



Königstone

Privacy Policy

OVERVIEW	1
PURPOSE	2
SCOPE	2
POLICY STATEMENT	2
Information we collect and process as Data Controllers	3
Information we collect and process as Data Processors	5
Recipients	5
Managing Consents	5
Information Security	6
POLICY COMPLIANCE MEASUREMENT	6
EXCEPTIONS	6
NON-COMPLIANCE	6
APPENDIX 1 – LAWFULNESS OF PROCESSING	7
APPENDIX 2 – PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA	8
APPENDIX 3 – DATA PROCESSOR OBLIGATIONS	10

Overview

Königstone Ltd observes the highest standards when protecting personal information and requires clear policies and practices to ensure it maintains and improves these standards on a continuous basis. This will inspire confidence in those whose personal information we store and process that it is protected and gives them control over its use. Königstone Ltd is committed to “Privacy by Design” in its approach to projects and promoting privacy and data protection compliance. The Company recognises its responsibility to be accountable for the lawful processing of personal information.



Königstone

Purpose

This policy explains when and why we collect personal information about people in all circumstances, how we use it, the conditions under which we may disclose it to others and how we keep it secure. It also includes a summary of the key articles of the General Data Protection Regulation (“GDPR”) (Regulation (EU) 2016/679) which apply.

Scope

This policy applies to all staff, sub-contractors and agencies working for or on behalf of Königstone Ltd, and to the Company as a whole, whether operating as a Data Controller of customer, staff, sub-contractor and employee candidate information or a Data Processor of information on behalf of the Company’s customers.

Policy Statement

Königstone Ltd adheres to the following Data Protection principles as defined under the GDPR:

1. Personal data shall be processed fairly and lawfully and, in particular shall not be processed unless—
 - (a) at least one of the conditions in Article 6 is met, and
 - (b) in the case of sensitive personal data, at least one of the conditions in Article 9 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under the GDPR.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.



Königstone

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Königstone Ltd has established that consent is the most appropriate lawful basis for processing personal data.

Information we collect and process as Data Controllers

Standard Personal Data

With each individual's explicit consent, Königstone Ltd collects and holds the following personal data on its systems, where available, in its capacity as a Data Controller:

- Prefix, First and Last Name, Suffix
- Business Title
- Date of Birth
- National Insurance Number
- Telephone Numbers, including mobile number where available
- Email Address, including private email address where specifically authorised to do so by the individual
- Business Address
- Private Address where specifically authorised to do so by the individual
- Correspondence records
- Their Consent Opt-in/Opt-out preference
- Link to their LinkedIn Profile where available
- Participation and interest in the Company's products, services, events, research and other related information

Customer and Prospect Information

No further personal data is collected and retained on individual customers and prospects beyond the Standard Data above. This data is collected for the purposes of communicating about and delivering the Company's products and services. It is retained for as long as the individual consents.

Personnel Information

The following information is collected and retained on individual members of staff, in addition to the Standard Data above:



Königstone

- Identification documents, including copies of at least two of Birth Certificate, Passport and Driving Licence
- Information required by HMRC (male/female, date of birth, private address, National Insurance number, employment start date, job status and student loan details)
- Information on Königstone Ltd's Personnel Form
- Salary, Hourly Pay, Pension and other Benefit payments
- Employment contract
- Medical information where relevant
- Curriculum Vitae and former employer references, collected at the time of recruitment

This data is collected for the purposes of:

- Meeting the Company's obligations towards Government Agencies, including HMRC and the Pensions Authority
- Managing the Company's Human Resources including administering the Company's Payroll
- Ensuring employees meet or exceed the Company's Information Security, Data Privacy and Quality standards

The data is retained for a minimum of six (6) years in order to meet statutory requirements and protect the Company from any claims made against it in future.

Candidate Employee Information

In addition to the Standard Data above, during discussions with candidates for employment with the Company, the following information is collected:

- Curriculum Vitae and former employer references
- Salary details

This data is collected for the purposes of recruiting new employees and ensuring they meet the Company's business requirements as well as its Information Security, Data Privacy and Quality standards.

On acceptance of the Company's employment Offer Letter, further data will be collected as noted above under "Staff Information".

Data on unsuccessful candidates who have the potential to be recruited at a future date may be retained indefinitely with their explicit consent.



Königstone

Individual Sub-Contractor Information

From an individual Sub-Contractor perspective, both of the Company's roles as Data Controller and Data Processor apply.

A. Data Controller

As a Data Controller, the Company holds the following personal data in addition to the Standard Data above:

- Identification documents, including copies of any of the following; Birth Certificate, Passport and Driving Licence
- Curriculum Vitae
- Information on Königstone Ltd's Employee Form
- Employment Contract

This data is collected for the purposes of employing contractors and ensuring they meet the Company's business requirements as well as its Information Security, Data Privacy and Quality standards.

B. Data Processor

Depending on the role, the sub-Contractor may be required to process personal data on behalf of the Company in its capacity as a Data Processor both for internal personnel data and for one or more of its customers.

Information we collect and process as Data Processors

From time to time and as part of the Company's products and services, Königstone Ltd collects and processes personal data on behalf of its customers, acting as a Data Processor. This includes names, email addresses, business addresses and in some cases salary and other confidential information.

Königstone Ltd will comply with Article 28 of the GDPR (see Appendix 3) when acting as a Data Processor.

Königstone Ltd can be held liable for any GDPR infringements and therefore must have the appropriate contracts in place with its Data Controller customers to mitigate this risk as well as maintaining its own internal standards.



Königstone

Recipients

A. Königstone Ltd as Data Controller

Where Königstone Ltd is the Data Controller, with Personnel and Candidate Information, the following people will be the Recipients:

- The Managing Director
- Managers
- Line Managers

A. Königstone Ltd as Data Processor

Where Königstone Ltd is the Data Processor, the following people will be the Recipients:

- The Customer Account
- HMRC and other Government Bodies.
- The Privacy Officer, Scheduling Employees working on Customer Jobs.

A. Third Party Recipients

At no time will Königstone Ltd release personal information to third parties without the explicit consent of the Data Subject or unless required to do so by law.

Managing Consents

Königstone Ltd has a duty to manage the consents granted by individuals to process their personal data and has the systems in place for this purpose. This includes continuing to offer people the option to withdraw consent at any time, with a clear process, maintaining evidence of consents (eg. who, when, how and what was communicated), reviewing them periodically and refreshing them if there is any change in circumstances.

Information Security

Königstone Ltd's adherence to its policies and procedures with regard to Information Security and the protection of personal data. The Company uses encryption and passcodes where it is appropriate to do so, and we ensure that any Data Processor we use also implements appropriate technical and organizational measures that meet our Information Security standards.



Königstone

Policy Compliance Measurement

The Company's Information Security Impact Assessments include risk assessments for the processing of personal data. The Company will maintain records of all processing activities, whether as Data Controller or Data Processor, including details of data retention periods, transfers of personal data and any recipients outside the European Union. Although the Company is exempt from appointing a Data Protection Officer under Article 37 of the GDPR, the Company already has a Management Representative for its Information Security policies and processes, and the duties of Privacy Officer have been added to this role.


Separate contracts must be in place with any Sub-Processors the Company appoints from time to time setting out their obligations with regard to any Data Controller agreements.

Exceptions

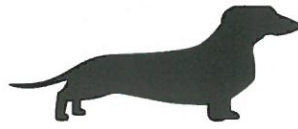
No exceptions will be permitted to this policy.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

signed: 

James Bull
Managing Director
Date: 06th February
2019



Appendix 1 – Lawfulness of Processing

GDPR Article 6 Summary

1. The data subject has given their consent to the processing of their personal data for one or more specific purposes.
2. The processing is necessary:
 - a. for the performance of a contract to which the data subject is a party, or
 - b. for the taking of steps at the request of the data subject with a view to entering into a contract.
3. The processing is necessary for compliance with any legal obligation to which the data controller is subject.
4. The processing is necessary in order to protect the vital interests of the data subject or of another natural person.
5. The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
6. The processing is necessary for the purposes of legitimate interests pursued by the data controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
7. The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.



Appendix 2 – Processing of special categories of personal data

GDPR Article 9 Summary

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.
2. Paragraph 1 shall not apply if one of the following applies:
 - (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
 - (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
 - (c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
 - (d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
 - (e) processing relates to personal data which are manifestly made public by the data subject;
 - (f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
 - (g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data



subject;

- (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
 - (i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
 - (j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.



Appendix 3 – Data Processor Obligations

GDPR Article 28 Summary

1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.
2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.
3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:
 - a. processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
 - b. ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
 - c. takes all measures required pursuant to Article 32
 - d. respects the conditions referred to in paragraphs 2 and 4 for engaging another processor
 - e. taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights
 - f. assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor



Königstone

- g. at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data
 - h. makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller. The processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.
4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.
5. Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.

Version	Date	Author	Comments
1.0	10/4/18	JAB	Document Creation
1.1	15/5/18	JAB	Further amendments following legal and other advice
1.2	06/02/2019	JRAB	Change of Director