Shadbolt International

Data Protection Policy

25th May 2018

Table of Contents

1. Introduction

The General Data Protection Regulation ("GDPR") in Europe and other related laws protecting personal data (the "Law") regulate the way in which all personal data is held and processed. This policy describes how personal data must be collected, handled, stored, disclosed and otherwise "processed" to meet the Company's data protection standards and to comply with the Law. The meaning of the terms "personal data" and "processing" are provided in sections 3 and 4 below.

The Company regards the lawful and correct treatment of personal data as integral to our successful operations, and to maintain the confidence of the people we work with. To this end, we fully endorse and adhere to the principles of the Law.

2. Purpose

The purpose of this policy is to ensure that:

(A) everyone involved in the processing of personal data at the Company is fully aware of, and complies with, the requirements of the Law; and

(B) data subjects (a "data subject" being a person to whom personal data relates) are aware of their rights under the Law.

This policy should be read in conjunction with the Company's Information Security Policy and related policies and guidance as these provide more detailed guidance on correct handling of data.

3. Scope

All staff, consultants and other authorised third parties who have access to any personal data held by or on behalf of the Company must adhere to this policy.

4. Personal Data

In this policy, "personal data" includes any data which relates to a living individual who can be identified from that data or from that data and other information which is in the possession of, or is likely to come into the possession of, the Company or its representatives or service providers. In addition to factual information, it includes any expression of opinion the about an individual and any indication of the intentions of the Company or any other person in respect of an individual. References to a "data subject" are to the individual whose data is being used.

Certain personal data is considered to be particularly sensitive and is subject to stricter rules regarding its processing. These categories of personal data are referred to as "sensitive personal data" and include any personal data relating to the racial or ethnic origin of the data subject; their political opinions; their religious (or similar) beliefs; their physical or mental health condition; details of criminal offences or criminal convictions (including the commission or alleged commission of any offence, any proceedings for any offence committed or alleged to have been committed and the disposal of such proceedings or the sentence of any court in such proceedings) and genetic and biometric data.

The Company only holds personal data which is directly relevant to its dealings with a given data subject. That data will be held and processed in accordance with the Law and this policy.

5. Processing Personal Data

The word "process" (and any derivative term) includes any operation that is carried out in respect of personal data, including but not limited to collecting, storing, using, disclosing, transferring or deleting personal data.

Personal data collected by the Company is generally collected in order to:

(A) ensure that the Company can facilitate efficient transactions with, and perform its obligations and exercise its rights under contracts with, third parties including, but not limited to, its customers, partners, associates and affiliates;

(B) efficiently manage its employees, contractors, agents and consultants;

(C) efficiently and effectively manage its business; and

(D) meet all relevant obligations imposed by law.

An explanation of the lawful grounds for which personal data may be processed by the Company is provided in section 8 below.

Personal data may be disclosed within the Company and may be passed from one department to another in accordance with the data protection principles and this policy. Under no circumstances will personal data be passed to any department or any individual within the Company that does not reasonably require access to that personal data in order to achieve the purpose(s) for which it was collected and is being processed.

No department or individual within the Company may process personal data for any reason other than for the lawful purposes for which it was collected and is being processed.

6. The Data Protection Principles

Any person processing personal data must comply with the following core principles:

(A) **Lawfulness, fairness and transparency.** Personal data must be processed fairly, transparently and lawfully. You must not process an individual's personal data unless you have a lawful ground for doing so and you must inform a data subject of how and why you will process their personal data upon or before collecting it.

(B) **Purpose limitation.** Personal data must be processed only for specified and lawful purposes. Personal data must not be processed in any manner which is incompatible with those purposes.

(C) **Data minimisation.** The personal data that is processed must be adequate, relevant and limited to the minimum data necessary for the lawful purposes for which it is processed.

(D) **Accuracy.** Personal data must be accurate and, where appropriate, kept up-to-date. Any personal data which is incorrect must be rectified as soon as possible.

(E) **Data retention.** Personal data must be kept for no longer than is necessary in light of the lawful purpose(s) for which it is processed.

(F) **Rights of data subjects.** Personal data must be processed in accordance with the rights of data subjects. Data subjects will have the right to see copies of their personal data, to have inaccuracies corrected and to object to the processing of their personal data or to have their personal data deleted if it is no longer required by the Company for another important reason.

(G) **Security.** Personal data must be protected against unauthorised or unlawful processing, accidental loss, destruction or damage through appropriate technical and organisational measures.

(H) **International data transfers.** Personal data must not be transferred to a country or territory outside of 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.

(I) **Accountability.** The Company and its third party service providers are responsible for and must be able to demonstrate their compliance with this policy.

7. Consent

Personal data must only be processed if the purpose of the processing satisfies one of the lawful grounds permitted under the Law. There are various legitimate reasons for which personal data can be collected and

used. One such reason is that the individual has consented to the use of their data. Other applicable reasons are described in section 8 below.

If consent is being relied on to justify using a person's personal data, it must satisfy each of the following criteria:

(A) the consent must be limited to specific processing activities;

(B) the data subject must have been informed the about the processing activities in sufficient detail so as to be able to fully understand what they are consenting to;

(C) the consent must be "freely given". In other words, the data subject must have a genuine free choice as to whether they give the consent. Consent will not be freely given where there is a "significant imbalance of power" such that the individual does not really have a free choice about giving consent;

(D) the performance of a contract or delivery of a service cannot be made conditional upon the data subject giving their consent to the data processing, unless the data processing is required in order to perform the contract or deliver the service;

(E) the consent must be given by way of an unambiguous statement or some other clear, active communication by the data subject, such as signing a form. Consent cannot be inferred from silence or inactivity (for example, the use of pre-ticked boxes); and

(F) the consent to the processing of personal data must be clearly distinguished from other matters that the data subject is asked to agree to (for example, it should not be buried within the terms of a broader contract that the data subject is asked to sign).

Where the processing relates to sensitive personal data, the data subject's "explicit" consent must be obtained, ideally by way of a signed statement or other means which very clearly and demonstrably indicate the consent of the data subject.

A record of consents should be retained by the Company to evidence that it has been authorised to carry out the processing of a data subject's personal data.

It is important to note that a data subject has the right to withdraw their consent at any time and it must be as easy for a data subject to withdraw consent as it was for them to provide it in the first place. It is important that there are appropriate processes in place to promptly action any withdrawal of consent.

8. **Grounds for Processing Personal Data**

As noted above, consent is not the only basis on which personal data can be collected and used. There are other lawful grounds for processing personal data that the Company may be able to rely upon.

This section describes the lawful grounds for processing which are most likely to be relevant to the Company's processing activities. If you are unable to satisfy one of these grounds then you should contact the Company Secretary for advice as to whether the proposed processing activities can be undertaken.

Non-sensitive personal data

The legal grounds for processing non-sensitive personal data include:

(A) where the data subject has given their consent to the processing of their personal data. The requirements for obtaining a valid consent are explained in section 7 above;

(B) where the processing is in the Company's legitimate interests and does not cause unwarranted prejudice to the data subject;

(C) where the processing is necessary for the performance of a contract to which the data subject is a party, or for the taking of steps (at the request of the data subject) with a view to entering into a contract; or

(D) where the processing is required by law.

Sensitive personal information

Sensitive personal data is subject to stricter legal controls and the circumstances in which it can be processed are more limited than in respect of other personal data. The legal grounds for processing sensitive personal data include:

(A) where the data subject has given their explicit consent;

(B) where the processing is necessary for the purposes of carrying out the obligations and exercising rights of the Company or the data subject in the field of employment law or social security law;

(C) for the purposes of occupational health or the assessment of the working capacity of an employee;

(D) for equal opportunity purposes, where the processing is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained; or

(E) where the processing is necessary for the purpose of, or in connection with, any legal proceedings, obtaining legal advice, or establishing, exercising or defending legal rights.

The lists above set out the commonly applicable grounds for using personal data and sensitive personal data. There are other grounds that have more limited application. If you are unable to satisfy one of these grounds then you should contact [the Data Protection Officer] for advice as to whether the proposed processing activities can be undertaken.

9. **High Risk Processing Activities**

Wherever the processing of personal data is likely to result in a "high risk" to the data subject (for example, where it is particularly intrusive to a data subject's privacy), the Company will need to, before carrying out the processing activity, perform an assessment of the potential impact of the intended processing on the rights and freedoms of the data subject. The impact assessment should be conducted by the Company Secretary.

The monitoring or profiling of data subjects and the processing of sensitive personal data on a large scale are examples of processing activities that might present a high-risk.

10. **Fair Processing Information**

Any forms (whether paper-based or web-based) that gather data on an individual should contain a statement explaining what the information is to be used for and to whom it may be disclosed.

Regardless of how personal data is obtained (whether it is obtained from the data subject or from a third party), the data subject must be provided with certain information the about the processing of their personal data by the Company. This information must be provided at or before the time at which the personal data is collected (or, if the personal data is obtained from a third party, within a reasonable time of obtaining the personal data or at the time of the first communication with the data subject, whichever is earlier).

The information provided to the data subject must include the following:

(A) the identity and contact details of the Company and Company Secretary;

(B) the categories of personal data collected in relation to the data subject;

(C) if the personal data is not obtained from the data subject, the source(s) of the personal data;

(D) the purpose(s) for which personal data will be processed, including the legal ground for the processing (see section 8 above). If the legal ground involves "legitimate interests", a description of those legitimate interests must also be provided;

(E) if personal data is processed based on the data subject's consent, an explanation of the data subject's right to withdraw their consent at any time;

(F) the categories of personal data that may be disclosed to third parties and the reasons for these disclosures;

(G) if the data processing is a contractual requirement, whether the data subject is obliged to provide the personal data on that basis, and the possible consequences of a failure to provide the information;

(H) any intention to transfer the personal data outside the European Economic Area and information the about the level of protection that will be afforded to the transferred data (including details of how the legal requirements for the transfer will be satisfied);

(I) information the about the existence of any automated decision making (for example, profiling) undertaken by the Company based on the personal data, including details of the logic involved and its impact on the data subject;

(J) the period for which the personal data will be retained, or (if it is not possible to provide a specific time period) the criteria that will be used to determine the retention period;

(K) a general description of the Company's policies and practices with respect to protecting the confidentiality and security of personal data;

(L) the existence of the data subject's rights; and

(M) any other information that is necessary to guarantee that the processing of the personal data is fair in the circumstances.

This information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language that will be easy for the data subject to understand.

If any of the information described above changes after it has been provided to the data subject, the data subject must be provided with an updated copy of the information.

11. **Third Party Service Providers**

Where the Company instructs a third party to process personal data on behalf of the Company (referred to as a "data processor"), the third party must enter into a written agreement with the Company that:

(A) provides details of the processing of personal data that they are being instructed to carry out;

(B) requires the third party to process the personal data only in accordance with the Company's written instructions and to the extent necessary for them to fulfil their obligations to the Company under the agreement;

(C) requires the third party to implement appropriate technical and organisational measures and controls to ensure the confidentiality and security of the personal data; and

(D) imposes any additional data processing obligations required by law. Guidance on the additional legal obligations that the agreement must include can be obtained from the Company Secretary.

The data processing agreement should be approved by the Company Secretary and signed by both parties before any personal data is transferred to the data processor.

When contracting with a data processor, it is important that the Company conduct appropriate due diligence both at the outset of the relationship and on a periodic basis thereafter, to ensure that the data processor is capable of complying, and does comply, with the requirements referred to in paragraphs (B) - (D) above.

12. Disclosure of Data

The Company must ensure that personal data is not disclosed to unauthorised third parties. All staff should exercise caution when asked to disclose any personal data to a third party. This section does not apply to data processors, which are addressed in section 11 above.

Personal data should not be disclosed orally or in writing to third parties without the consent of the data subject and approval from the Company Secretary.

In some circumstances, the Law permits the disclosure of personal data without needing to obtain the prior consent of the data subject. Such disclosures might (depending on the circumstances) be permitted where this is:

(A) necessary to safeguard national security;

(B) necessary for the prevention or detection of crime, in the substantial public interest, and where obtaining consent from the data subject would prejudice that purpose;

(C) necessary for the administration of justice;

(D) necessary to comply with applicable law; or

(E) necessary to protect the vital interests of the data subject (this refers to life and death situations), but only where their consent cannot be obtained.

Requests for personal data from third parties must be supported by appropriate paperwork and any disclosures must be approved by the Company Secretary.

13. International Transfers of Personal Data

Specific legal requirements apply to the transfer of personal data out of the European Economic Area ("EEA"). The "transfer" of data includes sending data to another country or allowing that data to be accessed remotely in another country, regardless of whether the Company transfers personal data outside the EEA itself or a data processor does so when acting on the Company's behalf.

Personal data must not be transferred outside the EEA unless the recipient country ensures an adequate level of protection for the rights and freedoms of data subjects. This requirement can be satisfied by:

(A) the recipient country having been subject to an "adequacy determination" by the European Commission (to date, only a handful of countries are subject to an adequacy determination, such as Canada and Israel);

(B) the entry into a data transfer agreement between the Company and the non-EEA recipient of the personal data which contains standard contractual clauses that have been approved by the European Commission; or

(C) certification of a US recipient under the EU-US Privacy Shield scheme.

Before such a transfer takes place, you must first check with the Data Protection Officer to determine whether the transfer is lawful.

14. **Retention and Disposal of Data**

Personal data must not be retained for longer than is necessary for the lawful purposes for which it is processed. To achieve this, each category of personal data processed by the Company must be subject to a retention period which can be justified by reference to those lawful grounds. Retention periods must be monitored and, upon their expiry, the relevant personal data must be deleted or anonymised (so that it is no longer possible to identify the data subject to whom the personal data relates).

For example, once an employee has left the Company, it will not be necessary to retain all the information held on them because much of this is only required to administer the employment relationship, such as bank details for salary payments. Some data will need to be kept for longer periods than others, for example where it is necessary to retain certain records in order for the Company to comply with its legal obligations.

Personal data must be disposed of securely in a way that protects the rights and privacy of data subjects and ensures the permanent erasure of the data (e.g. shredding, disposal as confidential waste, or secure electronic deletion). Hard drives of redundant PCs should be wiped clean before disposal.

15. **Data Protection and Data Security**

It is critical that the Company protects the personal data in its possession or control by applying appropriate technical and organisational security measures to protection the data.

In addition to the specific security policies that apply, all staff must comply with the following when processing and / or transmitting personal data:

(A) Personal data, whether held electronically or in paper form, must be kept securely at all times. the Company staff, consultants and authorised third parties must ensure that appropriate technical and organisational measures are in place to prevent unauthorised or accidental access, use, disclosure, loss or damage when personal data is being processed (including but not limited to when it is at rest or in transit). Technical measures, for example, include using encryption tools to protect personal data held in electronic form. Organisational measures, for example, include storing paper records containing personal data in locked cabinets.

(B) It is essential that if personal data is lost, damaged, compromised, misdirected or stolen, or otherwise processed in an unauthorised manner, that it is reported to the [Data Protection Officer].

(C) Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data in accordance with section 14 above.

(D) Personal data should not be disclosed except in accordance with sections 11 and 12 above.

16. **Data Subject Rights**

Data subjects are entitled to exercise certain rights in respect of their personal data. These rights include access to the personal data held by the Company the about them, the right to require the rectification of their data (where it is incorrect) and in certain circumstances the right to object to the processing of their personal data or to require it to be erased.

Data subjects have a number of legal rights in relation to their personal data. These rights include:

(A) the right to obtain information regarding the processing of their personal data and access to the personal data which the Company hold the about them (or which is held on the Company's behalf);

(B) the right to receive a copy of any personal data which the Company processes the about them;

(C) the right to request that the Company rectify their personal data if it is inaccurate or incomplete;

(D) the right to request that the Company erase their personal data in certain circumstances. This may include (but is not limited to) circumstances in which:

(1) it is no longer necessary for the Company to retain their personal data for the purposes for which we collected it; or

(2) the Company are only entitled to process the data subject's personal data with their consent (i.e. because no other lawful ground for processing the personal data applies), and the data subject withdraws their consent; and

(E) the right to lodge a complaint with the data protection regulator, the Information Commissioner's Office, if the data subject thinks that any of their rights have been infringed by the Company.

Requests to exercise these rights should be sent to the Company Secretary immediately upon receipt.

17. **Record Keeping**

Accurate and up to date records of the processing activities carried out by the Company must be maintained within the organisation. These records must include:

(A) details of the Company Secretary;

(B) the purposes of the processing;

(C) the categories of data subject;

(D) the categories of recipients of personal data;

(E) the categories of transfers of personal data to countries outside the European Economic Area;

(F) the envisaged time limits for erasure of the personal data (where possible); and

(G) a general description of the technical and organisational security measures adopted by the Company.

The Company Secretary will keep a central record of the Company's processing activities and new processing activities or material changes to existing processing activities must be notified to the Company Secretary.

18. **Roles and Responsibilities**

The Company board of directors are ultimately responsible for ensuring that the Company meets its legal obligations.

The Company Secretary is responsible for:

(A) keeping the Company board updated the about data protection responsibilities, risks and issues;

(B) reviewing all data protection procedures and related policies;

(C) arranging data protection training and advice for employees;

(D) handling all data protection queries for employees;

(E) dealing with all requests from individuals to see the data the Company holds the about them (Subject Access Requests); and

(F) checking and approving any contracts or agreements with data processors.

The Company Secretary is responsible for:

(A) ensuring all systems, services and equipment used for storing personal data meet acceptable security standards;

(B) performing regular checks to ensure hardware and software if functioning properly; and

(C) evaluating any third party services the Company is considering using to store or process personal data (i.e. cloud services).