Privacy Notice

Last Updated: August 11, 2026

At TRG Screen, trust is our foundation.

This Privacy Notice ("**Notice**") describes how TRGRP, Inc. and its Affiliates (collectively, "**TRG Screen,**" "**we,**" "**us,**" or "**our**") collect, use, share, or otherwise process Personal Data and the rights you have in relation to that processing. We believe you should always know what data we collect and how we use it, and that you should have meaningful control over both. For the purpose of this Notice, Affiliate means any entity that forms part of the TRG Screen group of companies. A current list of TRG Screen Affiliates is listed at the bottom of this Notice.

Privacy Notice Highlights

These highlights summarize our Personal Data processing practices and your related rights. The full Privacy Notice that follows contains more detailed information about each topic.

- **What we collect:** We collect Personal Data when you use our Services, visit our websites, communicate with us, or interact with us in other ways. This includes identifiers, commercial information, technical data, and professional information. See Section 3.
- **How we use it:** We process your Personal Data to provide and improve our Services, communicate with you, ensure security, and comply with legal obligations. We always have a lawful basis for processing. See Section 5.
- **Who we share it with:** We do not sell your Personal Data. We share data only with service providers, affiliates, and professional advisors who need it to support our operations, or when required by law. See Section 6.
- **Your rights:** You have rights to access, correct, delete, and port your Personal Data, among others, depending on where you reside. See Section 11.
- **How to contact us:** To exercise your rights, make a privacy complaint, or ask questions, email us at dataprivacy@trgscreen.com. See Sections 20 and 21.

1. Scope and Application

This Notice applies to the Personal Data we collect or process about you when you (i) visit or interact with our websites that display or link to this Notice; (ii) visit or interact with our branded social media pages; (iii) visit our offices or other premises; (iv) receive communications from us or otherwise communicate with us, including emails, phone calls, texts, or other messaging; (v) use our Services where we act as a controller of your Personal Data; (vi) register for, attend, or take part in our events, webinars, programs, trainings, or certifications; (vii) act as or work for a service provider, supplier, or other vendor to TRG Screen, to the extent TRG Screen acts as a controller with respect to your Personal Data; (viii) are employed by or otherwise associated with a Licensee or prospective Licensee, where your Personal Data has been shared with us in our capacity as a controller (for example, during the sales, contracting, or account-administration process); (ix) apply for employment with us through our careers page or other recruiting channels (such individuals, "**Applicants**"); or (x) participate in surveys, research, or similar data-collection activities facilitated by us.

TRG Screen acts as a Data Controller for a limited set of Personal Data that we collect to operate, secure, and improve our Services — including authorized-user account and login credentials, associated contact details, and usage, telemetry, and security log data — and this Notice describes how we process that information. For all other Personal Data we process on behalf of our enterprise customers ("**Licensees**") in connection with their use of the Services, we act as a Data Processor under the Data Processing Agreement ("**DPA**") executed between TRG Screen and the Licensee; that processing is governed by the DPA and not by this Notice, and questions about it should be directed to the Licensee.

We process Personal Data in accordance with the EU General Data Protection Regulation ("**GDPR**"), the UK GDPR and Data Protection Act 2018, the Swiss Federal Act on Data Protection ("**FADP**"), the California Consumer Privacy Act as amended by the California Privacy Rights Act ("**CCPA**" or "**CPRA**", as applicable) and other applicable U.S. state privacy laws, the Singapore Personal Data Protection Act ("**PDPA**"), India's Digital Personal Data Protection Act, 2023, including the rules thereunder ("**DPDPA**"), and other applicable data protection laws. We continuously monitor the global privacy landscape and adapt our privacy program accordingly.

Our websites may contain links to third-party websites or services. We are not responsible for the information practices or the content of such third-party websites, and we encourage you to review their privacy policies to understand their data practices.

2. Key Definitions

For the purposes of this Notice, the following terms shall have the meanings set forth below. Any capitalized terms used but not defined shall have the meaning given to such term under Applicable Data Protection Laws.

- "**AI**" means artificial intelligence, including machine-learning systems and generative models that, with varying degrees of autonomy and using machine and/or human-provided inputs, infer how to generate outputs such as predictions, recommendations, content, classifications, or decisions.
- "**Applicable Data Protection Law**" means all applicable laws, regulations, and binding guidance relating to the processing of Personal Data, including without limitation the EU GDPR, the UK GDPR and Data Protection Act 2018, the Swiss FADP, the CCPA/CPRA and other U.S. state privacy laws, the Singapore PDPA, India's DPDPA, and any other applicable federal, state, or international privacy law.
- "**Data Controller**" (or "**Business**" under CCPA, or "**Data Fiduciary**" under India's DPDPA) means the entity that determines the purposes and means of Processing Personal Data.
- "**Data Processor**" (or "**Service Provider**" under CCPA) means the entity that processes Personal Data on behalf of the Data Controller.
- "**Data Subject**" (or "**Consumer**" under CCPA, or "**Data Principal**" under the DPDPA) means an identified or identifiable natural person to whom the Personal Data relates.
- "**DPA**" means the Data Processing Agreement executed between TRG Screen and a Licensee, incorporating the Standard Contractual Clauses where applicable.
- "**Licensee**" means an enterprise customer that has licensed the use of TRG Screen products and services.
- "**Personal Data**" means any information relating to an identified or identifiable natural person, including but not limited to name, email address, telephone number, IP address, device identifiers, location data, online identifiers, and any other information defined as "personal data," "personal information," or an equivalent term under Applicable Data Protection Law.

- "**Processing**" means any operation or set of operations performed on Personal Data, whether or not by automated means, including collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination, alignment, combination, restriction, erasure, or destruction.
- "**Sensitive Personal Information**" means Personal Data that is afforded special protection under Applicable Data Protection Law, including (under the GDPR/UK GDPR/Swiss FADP) special categories of personal data such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a person's sex life or sexual orientation, and (under the CCPA/CPRA) Social Security numbers, driver's license, state ID or passport numbers, financial account credentials, precise geolocation, and other categories designated as "sensitive." As described in Section 4, we collect Sensitive Personal Information only in limited circumstances, primarily in connection with our recruiting and hiring activities.
- "**Services**" means TRG Screen's software products and platforms (including market-data spend management, enterprise subscription management, usage analytics, vendor and contract management, and related cloud-hosted, on-premise, or hybrid offerings), together with any related professional, support, and customer-success services made available by TRG Screen.

3. What Personal Data We Collect

We adhere to the principle of data minimization and collect only Personal Data that is relevant and limited to what is necessary in relation to the purposes for which it is processed. We may collect such information in the following situations:

3.1 Data You Provide to Us

- **Account and Identity Data:** Name, job title, employer name, business email address, business telephone number, work addresses, and login credentials
- **Commercial Information:** Records of products or services purchased, obtained, or considered; purchase history and tendencies; subscription records
- **Professional or Employment-Related Information:** Job title, employer name, professional qualifications
- **Communication Data:** Contents of correspondence, support tickets, feedback, and records of interactions with our sales support team; content you provide to us through form submissions and survey participation.
- **Applicant Data**: If you apply for a position with us, we collect the information you submit as part of your application (such as name, contact details, work-authorization information, resume, work history, education, qualifications, references, and salary expectations), together with information generated during recruiting (such as assessment responses, interview content where disclosed at the point of recording, interviewer notes, scoring, and correspondence). We may also receive data from third-party applicant tracking, assessment, or background-check providers and, where applicable, from Vista Equity Partners and its affiliates, including Vista's Value Creation Team (collectively, "**Vista**"), or other Vista portfolio companies in connection with recruiting administration, candidate evaluation, workforce analytics, and candidate pooling where you have consented to such pooling. Where required by law, we will collect gender and/or religion for statutory reporting. **Some Applicant Data may include Sensitive Personal Information or special-category personal data, as further described in Section 4**.

3.2 Data We Collect Automatically

- **Technical and Device Data:** IP address, browser type and version, browser language, operating system, time zone, referring URLs, screen resolution, language preferences, and device identifiers.
- **Internet or Other Electronic Network Activity:** Browsing history, search history, time, frequency, duration, and patterns of use; features used; files accessed; errors generated; clickstream data; session duration; in-application navigation paths; and other visitor details collected in our log files
- **Geolocation Data:** Approximate location (city and country) derived from IP address
- **Cookie and Tracking Data:** Information collected through cookies, web beacons, pixels, and similar technologies, as further described in our separate Cookie Policy (available at www.trgscreen.com/cookie-policy).

3.3 Data We Receive from Third Parties

- Criminal-record or credit history received from our background-check provider (where lawful and role-appropriate)
- Assessment Security Data: IP address and IP-derived approximate geolocation captured by our third-party online assessment providers during the administration of skills or personality assessments, used to support the security and integrity of the assessment process (for example, to help detect suspected proxy test-taking or unauthorized assessment sharing). (Note: IP address and IP-derived geolocation data collected by our assessment providers is never used as the sole basis to disqualify, deprioritize, or exclude an Applicant, and any location-based flag is reviewed by qualified TRG Screen personnel before it affects an Applicant's status)
- Enrichment Data: Business contact details, job titles, employer name, industry, and other professional profile information provided by data enrichment providers and integrated into our customer relationship management systems to supplement and verify information we already hold.
- Marketing and Engagement Data: Webinar registration and attendance records, advertising engagement data (such as ad clicks and impressions), and professional profile information received from social media, advertising, and event-hosting platforms when you interact with our content on those platforms.
- Authentication Data: Information provided by third-party authentication or single sign-on services when you choose to log in using those services.
- Inferences: Inferences drawn from any of the above to create a profile reflecting preferences, behavior, or characteristics.

In some circumstances, we also collect, or our partners provide us with, publicly available information which may contain Personal Data. The way in which our partners collect this is detailed in their own privacy policies available on their websites.

4. Sensitive Personal Information

Under both the GDPR and the CCPA/CPRA, certain categories of Personal Data receive additional protections. We may collect the following categories of Sensitive Personal Information:

- Criminal record or credit history received from our background-check provider (where lawful and role-appropriate)
- Social Security Number, driver's license number, state ID or passport number
- Precise geolocation data or address information

- Disability status
- Veteran status
- Racial or ethnic origin
- Gender identity
- Religion or religious beliefs

We collect Sensitive Personal Information only where strictly necessary, primarily in connection with the job Applicant and onboarding process — for example, to conduct background and right-to-work checks, to verify candidate identity, to make reasonable accommodations during the recruiting process where requested, and (where you voluntarily provide it and where lawful) for equal-employment-opportunity and diversity reporting. In certain jurisdictions, we also collect categories of sensitive personal data where required by applicable law for statutory reporting purposes (for example, gender pay gap or fair-employment monitoring obligations), and we use such data only for those reporting purposes. In each case, we collect such information either directly from the Applicant or, with the Applicant's knowledge, through an authorized service provider such as a background-check vendor. Where we process special category personal data of EEA, UK, or Swiss Data Subjects, we do so only on the basis of an applicable condition under Article 9 of the GDPR (or its UK or Swiss equivalent), such as compliance with employment-law obligations or your explicit consent where permitted. We do not use or disclose Sensitive Personal Information to infer characteristics about you, and we use it only for purposes permitted by Section 1798.121 of the CCPA/CPRA. We do not discriminate based on any protected class or characteristic.

5. Why We Process Your Personal Data

We process Personal Data only for specified, explicit, and legitimate purposes. We always ensure we have a proper legal basis for processing your Personal Data. The following table sets forth the purposes for which we process Personal Data, the categories of data involved, and the corresponding legal basis:

Purpose of Processing	Categories of Data	Legal Basis
Marketing, business development, and promotional communications	Account and Identity Data; Professional or Employment-Related Information; Communication Data; Enrichment Data	Legitimate interests (in promoting our products and services and developing our business); Consent where required in the EU, UK and Switzerland You may opt out of marketing emails at any time as described in Section 11.5
System administration, analytics, and product improvement	Usage and Telemetry Data; Technical and Device Data; Cookie and Tracking Data	Legitimate interests (in operating, analyzing, and improving our products, services, and website); Consent where required in the EU, UK and Switzerland
Security monitoring, fraud detection, and protection of infrastructure	Technical and Device Data; Usage and Telemetry Data; Cookie and Tracking Data; Account and Identity Data	Legitimate interests (in providing, securing, and improving our products, services, and website); Legal obligation

Compliance with legal and regulatory obligations	Account and Identity Data; Communication Data	Legal obligation
Detecting security incidents and protecting against malicious or illegal activity	Technical and Device Data; Usage and Telemetry Data; Cookie and Tracking Data	Legitimate interests (in providing, securing, and improving our products, services, and website); Legal obligation
Debugging to identify and repair errors	Technical Data; Usage Data	Legitimate interests (in maintaining the functionality and reliability of our products, services, and website)
Short-term, transient use such as customizing content displayed to you	Usage and Telemetry Data; Technical and Device Data; Cookie and Tracking Data	Legitimate interests (in providing a relevant and functional user experience on our products, services, and website)
Recruiting and hiring, including evaluating Applicants, conducting interviews and assessments, performing background and right-to-work checks, receiving and using information from third-party applicant tracking, assessment, and background-check providers, using IP address and IP-derived geolocation data collected by our assessment providers solely to support the security and integrity of the assessment process (for example, to help detect suspected proxy test-taking or unauthorized assessment sharing), sharing Applicant Data as described in Section 22, and managing the hiring process	Applicant Data (including, where applicable, Sensitive Personal Information as described in Section 4)	Steps prior to entering into a contract; Legitimate interests (in identifying, evaluating, and hiring qualified candidates and managing our recruitment process); Legal obligation (where required, e.g., right-to-work verification, equal-opportunity reporting); Article 9 GDPR / UK GDPR / Swiss FADP conditions for special category personal data (such as employment-law obligations or, where required, explicit consent); Consent and applicable statutory exceptions under the DPDPA (India) and PDPA (Singapore); Consent for sharing Applicant Data with other Vista portfolio companies for consideration for other job opportunities; Consent where otherwise required by local law

6. Who We Share Personal Data With

We may share your Personal Data with the following categories of recipients: (i) our Affiliates, in connection with any of the uses of your Personal Data set out in this Notice; (ii) third-party service providers, suppliers, agents, and other organizations that provide data processing services to us (for example, to support the delivery of, provide functionality on, or help to enhance the security of our Services), or that otherwise process Personal Data on our behalf for purposes that are described in this Notice or notified to you when we collect your Personal Data (such as cloud hosting and infrastructure, analytics, customer support, payment processing, fraud prevention, recruiting and applicant tracking, assessment administration, background checks, and professional services); (iii) Vista Equity Partners and its affiliates, including Vista's Value Creation Team, for administration, research, database development, workforce analytics, recruiting oversight, and business operations purposes, and, where you consent, other Vista portfolio companies so that you may be considered for other job opportunities, (iv) our legal counsel, auditors, accountants, insurers, and other professional advisors, to the extent reasonably necessary for obtaining professional advice or for establishing, exercising, or defending legal claims; (v) any government department, agency, court, or other official body where we believe disclosure is necessary (A) as a matter of applicable law or regulation (such as in response to a subpoena, warrant, court order, or other legal process), (B) to exercise, establish, participate in, or defend our legal rights, or to limit the damages we sustain in litigation or other legal dispute, or (C) to protect your vital interests, privacy, or safety, or those of our customers or any other person; (vi) a potential or actual buyer or transferee (and its agents and advisors) in connection with any proposed or actual transfer of control, purchase, merger, reorganization, consolidation, or acquisition of any part of our business; and (vii) any other person with your consent to the disclosure.

We do not "sell" or "share" your Personal Data as those terms are defined under the CCPA/CPRA (Cal. Civ. Code §1798.140(ad) and (ah)). We do not engage in cross-context behavioral advertising. See Section 11.2 for your rights, including the right to opt out of any future sale or sharing should our practices change.

Whenever we share Personal Data, we take reasonable steps to ensure that it is treated securely and in accordance with this Notice. We may also share aggregated or de-identified information that is not intended to be used by the recipient to identify you, for purposes such as analytics, benchmarking, and product improvement.

7. International Transfer of Personal Data

Your Personal Data may be collected, transferred to, and stored by us in the United States and by our affiliates and third parties in other countries. Therefore, your Personal Data may be processed outside your country or jurisdiction, including in places that may not provide the same level of data protection as your home jurisdiction. Where such transfers occur, we implement appropriate safeguards to ensure that Personal Data remains protected in accordance with Applicable Data Protection Law, including:

- **Standard Contractual Clauses ("SCCs"):** We execute the European Commission's Standard Contractual Clauses with data importers, supplemented by Transfer Impact Assessments ("**TIAs**") where required.
- **EU-U.S. Data Privacy Framework: See Section 8.**
- **Adequacy Decisions:** We may transfer Personal Data to countries or territories for which the European Commission or the UK Secretary of State has issued an adequacy decision.

You may obtain a copy of the relevant transfer safeguards by contacting us at the address set forth in Section 20.

8. Data Privacy Framework

TRGRP, Inc. (and its U.S.-based Affiliates) complies with the EU-U.S. Data Privacy Framework ("**EU-U.S. DPF**"), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework ("**Swiss-U.S. DPF**") as set forth by the U.S. Department of Commerce. TRG Screen has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. DPF Principles with regard to the processing of Personal Data received from the European Union and the United Kingdom, and the Swiss-U.S. DPF Principles with regard to Personal Data received from Switzerland. In the event of any conflict between the terms of this Notice and the DPF Principles, the DPF Principles shall govern. To learn more about the Data Privacy Framework program, and to view our certification, please visit https://www.dataprivacyframework.gov.

8.1 Onward Transfers

TRG Screen remains responsible under the DPF Principles for Personal Data it onward transfers to agents, requires those agents to provide equivalent protection, and is liable for any non-compliant processing by an agent unless it proves it is not responsible for the event giving rise to the damage.

8.2 Dispute Resolution and Binding Arbitration

TRG Screen is committed to resolving disputes regarding the collection or use of your Personal Data. If you have any questions, concerns, or complaints, please first contact us at dataprivacy@trgscreen.com.

In compliance with the DPF Principles, TRG Screen agrees to cooperate with the advice of the panel established by the EU data protection authorities (EU DPAs) for unresolved complaints concerning Personal Data transferred from the EU in reliance on the EU-U.S. DPF.

Individuals may also invoke binding arbitration under the DPF Principles for any unresolved complaints. The arbitration shall be conducted in accordance with the rules of a neutral arbitration organization (e.g., American Arbitration Association). The decision of the arbitrator shall be final and binding on all parties.

For unresolved complaints related to data transferred from the United Kingdom in reliance on the UK Extension to the EU-U.S. DPF, TRG Screen commits to cooperate with the UK Information Commissioner's Office (ICO). For unresolved complaints related to data transferred from Switzerland in reliance on the Swiss-U.S. DPF, TRG Screen commits to cooperate with the Swiss Federal Data Protection and Information Commissioner (FDPIC).

8.3 FTC Enforcement

The Federal Trade Commission (FTC) has jurisdiction over TRG Screen's compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF.

9. How Long We Retain Your Data

We retain Personal Data for as long as necessary to fulfill the purposes for which it was collected (see Section 5 above), to comply with our legal, accounting, tax, and regulatory obligations, and to establish, exercise, or defend legal claims. The criteria we use to determine retention periods include: the amount, nature, and sensitivity of the Personal Data; the potential risk of harm from unauthorized use or disclosure; whether we can achieve the purposes through other means; the nature and duration of our relationship with you; applicable statutes of limitation; and applicable legal, regulatory, tax, or accounting requirements. Where you have applied for a role with us, we may retain your Applicant Data after the conclusion of the recruiting process so that we may consider you for future opportunities, unless you ask us not to retain your information

for that purpose by contacting us at the address in Section 20. Where we are required by law to retain data for longer, or where retention is necessary to defend a legal claim, we will do so.

After expiry of the applicable retention periods, your Personal Data will be deleted. If there is any data that we are unable, for technical reasons, to delete entirely from our systems, we will implement appropriate measures to prevent any further use of such data.

10. How We Secure Your Data and What You Can Do

We take appropriate precautions including organizational, technical, and physical measures to help safeguard against accidental or unlawful destruction, loss, alteration, and unauthorized disclosure of, or access to, the Personal Data we process or use.

While we follow generally accepted standards to protect Personal Data, no method of storage or transmission is 100% secure. You can also take steps to protect the privacy of your information. You are responsible for protecting your password, limiting access to your devices, and signing out of websites after your sessions.

11. Your Rights Relating to Your Personal Data

You have certain rights relating to your Personal Data, subject to local data protection laws. Depending on the applicable laws and subject to certain conditions and exceptions, these rights may include the following:

11.1 Rights Under GDPR and UK GDPR

- **Right of Access:** You have the right to obtain confirmation of whether we process your Personal Data and, if so, to access such data together with supplementary information regarding the processing.
- **Right to Rectification:** You have the right to request correction of inaccurate Personal Data and completion of incomplete Personal Data.
- **Right to Erasure:** You have the right to request deletion of your Personal Data where, inter alia, the data is no longer necessary for the purpose for which it was collected, you withdraw consent, or there is no overriding legitimate ground for continued processing.
- **Right to Restriction of Processing:** You have the right to request restriction of processing in certain circumstances, including where the accuracy of the data is contested or where processing is unlawful.
- **Right to Data Portability:** You have the right to receive your Personal Data in a structured, commonly used, and machine-readable format, and to transmit that data to another controller.
- **Right to Object:** You have the right to object to processing based on legitimate interests or for direct marketing purposes at any time. Where you object to direct marketing, we will cease such processing without undue delay.
- **Right Not to Be Subject to Automated Decision-Making:** You have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or similarly significantly affects you. As described in Section 12, we do not make such solely automated decisions; the limited AI-assisted review used for India-based Applicants is supervised by, and decisions are made by, qualified TRG Screen personnel.
- **Right to Withdraw Consent:** Where processing is based on consent, you may withdraw your consent at any time. Withdrawal does not affect the lawfulness of processing prior to withdrawal.
- **Right to Complain to Us:** You have the right to make a complaint to us about our processing of your Personal Data. See Section 21 (Complaints) for how to submit a complaint and how we will respond.

- **Right to Lodge a Complaint:** You have the right to lodge a complaint with a supervisory authority in the EU Member State of your habitual residence, place of work, or place of the alleged infringement.

11.2 Rights Under CCPA/CPRA (California Residents)

If you are a California resident, you have the following additional rights under the CCPA as amended by the CPRA. See Section 17 for further details.

- **Right to Know:** You may request disclosure of the categories and specific pieces of Personal Information we have collected, the sources, the purposes, and the categories of third parties with whom it has been shared. You may make a verifiable consumer request to know up to twice within a 12-month period, free of charge.
- **Right to Delete:** You may request deletion of Personal Information we have collected from you, subject to certain exceptions permitted by law.
- **Right to Correct:** You may request correction of inaccurate Personal Information that we maintain about you.
- **Right to Opt-Out of Sale or Sharing:** We do not sell or share your Personal Information. Should our practices change, we will provide a conspicuous opt-out mechanism.
- **Right to Limit Use of Sensitive Personal Information:** You have the right to direct us to limit the use and disclosure of your Sensitive Personal Information to purposes authorized by the statute.
- **Right to Non-Discrimination:** We will not discriminate against you for exercising any of your CCPA/CPRA rights. We will not deny you services, charge you different prices, provide a different level or quality of service, or suggest that you will receive any of these as a consequence of exercising your rights.

11.3 Rights Under Other U.S. State Privacy Laws

Residents of states with comprehensive privacy legislation (including but not limited to Virginia, Colorado, Connecticut, Utah, Texas, Oregon, Montana, and Minnesota) may have additional rights, including rights of access, correction, deletion, data portability, and the right to opt out of targeted advertising, profiling, or the sale of personal data. We will process requests in accordance with the applicable state law.

11.4 Rights Under India's Digital Personal Data Protection Act

If you are located in India, the following rights under the Digital Personal Data Protection Act, 2023 ("**DPDPA**") apply to your Personal Data. We may transfer your Personal Data outside India to our Affiliates and service providers, in accordance with Section 16 of the DPDPA and any restrictions issued by the Central Government. Where we process your Personal Data, we do so on the basis of your consent or for "legitimate uses" permitted by the DPDPA.

- **Right to Information**: You have the right to obtain a summary of the Personal Data we process about you and the processing activities undertaken.
- **Right to Correction and Erasure**: You have the right to request correction of inaccurate or misleading Personal Data, completion of incomplete Personal Data, and erasure of Personal Data that is no longer necessary for the purpose for which it was processed.
- **Right to Grievance Redressal**: You have the right to a readily available means of grievance redressal in respect of any act or omission concerning the performance of our obligations.

- **Right to Nominate**: You have the right to nominate another individual to exercise your rights in the event of your death or incapacity.
- **Right to Withdraw Consent**: Where processing is based on your consent, you may withdraw that consent at any time. Withdrawal does not affect the lawfulness of processing prior to withdrawal.
- **Grievance Officer**: For DPDPA-related grievances, you may contact our Grievance Officer at dataprivacy@trgscreen.com. We will respond within the period prescribed by the DPDPA. If your grievance remains unresolved, you may lodge a complaint with the Data Protection Board of India.
- **Children and Persons with Disabilities**: We do not knowingly process Personal Data of any individual under the age of eighteen (18) located in India without verifiable consent from a parent or lawful guardian. We do not undertake tracking, behavioural monitoring of children, or targeted advertising directed at children, except as may be permitted by the DPDPA. For Personal Data of persons with disabilities who have a lawful guardian, we obtain consent from the guardian as required.

11.5 Exercising Your Rights

To exercise your rights relating to your Personal Data, make a complaint about our processing of your Personal Data, or if you have questions regarding our privacy practices, please submit a request via email to dataprivacy@trgscreen.com.

We will acknowledge receipt of your rights request within five (5) business days and will acknowledge receipt of any complaint to which Section 164A of the UK Data Protection Act 2018 applies within thirty (30) days, make appropriate enquiries into the complaint, keep you informed of our progress, and respond within the timeframes required by Applicable Data Protection Law.

We may request information reasonably necessary to verify your identity or authority before fulfilling a request. Where requests are manifestly unfounded, excessive, or repetitive, we may charge a reasonable fee or refuse to act on the request, in accordance with applicable law.

You may also opt out of marketing emails at any time by using the unsubscribe link in our marketing emails.

Where TRG Screen processes your Personal Data on behalf of a Licensee in connection with that Licensee's use of the Services (i.e., where TRG Screen acts as a Data Processor), you should direct your rights request to the relevant Licensee. We will redirect such requests to the relevant Licensee and will assist the Licensee in responding as required by the applicable DPA.

You may also designate an authorized agent to submit a request on your behalf. We may require the authorized agent to provide written proof of authorization and may verify your identity directly.

11.6 Right to Appeal

If we decline to take action on a request you have submitted under this Notice, we will inform you of our reasons and provide instructions on how to appeal the decision. You may submit an appeal by contacting us at dataprivacy@trgscreen.com. We will respond to your appeal within a reasonable period as required by applicable law. If your appeal is denied, we will provide you with information on how to contact the applicable supervisory authority, attorney general, or other regulator with jurisdiction over your data protection rights.

12. Use of AI

12.1 Use in TRG Screen Services

Where TRG Screen makes AI-powered features available within the Services or uses AI to assist in the provision of its obligations in providing the Services, the use is governed by the customer agreement between TRG Screen and the relevant Licensee. Individuals with questions about the AI features available within a particular Licensee's instance of the Services should contact that Licensee in the first instance.

12.2 Use in Hiring

For Applicants applying to positions based in India only, we may use AI tools to assist our recruiters by summarizing application materials (such as resumes) and flagging candidates whose stated qualifications appear to align with the relevant job description and required qualifications. AI is used solely as a decision-support tool: a human recruiter or hiring manager reviews any AI-generated summary or flag, and AI is not used to shortlist, reject, or otherwise make decisions about whether to interview, hire, or reject any candidate. All shortlisting and hiring decisions are made by qualified TRG Screen personnel. India-based Applicants who wish to object to AI-assisted review of their application materials, or who would like more information about how this tool is used, may contact us at the details set out in Section 20.

12.3 No Other Use

Other than the limited AI-assisted review described above for India-based Applicants, we do not make decisions producing legal effects concerning, or similarly significantly affecting, Data Subjects based solely on automated processing, including profiling. Where AI or automated tools are used, qualified TRG Screen personnel remain responsible for, and exercise meaningful human oversight over, any resulting decisions.

13. Third-Party Links and Integrations

We may disclose to you links to, or integrations with, third-party websites, platforms, or services that are not operated or controlled by us. The information practices of these third parties are governed by their Privacy Notices, which you should review to better understand their privacy practices. We are not responsible for the content, privacy practices, or security of any third-party site or service.

14. Children's Privacy

Our Services are designed for and directed to business users and enterprise professionals and are not intended for children. We do not knowingly collect, sell, or share Personal Data from individuals below the age of digital consent applicable in their jurisdiction (which is 16 in most of the EEA and the UK, under 13 in the United States under COPPA, and 18 in India under the DPDPA, in each case subject to local law). If we become aware that we have inadvertently collected Personal Data from a child below the applicable age, we will take prompt steps to delete such data. If you believe that a child has provided us with Personal Data, please contact us immediately at dataprivacy@trgscreen.com.

15. Data Breach Notification

In the event of a personal data breach that poses a risk to your rights and freedoms, we will notify the relevant supervisory authority without undue delay and, where feasible, within 72 hours of becoming aware of the breach (as required under the GDPR/UK GDPR). For breaches affecting individuals located in Singapore, we will notify the Personal Data Protection Commission as soon as practicable, and in any case no later than

three (3) calendar days after assessing that the breach is notifiable under the PDPA, and will notify affected individuals where the breach is likely to result in significant harm. For breaches affecting individuals located in India, we will notify the Data Protection Board of India and affected Data Principals in accordance with the DPDPA. Where the breach is likely to result in a high risk to your rights and freedoms, we will also inform you directly in accordance with applicable law and as soon as practicable. Data breach notification obligations for enterprise customers are governed by the timeframes set forth in the applicable DPA.

16. Enterprise Customers: Processor Obligations

As described in Section 1, where TRG Screen processes Personal Data on behalf of a Licensee acting as a Data Controller, the parties' respective obligations are governed by the DPA executed between them. The DPA incorporates, as applicable, the Standard Contractual Clauses adopted by the European Commission, the UK International Data Transfer Addendum to the EU SCCs, agreed technical and organizational measures, data breach notification timeframes, and return and deletion obligations on termination. Licensees may request a copy of our standard DPA by contacting dataprivacy@trgscreen.com.

17. Additional Disclosures for California Residents

To the extent we are a "business" subject to the CCPA, we make the following disclosures. The CCPA requires covered businesses to disclose whether they sell or share Personal Data. We do not sell, and do not share (as those terms are defined under the CCPA), Personal Data. We do not "share" Personal Data for cross-context behavioral advertising as that term is defined under the CCPA. We may allow third parties to collect Personal Data through our Services only where those third parties are authorized service providers that have agreed to contractual limitations on their retention, use, and disclosure of such Personal Data, or where you use our Services to interact with third parties or direct us to disclose your Personal Data to third parties.

California law also requires that we identify the categories of Personal Data we disclose for certain "business purposes," such as to service providers that assist us with securing or providing our Services, and to such other entities as described in Sections 5 and 6 of this Notice. We disclose the following categories of Personal Data for those business purposes:

- Identifiers;
- Commercial information;
- Internet or other electronic network activity information;
- Professional or employment-related information;
- Geolocation data;
- Sensitive Personal Information (as described in Section 4); and
- Inferences drawn from any of the above categories.

California law grants state residents certain rights, including the rights to know and access specific pieces of Personal Data, to learn how we process Personal Data, to request deletion of Personal Data, to request correction of Personal Data, to limit the use and disclosure of Sensitive Personal Information, to opt out of the sale or sharing of Personal Data, and not to be denied goods or services for exercising these rights. Those rights, and the conditions under which they apply, are described in Section 11.2. California residents may also request information regarding our disclosure, if any, of certain categories of Personal Data to third parties for those third parties' direct marketing purposes during the immediately preceding calendar year, as provided under California Civil Code § 1798.83. We do not currently disclose Personal Data to third parties for their own direct marketing purposes.

For information on how to exercise these rights or submit a request under California Civil Code § 1798.83, please refer to Section 11.5 of this Notice or contact us using the information in Section 20. If you are an authorized agent wishing to exercise rights on behalf of a California resident, please contact us using the information in Section 20 and provide a copy of the consumer's written authorization designating you as their agent. We may need to verify your identity, place of residence, and — in the case of an authorized agent — your authority before completing the request.

18. Additional U.S. State Privacy Law Disclosures

For residents of states not specifically addressed above, we will process data rights requests in accordance with the applicable state law. For information on how to exercise your rights or to appeal a decision, please refer to Sections 11.5 and 11.6.

19. Changes to This Notice

We will update this Privacy Notice from time to time to reflect changes in our practices, technologies, legal requirements, and other factors. Material changes will be communicated by posting the revised Notice on our Site with an updated "Last Updated" date and, where required by Applicable Data Protection Law, by providing direct notice to affected Data Subjects via email or in-application notification. We encourage you to review this Notice periodically. Non-material changes (such as typographical corrections, formatting updates, or clarifications that do not alter data processing practices) may be made without prior notice.

20. Contacting Us

To exercise your rights relating to your Personal Data, make a complaint about our processing of your Personal Data, or if you have questions regarding this Privacy Notice or our privacy practices, please contact us at:

TRGRP, Inc.
Attn: Compliance
Email: dataprivacy@trgscreen.com
Postal Address: 1 Penn Plaza, 3rd Floor, New York, NY 10119, United States
When you contact us, please indicate in which country and/or state you reside.
We may ask for proper identification to verify your identity and protect your privacy. To the extent you provide us with that identification, it will be used for the sole purpose of identity verification and shall be subsequently deleted.

21. Complaints

If you have a complaint or concern about our processing of your Personal Data, you may contact us using the details in Section 20. If Section 164A of the UK Data Protection Act 2018 applies to your complaint, we will acknowledge receipt within thirty (30) days, take appropriate steps to respond to your complaint (including making appropriate enquiries and keeping you informed of our progress), and inform you of the outcome without undue delay. If you believe that we have not been able to assist with your complaint or concern, or if you otherwise wish to do so, you have the right to lodge a complaint with the competent supervisory authority in your jurisdiction. If you are located in the EEA, you may complain to the supervisory authority in your country of residence, place of work, or place of the alleged infringement. In the UK, this is the Information Commissioner's Office (ICO) at www.ico.org.uk. In Switzerland, this is the Federal Data Protection and Information Commissioner (FDPIC) at www.edoeb.admin.ch. In Singapore, this is the Personal Data Protection

Commission (PDPC) at www.pdpc.gov.sg. In India, this is the Data Protection Board of India established under the DPDPA. For California residents, you may contact the California Privacy Protection Agency at https://cppa.ca.gov or the California Office of the Attorney General at https://oag.ca.gov/privacy. Applicants in any jurisdiction may also contact their local data protection authority where one exists.

22. TRG Screen Affiliated Companies

The following companies are Affiliates of TRGRP, Inc.: Axon Financial Systems Limited; BST America, LLC; Crizit LLC; Market Data Insights LLC; Priory Solutions LLC; Screen Asia Pte Ltd; Screen Consultants S.A.; Screen France SAS; Screen Germany GmbH; Screen Group B.V.; Screen INFOmatch B.V.; TRG Screen Holdings B.V.; TRGRP India Private Limited; Xpansion Financial Technology Services Limited.

In addition to sharing with our Affiliates, we disclose your personal information to Vista for administration, research, database development, workforce analytics, and business operations purposes in line with the terms of this Privacy Notice. Vista processes and shares your personal information on the basis of its legitimate interests in managing, administering and improving its business, research and workforce analytics, overseeing the recruitment process, and, if applicable, your employment relationship with TRG Screen.

If you have consented to us doing so, we and Vista also share your personal information with other Vista portfolio companies for the purpose of being considered for other job opportunities in the pooling system, both inside and outside of the European Economic Area ("**EEA**") and United Kingdom ("**UK**").

You can find a list of Vista portfolio companies at www.vistaequitypartners.com/companies/ and Vista's privacy notice at www.vistaequitypartners.com/privacy/. In connection with the recruitment process your personal data may be transferred outside of the EEA or UK to Greenhouse Software, Inc. and Criteria Corp., which provide applicant tracking and evaluation services.

Thank you for your interest in TRG Screen.