

PRIVACY AND CYBERSECURITY AT TPG

TPG's commitment to transparency and accountability shapes how we handle the information that is entrusted to us.

At TPG, we work hard to protect the privacy, confidentiality, and security of our stakeholders' personal information.

We maintain a comprehensive privacy and cybersecurity program that includes administrative, technical, and physical safeguards designed to ensure that personal information is handled responsibly and safely, and in compliance with global privacy and data security laws that apply to us.

Our privacy program is built on longstanding globally-recognized principles, including:

Transparency and Fairness

Accurately and comprehensively explaining our information practices, providing individuals with clear notice, to the extent applicable, and handling personal information in an ethical and respectful manner

Purpose Limitation

Collecting personal information only for limited and specified purposes, and not using the information in ways that are inconsistent with those purposes

Data Minimization

Collecting only that information which is necessary to fulfill the purpose for which it was collected, and avoiding the collection of excessive personal information

Data Quality

Working to ensure the personal information we process is accurate, up-to-date, and relevant to the purposes for which we collect it

Security

Implementing safeguards designed to protect the information entrusted to us against loss or unauthorized access, destruction, use, modification, or disclosure

Individual Choice

Providing individuals with choices about how we use their personal information in accordance with our legal obligations

TRANSPARENCY AND CHOICE

Pursuant to applicable laws and regulations there are individuals who are entitled to know what personal information we collect, how we use it, with whom we share it, and what choices they may have with respect to our processing. Our privacy policies explain why and how we collect and use personal information in connection with our business activities. These include privacy policies directed to investors in our funds and other stakeholders, which provide specific information about our privacy practices with respect to information obtained from such individuals.

We seek to use personal information in a way that is fair and respectful of individuals' choices. Each of our privacy policies describe the choices available to applicable individuals regarding how we handle their personal information, and how they may contact us to exercise those choices in accordance with applicable law.

GOVERNANCE AND ACCOUNTABILITY

TPG has designed our privacy program in furtherance of legal requirements applicable to us, which include applicable state and federal privacy laws in the U.S, as well as data protection laws applicable to us in the UK, EU, and Asia.

We continually seek to enhance our information governance framework as part of our commitment to protecting privacy, including through our internal policies designed to implement compliance; processes for honoring data subject rights in accordance with applicable law; privacy impact assessments designed to help us identify and manage privacy risk in accordance with applicable law; vendor risk management that involves diligence, contracting and ongoing monitoring of third parties who process personal information on our behalf; and cross-border data transfer risk assessment processes and remediation in accordance with applicable law. In addition, we provide periodic training and education on our data privacy obligations to TPG employees to help reinforce the importance of handling personal information in compliance with applicable laws and firm policies.

SECURITY

Ensuring the security of our systems and data is a core TPG commitment. We recognize that a cybersecurity event can strike anyone and have a dedicated team focused on identifying, preventing, detecting, responding to, and recovering from cybersecurity risk. Our program is grounded in the industry-standard US NIST Cybersecurity Framework.

As directed in our “Cybersecurity Governance Policy,” TPG has a dedicated Cybersecurity Team led by the Senior Director of Cybersecurity. This team is responsible for cybersecurity, data protection, and incident response operations from a tactical perspective. The Senior Director of Cybersecurity reports at least quarterly directly to TPG’s Operational Risk Committee and at least annually to TPG’s Enterprise Risk Committee, with briefings to TPG’s Board of Directors as appropriate.

TPG’s Cybersecurity team includes individuals dedicated to threat management and incident detection and response. This team is responsible for identifying threats that can impact TPG and designing controls to mitigate vulnerabilities before they are exploited and to detect and neutralize any threats that do materialize.

We appreciate the evolving nature of cyber threats. All TPG employees and contractors with access to the TPG network receive annual training on data security best practices as well as applicable cybersecurity policies. Likewise, every year, TPG engages a third party to conduct penetration testing. In addition, TPG’s Internal Audit team engages independent third parties to conduct annual testing on the cybersecurity program. Any risks identified through these assessments are addressed according to the “Technology Risk Management Policy.” Every week, TPG performs vulnerability scans of its systems, and we address any vulnerabilities identified in accordance with our “Vulnerability Management Policy.” TPG also performs annual cybersecurity security assessments of our key vendors to help protect TPG data when it leaves our network.