TITAN DATA
SOLUTIONS

DATA PROTECTION POLICY

INTRODUCTION

This Data Protection Policy sets out how Titan Data Solutions Limited ("we", "our", "us", "the Company") handle the personal data we deal with in the course of our business.

This Data Protection Policy applies to all personal data we process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, consultants, apprentices, volunteers, customers, clients, suppliers, shareholders, business partners and professional contacts, website users or any other data subject.

All Company personnel must read, understand and comply with this Data Protection Policy when processing personal data on our behalf and attend training on its requirements. This Data Protection Policy sets out what we are required to do under applicable data protection laws, and what we expect from our staff in order for the Company to comply with such laws. When carrying out their duties for the Company, staff must always comply with this Data Protection Policy and the policies and procedures referred to in it, and act in a way which ensures the Company is compliant with the rules and requirements set out.

Any breach of this Data Protection Policy, or action which results in the Company failing to comply with the requirements of this policy, may result in disciplinary action up to and including dismissal.

This Data Protection Policy (together with related policies and procedures) is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the Data Privacy Manager, Lula Cunningham (lula@titandatasolutions.com) and tel: 0203 870 2136 (the "Data Privacy Manager").

At the end of this policy is a glossary setting out the meaning of certain key terms.

2. SCOPE

We recognise that the correct and lawful treatment of personal data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of personal data is a responsibility that we take seriously at all times.

The Data Privacy Manager is responsible for overseeing this Data Protection Policy and, as applicable, developing related policies and procedures.

Staff should contact the Data Privacy Manager with any questions about the operation of this Data Protection Policy or if they have any concerns about data protection or that this Data Protection Policy is not being or has not been followed. In particular, staff must always contact the Data Privacy Manager in the following circumstances:

A) If they are unsure of the lawful basis which they are relying on to process personal data (including the legitimate interests used by the Company) (See secton 4:1 below)

B) If they need to rely on consent and/or need to capture explicit consent (See secton 4:2) below)

C) If they need to draft Privacy Notices (See secton 4:3)

D) If they are unsure about the retention period for the personal data being processed (See secton 8);

E) If they are unsure about what security or other measures they need to implement to protect personal data (See secton 9.1 below)

F) If there has been a personal data breach (See secton 9.2 below);

G) If they are unsure on what basis to transfer personal data outside the EEA (See section 10 below);

H) If they need any assistance dealing with any rights invoked by a data subject (See secton 11 below);

I) Whenever they are engaging in a significant new, or change in, processing activity which is likely to require a Data Protection Impact Assessment (DPIA) (See section 12.5 below) or plan to use personal data for purposes others than what it was collected for;

J) If they plan to undertake any activities involving automated processing including profiling or automated decision-making (See section 12.5 below);

K) If they need help complying with applicable law when carrying out direct marketing activities (See section 12.6 below); or

L) If they need help with any contracts or other areas in relation to sharing personal data with third parties (including our vendors) (See section 12.7 below).

3. DATA PROTECTION PRINCIPLES

We adhere to the principles relating to processing of personal data set out in the General Data Protection Regulations (GDPR) which require personal data to be:

A) Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).

B) Collected only for specified, explicit and legitimate purposes (Purpose Limitation).

C) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (Data Minimisation).

D) Accurate and where necessary kept up to date (Accuracy).

E) Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed (Storage Limitation).

F) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).

G) Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).

H) Made available to data subjects and data subjects allowed to exercise certain rights in relation to their personal data (Data Subject's Rights and Requests).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

4. LAWFULNESS, FAIRNESS, TRANSPARENCY

4.1 Lawfulness and fairness

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

We 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 data subject.

The GDPR allows processing for specific purposes, some of which are set out below:

A) The data subject has given his or her consent;

B) The processing is necessary for the performance of a contract with the data subject;

C) To meet our legal compliance obligations;

D To protect the data subject's vital interests; or

E) To pursue our legitimate interests for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of data subjects. The purposes for which we process personal data for legitimate interests need to be set out in applicable Privacy Notices.

We shall identify and document the legal ground being relied on for each processing activity.

4.2 Consent

A data controller must only process personal data on the basis of one or more of the lawful bases set out in the GDPR, which include consent. Consent is not the only ground on which we can process personal data, and in most cases, we will seek to rely on other grounds (such as having a legitimate interest in processing the data).

A data subject consents 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.

Data subjects 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 we intend to process personal data for a different and incompatible purpose which was not disclosed when the data subject first consented.

Unless we can rely on another legal basis of processing, explicit consent (which must be a very clear and specific statement) 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 explicit consent) to process most types of sensitive data. Where explicit consent is required, we must issue a Privacy Notice to the data subject to capture explicit consent.

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

4.3 Transparency (notifying data subjects)

The GDPR requires data controllers to provide detailed, specific information to data subjects depending on whether the information was collected directly from data subjects 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 data subject can easily understand them.

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

When personal data is collected indirectly (for example, from a third party or publically available source), we must provide the data subject with all the information required by the GDPR as soon as possible after collecting/receiving the data. We 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.

5. 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.

We will not use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the data subject of the new purposes and they have consented where necessary.

6. DATA MINIMISATION

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

Staff may only process personal data when performing their job duties requires it. Staff cannot process personal data for any reason unrelated to their job duties.

We may only collect personal data that we require for our business activities, and we shall not collect excessive data. We must ensure any personal data collected is adequate and relevant for the intended purposes.

TITAN DATA
SOLUTIONS

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

7. ACCURACY

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

We 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. We must check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We must take all reasonable steps to destroy or amend inaccurate or out-of-date personal data.

8. STORAGE LIMITATION

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

We shall not keep personal data in a form which permits the identification of the data subject 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.

We 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. Staff will need to ensure that our guidelines on data retention are complied with.

We 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 Company's applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable.

9. SECURITY INTEGRITY AND CONFIDENTIALITY

9.1. 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. We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of personal data. We will 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. We will exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure.

Staff 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. We 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.

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

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

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

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

Staff must comply with all applicable aspects of our information security policy and comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR and relevant standards to protect personal data.

9.2. Reporting a personal data breach

We have put in place procedures to deal with any suspected personal data breach and will notify data subjects or any applicable regulator where we are legally required to do so.

If staff know or suspect that a personal data breach has occurred, they should not attempt to investigate the matter themselves, or seek to remedy it. Staff must immediately contact the Data Privacy Manager and follow any instructions given by them. Staff will need to preserve all evidence relating to the potential personal data breach.

In certain circumstances, we may be required to notify the Information Commissioner's Office of a personal data breach within 72 hours of the breach. It is therefore essential that Staff notify the Data Privacy Manager as soon as they become aware of a personal data breach.

10 TRANSFER LIMITATION

The GDPR restricts data transfers to countries outside the European Economic Area (EEA) (consisting of the 28 countries in the EU, and Iceland, Liechtenstein and Norway) in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. We transfer personal data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

We may only transfer personal data outside the EEA if one of the following conditions applies:

A) The European Commission has issued a decision confirming that the country to which we transfer the personal data ensures an adequate level of protection for the data subjects' rights and freedoms;

B) Appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the Data Privacy Manager;

C) The data subject has provided explicit consent to the proposed transfer after being informed of any potential risks; or

D) The transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the data subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent and, in some limited cases, for our legitimate interest.

You must comply with any guidelines implemented by the Company on cross border data transfers.

11. DATA SUBJECT'S RIGHTS AND REQUESTS

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

A) Withdraw consent to processing at any time;

B) Receive certain information about the data controller's processing activities;

C) Request access to their personal data that we hold;

D) Prevent our use of their personal data for direct marketing purposes;

E) Ask us 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;

F) Restrict processing in specific circumstances;

G) Challenge processing which has been justified on the basis of our legitimate interests or in the public interest;

H) Request a copy of an agreement under which personal data is transferred outside of the EEA;

I) Object to decisions based solely on automated processing, including profiling (ADM); prevent processing that is likely to cause damage or distress to the data subject or anyone else;

J) prevent processing that is likely to cause damage or distress to the data subject or anyone else;

K) Be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;

L) Make a complaint to the supervisory authority; and

M) 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.

We 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).

Staff must immediately forward any data subject request you receive to your supervisor and the Data Privacy Manager and comply with the company's data subject response process.

12. ACCOUNTABILITY

12.1 We must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Data controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

We shall put suitable resources and controls in place to ensure and to document GDPR compliance including:

A) Appointing an executive accountable for data privacy;

B) Implementing Privacy by Design when processing personal data and completing Data Protection Impact Assessments (DPIAs) where processing presents a high risk to rights and freedoms of data subjects;

C) Integrating data protection into internal documents including this Data Protection Policy, related policies, Data Retention Policy, Privacy Notices;

D) Regularly training Company personnel on the GDPR, this Data Protection Policy, related policies and data protection matters including, for example, data subject's rights, consent, legal basis, DPIA and personal data breaches. The Company must maintain a record of training attendance by Company personnel; and

E) Regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

TITAN DATA
SOLUTIONS

l2.2 Record keeping

The GDPR requires us to keep full and accurate records of all our data processing activities.

We shall keep and maintain accurate corporate records reflecting our processing including records of data subjects' consents and procedures for obtaining consents

l2.3 Training and audit

We are required to ensure all Company 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.

Staff must undergo data privacy related training and ensure that their team undergo similar mandatory training.

Staff must regularly review all the systems and processes under their 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.

12.4 Privacy by Design and Data Protection Impact Assessment (DPIA)

We are 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.

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

A) The state of the art;

B) The cost of implementation;

C) The nature, scope, context and purposes of processing; and

D) The risks of varying likelihood and severity for rights and freedoms of data subjects posed by the processing.

We also conduct DPIAs in respect to high risk processing.

We shall conduct a DPIA when implementing major system or business change programs involving the processing of personal data including:

A) Use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

B) Automated processing including profiling and automated decision-making (ADM);

C) Large scale processing of sensitive data; and

D) 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;

B) An assessment of the necessity and proportionality of the processing in relation to its purpose;

C) An assessment of the risk to individuals; and

D) The risk mitigation measures in place and demonstration of compliance.

Staff must comply with any guidelines issued by the Company on DPIA and Privacy by Design.

12.5. Automated Processing (including profiling) and Automated Decision-Making (ADM)

Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

A) A data subject has explicitly consented;

B) The processing is authorised by law; or

C) 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 data subjects 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 data subject's rights and freedoms and legitimate interests.

We must also inform the data subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the data subject 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 ADM activities are undertaken.

Where staff are involved in any data processing activity that involves profiling or ADM, you must comply with any guidelines issued by the Company on profiling or ADM.

TITAN DATA
SOLUTIONS

l2.6 Direct marketing

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

For example, a data subject'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 data subject in an intelligible manner so that it is clearly distinguishable from other information.

A data subject'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.

Staff must comply with any guidelines issued by the Company on direct marketing to customers.

12.7 Sharing personal data

Generally we are not allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put in place.

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

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

A) They have a need to know the information for the purposes of providing the contracted services;

B) Sharing the personal data complies with the Privacy Notice provided to the data subject and, if required, the data subject's consent has been obtained;

C) The third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

D) The transfer complies with any applicable cross border transfer restrictions; and
a fully executed written contract that contains GDPR approved third party clauses has been obtained.

Staff must comply with any guidelines issued by the Company on data sharing with third parties.

TITAN DATA
SOLUTIONS

13 CHANGES TO THIS DATA PROTECTION POLICY

We may change and update this Data Protection Policy at any time. Staff should check back regularly to obtain the latest copy of this Data Protection Policy. We last revised this Data Protection Policy on January 2019.

14 GLOSSARY OF KEY TERMS

Sensitive personal data
Personal data revealing racial or ethnic origin, political opinions, or religious or philosophical beliefs, details of trade union membership, genetic data, biometric data that can uniquely identify a natural person, data concerning health, data concerning a person's sex life or sexual orientation.

Personal data
Any data from which a living individual can be identified. If in doubt as to whether any particular data amounts to personal data, we shall assume that it does

Personal data breach
A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed by the Company

15 ACKNOWLEDGEMENT OF RECEIPT AND REVIEW

I, acknowledge that I have received and read a copy of the Titan Data Solutions Limited's Data Protection Policy, dated 05/02/19 and understand that I am responsible for knowing and abiding by its terms. I understand that the information in this Data Protection Policy is intended to help Company personnel work together effectively on assigned job responsibilities and assist in the use and protection of personal data. This Data Protection Policy does not set terms or conditions of employment or form part of an employment contract.

Signed .....

Printed Name .....

Date .....