DATA PROTECTION

This Policy sets out how Titan Environmental Surveys Ltd ("we", "our", "us", "the Company") handles the Personal Data of our customers, suppliers, employees, workers and other third parties. Capitalised terms are used throughout this document, where a term is capitalised its definition can be found in clause 13 of this policy.

This 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, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

This Policy applies to all Company Personnel ("you", "your"). You must read, understand and comply with this Policy when Processing Personal Data on our behalf and attend training on its requirements. This Policy sets out what we expect from you in order for the Company to comply with applicable law. Any breach of this Policy may result in disciplinary action.

This Policy (together with Related Policies and Guidelines) is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the DPM.

1. Scope

Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. Failure to comply with the GDPR exposes the Company to potential fines of up to EUR20 million or 4% of total worldwide annual turnover, whichever is higher. We are also subject to the DPA, which is the UK specific legislation replacing the old Data Protection Act 1998.

We are all responsible for ensuring compliance with this policy and ensuring that appropriate practices, processes and controls are implemented.

The DPM is responsible for overseeing this Policy and, as applicable, developing Related Policies and Guidance. You should contact the DPM with any questions about the operation of this Policy or the Legislation or if you have any concerns that this Policy is not being or has not been followed.

2. Personal data protection principles

We adhere to the principles relating to Processing of Personal Data set out in the Legislation which require Personal Data to be:

- Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).
- Collected only for specified, explicit and legitimate purposes (Purpose Limitation).
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation).
- Accurate and where necessary kept up to date (Accuracy).

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

3. Lawfulness, fairness, transparency

3.1 Lawfulness and fairness

You may only collect, Process and share Personal Data if you do so fairly and lawfully and for specified purposes. The key purposes considered fair and lawful under the Legislation are as set out below:

- The Data Subject has given his or her Consent
- The Processing is necessary for the performance of a contract with the Data Subject
- To meet our legal compliance obligations
- To protect the Data Subject's vital interests
- To pursue our legitimate interests where our interests are not overridden by the rights and freedoms of Data Subjects

As set out in the Privacy Notices for our employees and third parties (see further comments below under the heading ‘Transparency’), we will usually rely on the need to perform a contract or our legitimate interests as the basis for Processing. With employees imbalance of power between employee and employer can make obtaining true Consent difficult.

3.1.1 What if consent is required?

Consent is given by a Data Subject only if the Data Subject has been informed of the specific reasons for processing their Personal Data and such consent is then given freely. Consent can be given by a statement or by a clear positive action, so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. Consent can be withdrawn at any time and withdrawal must be promptly honoured.

If you think you may need Consent for any processing you plan to undertake you should contact the DPM who will be able to advise whether it is appropriate and what steps need to be taken.

3.2 Transparency (notifying data subjects)

We are required to provide detailed, specific information about Processing to Data Subjects via a Privacy Notice. The Privacy Notice must contain various information including how and why we will use, Process, disclose, protect and retain that Personal Data. It should be provided to the Data Subject when the data is collected.

When Personal Data is collected indirectly (for example, from a third party), the Privacy Notice should be provided 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 Legislation and on a basis which contemplates our proposed Processing of that Personal Data.

We have developed Privacy Notices for employees, workers, contactors, prospective employees and third parties. You should ensure you are familiar with these and in the event you intend to carry out processing which is not covered by a Privacy Notice you must contact the DPM before processing so that the DPM can advise on next steps.

4. Purpose limitation

Personal Data must be collected only for specified, explicit and legitimate 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 Data Subject of the new purposes and they have Consented where necessary.

5. 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 collect and/or Process Personal Data that you require for your job duties. You should not collect excessive data and must 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 the Company's Personal Data Retention Guidelines.

6. Accuracy

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

checked at the point of collection and at regular intervals afterwards and reasonable steps should be taken to destroy or amend inaccurate or out-of-date Personal Data.

7. Storage limitation

The Company will maintain guidelines on Data Retention 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 will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with the Company's Personal Data Retention Guidelines.

8. Security integrity and confidentiality

8.1 Protecting Personal Data

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 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 share responsibility for the security of the Personal data and 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. To assist with this we have prepared Personal Data Security Guidelines for you to follow, these are not exhaustive. You must not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect Personal Data.

8.2 Reporting a Personal Data Breach

We are required to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the DPM who will review the situation

and will notify Data Subjects or any applicable regulator where we are legally required to do so. You should preserve all evidence relating to the potential Personal Data Breach.

9. Transfer limitation

In order to ensure that the level of data protection afforded to individuals by the Legislation is not undermined transfers of Personal Data outside of the EEA are only permitted if one of the following conditions applies:

- 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
- Appropriate safeguards are in place, such as standard contractual clauses approved by the European Commission
- The Data Subject has confirmed their Consent to the proposed transfer after being informed of any potential risks; or
- The transfer is necessary for one of the other reasons set out in the Legislation 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. Reliance on our legitimate interests in these circumstances is exceptionally limited and will require an assessment to be carried out by the DPM and should only be relied upon if no other option is available

You must comply at all times with the Company's Personal Data Sharing and Cross Border Transfer Guidelines.

10. Data Subject's rights and requests

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

- Receive certain information about the Data Controller's Processing activities
- Request access to their Personal Data that we hold
- Ask us to erase Personal Data if it is no longer necessary for us to hold it
- Ask us to rectify inaccurate data or to complete incomplete data
- Challenge Processing which has been justified on the basis of our legitimate interests
- Prevent our use of their Personal Data for direct marketing purposes
- Where Consent is relied upon for Processing, withdraw that Consent at any time

- Be notified of a Personal Data Breach likely to result in high risk to their rights and freedoms
- Make a complaint to the supervisory authority

You must immediately forward any Data Subject request you receive to the DPM who will coordinate the response to such requests. Among other issues, the identity of an individual requesting data under any of the rights listed above must be verified; do not allow third parties to persuade you into disclosing Personal Data without proper authorisation.

11. Accountability

11.1 Responsibility

We are responsible for implementing appropriate and effective technical and organisational measures to ensure compliance with data protection principles. As part of this we have developed the adequate resources and controls, including:

- Implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects
- Integrating data protection principles into internal documents including this Policy, Related Policies and Guidelines and Privacy Notices
- Regularly training Company Personnel on the Legislation, this Policy, Related Policies and Privacy Guidelines and data protection matters

11.2 Record keeping

We must keep and maintain a Record of Processing Activities which can be access on the intranet. We will also need to keep a record of Data Subjects' Consents (where obtained) but this will not be generally available, if you have any questions on consents you should contact the DPM. You are responsible for ensuring your line manager and in turn the DPM is aware of any Processing carried out by you.

11.3 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.

You must regularly review all the systems and processes under your control to ensure they comply with this Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data. If you have any concerns these should be raised with the DPM straight away.

11.4 Privacy By Design and Data Protection Impact Assessment (DPIA)

We are required to implement Privacy by Design measures when Processing Personal Data. This means we need to implement 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 technology available
- The cost of implementation
- The nature, scope, context and purposes of Processing
- The risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing

DPIAs must be conducted where there is high risk Processing in order to assess the necessity of the Processing and proportionality and compliance measures. A DPIA is likely to be required when implementing major system or business change programs involving the Processing of Personal Data including:

- Use of new technologies or a change in technologies
- Automated Processing including profiling and ADM
- Large scale Processing of Sensitive Data
- Large scale, systematic monitoring of a publicly accessible area

If you think you are about to undertake an activity which may require a DPIA, or you are planning on making changes to existing processes or adopting a new use for Personal Data, you should contact the DPM before taking any further action so that an assessment can be undertaken and if necessary a DPIA. We have developed Data Protection Impact Assessment Guidelines which you can use to assist you in deciding whether a DPIA is likely to be required.

11.5 Automated Processing (including profiling) and Automated Decision-Making

Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual although there are limited exceptions under the Legislation.

It is not expected that we will carry out any Automated Processing (including profiling) or ADM activities however a DPIA must be carried out before any such activities are undertaken. You should contact the DPM before carrying out any such activities.

11.6 Direct marketing

We are subject to certain rules and privacy laws when directly marketing our products and services. You must comply at all times with our Marketing Guidelines.

11.7 Sharing Personal Data

Generally we are not allowed to share Personal Data with third parties unless certain safeguards and/or contractual arrangements have been put in place. Wherever possible any data to be shared should be fully anonymised or Pseudonymised.

You may only share the Personal Data we hold with another employee, agent or representative of our group (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) 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 and our clients in limited circumstances.

We have produced a set of Personal Data Sharing and Cross Border Transfers Guidelines which provide further details on this area and if you have any questions or concerns in this area you should contact the DPM before any information is shared.

12. Definitions

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work. Profiling is an example of Automated Processing.

Company Personnel: all employees, workers contractors, agency workers, consultants and directors.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's agreement to the Processing of Personal Data relating to them.

Data Controller: the person or organisation that determines when, why and how to process Personal Data. We are the Data Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data.

Data Privacy Impact Assessment (DPIA): an assessment to identify and reduce data processing risks.

Data Protection Manager (DPM): the person with responsibility for data protection compliance within the Company. Any reference to the DPM within a Titan document refers to a Gardline person.

DPA: the Data Protection Act 2018 (once in force).

General Data Protection Regulation (GDPR): the General Data Protection Regulation ((EU) 2016/679). Personal Data is subject to the legal safeguards specified in the GDPR.

Legislation: the GDPR and the DPA

Personal Data: any information identifying a Data Subject or any information relating to a Data Subject which identifies the Data Subject (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or compromises the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, unauthorised access, disclosure or acquisition of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Notices: notices setting out information that may be provided to Data Subjects when the Company collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, organising, amending, retrieving, using, disclosing, erasing or destroying it.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Related Policies and Guidelines: the Company's guidelines, operating procedures or processes related to this Policy and designed to protect Personal Data, available here within the IMS.

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.