# KWT GLOBAL DATA PROTECTION POLICY

## TABLE OF CONTENTS

## 1. Overview of Data Protection Policy

This Data Protection Policy sets out how Kwittken Ltd ("KWT Global") handles the personal data of our clients, suppliers, employees, workers and other individuals.

This Data Protection Policy applies to all personal data we process regardless of how that data is stored or whether it relates to past or present employees, clients, supplier contacts, research and survey subjects, website users or any other individual.

This Data Protection Policy applies to all KWT Global personnel. This Data Protection Policy sets out what we expect from you in order for KWT Global to comply with applicable law. Your compliance with this Data Protection Policy is mandatory.

## 2. The Data Protection Officer (DPO)

KWT Global's Data Protection Officer is Mitchell Gendel, EVP and General Counsel of MDC Partners (mgendel@mdc-partners.com). The DPO's work as DPO is independent of KWT Global reports directly to the MDC Board. The DPO is involved in all issues relating to the processing and protection of personal data, including monitoring compliance with data protection laws and communicating with applicable governmental authorities. The DPO will be responsible to assist MDC Partner agencies complying with applicable privacy laws as part of MDC's ongoing commitment to the lawful processing of personal data.

## 3. What is personal data?

"***Personal data***", as used in this Data Protection Policy, means any information relating to an identified or identifiable natural person (an individual). An identifiable natural person is one who can be identified, directly or indirectly, in particular 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.

## 4. What is processing of personal data?

"***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.

## 5. Personal Data Protection Principles

KWT Global must adhere to the principles relating to processing of personal data set out in the GDPR. Specifically, these principles require personal data to be:

- processed lawfully, fairly and in a transparent manner in relation to the individual ('**lawfulness, fairness and transparency**');
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('**purpose limitation**');
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('**data minimisation**');
- accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('**accuracy**');
- kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the personal data are processed ('**storage limitation**');
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('**integrity and confidentiality**').

The [controller][?] shall be responsible for, and be able to demonstrate compliance with these principles ('**accountability**').

## 6. Processing Personal Data Lawfully

You may only collect, process and share personal data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding personal data to specified "***lawful purposes***". These restrictions are not intended to prevent processing, but ensure that we process personal data fairly and without adversely affecting the individual.

### a. Lawful purpose

The GDPR only allows processing for specific purposes, which include situations where:

- The individual has given his or her consent.
- The processing is necessary for the performance of a contract with the individual (e.g., processing of employee payroll amounts).
- processing is necessary to meet legal compliance obligations.
- processing is necessary to protect the individual's vital interests.

- To pursue the controller's legitimate interests for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of the individual concerned. The purposes for which we process personal data for legitimate interests need to be set out in an applicable Privacy Notice.

You must identify and document the legal ground being relied on for each processing activity.

In most cases, KWT Global will be relying on the basis that the processing is necessary for the performance of a contract or to pursue KWT Global's legitimate interests. In cases where this does not apply, it will usually be necessary to obtain the individual's consent.

**b. Purpose limitation**

Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

You cannot use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the individual of the new purposes and they have given consent.

**c. Data minimisation**

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

You may only process personal data when performing your job requires it. You cannot process personal data for any reason unrelated to your general duties and responsibilities.

You may only collect personal data that you require for your job: do not collect excessive data. Ensure any personal data collected is adequate and relevant for the intended purposes.

You must ensure that when personal data is no longer needed for specified purposes, it is deleted or anonymised in accordance with KWT Global's data retention guidelines.

**d. Accuracy**

Personal data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

You will ensure that the personal data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any personal data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date personal data.

## 7. Requesting consent

An individual may consent to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked

boxes or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, then the consent must be kept separate from those other matters.

Individuals must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to process personal data for a different and incompatible purpose which was not disclosed when the individual first consented.

Unless we can rely on another legal basis of processing, express consent is usually required for processing sensitive personal data, for Automated Decision-Making and for cross border data transfers. Usually we will be relying on another legal basis (and not require express consent) to process most types of Sensitive Data. Where express consent is required, you must issue a Fair Processing Notice to the individual to capture express consent.

You will need to evidence consent captured and keep records of all consents so that the KWT Global can demonstrate compliance with consent requirements.

## 8. Notifying individuals

The GDPR requires Data Controllers to provide detailed, specific information to individuals depending on whether the information was collected directly from individuals or from elsewhere. Such information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a individual can easily understand them.

Whenever we collect personal data directly from individuals, including for human resources or employment purposes, we must provide the individual with all the information required by the GDPR including the identity of the Data Controller and DPO, how and why we will use, process, disclose, protect and retain that personal data through a Privacy Notice which must be presented when the individual first provides the personal data.

When personal data is collected indirectly (for example, from a third party or publicly available source), you must provide the individual with all the information required by the GDPR as soon as possible after collecting/receiving the data. You must also check that the personal data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed processing of that personal data.

## 9. Storing, retaining and deleting personal data

Personal data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

You must not keep personal data in a form which permits the identification of the individual for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

KWT Global will maintain retention policies and procedures to ensure personal data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time. You must comply with KWT Global's guidelines on data retention.

You will take all reasonable steps to destroy or erase from our systems all personal data that we no longer require in accordance with all the KWT Global's applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable.

You will ensure individuals are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

## 10. Protecting personal data

Personal data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of personal data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of personal data. You are responsible for protecting the personal data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. You must exercise particular care in protecting Sensitive personal data from loss and unauthorised access, use or disclosure.

You must follow all procedures and technologies we put in place to maintain the security of all personal data from the point of collection to the point of destruction. You may only transfer personal data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

You must maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it.

Integrity means that personal data is accurate and suitable for the purpose for which it is processed.

Availability means that authorised users are able to access the personal data when they need it for authorised purposes.

You must comply with all applicable aspects of the MDC IT Operations manual when processing personal data on behalf of KWT Global.

## 11. Sharing personal data

Generally, KWT Global is not allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the personal data we hold with another employee, agent or representative of the MDC group if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

You may only share the personal data we hold with third parties, such as our service providers if:

- They have a need to know the information for the purposes of providing the contracted services.
- Sharing the personal data complies with the Privacy Notice provided to the individual and, if required, the individual's consent has been obtained.
- In the case of a service provider, they are in compliance with part 2 below.

## 12. Service Providers who process personal data

The GDPR requires that all suppliers who process personal data enter into a contract that contains certain minimum stipulations. If you are instructing another company or business to do work that involves personal data, you must ensure they have entered into a contract for these purposes. If you are negotiating a contract please contact the DPO to ensure these clauses are If you are in any doubt please contact the DPO.

## 13. Individuals' Rights and Requests

Iindividuals have rights when it comes to how we handle their personal data. These include rights to:

- Withdraw consent to processing at any time.
- Receive certain information about KWT Global's processing activities.
- Request access to their personal data that KWT Global holds.
- Prevent use of their personal data for direct marketing purposes.
- Ask KWT Global to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data.
- Restrict processing in specific circumstances.

- Challenge processing which has been justified on the basis of our legitimate interests or in the public interest.
- Request a copy of an agreement under which personal data is transferred outside of the EEA.
- Object to decisions based solely on Automated processing, including profiling (Automated Decision-Making).
- Prevent processing that is likely to cause damage or distress to the individual or anyone else.
- Be notified of a personal data breach which is likely to result in high risk to their rights and freedoms.
- Make a complaint to the supervisory authority.
- In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing personal data without proper authorisation.

You must immediately forward any individual request you receive to your supervisor and/or the DPO.

## 14. Transferring Personal Data Overseas

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. KWT Global can only transfer personal data outside the EEA where it can show it has appropriate safeguards in place. This is only available in quite limited situations. Do not transfer any data overseas unless you are sure it is not leaving the EEA or you have the approval of the DPO. Personal Data Breaches

## 15. Personal Data Breaches

### a. What constitutes a breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

### b. Examples of Possible Breaches

This list is intended to give you an idea of what could constitute a breach. It is not an exhaustive list. If you are doubt about whether a breach has occurred, please contact the DPO immediately.

- Your mobile device or laptop is lost or stolen and it contains copies of personnel files or emails;

- You send an email containing personal data to the wrong or mistyped email address;
- Documents containing personal data are mailed or couriered to the wrong address; or
- Someone accesses your mobile device or computer without your authorisation.

**c. What to do if you think a breach has occurred**

If you think a breach may have occurred, report it immediately to the DPO. Preserve all the relevant materials in your possession or control but do not take any steps to investigate the breach yourself or take any other action. On no account should you contact the individual whose personal data is concerned by the suspected breach.

Time is of the essence in reporting a breach to the DPO. KWT Global has only 72 hours to report a breach to the relevant authorities. If you delay reporting the breach it could directly result in a severe penalty for failure to notify the authorities even where the breach itself was not caused by any fault of KWT Global and no individual was harmed by the breach.

## 16. Training and Audit

KWT Global is required to ensure all personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

You must undergo all mandatory data privacy related training and ensure your team undergo similar mandatory training in accordance with KWT Global's mandatory training guidelines.

You must regularly review all the systems and processes under your control to ensure they comply with this Data Protection Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of personal data.

## 17. Privacy by Design and Data Protection Impact Assessment (DPIA)

KWT Global is required to implement Privacy by Design measures when processing personal data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

You must assess what Privacy by Design measures can be implemented on all programs/systems/processes that process personal data by taking into account the following:

- The state of the art.
- The cost of implementation.
- The nature, scope, context and purposes of processing.

- The risks of varying likelihood and severity for rights and freedoms of individuals posed by the processing.

Data controllers must also conduct DPIAs in respect to high risk processing.

You should conduct a DPIA (and discuss your findings with the DPO) when implementing major system or business change programs involving the processing of personal data including:

- Use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes).
- Automated processing including profiling and Automated Decision-Making.
- Large scale processing of Sensitive Data.
- Large scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

- A description of the processing, its purposes and the Data Controller's legitimate interests if appropriate.
- An assessment of the necessity and proportionality of the processing in relation to its purpose.
- An assessment of the risk to individuals.
- The risk mitigation measures in place and demonstration of compliance.

**18. <u>Automated Processing (Including Profiling) and Automated Decision-Making</u>**

Generally, Automated Decision-Making is prohibited when a decision has a legal or similar significant effect on an individual unless:

- An individual has given their express consent.
- The processing is authorised by law.
- The processing is necessary for the performance of or entering into a contract.

If certain types of Sensitive Data are being processed, then grounds (b) or (c) will not be allowed but such Sensitive Data can be processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

If a decision is to be based solely on Automated processing (including profiling), then individuals must be informed when you first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must

be put in place to safeguard the individual's rights and freedoms and legitimate interests.

We must also inform the individual of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the individual the right to request human intervention, express their point of view or challenge the decision.

A DPIA must be carried out before any Automated processing (including profiling) or Automated Decision-Making activities are undertaken.

## 19. Direct Marketing

We are subject to certain rules and privacy laws when marketing to our customers.

For example, an individual's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the individual in an intelligible manner so that it is clearly distinguishable from other information.

An individual's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.