMPLY**

We take compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk. The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal. The penalty imposed by ICO can be a maximum of 4% of annual turnover.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the DSM.

**REVIEWS**

|  |  |  |
| --- | --- | --- |
| **DATE** | **RESPONSIBLE PERSON** | **SUMMARY OF REVIEW** |
| 9th May 2018 | EDDIE HARRIS | POLICY WRITTEN - VERSION 1 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

****

**Eddie Harris**

**Compliance Manager**

**Dated 9th May 2018**