PICKSTOCK TELFORD PRIVACY POLICY

1. SCOPE, AIM, ACCESSIBILITY

(1) This Company policy is the binding basis for a legally compliant and sustainable protection of personal data for Pickstock Telford Ltd (PT).

(2) PT is committed to data protection and has taken appropriate measures to achieve a high level of protection in the handling of personal data. PT sees its commitment to data protection as a matter of course. This Company policy sets out the basic principles for the handling of personal data and serves PT employees as a guideline for the protection of the personal rights of data subjects.

(3) The Company policy must be easily accessible to all employees and senior executives at all times.

2. SCOPE OF APPLICATION

(1) This Company policy applies personally to all PT employees and officers.

(2) The rules and prohibitions of this company policy and the other guidelines and work instructions that apply to it apply to any handling of personal data, regardless of whether this takes place electronically or in paper form. They also include all types of persons affected (customers, employees, business partners, etc.) in their scope of application.

3. DEFINITIONS

(1) **Personal Data** means any information relating to an identified or identifiable natural person; 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;

(2) **Special Categories** of personal data are details of racial and ethnic origin, political opinions, religious or philosophical beliefs, possible membership of a trade union, health, sex life or sexual orientation as well as genetic and biometric data of a natural person.

(3) **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;

In detail

(a) **Collection** means collecting data of the data subject.
(b) **Storing** means storing of personal data on a data carrier for the purpose of further processing or use,
(c) **Alteration** means modifying the content of stored personal data,
(d) **Transfer** means to disclose stored or processed personal data to a third party in such a way that
  (aa) the data are passed on to the third party or
  (bb) the third party views or retrieves data made available for inspection or retrieval,
(e) **Deleting** means to make stored personal data unidentifiable.

(4) **Restriction Of Processing** means the marking of stored personal data with the aim of limiting their processing in the future;

(5) **Profiling** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

(6) **Pseudonymisation** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional

information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

(7) **Controller** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

(8) **Processor** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller;

(9) **Recipient** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not;

(10) **Third Party** means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

(11) **Consent** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

4. ORGANISATION OF DATA PROTECTION

(1) PT has appointed a data protection officer. You can reach them under the following contact details:

Prof. Dr. h.c. Heiko Jonny Maniero, DGD Deutsche Gesellschaft für Datenschutz GmbH,
Robert-Bosch-Str. 11,85221 Dachau, Germany
Phone: +49 (0) 8131-77987-0
Email: dpo@osieurope.com

(2) The Data Protection Officer monitors compliance with the GDPR and other legal requirements, including the requirements of this and other guidelines of PT on data protection. The data protection officer advises and informs the company management regarding existing data protection obligations and is responsible for communication with supervisory authorities. Selected processes are randomly, risk-oriented and monitored for data protection compliance at appropriate intervals.

(3) The data protection officer shall perform his duties without instruction and using his technical expertise. He reports directly to the Executive Board.

(4) PT and/or its employees shall support the data protection officer in the performance of his duties.

5 HANDLING OF PERSONAL DATA

(1) The processing of personal data is generally prohibited unless a statutory provision explicitly permits the handling of data. Personal data may in principle be processed in accordance with the GDPR:

(a) In an existing contractual relationship with the data subject.
Example: The storage and use of required personal data in the context of an employment relationship.

(b) In the course of the initiation or execution of the contract with the data subject.
Example: Customer K requests and purchases information about product X. The data required to send the information material and to process the legal transaction (delivery of the goods and payment of the purchase price, customer complaints) may be collected, processed and used.

(c) If and to the extent that the data subject has consented to the processing of his/her data in advance and the consent for proof to be provided in a documented form at any time and at a later date.
Example: The person concerned registers by e-mail to receive a newsletter.

(d) When a specific law permits and requires processing.
Example: Legal retention periods for financial and tax documents.

(e) If there are legitimate interests of PT, provided that the interests or fundamental rights of the person concerned do not prevail, especially if it concerns a child. However, data processing based on a legitimate interest should not be carried out without prior consultation with the data protection officer.
Example: The use of personal data for advertising purposes.

(2) Data subjects shall not be subject to a decision based exclusively on automated processing, including profiling, which has a legal effect on them or significantly affects them in a similar manner.

(3) Personal data shall be processed for a previously defined purpose and shall accordingly only be used or further transmitted to the extent that this is compatible with the originally defined purpose. Data storage without purpose, such as data retention, is not permitted.

(4) The change of a purpose, which was originally the basis for a data handling, is - apart from the declared consent of the data subject - only permissible if the purpose of the further processing is compatible with the original purpose. In particular, the reasonable expectations of the data subject regarding such further processing vis-à-vis PT, the type of data used, the consequences for the data subject and the possibilities of encryption or pseudonymisation must be taken into account.

(5) If personal data are not collected from the data subject, but are procured for example from another company, the data subject must be informed subsequently and comprehensively about the handling of his data in accordance with Art. 14 GDPR. This also applies to changes in the purpose of data processing.

(6) When collecting personal data, the data subject shall be fully informed about the handling of his data. The information must contain the purpose, the identity of the controller, the recipients of his personal data and all other information within the meaning of Art. 13 GDPR in order to ensure fair and transparent processing. The information shall be written in a comprehensible and easily accessible form and in as simple a language as possible.

(7) Personal data must be factually correct and, if necessary, up-to-date. The scope of data processing should be necessary and relevant to the specified purpose. The respective specialist department must ensure implementation by establishing appropriate processes. Likewise, databases must be regularly checked for their correctness, necessity and up-to-date.

(8) If possible, personal data should not be handled. Pseudonymisation is preferable. For example, it may not be necessary to know and use the full name of a data subject for statistical evaluation of data. Rather, this information can be replaced by a random value that can also ensure that the underlying information is distinguishable.

6. SPECIAL CATEGORIES OF PERSONAL DATA

Special categories of personal data (see definitions above) may only be processed with the express consent of the data subject or exceptionally on the basis of an explicit legal permission, for example if the processing is necessary for purposes of health care or occupational medicine or for assessing the ability to work and only by qualified personnel or their responsibility, which are subject to an obligation of professional secrecy. Furthermore, additional technical and organisational measures (e.g. encryption during transport, minimum assignment of rights) must be taken to protect special personal data.

7. DATA TRANSMISSION / TRANSFER

(1) The transmission of personal data to third parties is only permitted based on a statutory provision or the consent of the data subject.

(2) If the recipient of personal data is outside the European Union or the European Economic Area, special measures are required to safeguard the rights and interests of data subjects. Data shall not be transmitted if the receiving body does not have an adequate level of data protection or if it cannot be established, for example, by means of special contractual clauses.

8. EXTERNAL SERVICE PROVIDERS

(1) If external service providers are to have access to personal data, the data protection officer shall be informed in advance. Examples of external service providers are, in particular, IT service providers, marketing agencies, external cleaners, but also craftsmen who gain access to premises where personal data is processed when carrying out their work.

(2) Service providers with possible access to personal data shall be carefully selected before placing an order. The selection must be documented and should in particular take the following aspects into account:

(a) Technical suitability of the contractor for the specific data handling
(b) Technical-organizational safety measures
(c) Experience of the supplier in the market
(d) Other aspects that indicate the reliability of the provider (data protection documentation, willingness to cooperate, reaction times, etc.)

(3) If a service provider is to process personal data for PT, a contract for data processing must be concluded. This must regulate data protection and IT security aspects. Therefore, please contact the data protection officer.

(4) The service provider shall be regularly inspected with regard to the technical and organisational measures agreed with him in the contract. The result must be documented.

9. DATA AVOIDANCE, DATA MINIMIZATION, PRIVACY BY DESIGN

(1) The handling of personal data shall be oriented towards the goal of processing as little data as possible from a data subject ("data minimisation"). In particular, personal data must be anonymised or pseudonymised insofar as this is possible according to the intended use. For example, it will not be necessary to know and use the full name of a data subject in the context of a statistical evaluation of data. Rather, this information can be replaced by a random value that can also ensure that the underlying information is distinguishable.

(2) The same applies to the selection and design of data processing systems. Data protection shall be integrated from the outset into the specifications and architecture of data processing systems in order to facilitate compliance with the principles of privacy and data protection ("privacy by design").

10. RIGHTS OF DATA SUBJECTS

(1) Data subjects have the right to information about the personal data stored by PT about their person.

(2) When processing requests for information, the identity of the data subject must be established beyond any doubt. If necessary, a copy of the applicant's identity card must be requested, showing the applicant's name, address and date of birth. Only copies of ID cards in paper form are accepted, scanning is not permitted. According to the information provided, the copy of the ID card must be destroyed immediately in conformity with data protection regulations.

(3) Information shall be provided electronically if the data subject has submitted the application electronically; otherwise in writing. The information must be accompanied by a copy of the data of the data subject, which, in addition to the personal data available, also includes the recipients of data, the purpose of storage and all other information required by law in accordance with Art. 15 GDPR, in order to make the data subject aware of the processing and have the legality assessed by him or herself. At the special request of the data subject, the data is made available in a structured, common and machine-readable format. The IT department responsible determines the standard to be set for this purpose.

(4) The data protection officer shall be available to advise on the processing of requests for information.

(5) Data subjects are entitled to have their personal data corrected if this proves to be incorrect. They may also request the completion of incomplete personal data.

(6) Personal data shall be deleted under the following conditions:
(a) Personal data are no longer necessary for the purposes for which they were collected or otherwise processed.
(b) the data subject withdraws his/her consent and there is no other legal basis for the processing.

(c) The data subject objects to the processing for advertising purposes or invokes a right of objection on the basis of a special - to be justified - personal situation.
(d) The personal data have been processed unlawfully.
(e) The controller is obliged to delete the personal data.

If there is an obligation to delete and if the personal data was previously made public, other controllers must be informed of a request for deletion by the data subject with regard to all copies of his data and all links to this data.

(7) The processing of personal data shall be restricted if

(a) the accuracy of the personal data is disputed by the data subject for a period which enables the data controller to verify the accuracy of the personal data,
(b) the processing is unlawful and the data subject refuses to delete the personal data;
(c) the data controller no longer needs the personal data for the purposes of the processing, but the data subject needs them for the enforcement, exercise or defense of legal claims; or
(d) the data subject has lodged an objection to the processing on the basis of a particular situation and the relevant department is still examining the objection.

(8) The data subject shall be informed of any action taken at his request within one month at the latest.

(9) The data protection officer is available to advise on the protection of the rights of data subjects.

11. REQUESTS FOR INFORMATION FROM THIRD PARTIES ABOUT DATA SUBJECTS

Should a body request information about data subject, such as customers or employees of a company, information may only be disclosed if
(a) the party providing the information can demonstrate a legitimate interest; and
(b) a legal standard requires information, and
(c) the identity of the person making the request or the body making the request is beyond any doubt.

12. PROCEDURAL NOTIFICATION, LIST OF PROCESSING ACTIVITIES

(1) The data protection officer shall keep a register of all data processing operations. Each department must appoint a responsible person who documents all necessary information on the procedures of the respective department in accordance with the legal requirements of Art. 30 GDPR. The data protection officer may be consulted with regard to the information required by law.

(2) PT shall make the list available to the supervisory authority on request. The data protection officer is responsible for this in agreement with the Company management.

13. ADVERTISMENT

(1) The advertising approach of data subjects by letter, telephone, fax or e-mail is only permitted if the data subject has given his prior consent to the use of his data for advertising purposes. The consent must be documented for later proof at any time.

(2) Exceptions are only permitted if a permit standard is available. Please consult the data protection officer.

14. TRAINING

Employees who have permanent or regular access to personal data, collect such data or develop systems for processing such data must receive appropriate training on data protection regulations. The data protection officer decides on the form and frequency of the corresponding training courses.

15. CONFIDENTIALITY

(1) Employees are prohibited from processing personal data without authorization. Before taking up their duties, they must be obliged to treat personal data confidentially. The commitment is made by the management using the confidentiality obligation form provided for this purpose.

(2) Employees with special confidentiality obligations are also bound by this in writing.

16. COMPLAINTS

(1) Every data subject has the right to complain about the processing of his data if he feels that his rights have been infringed. Employees may also report violations of this company policy at any time.

(2) The competent authority for the above complaints shall be the data protection officer, who shall be an independent authority not bound by instructions.

17. AUDITS

(1) In order to ensure a high level of data protection, relevant processes are reviewed by regular audits of internal bodies or by external auditors. If potential for improvement is identified, immediate remedial action must be taken.

(2) The findings of the audit shall be documented. The documentation must be handed over to the data protection officer, the Company management and the line manager for the respective process.

(3) An audit is successfully completed when all measures documented in the report have been implemented. If necessary, follow-up audits are carried out by subjecting recommendations of the initial audit to a review of their implementation.

18. INTERNAL INVESTIGATIONS

(1) Measures to clarify the facts of the case and to prevent or detect criminal offences or serious breaches of duty in the employment relationship shall be carried out in strict compliance with the relevant statutory data protection provisions. In particular, the data collected and used must be necessary, appropriate and proportionate to the legitimate interests of the parties concerned in order to achieve the purpose of the investigation.

(2) The data subject shall be informed as soon as possible of the measures taken in respect of him or her.

(3) The data protection officer shall be involved in all forms of internal investigations in advance with regard to the selection and design of the measures.

19. AVAILABILITY, CONFIDENTIALITY AND INTEGRITY OF DATA

(1) Depending on the type of data and its need for protection, a documented determination of protection requirements and risk analysis shall be carried out for each procedure.

(2) In order to safeguard the availability, confidentiality and integrity of data, a general security concept shall be established which is binding for all procedures. In particular, this shall include means and measures for encryption and data backup. The safety concept shall be regularly reviewed, evaluated and evaluated with regard to the effectiveness of the technical and organisational measures provided for therein.

(3) It shall be prevented that data processing systems can be used by unauthorised persons. Doors in unoccupied rooms must be locked. Effective measures to control access to devices must be in place and activated. System accesses must always be blocked in the absence.

(4) Passwords allow access to systems and the personal data stored therein. They represent a personal identification of the user and are not transferable. It must be ensured that passwords are always kept under lock and key. Passwords must have a minimum length of eight characters and consist of a character mix. Passwords may not appear in a dictionary or be formed from easily guessed terms, especially not terms that are related to PT.

(5) Access to personal data shall only be granted to those persons who must be made aware of the data in the course of their duties ("need-to-know principle"). Access authorizations must be precisely and completely defined and documented.

(6) Where possible, data transmissions over public networks shall be encrypted. Encryption is mandatory if the protection of personal data requires it.

(7) Personal data collected for different purposes shall be processed separately. The separation of data must be ensured by suitable technical and organisational measures.

(8)	Maintenance work on systems or telecommunications equipment by external service providers shall be supervised. It must also be ensured that service providers cannot access personal data without authorisation. Remote maintenance accesses are only to be granted in individual cases and must follow the principle of minimal assignment of rights. Remote maintenance activities shall, if possible, be recorded or logged**.**
20.	**ILLEGAL KNOWLEDGE OF DATA ("DATA BREACH")**
(1)	Should personal data have been unlawfully disclosed to third parties, the data protection officer shall be informed immediately.
(2)	The notification shall include all relevant information to clarify the facts of the case, in particular the receiving authority, the persons concerned and the nature and extent of the data transmitted.
(3)	Any obligation to provide information to data subjects or supervisory authorities shall be fulfilled exclusively by the data protection officer. Those data subjects will be informed by the management, whereby the data protection officer will be consulted in an advisory capacity.
21.	**CONSEQUENCES OF INFRINGEMENTS**
	A negligent or even deliberate breach of this company policy may result in action under employment law, including termination without notice or in due time. Criminal sanctions and civil law consequences such as damages may also be considered.
22.	**ACCOUNTABILITY**
	Compliance with the requirements of this company policy must be verifiable at all times. Particular attention must be paid to the traceability and transparency of measures taken, for example by means of associated documentation.
23.	**UPDATING THE DIRECTIVE**
(1)	In the context of the further development of data protection law and technological or organisational changes, this company policy shall be regularly reviewed with a view to any need for adaptation or addition.
(2)	Amendments to this company policy shall take informal effect. Employees and managerial staff must be informed immediately and in an appropriate manner of the changed requirements.