

## PRIVACY NOTICE FOR TRANSACTION PARTICIPANTS - APAC

Last modified: March 2026

### **Our Commitment to Your Privacy**

TPG respects your concerns about privacy. This Privacy Notice (“Notice”) applies to personal data regarding representatives of counterparties obtained by TPG in connection with potential transactions between the organizations they represent in which TPG is involved, including but not limited to investment funds or vehicles managed, advised or invested in by TPG. The TPG entity that obtains your personal data is responsible for the personal data about you. The relevant TPG entities are listed at the end of this Notice.

In this Notice, we describe the types of personal data we obtain about counterparties, how we may use the data, with whom we may share it, and the choices available to you. We also tell you how to contact us about our privacy practices.

### ***Personal Data We Obtain and How We Use It***

We may collect and use the following personal data about counterparties:

- Contact details – name, address, telephone numbers, email address, and other contact information;
- Other identifiers such as date of birth and gender;
- Communications between counterparties and TPG employees, as well as the contents of any electronic communications with TPG including but not limited to Bloomberg Messaging, Teams Chat, WhatsApp, WeChat, LinkedIn, and any other messaging platform; and
- Due diligence/assessment information – nationality, passport and other government-issued identification numbers, information relating to background checks provided to us by third party background screening providers or from publicly available sources, including criminal conviction and offense related data, such as details of prior criminal charges, convictions, or allegations.

We also may obtain sensitive personal data about counterparties if we are required or permitted to do so by applicable law, or if counterparties have, in accordance with applicable law, provided explicit consent to the collection and processing of their sensitive personal data.

We use the personal data that we collect about counterparties, subject to applicable law, to:

- Comply with legal and regulatory obligations – for example, to comply with applicable legal obligations related to preventing bribery and corruption, complying with international economic sanctions and export controls, preventing money laundering and tax evasion, and meeting binding requests for data related to third parties and associated persons from courts and/or law enforcement agencies, regulators, or other government authorities;
- Ensure that TPG only engages with reputable and law abiding third parties and to monitor third party intermediaries’ and associated persons’ compliance with TPG policies, procedures and ethical standards, and applicable laws, and to comply with voluntary requests for data related to third parties and associated persons from courts and/or law enforcement agencies, regulators, or other government authorities;
- Communicate with counterparties; and
- Establish and manage our business relationships.

We use the personal data about counterparties for the purposes described above because we are required to do so by a legal or regulatory obligation to which we are subject, or because we have a legitimate interest in operating and improving our business that is not overridden by the interests, rights, and freedoms of counterparties in respect of their personal data. We also may use this personal data to enter into a contract with a counterparty (as a natural person), and to perform such contract.

We also may use personal data about counterparties to protect against and prevent fraud, claims, and other liabilities and to comply with or enforce applicable legal requirements, industry standards, and our policies and terms. We use personal data for these purposes when it is necessary to protect, exercise, or defend their legal rights, or when we are required to do so by applicable law.

We may use counterparties' personal data for purposes other than those described above, in which case we will, to the extent required by law, provide prior notice to you and obtain your consent.

If you do not provide personal data which we require to comply with our applicable legal requirements, or to enter into or perform a contract with a counterparty (as a natural person), we may not be able to complete the transaction with the organization you represent.

### ***Data Sharing***

We may share your personal data with TPG, Inc. and its affiliates for the purposes described in this Notice. To the extent required by law, we will obtain your consent to share your personal data with these parties.

We may share personal data with service providers that perform services on our behalf such as our hosting providers, IT service providers, third party intelligence providers, third party fund administrators, and due diligence and screening providers. To the extent required by law, we will obtain your consent to share your personal data with these parties.

In addition, we may disclose personal data about you (a) if we are required or permitted to do so (i) by law or legal process, for example due to a court order or a request from a law enforcement agency, or (ii) to establish, exercise or defend our legal rights, or (iii) by our regulator(s) or any applicable regulations; (b) when we believe disclosure is necessary or appropriate to prevent physical harm or financial loss, (c) in connection with an investigation of suspected or actual fraudulent or other illegal activity, or (d) in connection with (i) fundraising, (ii) the making, management or disposition of any of our investments, or (iii) business continuity efforts. If such a sale or transfer occurs, we will inform you of the identity and contact information of the receiving party, if required by law.

### ***Data Transfers***

We may transfer the personal data that we collect about you to recipients in countries other than the country in which the personal data originally was collected, including the United States of America, the United Kingdom, the European Union, China, Hong Kong, Australia, the United Arab Emirates, India, Japan, Singapore and South Korea. Those countries may not have the same data protection laws as the country in which you initially provided the personal data. When we transfer your personal data to recipients in other countries (such as the U.S.), we will protect that personal data in a manner that is consistent with this Notice and applicable legal requirements.

### ***Data Retention***

Personal data about counterparties is retained for the period reasonably necessary to achieve the purposes outlined in this Notice, unless a longer retention period is required or permitted by applicable law, considering relevant statutes of limitations and TPG's records retention requirements.

### ***Your Rights and Choices***

Subject to applicable law, you may have the right to:

- Request confirmation of whether we process personal data relating to you and, if so, to request a copy of that personal data;
- Request that we rectify or update your personal data that is inaccurate, incomplete or outdated;
- Request that we erase your personal data in certain circumstances, such as where we collected personal data on the basis of your consent, and you withdraw that consent;
- Request that we restrict the use of your personal data in certain circumstances, such as while we consider another request that you have submitted, for example a request to update your personal data;
- Object at any time to the processing of your personal data;
- Withdraw your consent where you have given us consent to process your personal data; and
- Request that we provide a copy of your personal data to you in a structured, commonly used, and machine-readable format in certain circumstances, and where technically feasible, that we transmit it to another company.

If you wish to exercise any of your data protection rights or if you consider that we have processed your personal data in violation of applicable law, please contact us as detailed in the “How to Contact Us” section below.

You also may lodge a complaint with the personal data protection authority in your country.

***Who is Responsible for your Personal Data?***

The TPG entity that collects or obtains your personal data is responsible for it under applicable data protection law, and may be TPG Capital, Limited, TPG Capital (Australia) Pty Ltd, TPG Angelo, Gordon International LLC, Angelo, Gordon Asia Limited, Angelo, Gordon Asia Co., Ltd., or Angelo, Gordon Singapore Private Ltd (“TPG”, “we”, “us”), depending on where you are located.

***Updates to this Notice***

We may change or update portions of this Notice at any time without notice to you. The revision date appearing on the first page of this Notice underneath the title will identify the date of the last update or revision.

***How to Contact Us***

If you have any questions about this Notice, or you would like to exercise any of your rights, please contact us by email at [Privacy@tpg.com](mailto:Privacy@tpg.com).

## **For individuals located in Japan**

If you are located in Japan, please review the following additional information.

We permit employees to access personal data only to the extent necessary for the purposes described above, and we restrict access to personal data for other purposes.

In addition, we have implemented the following security measures to protect personal data processed:

1. Internal data protection policy and rules relating to the handling of personal data
  - We have adopted an internal policy that addresses the collection, use and handling of personal data in compliance with relevant laws and regulations as well as handling any questions and complaints received from data subjects.
2. Organizational security control measures
  - We have appointed a person who is responsible for oversight of personal data processing carried out by TPG, who may be contacted at:  
  
Head of Japan, Tetsu Yaoka  
  
TPG Angelo, Gordon International LLC  
  
Toranomon Hills Mori Tower 28th, 1-23-1 Toranomon, Minato-ku, Tokyo
3. Personnel safety control measures
  - We provide periodic training to employees regarding the handling of personal data.
  - Our employees are subject to appropriate confidentiality obligations.
4. Physical security control measures
  - We implement appropriate physical security measures designed to ensure the protection of personal data we process.
5. Technical security control measures
  - We implement appropriate technical security measures designed to ensure the protection of personal data we process.
6. Sharing of personal data with third parties
  - We implement appropriate contractual and other measures designed to ensure the protection of personal data when we share it with third parties.

You may obtain more details by contacting us, using information indicated in the “How to contact us” section above.