Remote Leverage Global Privacy, Data Protection and Data Processing Agreement

Version 1.0. Effective Date: October 7, 2026. Last updated October 2026.

Table of Contents

SECTION 0. INTRODUCTION, SCOPE, AND ACCEPTANCE 5
0.1 Identity of the controller 5
0.2 What this Privacy Agreement does 5
0.2A Nature of this Privacy Agreement 5
0.2B Key points at a glance 6
0.3 The three Services and Leve 6
0.4 Acceptance 7
0.4A Authorizations given on acceptance 8
0.4B Global Data Processing Authorization 10
0.5 Governing law and dispute resolution 11
0.6 Definitions 11
Defined terms 12
SECTION 1. GLOBAL BASELINE PRIVACY NOTICE 15
1.1 Controller identity and contacts 15
1.2 Categories of Personal Data and sources 15
1.3 Purposes of Processing 18
1.4 Secondary use, analytics, and service and model improvement 19
1.5 Legal bases 19
1.6 Recipients and categories of recipients 19
1.7 International transfers 20
1.8 Retention 20
1.9 Sensitive, special-category, and children's data 21
1.9A Biometric identity verification and retention schedule 21
1.9B Video Introductions and the Talent Marketplace 22
1.10 Cookies and similar technologies 23
1.11 Automated decision-making and profiling 23
1.12 Your rights 24
1.13 Complaints 24
1.14 Effective date and changes 24
SECTION 2. PLACEMENT CANDIDATE AND CONTRACTOR USER TERMS 24
2.1 Data map for Placement Candidates and Contractor Users 24
2.2 Role determination for Placement Candidate and Contractor User data 24
2.3 Lawful basis for core Processing of Placement Candidate and Contractor User data 25

2.4 Rights and channels for Placement Candidates and Contractor Users 25
SECTION 3. CLIENT TERMS 25
3.1 Client and Authorized User data 25
3.2 Client business and confidential information 25
3.3 Client roles 25
3.4 Client warranties 26
3.5 Third-Party Processors and Integrations 26
SECTION 4. DATA USE, LICENSE, AND CONTROL 27
4.1 Operational rights 27
4.2 De-identified and aggregated data 27
4.3 Statutory ceiling and read-down 27
4.4 Controller-to-Controller Mutual Obligations (Recruitment Services, Managed: Contractor of Record Services, and Messages) 27
4.5 Leve Records and acceptance records 28
SECTION 5. DATA PROCESSING AGREEMENT (PROCESSOR TERMS) 28
5.1 Subject matter, duration, nature, purpose, categories 29
5.2 Documented instructions 29
5.3 Confidentiality 29
5.4 Security 30
5.5 Subprocessors 29
5.6 Assistance 29
5.7 Personal data breach 30
5.8 Return or deletion 30
5.9 Audit and information 30
5.10 International transfers under this Section 30
5.11 United States service-provider terms 30
SECTION 5A. CONTROLLER ARRANGEMENT (MANAGED: CONTRACTOR OF RECORD SERVICES) 31
5A.1 Independent controllers 31
5A.2 Allocation of responsibilities 31
5A.3 Liability toward data subjects 31
SECTION 6. MONITORING, WORK VERIFICATION, AND DEVICE SECURITY 31
6.1 Purposes 32
6.2 Lawful basis 33
6.3 Scope of monitoring 32
6.4 Device management and endpoint security 32
6.5 Transparency 33
6.6 Retention and access 34
6.7 Limits on monitoring 33
6.8 Monitoring Authorization and withdrawal 33
6.9 Recipients of Work-Verification Data and roles 33
SECTION 6A. MESSAGING SERVICE AND ACCESS TO MESSAGES 35
6A.1 Scope and data processed 35

6A.2 Who can see Messages; Client access 34
6A.3 Access and use by Remote Leverage 34
6A.4 Automated scanning and optional features 34
6A.5 Consent of all parties 36
6A.6 Call and meeting recordings 35
6A.7 Prohibited content and user responsibility 35
6A.8 Retention 35
6A.9 Roles and Client obligations for Messages 35
6A.10 Legal basis by jurisdiction and non-waivable rights 36
6A.11 In-product notice 37
SECTION 6B. PAYMENTS, CONTRACTS, AND TAX DOCUMENTS 37
6B.1 Payment Partners and payment data flows 37
6B.2 Identity verification, know-your-customer, and sanctions screening 38
6B.3 Sanctions and restricted jurisdictions 38
6B.4 Contracts and electronic signatures 38
6B.5 Tax documents and information reporting 38
6B.6 Chargebacks, collections, and disputes 38
6B.7 Currency conversion and exchange-rate records 38
SECTION 6C. SMS AND RCS MESSAGING PROGRAM 39
6C.1 Program description and message types 39
6C.2 Consent and revocation 39
6C.3 How consent is given and recorded 39
6C.4 Message frequency and message and data rates 40
6C.5 Consent records 40
6C.6 Help and customer care 40
6C.7 Opting out and revoking consent 40
6C.8 Time-of-day and frequency limits 40
6C.9 Changed or reassigned phone numbers 40
6C.10 Delivery and supported devices 41
6C.11 Eligibility 41
6C.12 Privacy 41
6C.13 Compliance with telephone and messaging laws 41
6C.14 Recipients outside the United States 41
SECTION 7. INTERNATIONAL DATA TRANSFERS 41
7.1 Data flows and mechanisms 41
7.2 Contractual safeguards 42
7.3 Controller responsibility (Managed: Contractor of Record Services) 42
7.4 Transfer documentation 43
SECTION 8. DATA-SUBJECT RIGHTS MECHANICS 43
SECTION 9. SECURITY 43
SECTION 10. PERSONAL DATA BREACH RESPONSE 44
SECTION 11. RECORDS OF PROCESSING AND GOVERNANCE 44

SECTION 11A. ARTIFICIAL INTELLIGENCE AND AUTOMATED DECISION TOOLS 44
11A.1 Use of automated tools 44
11A.2 Notice and jurisdiction-specific requirements 44
11A.3 Non-discrimination 45
11A.4 Client decisions 45
11A.5 Third-party artificial-intelligence services 45
11A.6 Use of Personal Data to improve tools and models 45
SECTION 12. GENERAL 45
ANNEX A. EUROPEAN ECONOMIC AREA, UNITED KINGDOM, AND SWITZERLAND 46
ANNEX B. UNITED STATES (FEDERAL AND STATE) 48
ANNEX C. CANADA (FEDERAL AND PROVINCIAL) 49
ANNEX D. PHILIPPINES 50
ANNEX E. LATIN AMERICA 51
E.1 Argentina 51
E.2 Brazil 52
E.3 Chile 52
E.4 Colombia 52
E.5 Costa Rica 53
E.6 Dominican Republic 53
E.7 Ecuador 53
E.8 El Salvador 53
E.9 Mexico 53
E.10 Panama 54
E.11 Paraguay 54
E.12 Peru 54
E.13 Uruguay 54
ANNEX F. OTHER JURISDICTIONS 54
ANNEX G. SUBPROCESSORS, IDENTITY-VERIFICATION AND MONITORING TOOLS, AND SECURITY MEASURES 56
G.1 Subprocessors and service providers 56
G.2 Identity-verification and monitoring tools 61
G.3 Technical and organizational measures 61
ANNEX H. COOKIE AND TRACKING TECHNOLOGIES NOTICE 62
H.1 What we use 62
H.2 Your choices 63
H.3 United States opt-outs 63
H.4 Talent Marketplace pages and duration 63

About this Privacy Agreement. This Remote Leverage Global Privacy, Data Protection and Data Processing Agreement (this "Privacy Agreement") is a single, layered, binding document that combines (a) a worldwide privacy notice, including the Cookie and Tracking Technologies Notice in Annex H and the SMS and RCS Messaging Program terms in Section 6C, (b) a data protection and data use agreement, and (c) a data processing agreement and controller arrangement. It is the "Privacy Agreement" to which the Leve Platform Terms and Conditions (the

"Terms") refer, and it applies to Leve and to every Service. Section 0.2A explains which parts are contractual terms and which are provided as notice, and Section 0.2B summarizes the key points.

Parties and subjects. It applies to and binds Remote Leverage and every User that accepts it, including every Client (together with its Authorized Users and Account Administrators), every Placement Candidate, every Direct Contractor, and every COR Contractor. For Visitors, Prospects, and other individuals whose Personal Data is Processed without their accepting it, such as references and Client personnel named by a User, it operates as a privacy notice only, as described in Section 0.4.

Order of precedence. This Privacy Agreement is incorporated into the Terms, and Terms Section 4.5 sets the order of precedence among the Terms, this Privacy Agreement, the COR MSA, each COR Contractor's independent contractor agreement with Remote Leverage, and any placement agreement or Service Order. Within this Privacy Agreement, an Annex controls over the global baseline for data subjects in its jurisdiction where its law grants a stronger protection or imposes a different requirement; Section 5A governs the controller relationship in the Managed: Contractor of Record Services; and Section 5 governs where Remote Leverage acts as processor or service provider.

SECTION 0. INTRODUCTION, SCOPE, AND ACCEPTANCE

0.1 Identity of the controller

This Privacy Agreement is issued by Remote Leverage Inc. doing business as Remote Leverage, a Profit Corporation organized under the laws of Florida, with its principal place of business at 1395 Brickell Avenue Suite 800 Miami, Florida 33131 ("Remote Leverage," "we," "us," or "our"), which operates Leve. Where an Affiliate of Remote Leverage determines the purposes and means of a given Processing activity, that Affiliate and its role are identified at or before the time that Processing begins, or on request to the privacy contact below. Privacy contact, including for every request about Personal Data that Terms Section 17.4 refers to this Privacy Agreement: privacy@remoteleverage.com. Security contact, including for reports of suspected vulnerabilities or Security Incidents: security@remoteleverage.com; a report sent to the Support Email is also treated as received. SMS and RCS Messaging Program customer care: paula@remoteleverage.com or +1 (650) 668-0728, as described in Section 6C. Notices under the Terms, other than requests about Personal Data, are given as Terms Section 17.4 provides.

0.2 What this Privacy Agreement does

This Privacy Agreement explains and governs how we collect, use, disclose, transfer, retain, secure, and otherwise Process Personal Data through Leve and in providing the Services, and it sets out the binding rights and obligations of the parties in relation to that data across every jurisdiction implicated by our global operations.

0.2A Nature of this Privacy Agreement

Notice. Section 1, Section 0.2B, the jurisdictional disclosures in Annexes A through F, the descriptive content of Sections 6, 6A, 9, and 11A, Annex G, and Annex H are provided to inform data subjects about how Personal Data is Processed. They describe Remote Leverage's practices and policies as at the version date, are made to satisfy the transparency requirements of Applicable Data Protection Law, and do not create contractual obligations of Remote Leverage, or contractual rights of any person, beyond those that Applicable Data Protection Law itself imposes or confers, except to the extent Section 5 or Section 5A expressly incorporates them as obligations.

Contract. The following are binding contractual terms between Remote Leverage and each User who accepts this Privacy Agreement: the order-of-precedence paragraph that precedes Section 0; Sections 0.2A, 0.3 (as to the allocation of roles and the disclaimers it contains), 0.4, 0.4A, 0.4B, 0.5, and 0.6; the amendment mechanism in Section 1.14; Sections 2, 3, 4, 5, and 5A, including Section 9 and Annex G to the extent Section 5 or Section 5A incorporates them; Sections 6.8, 6.9, 6A.2, 6A.3, 6A.5, 6A.7, 6A.9, 6B.1, 6B.3, 6B.4, 6B.6, and 6B.7; Section 6C, as between Remote Leverage and each participant in the SMS/RCS Program; the limits in Section 8; Section 11A.3; Section 7 as between Remote Leverage and Clients; Section 12; and the provisions of the Annexes that allocate

responsibilities between Remote Leverage and Clients, Placement Candidates, or Contractor Users. Nothing in this Section limits a right that Applicable Data Protection Law confers on a data subject. Section 0.4A(i) and paragraphs (b), (e), (f), (g), and (i) of Section 1.9B are also binding contractual terms between Remote Leverage and each User who accepts this Privacy Agreement.

0.2B Key points at a glance

This summary is provided for convenience; the rest of this Privacy Agreement controls.

- **One acceptance.** Checking the single acceptance box, at registration or before first accessing the Talent Marketplace, accepts the Terms and this Privacy Agreement and gives every authorization in Section 0.4A, including for sensitive data, biometric identity verification, international transfers, monitoring where activated, access to Messages, display of a Video Introduction if one is recorded, account text messages, and marketing email. Each may be withdrawn as this Privacy Agreement describes.
- **Who we are.** Remote Leverage operates Leve and the Recruitment Services, the Self Serve: Direct Pay Services, and the Managed: Contractor of Record Services. Our role differs by Service, as Section 0.3 explains.
- **What we collect.** Account, identity, verification, professional, Engagement, tax, payment-instruction, Messaging Service, Work-Verification Data (only where monitoring is activated and authorized), device, usage, Tracking Technology, and SMS/RCS Program data, as listed in Section 1.2.
- **Talent Marketplace.** If you are a Placement Candidate and choose to record a Video Introduction, your Video Introduction, first name, country, role, rate range, and experience are shown in the Talent Marketplace to Marketplace Viewers so that they can search for you and request interviews. Videos are never used for facial recognition or to identify you from your face or voice. Appearing in the Talent Marketplace requires your consent, and you can remove your profile at any time (Section 1.9B).
- **Messages are not private from Remote Leverage or the Client.** Messages are encrypted in transit and at rest but not end-to-end. Remote Leverage may access them for the purposes in Section 6A.3, and a Client, through its Account Administrators, may access Messages within its Workspace or about its Engagements, as Section 6A.2 describes.
- **Monitoring happens only where activated and authorized.** It applies only during working time, is never covert, and never captures keystroke content or webcam images as a standard measure (Section 6).
- **Payments are executed by Payment Partners.** Remote Leverage collects and transmits payment instructions and payment data; licensed Payment Partners execute debits, conversions, and payouts and hold funds under their own licenses (Section 6B.1).
- **We do not sell Personal Data for money,** and we do not share mobile numbers or text-messaging consent with third parties for their marketing (Sections 1.4 and 6C.12).
- **Your rights.** Depending on where you are, you may access, correct, delete, or port your data, object, withdraw consent, and opt out of targeted advertising. Write to privacy@remoteleverage.com (Section 1.12 and Section 8).

0.3 The three Services and Leve

Remote Leverage provides three Services with distinct data-protection footprints, all covered here, and delivers them through Leve.

- **Recruitment Services.** Remote Leverage sources, screens, and presents Placement Candidates to a Recruitment Client, and the Client alone decides whether to engage any Placement Candidate and on what terms. Remote Leverage is an independent controller of Placement Candidate data, and presentation of a Placement Candidate to a Client is a controller-to-controller disclosure. From receipt, the Client is an independent controller of the Placement Candidate data it receives, as Terms Section 13.2 provides. Remote Leverage is not a party to any work relationship that results, unless it is set up as a COR Engagement.

- **Managed: Contractor of Record Services.** Remote Leverage is the contracting party with each COR Contractor, as an independent contractor, under the COR Contractor's own agreement with Remote Leverage, and it invoices the COR Client under the COR MSA. Through Leve, Remote Leverage administers onboarding, contracting, compliance documentation, identity verification and know-your-customer checks, Timesheets and Work-Verification Data where activated, invoicing, payment instructions for COR Contractor payouts executed by Payment Partners, tax documentation and information reporting, and Leve Records. For this Service, Remote Leverage and the COR Client are each an independent controller of the COR Contractor Personal Data each Processes for its own purposes, as set out in Section 5A, and Remote Leverage acts as processor only for discrete Processing it performs solely on the Client's Documented Instructions under Section 5.
- **Self Serve: Direct Pay Services.** Remote Leverage provides Leve tools and payment-facilitation functions that support a Direct Pay Client's direct engagement of Direct Contractors, including Templates, document collection, electronic signature, tax-form collection and transmission, optional time tracking, the project module, invoicing, approvals, messaging, Leve Records, and the transmission of payment instructions to Payment Partners, which execute payments under their own licenses. Each Direct Contract is solely between the Direct Pay Client and the Direct Contractor. Remote Leverage is not a party to it and does not hire, supervise, direct, evaluate, or terminate any Direct Contractor. For this Service the Direct Pay Client is the controller of Direct Contractor Personal Data relating to its Engagement, and Remote Leverage acts as its processor or service provider under Section 5, except for the Processing Remote Leverage performs for its own purposes described in Section 2.2, for which it is an independent controller.
- **Contractor User Processing Disclaimer.** Remote Leverage is neither a Controller nor a Processor for Processing that a Placement Candidate hired by a Client, a Direct Contractor, or a COR Contractor carries out under the Client's direct authority or instruction in the course of performing services for the Client. Remote Leverage does not direct, instruct, monitor, or control that Processing. The Client is solely responsible for ensuring that the Processing complies with Applicable Data Protection Law and for entering into separate contractual arrangements requiring each such individual to comply with data-protection obligations appropriate to the Personal Data and Processing involved.
- **No employment relationship.** Except for its role as contracting party with COR Contractors under the Managed: Contractor of Record Services, Remote Leverage is not an employer, employer of record, professional employer organization, staffing agency, or joint employer of any User, as Terms Sections 3.3, 5.4, and 5.5 state. Nothing in this Privacy Agreement, including any reference to a law that uses employment terminology, implies otherwise. Administering Engagements, Timesheets, payment instructions, verification, and enforcement is not supervision.

0.4 Acceptance

Single acceptance and authorization. Checking the acceptance box described in Terms Section 1.1 is the data subject's acceptance of this Privacy Agreement and the data subject's grant, at that moment and without any further act, of every authorization, consent, release, acknowledgment, and agreement described anywhere in this Privacy Agreement, including its Annexes, whatever name this Privacy Agreement gives it. Wherever this Privacy Agreement describes an authorization, consent, release, or acknowledgment as separate, specific, express, explicit, written, prior, individually recorded, or given through a checkbox, form, or other mechanism, that requirement is met by checking the acceptance box, which expressly refers to these authorizations, is presented together with conspicuous hyperlinks to this Privacy Agreement and the Terms, and is recorded as a Leve Record. Remote Leverage calls out these authorizations expressly and prominently in the acceptance box, in this Section, and in Section 0.2B so that each data subject knowingly gives them. Nothing in this paragraph limits any right of withdrawal or any right that Applicable Data Protection Law confers on a data subject.

Users accept this Privacy Agreement, and give every authorization in Section 0.4A, by checking a single unchecked acceptance box presented together with conspicuous hyperlinks to the Terms and this Privacy Agreement, at registration, before first accessing the Talent Marketplace, or at first login after a material update, in the manner Terms Section 1.1 describes. Remote Leverage records each acceptance with its date and time stamp, the version accepted, the text of the acceptance box, the method of acceptance, the Account identifier or, for a person without

an Account, the device and session identifiers and any email address provided, and the IP address, as an acceptance record under Terms Section 1.4 and a Leve Record, and retains that record for as long as the acceptance may be relevant to a claim or legal obligation.

Safeguards for the single acceptance. The acceptance box is the only acceptance step for the Terms and this Privacy Agreement, and Leve presents it only as follows: (a) the box is unchecked and the registration or continue button stays disabled until it is checked; (b) the box text is the text set out in Terms Section 1.1A, which names the Terms, this Privacy Agreement, the arbitration agreement, and each authorization in Section 0.4A; (c) the summary in Section 0.2B, or a link to it, is displayed next to the box; (d) where local law requires it, the box text and Section 0.2B are shown in Spanish or Portuguese; and (e) a short notice is shown before each function that depends on an authorization is first activated. No authorization or consent is inferred from silence, inactivity, or use of Leve without checking the box, and no function that depends on one is activated for a person who has not checked it.

Acceptance for a Client. An individual who accepts this Privacy Agreement on behalf of a Client represents and warrants that he or she has authority to bind the Client. The Client's acceptance binds the Client and applies to the use of Leve by its Authorized Users and Account Administrators, and the Client is responsible for informing them of this Privacy Agreement and for their compliance with it, as Terms Section 1.6 provides.

Visitors and Prospects. Visitors and Prospects are not asked to accept this Privacy Agreement as a contract, except to access the Talent Marketplace, in which case the person checks the acceptance box and is bound as a User and a Marketplace Viewer; for them, Section 1, Annex H, Section 6C (for Prospects who join the SMS/RCS Program, to whom Section 6C also applies as program terms), and the applicable Annexes operate as a privacy notice.

Electronic records and signatures. Acceptance and the authorizations in Section 0.4A are given electronically, through the acceptance box. Each person accepting agrees to transact electronically, and acceptance and authorizations given in this manner have the same legal effect as a signed writing under applicable electronic-signature law, as Terms Section 1.1 provides.

0.4A Authorizations given on acceptance

Each User gives the following authorizations by checking the acceptance box described in Section 0.4, together with and as part of accepting the Terms and this Privacy Agreement, and the acceptance record evidences each of them as a Leve Record. Each authorization applies only to the persons, and in the circumstances, to which it relates, and takes effect for a function when that function is activated, after the notice described in Terms Section 1.7.

(a) Agreement to this Privacy Agreement, required to register for and use Leve.

(b) The Global Data Processing Authorization in Section 0.4B, covering the Processing of Personal Data, including sensitive Personal Data, for the purposes in Section 1.3, its disclosure to the recipients in Section 1.6, and the transfers described in Section 7, given by every User through the acceptance box and relied on wherever Applicable Data Protection Law requires prior, express, or informed authorization or consent (for example, under the laws of Colombia and Argentina and other authorization-based regimes, and, for sensitive personal information, under the Data Privacy Act of 2012 of the Philippines).

(c) Explicit consent and written release for biometric identity verification, given before any biometric identifier or biometric information is collected through identity verification, after the individual has been informed in writing of the collection, the specific purpose, and the retention and destruction schedule in Section 1.9A. The release extends to Remote Leverage and to its identity-verification Subprocessor. This is the consent that Terms Section 7.3 refers to.

(d) Monitoring Authorization, given by each Contractor User on acceptance and effective if and when time tracking or work verification is activated for that Contractor User by the Client for whom it works or by Remote Leverage. This Privacy Agreement, and the notice Leve shows before monitoring begins, describe the Monitoring Tool, the Work-Verification Data collected, when collection occurs, who may access the data, the purposes, retention, and how to withdraw, as Section 6 and Terms Section 14.2 describe.

(e) Personal-Device Consent, given by each Contractor User on acceptance and relied on only where a Contractor User will run the Monitoring Tool, or will be subject to device management under Section 6.4, on a personal device instead of a device provided by Remote Leverage or the Client.

(f) Messaging Acknowledgment, given by each User on acceptance, before the User first uses the Messaging Service. It confirms that Messages are visible to Remote Leverage under Section 6A.3 and, for Messages within a Client's Workspace or about its Engagements, to that Client under Section 6A.2, and records each participant's consent, as a party to the communication, to the access, recording, retention, and use described in Section 6A, as Terms Sections 1.7 and 15.4 describe.

(g) Consent to receive Informational Messages through the SMS/RCS Program, given by each User that provides a mobile number. Consent to Promotional Messages is not given through the acceptance box and is never a condition of any Service; it is given only through the opt-in methods in Section 6C.3 and may be withdrawn at any time as Section 6C.7 describes.

(h) Consent to marketing email communications, given on acceptance, which may be withdrawn at any time.

(i) Marketplace Display and Likeness Authorization, given by each Placement Candidate on acceptance and effective only when the Placement Candidate records or submits a Video Introduction after the notice described in Section 1.9B(c): the Placement Candidate's authorization and express consent for Remote Leverage to record, store, display, and make available in the Talent Marketplace the Placement Candidate's Marketplace Profile, including the Placement Candidate's first name, image, likeness, and voice as they appear in the Video Introduction, to Marketplace Viewers, solely to present the Placement Candidate for placement and Engagement opportunities, for as long as the Marketplace Profile remains active. This is the express consent to the use of a person's name, portrait, photograph, or other likeness that Section 540.08 of the Florida Statutes requires, and the consent or authorization for the capture, reproduction, publication, or use of a person's image or voice that the laws described in Annex E require. It does not extend to use of a Video Introduction in advertising, on social media, or in any medium other than the Talent Marketplace and private presentation to Clients, which requires the Placement Candidate's separate consent. It is a condition of appearing in the Talent Marketplace and may be withdrawn at any time under Section 1.9B(f), with the effect described there.

Authorizations (b) to (h) are stated expressly and prominently in the acceptance box and in this Section, and are given together with agreement to this Privacy Agreement and to the Terms; authorization (b) is given on the terms of Section 0.4B. Where a data subject refuses or withdraws authorization (b), (c), (d), (e), or (f), Remote Leverage may be unable to provide, or may suspend, the Services or features that depend on it, without liability to the extent permitted by law, and the data subject may use any alternative that Remote Leverage makes available, such as a provided device instead of a personal device. Where monitoring has been activated for an Engagement and a Contractor User withdraws authorization (d) by Notice, the Client may end the time-verified Engagement or, for a COR Engagement, Remote Leverage may end it, as Terms Section 14.2 provides, subject to payment of amounts the Client has already approved and funded. Withdrawing authorization (g) or (h) does not affect any Service. Withdrawal does not affect Processing carried out before it, or Processing that rests on another lawful basis. Authorization (i) is also stated expressly and prominently in the acceptance box. Its refusal or withdrawal affects only the Talent Marketplace, as Section 1.9B(b) and (f) describe.

Effect of authorizations that are a condition of an Engagement. Where an authorization is a condition of an Engagement, as Terms Section 14.2 permits for monitoring, Remote Leverage does not treat it as consent for the purposes of the GDPR, the UK GDPR, the Brazilian Lei Geral de Proteção de Dados Pessoais, or any other Applicable Data Protection Law under which consent that is a condition of a contract or given in an unequal relationship is not freely given. For those laws, the authorization operates as the transparency notice and acknowledgment that the law requires, and as the consent required by communications-interception and recording laws, and the Processing rests on the legal bases set out in Sections 6.2 and 6A.10. Where an authorization-based regime, such as Colombia's, requires the data subject's authorization as such, the authorization is given for that regime.

0.4B Global Data Processing Authorization

(a) How it is given. The Global Data Processing Authorization is given by checking the acceptance box described in Section 0.4, whose text expressly refers to the authorizations in this Privacy Agreement, including for sensitive data and international transfers. Checking that box is the data subject's electronic signature and authorization on the terms of this Section, with the same effect as a signed writing under the laws referred to in Section 0.4, and is recorded as a Leve Record under Section 0.4.

(b) What is authorized. By giving the Global Data Processing Authorization, the data subject, having been informed through this Privacy Agreement of the identity and contact details of Remote Leverage (Section 0.1), the purposes of Processing, the recipients, the transfers, the data subject's rights, and how to withdraw, gives Remote Leverage prior, express, informed, specific, and unambiguous authorization to:

(i) collect, record, organize, store, use, analyze, update, disclose, and otherwise Process the data subject's Personal Data in the categories described in Section 1.2, for each of the purposes described in Section 1.3, including Account creation and security, identity verification and sanctions screening, sourcing, assessment, matching, and presentation to Clients, administration of Engagements and placements, Timesheets, invoicing, payment instructions and payouts executed by Payment Partners, tax documentation and information reporting, operation of the Messaging Service, Leve Records, fraud prevention, dispute and chargeback resolution, legal compliance, the establishment, exercise, or defence of legal claims, and the improvement of the Services within the limits of Sections 1.4 and 11A.6;

(ii) Process the data subject's sensitive Personal Data for those purposes, namely government-issued identity documents and identification numbers, taxpayer identification numbers, date of birth and age, nationality and residency, education history, financial-account and payout details, and any marital status or other sensitive information the data subject chooses to provide, it being understood that the data subject is not obliged to provide sensitive Personal Data that is not required for a Service, and that biometric data is Processed only under the consent in Section 0.4A(c);

(iii) disclose the data subject's Personal Data to the recipients described in Section 1.6, including Clients, Payment Partners, the Monitoring Tool operator, the Subprocessors and service providers listed in Annex G and on the Subprocessor Page, professional advisers, and competent authorities, each for the purposes described in this Privacy Agreement; and

(iv) transfer the data subject's Personal Data to, and store and Process it in, the United States and every other country in which Remote Leverage, its Affiliates, Clients, Payment Partners, Subprocessors, or service providers are located, as described in Section 7 and Annex G, with the data subject's acknowledgment that those countries may not provide a level of protection equivalent to that of the data subject's own country, and that Remote Leverage applies the safeguards described in Section 7.

(c) Effect under authorization-based laws. Where Applicable Data Protection Law requires the data subject's consent or authorization for any Processing, disclosure, or transfer described in paragraph (b), the Global Data Processing Authorization is that consent or authorization, including: the prior, express, and informed authorization (autorización previa, expresa e informada) required by Ley Estatutaria 1581 de 2012 and Decreto 1377 de 2013 of Colombia, including for sensitive data and international transfers; the free, express, and informed consent required by Ley 25.326 of Argentina, including for international transfers; the consent specific to the purpose and given before Processing required by Section 13 of the Data Privacy Act of 2012 of the Philippines for sensitive personal information; the express consent required by the Ley Federal de Protección de Datos Personales en Posesión de los Particulares of Mexico for sensitive data and for transfers that require consent; and the consent required by the laws of Chile, Costa Rica, El Salvador, Peru, Uruguay, and any other jurisdiction addressed in Annexes D through F.

(d) Relationship to other legal bases. The Global Data Processing Authorization supplements, and does not replace, the other legal bases described in Section 1.5. Where Applicable Data Protection Law, including the GDPR, the UK GDPR, the Swiss Federal Act on Data Protection, and the Lei Geral de Proteção de Dados Pessoais, does not treat consent as freely given in the circumstances, or where another basis applies, Remote Leverage relies on

contract, legal obligation, or legitimate interests, and the Global Data Processing Authorization operates as the data subject's acknowledgment of the notice in this Privacy Agreement.

(e) Withdrawal. The data subject may withdraw the Global Data Processing Authorization at any time, free of charge, by writing to privacy@remoteleverage.com or through any request functionality on Leve, and withdrawal is as easy as giving it. Withdrawal takes effect for the future and does not affect Processing carried out before it, Processing that rests on another legal basis, or retention that law requires or that is needed for the establishment, exercise, or defence of legal claims. Because the Processing it covers is necessary to provide the Services, withdrawal may prevent Remote Leverage from continuing to provide them, and Section 12 (Suspension) applies.

(f) Other authorizations given through the same box. The biometric consent and written release (Section 0.4A(c)), the Monitoring Authorization and Personal-Device Consent (Sections 0.4A(d) and 0.4A(e)), the Messaging Acknowledgment (Section 0.4A(f)), consent to Promotional Messages (Section 0.4A(g)), and consent to marketing email (Section 0.4A(h)) are distinct from the Global Data Processing Authorization, and each is given through the same acceptance box on its own terms in Section 0.4A. The Marketplace Display and Likeness Authorization (Section 0.4A(i)) is likewise distinct from the Global Data Processing Authorization and is given on its own terms in Section 0.4A.

0.5 Governing law and dispute resolution

This Privacy Agreement, and every dispute between Remote Leverage and a User arising out of or relating to it, are governed by the laws of the State of Florida, United States, without regard to conflict-of-laws rules, consistently with Terms Section 31.1, and are resolved exclusively under Terms Section 30, including its informal resolution and mediation steps, binding individual arbitration administered by the American Arbitration Association and seated in Miami-Dade County, Florida, under the Federal Arbitration Act, its class and collective action waiver, its jury trial waiver, and its court carve-outs, which apply to those disputes in accordance with their terms and are not duplicated here. Where a User has signed the COR MSA and it contains its own governing law, forum, or arbitration terms, those terms govern disputes relating to the COR MSA, as Terms Section 30.10 provides. The following exceptions apply because the law requires them, and the Terms and this Section are read accordingly:

(a) Standard Contractual Clauses and other transfer instruments incorporated under Section 7 are governed by the law, and subject to the forum, that the instrument itself specifies or requires: for the European Union Standard Contractual Clauses, the law of Ireland and the courts of Ireland under Clauses 17 and 18; for the United Kingdom Addendum or International Data Transfer Agreement, the law of England and Wales and the courts that instrument specifies; for the standard contractual clauses of the Brazilian Agência Nacional de Proteção de Dados, Brazilian law; and for any other model clauses, the law and forum they mandate.

(b) Nothing in this Section deprives a data subject of a right that mandatory Applicable Data Protection Law confers to bring a claim in the courts of, or to lodge a complaint with a Supervisory Authority of, the place of the data subject's habitual residence, place of work, or the place of the alleged infringement, or to enforce third-party beneficiary rights under Standard Contractual Clauses.

(c) This Section does not apply to the extent a mandatory law of the data subject's jurisdiction provides otherwise, consistently with Terms Sections 1.9 and 31.4.

0.6 Definitions

In this Privacy Agreement: the words "include," "includes," and "including" mean include, includes, and including without limitation, and an example or enumeration does not limit the general words it follows; the singular includes the plural and the reverse; headings are for convenience only and do not affect interpretation; a reference to a statute, regulation, or instrument includes its implementing rules, amendments, and successors in force from time to time; a reference to a Section or Annex is to a Section or Annex of this Privacy Agreement; and a reference to a "Terms Section" is to a section of the Terms. **Capitalized terms defined in the Terms have the meanings given there.** The terms defined below are terms the Terms do not define, and, as Terms Section 2.1 provides, they also give meaning to any capitalized term used but not defined in the Terms. Within each jurisdictional Annex, a term

that is defined by that jurisdiction's Applicable Data Protection Law has the meaning given by that law for the Processing governed by that Annex; elsewhere, and where a term is not defined by an Applicable Data Protection Law, the definitions in this Section apply. Where a term could bear more than one meaning, it is read in the manner consistent with Applicable Data Protection Law that best preserves the lawful operation of the Services.

Defined terms

Affiliate. Any entity that directly or indirectly controls, is controlled by, or is under common control with Remote Leverage, where control means the ownership of more than fifty percent of the voting interests of an entity or the power to direct or cause the direction of its management, whether through ownership, contract, or otherwise.

Applicable Data Protection Law. The data-protection, privacy, consumer-protection, communications, and related laws and binding regulations that are in force and actually applicable to a specific act of Processing under this Privacy Agreement, together with the binding guidance and decisions of the competent Supervisory Authority, as amended and in force from time to time. A law that does not by its terms apply to a given data subject or act of Processing is not an Applicable Data Protection Law for that Processing.

Client Personal Data. Personal Data that Remote Leverage Processes as a processor or service provider on behalf of a Client under Section 5, including Personal Data described in category L of Section 1.2 and Direct Contractor Personal Data Processed in providing the Self Serve: Direct Pay Services on the Direct Pay Client's Documented Instructions.

Commercial Agreement. The COR MSA, any Service Order, any placement agreement, and any other written agreement signed by Remote Leverage and a Client, in each case as it applies to the relevant Service.

Consent. A freely given, specific, informed, and unambiguous indication of a data subject's agreement, by a statement or clear affirmative action, to the Processing of Personal Data, to the standard Applicable Data Protection Law requires, and, where that law requires, express or explicit consent. Where consent is the basis, it may be withdrawn at any time without affecting the lawfulness of Processing before withdrawal.

Consent Record. The record of a consent or opt-out under the SMS/RCS Program described in Section 6C.5.

Controller. The natural or legal person that, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

COR Engagement. An Engagement under the Managed: Contractor of Record Services.

Data Privacy Framework. The EU-U.S. Data Privacy Framework, the UK Extension to it, and the Swiss-U.S. Data Privacy Framework, administered by the United States Department of Commerce, for so long as they remain in force. A recipient may be relied on under the Data Privacy Framework only while it is certified under it, and this Privacy Agreement does not represent that Remote Leverage is certified.

Data Protection Officer. The individual appointed, where Applicable Data Protection Law requires or where Remote Leverage elects, to oversee compliance with data-protection obligations and to serve as a contact point for data subjects and Supervisory Authorities.

Data Subject. An identified or identifiable individual to whom Personal Data relates. A Data Subject does not include a legal person except where Applicable Data Protection Law expressly extends protection to legal persons.

De-Identified Data. Information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular individual or household, including information that has been de-identified, anonymized, or aggregated to that standard, that Remote Leverage maintains and uses without attempting to re-identify except to test the effectiveness of the de-identification, and does not disclose except subject to a comparable commitment. De-Identified Data is not Personal Data and is not subject to the Personal-Data restrictions of this Privacy Agreement.

Documented Instructions. The Client's instructions to Remote Leverage for the Processing of Client Personal Data where Remote Leverage acts as processor, as set out in and evidenced by this Privacy Agreement, the Terms, Leve and the Client's configuration and settings in its Workspace, the applicable Service Order, and any Commercial Agreement, together with any further written instruction the parties agree.

Informational Message. A Program Message that is not a Promotional Message, such as an appointment reminder, scheduling confirmation, Account, placement, Placement Candidate, or Engagement status update, security or verification code, or customer care message.

Joint Controller. Remote Leverage and a Client acting together to jointly determine the purposes and means of Processing, as contemplated by Article 26 GDPR and equivalent provisions. The parties do not intend to act as Joint Controllers; where a competent Supervisory Authority or court determines that they do, the allocation of responsibilities in Section 5A applies.

Marketplace Display and Likeness Authorization. The authorization described in Section 0.4A(i), given on acceptance under Section 0.4.

Marketplace Profile. The profile of a Placement Candidate displayed in the Talent Marketplace, which may include a Video Introduction, first name, country, role or category, hourly rate range, skills and experience tags, application-status labels, and a link to the Placement Candidate's resume, and which does not include the Placement Candidate's surname, contact details, government identifiers, date of birth, precise location, or identity-verification media.

Marketplace Viewer. A User who has accepted the Terms and this Privacy Agreement through the acceptance box in Section 0.4 and to whom Remote Leverage makes the Talent Marketplace available, including any such User who views, searches, shortlists, or requests an interview with a Placement Candidate through it.

Messaging Acknowledgment. The authorization described in Section 0.4A(f), given on acceptance under Section 0.4.

Monitoring Authorization. The authorization described in Section 0.4A(d), given on acceptance under Section 0.4.

Personal Data or **Personal Information.** Any information relating to an identified or identifiable individual, as defined by Applicable Data Protection Law. Information that has been de-identified, anonymized, or aggregated so that it is not, and cannot by means reasonably likely to be used be, linked to an identified or identifiable individual is not Personal Data.

Personal Data Breach. A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed, that meets the definition and notification threshold of Applicable Data Protection Law. An event that affects only data that has been encrypted, tokenized, de-identified, or anonymized in a manner that renders the Personal Data unintelligible to any person not authorized to access it, where the means of rendering it intelligible has not been compromised, is not a Personal Data Breach requiring notification under Applicable Data Protection Law.

Personal-Device Consent. The consent described in Section 0.4A(e), given on acceptance under Section 0.4.

Processing. Any operation or set of operations performed on Personal Data, whether or not by automated means, including collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure, transmission, combination, restriction, erasure, or destruction.

Processor. A natural or legal person that Processes Personal Data on behalf of and on the Documented Instructions of a Controller. Where Remote Leverage acts as a processor, it is a service provider or contractor to the Client, with the limitations on liability that status confers, to the maximum extent available under Applicable Data Protection Law.

Program Message. A text message delivered by SMS, MMS, or RCS through the SMS/RCS Program.

Promotional Message. A Program Message that includes or introduces an advertisement or constitutes telemarketing or a telephonic sales call under Applicable Data Protection Law, including promotional offers, news, and information about the Services.

Prospect. An individual who submits a form on Leve, books or attends a consultation, contacts Remote Leverage, or joins the SMS/RCS Program, without holding a role under Terms Section 3.1.

Published Page. The page on remoteleverage.com on which Remote Leverage publishes the current version of this Privacy Agreement, currently https://remoteleverage.com/privacy-policy/.

Restricted Transfer. A transfer of Personal Data to a country, territory, or recipient for which Applicable Data Protection Law requires a transfer mechanism, safeguard, authorization, or notice.

Security Incident. An actual or suspected event that may affect the security of Personal Data or the systems that Process it. A Security Incident is not a Personal Data Breach unless and until Remote Leverage, acting reasonably, determines that it meets the definition and notification threshold of Applicable Data Protection Law. Unsuccessful attempts, and events that do not compromise the security, confidentiality, or integrity of Personal Data, including pings and port scans, denied access attempts, and routine security events, are not Personal Data Breaches.

Sensitive Personal Data or **Sensitive Personal Information** or **Special-Category Data.** The categories of Personal Data that Applicable Data Protection Law designates as sensitive or special, which may include, depending on the regime, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data used to identify an individual, data concerning health, data concerning sex life or sexual orientation, precise geolocation, government identifiers, financial-account information, and criminal-record or background-check data.

SMS/RCS Program. The recurring SMS and RCS messaging program that Remote Leverage operates, described in Section 6C.

Standard Contractual Clauses. The standard data-protection clauses adopted or approved by a competent authority for the transfer of Personal Data to a third country, including the European Commission's 2021 clauses (Implementing Decision (EU) 2021/914) and, as supplemented, the United Kingdom Addendum or International Data Transfer Agreement and the adaptations recognized by the Swiss Federal Data Protection and Information Commissioner, the standard contractual clauses adopted by the Brazilian Agência Nacional de Proteção de Dados, and model clauses that a competent authority has adopted or recognized, such as the model clauses of the Ibero-American Data Protection Network and the ASEAN Model Contractual Clauses.

Subprocessor. A Processor engaged by Remote Leverage to Process Client Personal Data in connection with the Services.

Subprocessor Page. The page on remoteleverage.com on which Remote Leverage publishes its current list of Subprocessors and other service providers, linked from the Published Page.

Supervisory Authority. A data-protection, privacy, or other authority competent to enforce Applicable Data Protection Law.

Talent Marketplace. The part of Leve, currently at https://remoteleverage.com/marketplace/, and any successor or embedded version of it, through which Marketplace Profiles are displayed and can be searched, filtered, sorted, shortlisted, and selected for interview, including its artificial-intelligence search function.

Terms. The Leve Platform Terms and Conditions published by Remote Leverage, as amended from time to time, which the Terms themselves call "these Terms."

Tracking Technologies. Cookies, pixels, web beacons, tags, software development kits, local storage, device identifiers, and similar technologies described in Annex H.

Video Introduction. A video or audio recording that a Placement Candidate makes or submits, or that Remote Leverage records with the Placement Candidate's knowledge, to present the Placement Candidate to Clients, including the image, likeness, voice, and statements it contains and any transcript, thumbnail, or still frame generated from it.

Visitor. A User, other than a Marketplace Viewer, who accesses remoteleverage.com or another part of Leve without registering for an Account and without holding a role under Terms Section 3.1.

SECTION 1. GLOBAL BASELINE PRIVACY NOTICE

1.1 Controller identity and contacts

The controller is Remote Leverage, at the address in Section 0.1, contactable at privacy@remoteleverage.com. For a Placement Candidate presented to a Client through the Recruitment Services, the Client is a separate controller for its own use of the Placement Candidate's data from the point of receipt, and the Client's identity is disclosed at or before presentation. For the Managed: Contractor of Record Services, Remote Leverage and the COR Client are independent controllers under Section 5A. For the Self Serve: Direct Pay Services, the Direct Pay Client is the controller of Direct Contractor Personal Data relating to its Engagement and Remote Leverage is its processor, except as described in Section 2.2. For Messages, the roles are set out in Section 6A.9.

1.2 Categories of Personal Data and sources

A. Identity, contact, and status data of Placement Candidates and Contractor Users. Full legal name, prior or preferred names, date and place of birth, gender where volunteered, nationality and residency, national and government identification numbers, tax identification numbers, social security or equivalent numbers, passport, identity-card, driver-licence and similar document images, photograph, signature, home and postal address, personal and professional email addresses, telephone numbers, time zone, and emergency-contact details.

B. Eligibility, verification, know-your-customer, sanctions, and biometric data. Location and residency verification, and, where relevant to an Engagement or placement, work-authorization status, together with the media and results of identity verification. Identity and biometric verification are performed through third-party identity-verification providers (currently Veriff, as listed in Annex G), which compare a government identity document with a live selfie or video, perform liveness checks, and may use facial-recognition technology to create biometric identifiers for that comparison. Identity documents and verification media submitted through the identity-verification flow are processed by the identity-verification provider and are not intended to be retained on Remote Leverage's own systems; Remote Leverage receives the verification result, decision, and related metadata and may receive limited verification media where needed to review, investigate, or support a verification decision. This Privacy Agreement governs any identity and biometric data and results that Remote Leverage receives or controls, and Section 1.9A sets out the retention and destruction schedule. This category also includes results of screening against sanctions lists for Sanctioned Persons, and of politically-exposed-person, fraud-prevention, and, where lawful and separately authorized, background and reference checks. Payment Partners may separately collect identity, beneficial-ownership, and anti-money-laundering data under their own licenses and privacy notices, as Section 6B.2 describes.

C. Professional and assessment data of Placement Candidates and Contractor Users. Curriculum vitae or resume, cover letters, work history, education and qualifications, certifications and licences, skills, competencies, language proficiency and English voice recordings, Video Introductions and the image, likeness, and voice they contain, test and assessment results, work samples and portfolio, interview recordings, notes and scorecards, references and referee statements, and recruiter and matching assessments.

D. Engagement and compliance-document data. The Service and Engagement type, Direct Contracts uploaded to or signed through Leve, each COR Contractor's independent contractor agreement with Remote Leverage, intellectual-property-assignment and confidentiality agreements, scope, Payment Arrangement and rate, working schedule and time zone, Projects, Milestones, submissions, acceptances, and revision requests, start and end

dates, reviews and ratings, Recruitment Services guarantee and replacement records, records of Prohibited Conduct, falsification, and enforcement action under Terms Sections 14.7 and 20, accommodation requests made by Placement Candidates in the recruiting process, and onboarding and Engagement-end records.

E. Contractor User payout, tax, and invoicing data. Payout destination details and Payment Partner account identifiers, tax forms and tax-residency and information-reporting data, invoices and Timesheets, payment instructions and the payout status and history reported by Payment Partners, currency and exchange-rate records, and reimbursement data where an Engagement provides for it.

F. Work-Verification Data and device and security data. As described in Section 6, and only where monitoring has been activated and authorized: Work-Verification Data, including screenshots, applications and URLs used, activity levels, idle time, and approximate location only where enabled and lawful; account, device, and usage data collected by the Monitoring Tool; security, access, and audit logs; and, where Section 6.4 applies, device-management and endpoint-security telemetry.

G. Client corporate and account data. Legal and trading name, entity type and legal form, registration, incorporation, and tax numbers, jurisdiction of formation, industry, size, website and domains, Account credentials and settings, Workspace configuration, and, where required for know-your-customer, know-your-business, anti-money-laundering, or sanctions compliance, beneficial-ownership and control-person information.

H. Authorized User and Account Administrator data. Names, roles and titles, business email and telephone, business address, authorized signatories and Account Administrators, authentication data, permission settings, and communications with us.

I. Client commercial, contractual, and billing data. Service Orders, placement Requests, statements of work, service selections, fee and pricing arrangements, negotiated and discounted terms, placement history, guarantee and refund claims and dispute records, purchase orders, and Account and relationship history.

J. Client financial and payment data. Billing contacts and addresses, funding bank-account and routing details, payment-card data (collected and tokenized by Payment Partners), debit authorizations, value-added-tax and other tax identifiers, credit, chargeback, and collections data, invoices, and payment history.

K. Client business, operational, and confidential information provided to enable the Services. Role and job descriptions, organizational structure and hiring plans, rate bands and budgets, internal processes, standard operating procedures, systems and tools in use, project and workflow details, expectations for Deliverables and service levels, and any business, commercial, or sensitive operational information, trade secrets, or other confidential information the Client transmits to us or makes available through Leve to enable sourcing, placement, or the administration of Engagements. Such information is handled under the confidentiality terms in Section 3 and, where it contains Personal Data, under this Privacy Agreement. This category also includes search requests, prompts, and job descriptions that a Client or other Marketplace Viewer enters or uploads into the Talent Marketplace search function, which are Processed to set search filters and order results and are used to improve tools and models only as Section 11A.6 permits.

L. Client-supplied personnel and third-party data. Personal Data about the Client's own personnel, contractors, or third parties that the Client uploads or instructs us to Process for administration through Leve. For this data, where Remote Leverage acts solely on the Client's Documented Instructions, Remote Leverage is processor under Section 5.

M. Leve usage, device, and Tracking Technology data. Device, browser, operating-system, and hardware identifiers, IP address and approximate location derived from it, log, clickstream, session, and usage data, Tracking Technology identifiers as described in Annex H, referral data, and data collected from Visitors and Prospects through forms and consultation bookings.

N. Data obtained from third parties. From Clients (about Placement Candidates, Contractor Users, and their own personnel), from Placement Candidates and Contractor Users (about references and emergency contacts), from

references and referees, from identity-verification, background-check, sanctions, and fraud-prevention providers, from Payment Partners and financial institutions, from the Monitoring Tool operator, from the electronic-signature provider, from integrations and third-party accounts that a Client connects under Terms Section 23, from public professional and corporate sources and registries, and from our Affiliates and Subprocessors.

O. Data we generate or derive. Account and matching identifiers, automated and artificial-intelligence outputs such as matches, rankings, scores, summaries, and flags under Terms Section 8.2, transcripts, summaries, tags, and match results generated from Video Introductions and from Talent Marketplace searches, fraud and risk signals and scores, analytics and inferences, audit trails, and model inputs and outputs generated in operating and improving the Services, subject to Section 11A.6.

P. Special-category and sensitive Personal Data. Processed only where strictly necessary and on a heightened lawful basis: for example, biometric data used for identity verification, government and tax identifiers, financial-account data, and health information only where a Placement Candidate chooses to provide it to request an accommodation in the recruiting process, and any other category treated as sensitive or special under an applicable regime (which may include, depending on the regime, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic or biometric data, health, sex life or sexual orientation, and criminal-record or background-check data). We do not seek such data except where a lawful and specific basis applies, and Users must not send it through the Messaging Service, as Section 6A.7 provides.

Q. Account, authentication, session data, and Leve Records. Login identifiers, including identifiers received when a User signs in with a Google account, one-time passcodes and their validation records, trusted-device records, session identifiers and timeouts, role and permission assignments, acceptance records under Terms Section 1.4, and the Leve Records described in Terms Section 16.1, including the record of every login, view, click, entry, upload, download, Message, Request, approval, rejection, invoice, payment instruction, signature, acceptance, change, and cancellation, with its date and time, the Account used, and device and IP information.

R. Tax-documentation and information-reporting data. Taxpayer identification numbers, including United States Social Security numbers, individual taxpayer identification numbers, and employer identification numbers (the name the Internal Revenue Service gives to that identifier), and foreign tax identifiers such as the Colombian NIT or RUT, the Mexican RFC or CURP, the Brazilian CPF or CNPJ, and the Argentine CUIT or CUIL; Forms W-9, W-8BEN, W-8BEN-E, and other tax forms, including certifications of foreign status and claims of treaty benefits; information-return data for Forms 1099-NEC, 1099-K, and 1042-S and equivalent local filings; taxpayer-identification-number validation results; and backup-withholding records.

S. Contract, electronic-signature, and document data. Each COR Contractor's independent contractor agreement with Remote Leverage, Direct Contracts, offers made through Leve under Terms Section 13.2, statements of work, confidentiality and intellectual-property-assignment agreements, Templates as completed by Users, and other documents executed through Leve, together with the electronic-signature audit trail, including signer names, email addresses, IP addresses, timestamps, and signature images.

T. Payment-instruction, payout, and billing-execution data. Payout account and routing numbers, IBAN and SWIFT or BIC codes, Payment Partner account identifiers and payout destination details, payment instructions and their approvals, payout amounts, status, and history reported by Payment Partners, Payment Arrangements and rates, currency and exchange-rate records, Client bank-account data used for debits (tokenized by the Payment Partner that executes the debit), invoice line items, and records of disputes, chargebacks, refunds, guarantee and replacement claims, and collections. Payment-card data is collected and processed by the Payment Partner and is not stored by Remote Leverage.

U. Time-tracking, Timesheet, and scheduling data. Hours recorded through the Monitoring Tool where activated, entered manually, or established in any other way the Approving Party accepts, and reconciled into Timesheets; Timesheet data read from spreadsheets, including names, hourly rates, and hours recorded; and calendar invitations, attendee email addresses, and scheduling details for onboarding events, interviews, and consultations.

V. Messaging Service, support, and communications data. The content of Messages and their attachments, including chat, channel, comment, and call content; call and meeting recordings made after notice; Message metadata, including senders, recipients, Workspace and channel identifiers, timestamps, read, delivery, and status indicators, edits, and deletions; support tickets and their attachments; tool-access requests and the tools requested; the content of transactional emails sent to Users (which may include offer details such as role, rate, Payment Arrangement, currency, and start date, and attachments); and internal announcements of new Engagements and placements (name, role, Client name, and start date), all as described in Section 6A.

W. Technical, analytics, security, and diagnostic data. Product-usage analytics events, such as page views, interface interactions, and session and device metadata, which may incidentally capture text displayed on screen; application error reports, stack traces, and diagnostic logs, which may contain email addresses; masked session recordings associated with errors; IP addresses and request headers used for bot detection and rate limiting; and email-deliverability and validity results used to block invalid or disposable addresses.

X. Business-relationship and commission data. Deal, job, and placement records and commission data, including the names and roles of recruiters, salespersons, and referral partners credited with a placement, and placement status and Engagement-end flags.

Y. Reviews, ratings, and profile display data. Reviews and ratings that Users give or receive under Terms Section 21.3, and the profile, credential, and assessment information of Placement Candidates and Contractor Users that Remote Leverage displays to prospective Clients under Terms Section 21.1. This category includes Marketplace Profiles and Video Introductions displayed to Marketplace Viewers in the Talent Marketplace under Section 1.9B.

Z. SMS/RCS Program data. Mobile telephone number, carrier and device-capability data needed to deliver SMS or RCS messages, the Consent Record described in Section 6C.5, the content and metadata of Program Messages sent and received, HELP and opt-out requests, and opt-out status, as described in Section 6C.

AA. Talent Marketplace viewer data. Shortlists, saved Placement Candidates, search history, interview requests, the name, work email, telephone number, company, and website that a Marketplace Viewer submits to request interviews, and records of which Marketplace Profiles and Video Introductions a Marketplace Viewer accessed, Processed to operate the Talent Marketplace, follow up on interview requests, enforce Section 1.9B(e), and secure the Talent Marketplace.

1.3 Purposes of Processing

We Process Personal Data to: create, operate, secure, and maintain Leve and Accounts; source, screen, assess, verify, match, and present Placement Candidates, and facilitate placements, including guarantees and replacements; provide the Managed: Contractor of Record Services, including onboarding, contracting, compliance documentation, identity and biometric verification, Timesheet reconciliation, invoicing, payment instructions for payouts executed by Payment Partners, tax documentation and information reporting, and contractor administration; provide the Self Serve: Direct Pay Services on the Direct Pay Client's instructions; operate the Messaging Service and support Client access to Messages as described in Section 6A; administer monitoring and work verification where activated and authorized, and secure devices, as described in Section 6; collect and transmit payment instructions and payment data to Payment Partners and manage billing, collections, and financial administration; verify identity, screen for Sanctioned Persons, and prevent, detect, and investigate fraud, falsification, abuse, and Security Incidents; meet tax information-reporting, sanctions, recordkeeping, and other legal obligations, and support the know-your-customer and anti-money-laundering obligations that Payment Partners carry out under their licenses; communicate with Users, Visitors, and Prospects, provide support, and operate the SMS/RCS Program as described in Section 6C; create and maintain Leve Records and acceptance records; display profiles and reviews; operate the Talent Marketplace, including displaying Marketplace Profiles and Video Introductions to Marketplace Viewers and Processing their search requests, as Section 1.9B describes; conduct analytics and maintain, improve, develop, secure, and troubleshoot the Services and, subject to Sections 1.4 and 11A.6, build and improve tools and models; operate Tracking Technologies as described in Annex H; manage disputes and enforce the Terms and other agreements and legal rights, including guarantee, replacement,

refund, chargeback, and collection matters, and establish, exercise, or defend legal claims; and carry out corporate transactions.

1.4 Secondary use, analytics, and service and model improvement

We may Process Personal Data that we control to analyze, maintain, improve, develop, secure, and troubleshoot the Services, and to build, evaluate, and improve tools and models used for sourcing, matching, vetting, fraud detection, and Service operation, subject to the limits in Section 11A.6. Where a regime requires a specific lawful basis, an opt-out, or an opt-in for a particular secondary use (for example use for targeted advertising, any activity constituting a sale or sharing under United States state law, certain profiling, or use of Personal Data to train models), we honor that requirement as set out in the relevant Annex, and we apply de-identification, pseudonymization, or aggregation where feasible. We use Client Personal Data only as Section 5 permits a processor or service provider to use it. We do not sell Personal Data for monetary consideration, and we do not sell, rent, or share mobile telephone numbers or text-messaging consent with third parties or Affiliates for their marketing purposes.

1.5 Legal bases

The controlling basis for a data subject is the one that subject's regime provides, applied per purpose:

- Performance of a contract, or steps taken at the data subject's request before contracting: registration and Accounts, presentation of Placement Candidates, administration of placements, the Managed: Contractor of Record Services, the Self Serve: Direct Pay Services, transmission of payment instructions, the Messaging Service, and support.
- Compliance with a legal obligation: tax information reporting, including by Remote Leverage where it is the payer under the Managed: Contractor of Record Services, sanctions screening, recordkeeping, responses to lawful requests, and the support Remote Leverage gives to the know-your-customer and anti-money-laundering obligations that Payment Partners carry out under their own licenses.
- Legitimate interests, or the local authorized-purpose or equivalent basis, balanced against the data subject's rights: securing and improving the Services, fraud and falsification prevention, proportionate monitoring and work verification under Section 6, operation and moderation of the Messaging Service and Client access to Messages under Section 6A, Leve Records, analytics, enforcement of agreements, the establishment, exercise, or defence of legal claims, Informational Messages, and corporate transactions. The balancing assessment is available on request.
- Consent, or a specific authorization, only where a regime requires it and only for the Processing that requires it: non-essential Tracking Technologies, Promotional Messages and direct marketing where required, sensitive-data Processing where consent is the applicable basis, Personal-Device Consent, biometric Processing, and the authorizations that authorization-based regimes require under Section 0.4A(b). Where consent is the basis, it may be withdrawn at any time without affecting prior lawful Processing, and withdrawal is as easy as giving. Consent given for the purposes of communications-interception and recording laws, as Section 6A.5 describes, is distinct from the data-protection legal basis.

1.6 Recipients and categories of recipients

Personal Data is disclosed to: Clients, according to the Service (for Placement Candidate presentation, controller to controller; for the Managed: Contractor of Record Services, as independent controller under Section 5A; for the Self Serve: Direct Pay Services, as controller; and for Messages and Work-Verification Data, as described in Sections 6.9 and 6A.2); other participants in conversations on the Messaging Service; Payment Partners, which act as independent controllers for their own know-your-customer, anti-money-laundering, sanctions, fraud, and regulatory recordkeeping obligations and, for the execution of debits, conversions, and payouts on payment instructions transmitted through Leve, as processors or service providers to the extent their role and Applicable Data Protection Law so characterize it, with their own privacy notices governing their independent Processing; the Monitoring Tool operator; our Affiliates; Subprocessors and service providers acting on our instructions (hosting

and cloud infrastructure, identity and biometric verification, background checks where authorized, electronic signature and document management, form collection, applicant tracking, accounting, customer support, email delivery, SMS and RCS delivery, communications, analytics, error monitoring, bot protection, and device-management vendors); third-party services and integrations that a Client connects under Terms Section 23, at the Client's direction; professional advisers, auditors, insurers, collection agencies, and legal counsel; card networks and financial institutions; acquirers or successors in a corporate transaction; and authorities, courts, arbitral bodies, and other parties where legally required or permitted. Reviews and profile information are displayed to prospective Clients as Terms Section 21.1 describes. Current Subprocessors and other service providers are listed in Annex G and on the Subprocessor Page. Marketplace Profiles, including Video Introductions, are made available to Marketplace Viewers only as Section 1.9B describes.

1.7 International transfers

We operate globally and transfer Personal Data across borders, including to the United States, where our principal operations and certain Subprocessors are located. Personal Data of Placement Candidates and Contractor Users originating in the markets from which we source, across the Americas and elsewhere, is transferred to Clients and to infrastructure that may be located in the United States and other countries. Transfer mechanisms are set out in Section 7.

1.8 Retention

We retain Personal Data only as long as necessary for the purposes in this Section or as required by law, then delete, block, or de-identify it. The category-level schedule below is Remote Leverage's retention schedule for Leve Records and other Personal Data and is available to authorities on request. Where a regime requires a blocking step before deletion, we apply it.

Retention by category. The following periods or criteria apply unless a longer period is required by law, by a legal hold, or for the establishment, exercise, or defence of legal claims, or a shorter period is required by Applicable Data Protection Law:

- Data of Placement Candidates (categories A to C): 24 months after the last interaction or, for a placed Placement Candidate, after the end of the replacement guarantee period in the Client's Service Order, whichever is later, to support re-matching and guarantees, unless the Placement Candidate asks for earlier deletion or a shorter local limit applies.
- Engagement, contract, and electronic-signature records (categories D and S): the duration of the Engagement or placement relationship and seven years after it ends.
- Tax-documentation, information-reporting, payment-instruction, payout, and billing records (categories E, J, R, and T): for the period tax law requires, generally seven years after the end of the calendar year to which they relate, and longer where a tax authority's assessment period remains open, a local equivalent requires it, or a legal hold applies.
- Identity-verification results and know-your-customer and sanctions-screening records (category B): the duration of the relationship and seven years after it ends; biometric data is retained only as set out in Section 1.9A.
- Client Account, commercial, billing, and confidential data (categories G to K): the duration of the relationship and seven years after it ends.
- Account, authentication, session data, acceptance records, and other Leve Records (category Q): the life of the Account and thereafter for as long as needed for security, fraud prevention, and evidence of the actions recorded, generally not exceeding seven years after the Account is closed.
- Work-Verification Data and device-management data (category F) and Monitoring Tool time data (category U): the limited period necessary for the purposes in Section 6.1, generally not exceeding 12 months after collection, except that Timesheets and time records used for invoicing or payment are kept with the related billing records and data relevant to a Security Incident or dispute is kept until it is resolved.
- Messages, attachments, call recordings, and their metadata (category V): as set out in Section 6A.8.

- Technical, analytics, security, and diagnostic data (category W): the period configured for the relevant tool, generally not exceeding 24 months, except that security logs relevant to a Security Incident are kept until the incident and any resulting claim are resolved.
- Reviews and profile display data (category Y): while the relevant profile or Account is active, and thereafter under the Leve Records period where relevant to a dispute.
- Video Introductions, Marketplace Profiles, and the transcripts, thumbnails, and still frames generated from them: while the Marketplace Profile is active and, for a Placement Candidate who is not placed or engaged, no longer than 24 months after the Placement Candidate's last interaction, or until removal under Section 1.9B(f), whichever is earlier, except where retention is needed for a pending dispute or a legal obligation.
- SMS/RCS Program data and Consent Records (category Z): Consent Records and opt-out records for at least five years after the later of the last Program Message sent to the number and the opt-out; Program Message content for up to 24 months unless relevant to a dispute.
- Tracking Technology data (category M): the periods stated in Annex H and the preference center.
- Data that a Client may export at the end of its use of a Service: available for export for thirty (30) days, as Terms Sections 11.16 and 28.3 provide, after which Remote Leverage may delete it subject to the periods in this Section.

1.9 Sensitive, special-category, and children’s data

We minimize sensitive and special-category Processing and Process it only on a heightened lawful basis. Biometric data used for identity verification is Processed only where permitted, on the applicable heightened basis, and subject to stricter jurisdictional biometric laws where they apply. Leve is intended for adults and business use only, as Terms Section 1.5 provides. Users must be at least 18 years of age and have reached the age of majority where they live to register for or use Leve, and participants in the SMS/RCS Program must be at least 18 years of age. We do not knowingly collect Personal Data from anyone under 18 through Leve. If we learn that we have collected such Personal Data, we delete it, subject to any legal retention obligation.

1.9A Biometric identity verification and retention schedule

Where identity verification uses facial-recognition technology, the identity-verification provider listed in Annex G captures a selfie or video and an image of a government identity document and may create biometric identifiers or biometric information, such as a scan of face geometry, solely to verify that the individual is the person shown in the document, to perform liveness checks, and to prevent fraud and duplicate or impersonated Accounts. Remote Leverage and its provider: (a) inform the individual in writing, before collection, that biometric identifiers or biometric information are being collected or stored, and of the specific purpose and length of term for which they are collected, stored, and used; (b) obtain the individual’s explicit consent and written release, which may be given by electronic signature, through the authorization in Section 0.4A(c), given by checking the acceptance box in Section 0.4 after the written notice in this Section; (c) do not sell, lease, trade, or otherwise profit from biometric identifiers or biometric information; (d) do not disclose them except to the provider and its subprocessors performing the verification, with the individual’s consent, to complete a financial transaction the individual requested or authorized, or as required by law or by a valid warrant or subpoena; and (e) store, transmit, and protect them using the reasonable standard of care within Remote Leverage’s industry and in a manner at least as protective as that used for other confidential and sensitive information.

Retention and destruction schedule. Biometric identifiers and biometric information are permanently destroyed when the initial purpose for collecting or obtaining them has been satisfied, being the completion of the verification and of any review, re-verification, or fraud investigation to which it gives rise, and in any event no later than 24 months after the individual’s last interaction with Remote Leverage, or any shorter period that Applicable Data Protection Law requires, unless a valid warrant or subpoena requires otherwise. This schedule applies to biometric data that Remote Leverage holds and to biometric data that its identity-verification provider processes on Remote Leverage’s behalf. Verification results that contain no biometric identifier or biometric information, such as a pass or fail decision and its date, are retained under Section 1.8.

1.9B Video Introductions and the Talent Marketplace

(a) Purpose and content. Remote Leverage operates the Talent Marketplace to present Placement Candidates to prospective Clients and to let Marketplace Viewers search for, shortlist, and request interviews with them. A Marketplace Profile contains only the elements listed in the definition of Marketplace Profile. Remote Leverage does not display a Placement Candidate's surname, contact details, government identifiers, date of birth, precise location, or identity-verification media in the Talent Marketplace.

(b) Condition of participation. Appearing in the Talent Marketplace requires a Video Introduction and the authorization in Section 0.4A(i), which takes effect when the Placement Candidate records or submits a Video Introduction after seeing the notice in paragraph (c). Leve provides a setting through which the Placement Candidate may hide or remove the Marketplace Profile at any time. A Placement Candidate who does not record a Video Introduction, or who withdraws the authorization, does not appear in the Talent Marketplace, and Remote Leverage may decline to present that Placement Candidate through the Recruitment Services.

(c) Notice before recording and access controls. Before a Video Introduction is recorded or submitted, Leve shows the Placement Candidate a short notice, in English and, where Annex E requires it, in Spanish or Portuguese, that the recording will be displayed in the Talent Marketplace, identifies the categories of Marketplace Viewers who can see it, describes the automated Processing permitted by paragraph (d), and links to this Section. Remote Leverage makes Marketplace Profiles available only to Marketplace Viewers, who must accept the Terms and this Privacy Agreement by checking the acceptance box in Section 0.4 before accessing the Talent Marketplace, without any need to register for an Account, uses technical measures designed to restrict access to those persons, including access controls, expiring signed links for video files, and instructions to search engines not to index Talent Marketplace pages, and does not publish Marketplace Profiles on social media or in advertising without the Placement Candidate's separate consent. This access control also meets the principle of restricted access and circulation in Article 4(f) of Ley Estatutaria 1581 de 2012 of Colombia and similar laws.

(d) Automated Processing; no biometric Processing. Remote Leverage may use automated tools, including artificial intelligence, to transcribe, translate, and summarize the spoken content of a Video Introduction, to assess English-language proficiency from that content, to generate tags and thumbnails, and to match Marketplace Profiles to a Marketplace Viewer's search request, as Sections 1.11 and 11A.1 describe. Remote Leverage does not use Video Introductions, and does not permit its Subprocessors to use them, to: (i) create, collect, or store a biometric identifier or biometric information, including a scan of face geometry or a voiceprint, or to identify or verify any individual from his or her face or voice; (ii) recognize or infer emotions, personality traits, honesty, or similar characteristics; or (iii) infer or estimate race, ethnicity, sex, age, health, disability, or any other characteristic protected by applicable anti-discrimination law. Biometric Processing remains limited to identity verification under Section 1.9A.

(e) Restrictions on Marketplace Viewers. Each Marketplace Viewer will use Marketplace Profiles and Video Introductions only to evaluate Placement Candidates for a placement or Engagement through Remote Leverage, and will not: (i) download, record, screen-capture, copy, scrape, or store a Video Introduction outside Leve; (ii) publish, post, or share a Marketplace Profile or Video Introduction with any person other than its Authorized Users who are involved in the hiring decision; (iii) subject a Video Introduction to facial recognition, voice recognition, emotion analysis, or any other biometric or artificial-intelligence analysis, or use it to train or improve any model; (iv) use the appearance, apparent age, sex, race, ethnicity, disability, or any other protected characteristic of a Placement Candidate shown in a Video Introduction as a basis for selection; or (v) use a Marketplace Profile to contact or engage a Placement Candidate outside Leve in breach of the Terms or any Commercial Agreement. A Client that has saved or retained Marketplace Profile data deletes it when Remote Leverage so instructs under paragraph (f).

(f) Removal and withdrawal. A Placement Candidate may hide or delete a Marketplace Profile or Video Introduction at any time through Leve or by writing to privacy@remoteleverage.com, and may withdraw the authorization in Section 0.4A(i) in the same way. Remote Leverage removes the Marketplace Profile from the Talent Marketplace within fifteen (15) business days after the request, deletes the Video Introduction and the transcripts,

thumbnails, and still frames generated from it within thirty (30) days after the request unless retention is required under Section 1.8 for a pending dispute or a legal obligation, and instructs any Client that has shortlisted, saved, or received the Video Introduction to delete it. Removal does not undo a presentation already made to a Client and does not affect the Client's obligations as an independent controller under Section 3.3.

(g) Placement Candidate responsibilities. A Placement Candidate who submits a Video Introduction confirms that it shows only himself or herself, that it does not show or name any other person without that person's permission, and that it does not disclose confidential information of a current or former client or employer, Sensitive Personal Data, or Regulated Data. A Placement Candidate may re-record a Video Introduction at any time.

(h) Tracking Technologies on Talent Marketplace pages. Remote Leverage configures Tracking Technologies on Talent Marketplace pages so that they do not transmit to any advertising or social-media provider a Placement Candidate's name, profile identifier, or video identifier, or information identifying a Marketplace Viewer as having requested or viewed a specific Video Introduction, and limits advertising Tracking Technologies on those pages to page-level events, subject to the consent and opt-out mechanisms in Annex H.

(i) Video-interview laws. Where a Video Introduction, or any other recorded video interview, is used to consider a Placement Candidate for a position based in Illinois and is analyzed by artificial intelligence, Remote Leverage, for the analysis it performs, and the Client, for any analysis it performs or directs, gives the notice and explanation and obtains the consent that the Illinois Artificial Intelligence Video Interview Act, 820 ILCS 42, requires before the video is recorded, shares the video only with persons whose expertise or technology is necessary to evaluate the Placement Candidate, and, within thirty (30) days after the Placement Candidate's request, deletes the video and instructs every other person who received a copy to delete it. Remote Leverage does not use facial-recognition technology during interviews, and a Client that does so for a position based in Maryland first obtains the signed waiver that Section 3-717 of the Labor and Employment Article of the Annotated Code of Maryland requires.

(j) No sale or licensing. Remote Leverage does not sell, rent, or license Video Introductions or Marketplace Profiles to third parties, and discloses them only to Marketplace Viewers at the Placement Candidate's direction given under Section 0.4A(i).

1.10 Cookies and similar technologies

Leve uses Tracking Technologies for strictly necessary operation, security, preferences, analytics, and, where applicable, advertising. Annex H is Remote Leverage’s Cookie and Tracking Technologies Notice. It explains the categories and purposes of Tracking Technologies, the difference between first-party and third-party technologies, typical durations, how to manage preferences through the cookie banner, preference center, browser, and device settings, prior consent for non-essential Tracking Technologies where the law requires it, the opt-out of sale, sharing, and targeted advertising under United States state law, how Remote Leverage honors Global Privacy Control and other universal opt-out signals, session replay and chat disclosures, and how Do Not Track signals are handled.

1.11 Automated decision-making and profiling

We use automated tools to help source, match, score, and vet Placement Candidates and to detect fraud and falsification. Automated and artificial-intelligence outputs are aids to human decisions, as Terms Section 8.2 states. Where a decision producing legal or similarly significant effects is based solely on automated Processing, we provide, to the extent a regime requires, meaningful information about the logic and the significance and consequences, human review, and the ability to contest. Our governance of artificial intelligence and automated tools is set out in Section 11A. In the Talent Marketplace, an artificial-intelligence function converts a Marketplace Viewer's search request into filters and orders Marketplace Profiles by relevance (for example, a "Best match" ordering), using role, skills, experience, language proficiency, country of residence, and rate range, and not any characteristic protected by applicable anti-discrimination law. The order in which Marketplace Profiles appear is not a decision about any Placement Candidate, every Marketplace Profile remains available through filters and other orderings, and a Placement Candidate may ask privacy@remoteleverage.com for the main factors that determine ordering.

1.12 Your rights

Subject to your regime, you may request access, rectification, erasure or cancellation, restriction, objection, portability, and withdrawal of consent, and, under United States state law, opt-out of sale or sharing and of targeted advertising and limits on sensitive-data use, and, where applicable, rights regarding automated decisions. Exercise a right at privacy@remoteleverage.com or through any request functionality made available on Leve. Changes to profile, Account, payout, tax, entity, or contact information that you submit through Leve are processed under Terms Section 7.6; that processing period does not extend the period within which Applicable Data Protection Law requires us to respond to a request for rectification. We verify requests, respond within the timeline your regime requires, and do not discriminate against you for exercising a right. Mechanics, including the channel for each role, are in Section 8; regime-specific catalogues and timelines are in the Annexes.

1.13 Complaints

Contact us at privacy@remoteleverage.com. You may lodge a complaint with your competent Supervisory Authority, identified in the Annexes.

1.14 Effective date and changes

The version and effective date of this Privacy Agreement are stated on its cover page. This version applies to a User from the date of its acceptance under Section 0.4 or, for an existing User, from the effective date stated in the Notice of update, and to Visitors and Prospects from its publication on the Published Page. Changes apply prospectively, and a material change that would permit a materially different use of Personal Data already collected is made only with any consent that Applicable Data Protection Law requires. For material changes we give Notice by email to the Notice Email or through the Leve dashboard, and, for a material change that is adverse to Users, at least fifteen (15) days before it takes effect, consistently with Terms Section 29, except where law, a regulator, a Payment Partner requirement, or a security need requires the change to take effect sooner; where a regime requires, we obtain renewed consent or authorization. Where practicable, Users are asked to accept a materially updated version through the acceptance mechanism in Section 0.4. Continued use after an update's effective date constitutes acceptance, except where renewed consent or authorization is legally required. Prior versions are available on request to privacy@remoteleverage.com.

SECTION 2. PLACEMENT CANDIDATE AND CONTRACTOR USER TERMS

2.1 Data map for Placement Candidates and Contractor Users

The categories, sources, purposes, bases, recipients, transfers, and retention in Section 1 apply across the lifecycle of Placement Candidates and Contractor Users: application and screening; presentation to Clients; engagement by a Client after placement, a COR Engagement, or a Direct Pay Client's engagement of a Direct Contractor under a Direct Contract; onboarding, identity verification, contracting, Timesheets, invoicing, payment instructions and payouts executed by Payment Partners, and tax documentation; monitoring and work verification under Section 6 where activated and authorized; communications through the Messaging Service under Section 6A; reviews, guarantee, and replacement administration; and the end of the Engagement or placement relationship.

2.2 Role determination for Placement Candidate and Contractor User data

- Sourcing, screening, and presentation (Recruitment Services): Remote Leverage is an independent controller; presentation to a Client is a controller-to-controller disclosure, and the Client becomes an independent controller from receipt.
- Managed: Contractor of Record Services: Remote Leverage and the COR Client are independent controllers under Section 5A, each for the Processing it performs for its own purposes, including, for Remote Leverage, its obligations as contracting party with the COR Contractor, Paying Party, and information-reporting party where it is the payer; and for discrete Processing performed solely on the COR Client's Documented Instructions, Remote Leverage is processor under Section 5.

- Self Serve: Direct Pay Services: the Direct Pay Client is the controller of Direct Contractor Personal Data Processed for its Engagement of the Direct Contractor, and Remote Leverage is its processor or service provider under Section 5 for the administration it performs on the Client's instructions. Remote Leverage is an independent controller only for Processing for its own purposes, namely Account creation and administration with the Direct Contractor as a User, account security and access control, fraud and falsification prevention, identity verification and sanctions screening, payment-instruction compliance and its payee-side role under Terms Section 11.4, tax information reporting where law places a duty directly on Remote Leverage, Leve Records, enforcement of the Terms and other agreements, including the restrictions on off-Leve payments and circumvention, administration of chargeback and payment disputes, the establishment, exercise, or defence of legal claims, and the operation, security, and improvement of Leve.
- Messages and Work-Verification Data: the roles in Sections 6.9 and 6A.9 apply.

2.3 Lawful basis for core Processing of Placement Candidate and Contractor User data

Core Processing of Placement Candidate and Contractor User data rests on contractual necessity, legal obligation, and legitimate interests, except where Applicable Data Protection Law requires authorization or consent, in which case it is obtained through the acceptance mechanism in Section 0.4 and the authorizations in Section 0.4A. Outside those cases, we do not use consent as the basis for this Processing. Optional and separable Processing (for example marketing, Promotional Messages, or non-essential data sharing) is handled on consent where required and can be withdrawn without affecting the Engagement.

2.4 Rights and channels for Placement Candidates and Contractor Users

Placement Candidates and Contractor Users exercise the rights in Section 1.12 through the channels in Section 8. Where a jurisdiction confers a specific rights catalogue or requires local-language notice, that content is provided in the relevant Annex and, where required, the authorizations in Section 0.4A.

SECTION 3. CLIENT TERMS

3.1 Client and Authorized User data

We Process Client corporate, Authorized User, Account Administrator, commercial, billing, financial, and operational data (categories G to K of Section 1.2) as controller, on the bases of contract, legal obligation, and legitimate interests, and, where required for compliance screening, legal obligation.

3.2 Client business and confidential information

Business, commercial, and sensitive operational information a Client provides to enable the Services (category K) is used only to provide, secure, support, and improve the Services and to meet legal obligations, is disclosed only to recipients under Section 1.6 on a need-to-know basis, and is protected by confidentiality obligations, including those in Terms Section 22. Where such information contains Personal Data, this Privacy Agreement applies; where it is the Client's confidential or trade-secret information, the confidentiality terms of any Commercial Agreement also apply; where they conflict with this Section, the Commercial Agreement governs, and its limitations and exclusions of liability apply.

3.3 Client roles

Under the Recruitment Services, when a Client receives Placement Candidate data from us it becomes an independent controller and is responsible for its own compliance from receipt, as Terms Section 13.2 provides. Under the Managed: Contractor of Record Services, the COR Client and Remote Leverage are independent controllers under Section 5A. Under the Self Serve: Direct Pay Services, the Direct Pay Client is the controller of Direct Contractor Personal Data relating to its Engagement and Remote Leverage acts as processor under Section 5, except as described in Section 2.2. For Messages and Work-Verification Data that a Client accesses, exports, or

retains, the Client is an independent controller as described in Sections 6.9 and 6A.9. Where the Client uploads its own personnel or third-party data for administration, Remote Leverage acts as processor under Section 5.

3.4 Client warranties

The Client warrants that it will Process Placement Candidate, Contractor User, and personnel data lawfully; that it has provided any notices and obtained any authorizations its own Processing requires; that data it uploads about its personnel or third parties may lawfully be Processed by us for the instructed purposes; and that it will not use the data to circumvent the Recruitment Services or Leve in breach of the Terms or any Commercial Agreement.

Further Client obligations. The Client also warrants and undertakes that: (a) its instructions to Remote Leverage, its configuration of its Workspace, and any monitoring or time-tracking settings it selects comply with Applicable Data Protection Law and the law governing the engagement, and are used only to manage its Engagements and verify work and never to control the manner and means of a Contractor User's work, as Terms Sections 11.13 and 14.6 provide; (b) it has the right to provide, and has given the notices and obtained the authorizations required for, all Personal Data it uploads, enters, or makes available through Leve, including data about its personnel, references, and other third parties; (c) it is responsible for any onward transfer, integration, or export of Placement Candidate or Contractor User Personal Data that it initiates or directs, including through Third-Party Integrations under Section 3.5(b) and exports of Messages under Section 6A.2; (d) it will Process Placement Candidate and Contractor User Personal Data received through Leve only for the placement, Engagement, or administration for which it was provided, and Messages only for the purposes Terms Section 15.3 permits; (e) it will not give Placement Candidates or Contractor Users who are covered persons under 28 C.F.R. Part 202, including those primarily resident in a country of concern, access to government-related data or bulk United States sensitive personal data except in compliance with that Section; and (f) it will not send Sensitive Personal Data or Regulated Data through Leve except through the secure upload channels designated for it, and will not direct a Contractor User to do so, as Terms Section 11.13 provides.

Client indemnity. To the extent permitted by law, the Client will defend, indemnify, and hold harmless the Remote Leverage Parties from and against all claims, regulatory proceedings, fines and penalties (to the extent indemnifiable by law), losses, damages, and reasonable costs and attorneys' fees arising out of: (i) the Client's breach of this Privacy Agreement or of Applicable Data Protection Law; (ii) Processing that Remote Leverage performs in accordance with the Client's instructions; (iii) Personal Data the Client uploads or makes available through Leve; (iv) monitoring, time-tracking, or work-verification settings that the Client activates or selects; (v) the Client's onward transfers, Third-Party Integrations, exports of Messages or Work-Verification Data, or misuse of Placement Candidate or Contractor User Personal Data; and (vi) the Client's failure to give a notice or obtain an authorization for which it is responsible. This indemnity is in addition to Terms Sections 11.14 and 27, is subject to the procedures of Terms Section 27.2 and of any Commercial Agreement, and does not expand the allocation of classification risk in the COR MSA.

Talent Marketplace. The Client's warranties in this Section extend to its Authorized Users' use of the Talent Marketplace, and the Client indemnity in this Section also applies to claims, regulatory proceedings, losses, and costs arising out of a breach of Section 1.9B(e) by the Client or its Authorized Users.

3.5 Third-Party Processors and Integrations

(a) **Contractor Users and hired Placement Candidates.** Placement Candidates hired by a Client through the Recruitment Services and Direct Contractors engaged under the Self Serve: Direct Pay Services who access or Process Client Personal Data in performing services for the Client do so as the Client's own processors or personnel, receiving instructions directly from the Client, and are not Remote Leverage Subprocessors. The same applies to a COR Contractor's Processing of Client Personal Data under the Client's day-to-day direction, to the extent the COR MSA permits that direction. The Client is solely responsible for entering into separate contractual arrangements requiring them to comply with Applicable Data Protection Law with respect to any Personal Data they access or Process in performing that work.

(b) **Third-Party Integrations.** Where a Client connects a third-party account or integration, the Client appoints

Remote Leverage as its limited agent to access that account, store the credentials, and import and export data as needed to operate the connection, as Terms Section 23 provides. Remote Leverage may, at the Client's request or direction, transfer Client Personal Data to such third-party platforms and services (including accounting software, tax-filing services, and other integrations). Such third parties are not Remote Leverage Subprocessors. Remote Leverage stores integration credentials in encrypted form, uses them only to operate the connection the Client has enabled, and stops using them when the Client disconnects the integration or its Account ends. The Client is solely responsible for entering into separate contractual arrangements with such third parties requiring them to comply with Applicable Data Protection Law and to process Client Personal Data only on the Client's documented instructions. Remote Leverage is not a party to such arrangements and is not liable for the acts or omissions of such third parties.

SECTION 4. DATA USE, LICENSE, AND CONTROL

4.1 Operational rights

To the fullest extent permitted by applicable law, each User grants Remote Leverage a worldwide, non-exclusive, royalty-free right to host, store, reproduce, adapt, combine, analyze, and otherwise Process Personal Data and other data the User provides or generates, for the purposes in Sections 1.3 and 1.4, including operating and securing the Services, administering placements and Engagements, provisioning and securing devices, administering monitoring and work verification under Section 6 where activated and authorized, operating the Messaging Service under Section 6A, preventing fraud, meeting legal obligations, and analyzing, improving, developing, and securing the Services, tools, and models subject to Section 11A.6. This right operates alongside the license in Terms Section 21.1 and is limited by Section 4.3. We may engage Affiliates and Subprocessors, transfer data internationally, and select and change infrastructure and vendors at our discretion, subject to Sections 5, 5A, 6, 6A, and 7.

4.2 De-identified and aggregated data

We may create and use De-Identified Data and aggregated data for any lawful purpose, including analytics, benchmarking, and Service and model development, as Terms Section 21.2 contemplates. To the extent such data is no longer Personal Data under applicable law, it is not subject to the Personal-Data restrictions of this Privacy Agreement. We maintain de-identification, do not attempt re-identification except to test its effectiveness, and contractually require any recipient of De-Identified Data not to attempt re-identification.

4.3 Statutory ceiling and read-down

The rights in this Section are subject to and do not override the mandatory requirements of applicable data-protection law, including lawful basis, purpose limitation, data minimization, transfer restrictions, and data-subject rights. Where a regime requires consent, authorization, or an opt-out for a particular use, that use is conditioned on obtaining it. This Section grants no right to Process Personal Data for purposes incompatible with those disclosed. Any provision of this Privacy Agreement that would be unlawful, invalid, or unenforceable in a jurisdiction is read down to the minimum extent necessary to be lawful there, without affecting its validity elsewhere, consistently with Terms Section 31.4. Where Remote Leverage acts as processor or service provider, the rights in this Section apply to Client Personal Data only to the extent Section 5 and Applicable Data Protection Law permit a processor or service provider to exercise them.

4.4 Controller-to-Controller Mutual Obligations (Recruitment Services, Managed: Contractor of Record Services, and Messages)

For Processing under the Recruitment Services (Section 0.3, first bullet) where Remote Leverage and the Client are separate controllers, for Processing under the Managed: Contractor of Record Services (Section 0.3, second bullet, and Section 5A) where Remote Leverage and the COR Client are independent controllers, for Processing that Remote Leverage performs as an independent controller in providing the Self Serve: Direct Pay Services (Section

0.3, third bullet), and for Messages and Work-Verification Data that a Client accesses as an independent controller (Sections 6.9 and 6A.9), the following mutual obligations apply:

(a) **Confidentiality.** Each party ensures that its authorized personnel are bound by confidentiality obligations appropriate to the sensitivity of the Personal Data, and takes reasonable steps to ensure that they understand their data-protection obligations.

(b) **Data-Subject Rights Cooperation.** Each party will cooperate with the other without undue delay to respond to data-subject requests for access, rectification, deletion, objection, portability, or other rights under Applicable Data Protection Law, and will provide the other with necessary information and assistance to enable the other party to meet its obligations to the data subject within statutory timelines.

(c) **Complaint Notification.** Each party will notify the other without undue delay if it receives a complaint (whether from a data subject, a Supervisory Authority, or another competent authority) relating to the processing of Personal Data or to either party's compliance with Applicable Data Protection Law. Each party will provide reasonable cooperation, information, and assistance in relation to investigation or remedy of such complaint.

(d) **Breach Notification.** Each party will notify the other without undue delay after becoming aware of a Personal Data Breach affecting Personal Data shared with, or jointly controlled by, the other party, and will provide reasonable cooperation in investigation, mitigation, and notification to Supervisory Authorities and data subjects as required by Applicable Data Protection Law.

(e) **Third-Party Liability.** Each party is liable for the acts and omissions of its own subprocessors, service providers, and third parties to the same extent it would be liable for its own acts under Applicable Data Protection Law. Remote Leverage is not liable for acts or omissions of third parties not engaged by Remote Leverage.

(f) **Liability.** As between the parties, each party is responsible for losses arising from its own breach of this Privacy Agreement or of Applicable Data Protection Law, subject to the limitations and exclusions of liability in the Terms and any Commercial Agreement.

4.5 Leve Records and acceptance records

Remote Leverage records and logs every action of every User on Leve, as Terms Section 16.1 describes, and keeps acceptance records under Terms Section 1.4. Leve Records include records generated by the Monitoring Tool, Payment Partners, and the electronic-signature provider. Remote Leverage Processes Leve Records to operate and secure Leve, attribute and evidence Requests and approvals, verify time and payments, investigate falsification and Prohibited Conduct, respond to disputes and chargebacks, meet legal obligations, and establish, exercise, or defend legal claims, on the bases of contract, legal obligation, and legitimate interests. Access to Leve Records is restricted to authorized personnel with a need to know, and Leve Records are retained under Section 1.8. The evidentiary effect that the Terms give to Leve Records between the parties does not limit a data subject's rights of access and rectification under Applicable Data Protection Law, and a data subject may ask for a copy of, or the correction of, inaccurate Personal Data in a Leve Record through the channels in Section 8.

SECTION 5. DATA PROCESSING AGREEMENT (PROCESSOR TERMS)

This Section applies where Remote Leverage Processes Personal Data solely on a Client's Documented Instructions (the Client as controller, or, where the Client is itself a processor, Remote Leverage as subprocessor). It constitutes the Article 28 GDPR and UK GDPR terms and the equivalent processor terms under other regimes and flows down to Subprocessors. For Processing under the Managed: Contractor of Record Services that each party performs for its own purposes, Section 5A applies instead. This Section applies to the Self Serve: Direct Pay Services and to any discrete Processing that Remote Leverage performs solely on a Client's Documented Instructions.

5.1 Subject matter, duration, nature, purpose, categories

Subject matter and details are in Annex G and the applicable Service Order or Commercial Agreement; duration is coextensive with the Services plus the export period in Section 1.8 and any legally required tail; nature and purpose are the provision of the Self Serve: Direct Pay Services, including Engagement administration, Templates and electronic signature, tax-form collection and transmission, time tracking where activated, the project module, invoicing, approvals, Workspace Messaging Service functions, and the transmission of payment instructions to Payment Partners, and other Services performed on instruction; the categories of data subjects are Direct Contractors, Authorized Users, and other individuals whose data the Client submits, and the categories of data are those in Section 1.2 and Annex G.

5.2 Documented instructions

We Process Client Personal Data only on the Client's Documented Instructions, including as to international transfers, unless law requires otherwise, in which case we inform the Client unless legally prohibited. We inform the Client if, in our opinion, an instruction infringes applicable law.

5.3 Confidentiality

Persons authorized to Process Client Personal Data are bound by confidentiality obligations that survive their engagement.

5.4 Security

We implement the technical and organizational measures summarized in Section 9 and Annex G, appropriate to the risk and the state of the art.

5.5 Subprocessors

The Client gives general authorization for Remote Leverage to engage the Subprocessors listed in Annex G, as updated on the Subprocessor Page, and to add or replace Subprocessors, as Terms Section 23 contemplates. The list on the Subprocessor Page, which Annex G reproduces as at the version date of this Privacy Agreement, is incorporated by reference. Remote Leverage gives notice of an intended addition or replacement by updating the Subprocessor Page and, where the Client has subscribed to updates through the mechanism offered on that page or on Leve, by email, at least 14 days before the new Subprocessor Processes Client Personal Data, except that where a replacement is required urgently to protect the security or continuity of the Services or to comply with law, Remote Leverage may make it on shorter notice given as soon as reasonably practicable. The Client may object in writing within that notice period, and only on reasonable, documented grounds relating to the protection of Personal Data. The parties will seek in good faith to resolve the objection, and if it is not resolved within 30 days, the Client may, as its sole and exclusive remedy, terminate the affected Service by written notice, without refund of fees for Services already rendered. If the Client does not object within the notice period, the Subprocessor is deemed approved. Remote Leverage imposes data-protection obligations on each Subprocessor that are no less protective in substance than those in this Section and remains liable for its Subprocessors' performance to the extent required by Applicable Data Protection Law. Payment Partners are not Subprocessors when they act as independent controllers under their own licenses, as Section 6B.1 describes.

5.6 Assistance

Taking into account the nature of the Processing, we assist the Client with data-subject rights requests; with security, breach notification, data protection impact assessments, and prior consultations; and with demonstrating compliance. Requests that data subjects send us directly that concern Client-controlled Processing are, where appropriate, referred to the Client.

5.7 Personal data breach

We notify the Client without undue delay, and where feasible within 72 hours, after becoming aware of a Personal Data Breach affecting Client Personal Data, with the information reasonably available to enable the Client to meet its obligations, and we cooperate in investigation and remediation. Notification of a breach is not an acknowledgment of fault or liability. Our controller-level obligations are in Section 10.

5.8 Return or deletion

When the Client's use of a Service ends, the Client may export its Client Personal Data for thirty (30) days, as Terms Sections 11.16 and 28.3 provide, and Remote Leverage then deletes remaining Client Personal Data and existing copies within a reasonable period, generally not exceeding 90 days, except where law requires retention, where Remote Leverage retains the data as an independent controller under Section 2.2 or as a Leve Record under Section 4.5, or where the data is needed for the establishment, exercise, or defence of legal claims; data in backups is deleted in the ordinary backup cycle and is not restored except for continuity purposes. Where a regime requires a blocking step before deletion, we apply it.

5.9 Audit and information

We make available information reasonably necessary to demonstrate compliance with this Section. We satisfy this obligation first by providing written responses to reasonable security questionnaires, summaries of our policies and technical and organizational measures, and any independent third-party audit reports or certifications we hold from time to time. Where those materials are not sufficient to demonstrate compliance, or a Supervisory Authority requires it, the Client or an independent auditor that is bound by confidentiality and is not a competitor of Remote Leverage may conduct an audit, including an inspection, no more than once in any 12-month period (except following a Personal Data Breach affecting Client Personal Data or where a Supervisory Authority requires it), on at least 30 days' written notice, during normal business hours, in a manner that minimizes disruption, under a scope agreed in advance, and at the Client's cost, including Remote Leverage's reasonable costs of supporting the audit.

5.10 International transfers under this Section

Where Processing involves a Restricted Transfer, the mechanism in Section 7 applies and is incorporated by reference, including the European Union Standard Contractual Clauses (2021 modules), the United Kingdom Addendum, and the Swiss adaptations, completed to reflect the parties' roles, and any other mechanism required under Section 7.1.

5.11 United States service-provider terms

Where Remote Leverage Processes Client Personal Data as a service provider or contractor under the California Consumer Privacy Act, or as a processor under another United States state privacy law, Remote Leverage: (a) Processes it only for the limited and specified business purposes of providing the Services described in this Privacy Agreement, the Terms, and any Commercial Agreement; (b) does not sell or share it, as those terms are defined in that law; (c) does not retain, use, or disclose it for any purpose other than those business purposes, or outside the direct business relationship with the Client, except as that law permits; (d) does not combine it with Personal Data received from or on behalf of another person, or collected from its own interactions with the consumer, except as that law permits; (e) complies with that law and provides the level of privacy protection it requires; (f) notifies the Client if it determines that it can no longer meet its obligations under that law; and (g) permits the Client, on notice, to take reasonable and appropriate steps to stop and remediate unauthorized use. Remote Leverage certifies that it understands these restrictions.

SECTION 5A. CONTROLLER ARRANGEMENT (MANAGED: CONTRACTOR OF RECORD SERVICES)

5A.1 Independent controllers

For Processing carried out through Leve in the Managed: Contractor of Record Services (including onboarding, contracting, compliance documentation, identity verification, Timesheets and Work-Verification Data where activated, invoicing, payment instructions for payouts executed by Payment Partners, tax documentation and information reporting, contractor administration, and Leve Records), Remote Leverage and the COR Client each determine the purposes and means of the Processing it performs for its own purposes and are independent controllers, and not joint controllers, of that Processing: Remote Leverage in its role as contracting party with the COR Contractor, Paying Party, information-reporting party, and operator of Leve, and the COR Client in its receipt and use of the COR Contractor's services and its direction of the day-to-day work to the extent the COR MSA permits. Where Remote Leverage performs discrete Processing solely on the COR Client's Documented Instructions, it does so as processor under Section 5. If a competent Supervisory Authority or court determines that Remote Leverage and the COR Client are joint controllers of any Processing, this Section constitutes the arrangement required by Article 26 GDPR and the equivalent provisions of other regimes for that Processing, and its essence is made available to data subjects through this Privacy Agreement.

5A.2 Allocation of responsibilities

- Transparency and notice to COR Contractors: Remote Leverage provides the primary privacy notice through this Privacy Agreement and Leve; the COR Client provides any additional notice required for its own distinct purposes.
- Lawful basis: each party is responsible for ensuring a lawful basis for the Processing it directs; the parties rely on contractual necessity, legal obligation, and legitimate interests for core Processing in the Managed: Contractor of Record Services rather than COR Contractor consent, except where Applicable Data Protection Law requires authorization or consent, which Remote Leverage obtains under Section 0.4A.
- Data-subject rights: Remote Leverage is the designated primary point of contact for COR Contractors and coordinates responses; the COR Client cooperates and provides information and action within its control within the applicable timeline. Data subjects may nonetheless exercise their rights against either party.
- Security: each party implements appropriate technical and organizational measures for the Processing within its control; Remote Leverage maintains the Leve measures in Section 9 and Annex G.
- Retention: retention follows Section 1.8 and the parties' documented schedule.
- International transfers: transfers are conducted under Section 7.
- Client-directed Processing: the COR Client is responsible for Processing it directs, including monitoring settings it requests, access it grants to COR Contractors to its own systems and data, Messages it accesses or exports, and instructions it gives through Leve, and the indemnity in Section 3.4 applies to it.

5A.3 Liability toward data subjects

As between the parties, each is responsible only for losses arising from its own breach of this Privacy Agreement or of Applicable Data Protection Law, and the COR Client is responsible for losses arising from Processing it directs, in each case subject to the limitations and exclusions of liability in the COR MSA and the Terms. If either party is held liable to a data subject or authority for loss caused in whole or in part by the other party, including on a joint and several basis where Applicable Data Protection Law so provides, it may recover from the other party the part of the compensation corresponding to the other party's responsibility. This Section does not limit any statutory right of a data subject to bring a claim against either party.

SECTION 6. MONITORING, WORK VERIFICATION, AND DEVICE SECURITY

Not every Contractor User is monitored. This Section applies only to a Contractor User for whom time tracking or work verification has been activated on Leve, by the Client for whom it works or by Remote Leverage, and who has given the Monitoring Authorization, as Terms Section 14.1 provides. Where monitoring has not been activated for a

Contractor User, no Work-Verification Data is collected about that Contractor User. Monitoring is carried out only through the Monitoring Tool, which is currently Time Doctor, operated by Time Doctor, LLC, or any successor or additional work-verification tool that Remote Leverage designates and identifies on the Subprocessor Page.

6.1 Purposes

Work-Verification Data is Processed to: verify work and reconcile Timesheets for invoicing and payment under the applicable Payment Arrangement; resolve disputes, including disputes about Milestones, invoices, and chargebacks; protect the security, confidentiality, and integrity of systems and data and prevent data loss; prevent, detect, and investigate falsification under Terms Section 14.7, Prohibited Conduct, misuse, and Security Incidents; provision, configure, update, and secure devices where Section 6.4 applies; and establish, exercise, or defend legal claims and meet legal obligations. Remote Leverage does not use Work-Verification Data to supervise, direct, or evaluate how any Contractor User performs work, as Terms Section 5.5 states. A Client may use Work-Verification Data only to manage its Engagements and verify work, and must not use it to control the manner and means of a Contractor User's work, as Terms Section 14.6 provides.

6.2 Lawful basis

Monitoring and work verification rest on the legitimate interests of Remote Leverage and the Client in verifying the time and work for which payment is requested and in preventing fraud and protecting systems, and on contractual necessity where the Payment Arrangement is based on hours, supported by a documented balancing assessment and, where Applicable Data Protection Law requires it for intrusive monitoring, a data protection impact assessment. The Monitoring Authorization operates as the prior notice and acknowledgment, and as the consent required by communications and computer-monitoring laws, and, as Section 0.4A explains, is not relied on as consent under regimes in which consent that is a condition of an Engagement is not freely given; where an authorization-based regime requires the data subject's authorization as such, it serves as that authorization. Running the Monitoring Tool on a personal device is not carried out on the basis of legitimate interests alone; it requires the specific, freely given Personal-Device Consent, and a Contractor User may decline it and instead use a device provided by Remote Leverage or the Client where one is offered, or decline to perform time-verified work on that personal device.

6.3 Scope of monitoring

Where activated and authorized, and only while the Contractor User's timer is running during the working time to which the activation applies, the Monitoring Tool may collect: account, device, and usage data; timer start and stop times and the time recorded; screenshots at the intervals configured within the scope Remote Leverage has enabled; the applications and URLs used; activity levels, measured as the presence or frequency of keyboard and mouse activity and not its content; idle time; and approximate location only where enabled and lawful. These categories are the Work-Verification Data described in Terms Section 14.4. No User may enable monitoring beyond the scope Remote Leverage has enabled, as Terms Section 14.6 provides, and we favor the least intrusive configuration that achieves the purpose. The Contractor User controls the timer and must stop it before any personal activity, as Terms Section 14.5 provides. Monitoring that a Client carries out on its own systems, accounts, or devices outside Leve is the Client's own Processing, for which the Client is solely responsible as controller.

6.4 Device management and endpoint security

On devices provided by Remote Leverage and, with Personal-Device Consent, on enrolled personal devices, Remote Leverage may deploy mobile-device-management, endpoint-detection-and-response, and security tooling to configure and enforce security settings, encryption, and access controls, deploy updates and applications, detect and respond to threats, enforce compliance policies, and, in cases of loss, theft, compromise, or the end of an Engagement, remotely lock or wipe Remote Leverage or Client data and, on devices Remote Leverage owns, the device. On enrolled personal devices we limit management to a separated work container or profile and do not access, monitor, or wipe personal content outside it. A Client that deploys device-management tooling on devices it provides does so as controller under its own policies and is responsible for its lawfulness.

6.5 Transparency

Before monitoring begins, the Monitoring Authorization gives each Contractor User clear notice of the Monitoring Tool, what is collected, when, why, the lawful basis, who has access, retention, and how to exercise rights and withdraw. Leve or the Monitoring Tool indicates when the timer is running, and the Contractor User can stop it at any time when not performing work. Where a law requires the engaging party to give notice of electronic monitoring, the Client gives that notice and obtains any acknowledgment it requires, and the Monitoring Authorization is designed so that its content can satisfy that notice.

6.6 Retention and access

Work-Verification Data is retained only for the limited period necessary for the purposes in Section 6.1, generally not exceeding 12 months after collection, then deleted or de-identified, except that Timesheets and time records used for invoicing or payment are kept with the related billing records and data relevant to a Security Incident or dispute is kept until it is resolved, as Section 1.8 provides. Access is restricted as Section 6.9 describes and is used only for the purposes in Section 6.1.

6.7 Limits on monitoring

We do not: access the content of purely personal communications; monitor a Contractor User outside working time or while the timer is stopped; log keystroke content or capture webcam images or video as a standard measure; or surveil legally protected activity, including lawful discussion of pay and working conditions. Any elevated or exceptional measure is assessed, documented, and limited in scope and time before use, and is disclosed in advance. Where a country requires prior authorization, notice to the authority, or a specific instrument for monitoring or for related international transfer, that requirement is met through the authorizations in Section 0.4A and our transfer documentation or Subprocessor arrangements.

6.8 Monitoring Authorization and withdrawal

A Contractor User may withdraw the Monitoring Authorization or the Personal-Device Consent by Notice through Leve or to the Support Email. After withdrawal, the Contractor User may stop running the Monitoring Tool for that Engagement, and Remote Leverage disables collection for that Engagement as soon as reasonably practicable after it processes the Notice. The Client may then end the time-verified Engagement or, for a COR Engagement, Remote Leverage may end it, as Terms Section 14.2 provides, subject to payment of amounts the Client has already approved and funded. Work-Verification Data collected before withdrawal is retained under Section 6.6.

6.9 Recipients of Work-Verification Data and roles

Work-Verification Data may be accessed only by: authorized Remote Leverage personnel with a need to know; the Client for whom the Contractor User works, through its Account Administrators and Authorized Users with the relevant permission, for that Client's Engagements only; the Monitoring Tool operator, which acts as Remote Leverage's Subprocessor or service provider and, for its own account administration and service purposes, under its own privacy notice; and Remote Leverage's other service providers, as Terms Section 14.4 provides. It may be transferred internationally under Section 7. In the Managed: Contractor of Record Services, Remote Leverage and the COR Client are each an independent controller of the Work-Verification Data each accesses for its own purposes. In the Self Serve: Direct Pay Services, the Direct Pay Client that activates monitoring is the controller, Remote Leverage collects and makes the data available as its processor under Section 5, and Remote Leverage is an independent controller only for its own purposes described in Section 2.2. A Client that exports or retains Work-Verification Data outside Leve is responsible for it as controller and must observe Section 6A.9(e) as applied to that data.

SECTION 6A. MESSAGING SERVICE AND ACCESS TO MESSAGES

6A.1 Scope and data processed

This Section applies to the Messaging Service, including its chat, channel, comment, file-attachment, and call functions, and to other communications made through or with Leve, including email exchanged with Remote Leverage, support requests, and calls and meetings with Remote Leverage personnel. In operating the Messaging Service, Remote Leverage Processes the content of Messages and attachments; call content and, where made after notice, call recordings; the identity of senders and recipients; Workspace and channel identifiers; timestamps; read, delivery, and status indicators; edits and deletions; and related IP address, device, and log data. Messages are User Content and Leve Records.

6A.2 Who can see Messages; Client access

Messages are visible to the participants in the conversation and to Remote Leverage as described in Section 6A.3. In addition, as Terms Section 15.3 provides, a Client, through its Account Administrators, may access, read, search, export, and retain all Messages, attachments, and metadata exchanged (i) between its personnel and any Contractor User working for it, and (ii) among Contractor Users working for it, where those Messages are in the Client's Workspace or concern the Client's Engagements, during the Engagement and the retention period in Section 6A.8. This access does not extend to:

- a Contractor User's Messages with or about other Clients; or
- a Contractor User's own Account, identity, tax, or payment communications with Remote Leverage support, which Leve keeps in support channels that Clients cannot view; or
- communications between a Placement Candidate and Remote Leverage recruiters, which are not shared with a Client except as part of a presentation under the Recruitment Services.

A Client may use Messages only to manage its Engagements, protect its information, and establish or defend its claims, as Terms Section 15.3 provides. A Client must not use Messages to control the manner and means of a Contractor User's work, to make decisions based on any characteristic protected by law, or to monitor a Contractor User's personal affairs. Each access and export by a Client is recorded as a Leve Record. The Messaging Service is protected by encryption in transit and at rest as described in Annex G, but it is not end-to-end encrypted, and Users should not expect that a Message will be visible only to its addressee.

6A.3 Access and use by Remote Leverage

Remote Leverage may access, review, scan (by automated means and authorized personnel), monitor, record, retain, and use Messages, attachments, and their metadata to: provide and support the Messaging Service and the Services; protect the safety and security of Users and of Leve; prevent, detect, and investigate fraud, spam, malware, abuse, falsification, and violations of law; enforce the Terms, this Privacy Agreement, and any Commercial Agreement, including the restrictions on circumvention and off-Leve payments; verify time, payments, and invoices; investigate complaints; administer and resolve guarantee, replacement, refund, chargeback, and payment disputes; comply with legal obligations, legal process, and legal holds; and establish, exercise, or defend legal claims, including by using Messages as evidence, as Terms Section 15.2 provides. Human review by Remote Leverage personnel is limited to authorized personnel with a need to know and is ordinarily prompted by an automated flag, a complaint, a dispute, a chargeback, a Request for support, a security or verification need, or a legal requirement. Each human access is logged.

6A.4 Automated scanning and optional features

Remote Leverage may use automated tools to scan Messages and attachments for spam, malware, fraud, falsification, and abuse, and to detect the exchange of off-Leve contact or payment details in breach of Terms Section 15.1. Remote Leverage may also offer optional features that use automated or artificial-intelligence tools, such as translation or summaries, which Process Message content to provide the feature; any provider of such a

feature is listed on the Subprocessor Page when engaged and is bound by Section 11A.5. Message content is not used to train artificial-intelligence models, as Section 11A.6 provides.

6A.5 Consent of all parties

By sending or receiving a Message through the Messaging Service, or by joining a call or meeting that is recorded after notice under Section 6A.6, each participant consents, on his or her own behalf and as a party to the communication, to the access, recording, retention, and use of the communication by Remote Leverage under Section 6A.3 and by the applicable Client under Section 6A.2, as Terms Section 15.4 provides, for the purposes of every federal, state, and foreign law governing the interception, recording, or storage of communications. The Messaging Acknowledgment, given on acceptance under Section 0.4, records this consent before a User first uses the Messaging Service. Remote Leverage also relies, as the provider of the Messaging Service, on the exceptions that communications laws provide for service providers. Each Client is responsible for ensuring that its Authorized Users accept the Terms and this Privacy Agreement and are informed of this Section. Calls are recorded only after notice to all participants, and a person who does not accept the recording may leave the call. As between the participants, Remote Leverage, and the applicable Client, and to the maximum extent permitted by law, no User has an expectation of privacy in Leve communications as against Remote Leverage or that Client, as Terms Section 15.4 states, subject to Section 6A.10.

6A.6 Call and meeting recordings

Calls with Remote Leverage personnel, including meetings held on the video-conferencing services listed in Annex G, may be recorded only after advance notice to all participants, given in the invitation or at the start of the call or meeting, and calls on the Messaging Service are recorded only where a recording indicator is displayed to all participants. A participant who does not consent may ask that the call or meeting not be recorded or may leave it. Recordings are used for the purposes in Section 6A.3 and, for interviews, for the assessment purposes in Section 1.2, and are retained under Section 6A.8.

6A.7 Prohibited content and user responsibility

Users must not send through the Messaging Service health or medical information, images or copies of identity documents, full bank-account, payment-card, or tax-identification numbers, passwords, one-time passcodes, or other credentials, Regulated Data, or other Sensitive Personal Data, except through the secure upload channels that Leve designates for that purpose, as Terms Sections 15.5 and 19(e) provide. Users are responsible for the content they send and must have the right to share any Personal Data of third parties they include. Remote Leverage may delete or restrict prohibited content, and, to the extent permitted by law, is not responsible for Personal Data that a User chooses to send through the Messaging Service in breach of this Section.

6A.8 Retention

Messages, attachments, call recordings, and metadata are Leve Records and are retained for the life of the relevant Workspace or Account and thereafter for the longest limitation period applicable to claims to which they may be relevant, generally not exceeding seven years after the Account is closed or the Engagement ends, whichever is later, subject to legal holds. Client access under Section 6A.2 continues during this retention period for Messages that remain within its scope. Deleting a Message or closing an Account may not delete copies held by other participants, copies that a Client has exported, or copies that Remote Leverage retains where retention is required or permitted by law or by this Section.

6A.9 Roles and Client obligations for Messages

(a) **Remote Leverage.** Remote Leverage is an independent controller of Messages for the purposes in Section 6A.3, in every Service.

(b) **Managed: Contractor of Record Services.** The COR Client is an independent controller of the Messages it accesses, reads, searches, exports, or retains under Section 6A.2, from the moment of access, for the purposes Terms Section 15.3 permits.

(c) **Self Serve: Direct Pay Services.** The Direct Pay Client is the controller of Messages within its Workspace that relate to its Engagements of Direct Contractors. Remote Leverage hosts those Messages and makes them available to the Client as its processor under Section 5, and is an independent controller only for its own purposes under Section 6A.3.

(d) **Recruitment Services.** A Recruitment Client is an independent controller of the Messages it exchanges with or receives about Placement Candidates.

(e) **Client obligations once Messages leave Leve.** A Client that exports or otherwise copies Messages outside Leve must: keep them confidential and secure, with protection at least equivalent to that described in Section 9; use them only for the purposes Terms Section 15.3 permits; apply its own retention schedule and delete them when no longer needed for those purposes; handle data subject requests about them as controller; meet any transfer requirements that apply to its onward transfers; not disclose them to any third party except its professional advisers, insurers, and authorities, or as law requires or as needed to establish or defend its claims; and notify Remote Leverage without undue delay of any Personal Data Breach affecting exported Messages that may involve Remote Leverage or other Users. The Client is responsible for exported Messages as controller, and the indemnity in Section 3.4 applies.

6A.10 Legal basis by jurisdiction and non-waivable rights

(a) **United States.** Access, recording, and retention rest on the consent of the parties to the communication under Section 6A.5, the provider exceptions, and the business purposes in Section 6A.3, and, under state privacy laws that apply, on the permitted purposes those laws recognize.

(b) **European Economic Area, United Kingdom, and Switzerland.** Delivering Messages rests on contractual necessity. Remote Leverage's access and use under Section 6A.3 rest on its legitimate interests in security, fraud and falsification prevention, enforcement, verification of time and payments, dispute resolution, and the establishment or defence of legal claims, supported by a documented balancing assessment, and on legal obligation where a law requires disclosure. A Client's access under Section 6A.2 rests on the Client's own legitimate interests in managing its Engagements and protecting its information, for which the Client is responsible as controller. Consent is not relied on as the data-protection legal basis for this Processing because of the imbalance in an engagement relationship. Consistently with the requirements of prior notice, proportionality, and the use of less intrusive means that European courts and authorities apply to the monitoring of work communications, Remote Leverage gives notice through the Messaging Acknowledgment and the in-product notice in Section 6A.11, limits human review as Section 6A.3 describes, and logs each access.

(c) **Brazil.** The bases are performance of a contract, compliance with a legal or regulatory obligation, the regular exercise of rights in judicial, administrative, or arbitral proceedings, and legitimate interests, under Article 7 of the Lei Geral de Proteção de Dados Pessoais.

(d) **Colombia.** The Processing rests on the prior, express, and informed authorization of the data subject, obtained through Sections 0.4A(b) and 0.4A(f), with the purposes in Sections 6A.2 and 6A.3 disclosed, as Ley Estatutaria 1581 de 2012 requires.

(e) **Mexico and other jurisdictions.** The bases in Annexes E and F apply, including consent through the privacy notice where the law requires it and the exceptions the law provides.

(f) **Non-waivable rights.** The statement in Terms Section 15.4 that no User has an expectation of privacy as against Remote Leverage or the applicable Client operates only as the parties' acknowledgment of the access described in this Section and only to the maximum extent permitted by law. It does not waive, and is read down to the extent it would conflict with, any right that cannot be waived by contract, including the rights of access, rectification,

deletion, objection, and complaint under the GDPR, the UK GDPR, the Swiss Federal Act on Data Protection, the Lei Geral de Proteção de Dados Pessoais, Ley Estatutaria 1581 de 2012 and the constitutional right of habeas data, and Mexico's Ley Federal de Protección de Datos Personales en Posesión de los Particulares, and every access remains subject to purpose limitation and proportionality.

6A.11 In-product notice

The Messaging Service displays, in each Workspace and before a User's first Message, a notice that Messages are visible to Remote Leverage and, for Messages within the Workspace or about the Client's Engagements, to the Client; that Messages are encrypted in transit and at rest but are not end-to-end encrypted; that calls may be recorded only with a visible recording indicator; and that health information, identity documents, full account or card numbers, credentials, and Regulated Data must not be sent except through designated secure channels. The notice links to this Section.

SECTION 6B. PAYMENTS, CONTRACTS, AND TAX DOCUMENTS

6B.1 Payment Partners and payment data flows

In every Service, Remote Leverage collects payment data and payment instructions through Leve and transmits them to Payment Partners, and the Payment Partners execute every debit, charge, currency conversion, and payout and hold any funds, in accounts maintained by or for them and never in Remote Leverage's operating accounts, under their own licenses and terms, as Terms Section 10.1 provides. Specifically:

- In the Self Serve: Direct Pay Services, payments are received for Direct Contractors by the Payment Partner, which each Direct Contractor appoints as its payee-side agent, together with Remote Leverage only to the extent needed to give payment instructions, as Terms Section 11.4 provides; Remote Leverage transmits the Direct Pay Client's approved payment instructions and the Direct Contractor's payout details to the Payment Partner.
- In the Managed: Contractor of Record Services, Remote Leverage pays COR Contractors as their contracting party and invoices COR Clients under the COR MSA, as Terms Section 10.2 provides; that payment obligation is executed through Payment Partners on Remote Leverage's payment instructions.
- In the Recruitment Services, the Client pays placement fees, and the related card or bank data is collected and processed by Payment Partners.
- Any multi-currency balance, card, early payout, or digital-asset payout is provided and held only by a Payment Partner under its own license and terms, as Terms Section 8.5 provides, and the Personal Data needed for it is shared with that Payment Partner only when the User elects to use it.

Payment Partners act as independent controllers for their own know-your-customer, anti-money-laundering, sanctions, fraud-prevention, and regulatory recordkeeping Processing, and their own privacy notices govern that Processing; for the execution of debits, conversions, and payouts on instructions transmitted through Leve, they act as processors or service providers to the extent their role and Applicable Data Protection Law so characterize it. A Client or Contractor User may be required to accept a Payment Partner's terms and privacy notice. Payment-card data is collected and tokenized by the Payment Partner, and Remote Leverage does not store full payment-card numbers. Bank-account data used for debits is tokenized by the Payment Partner that executes the debit.

6B.2 Identity verification, know-your-customer, and sanctions screening

Two different activities are involved. First, Remote Leverage verifies the identity, beneficial ownership, and location of Users and screens them against sanctions and fraud lists for its own purposes of Leve integrity, fraud prevention, and compliance with sanctions law, as Terms Section 7.3 provides; for that Processing Remote Leverage is controller, and biometric verification occurs only with the consent in Section 0.4A(c). Second, Payment Partners perform their own know-your-customer, anti-money-laundering, and sanctions checks under their licenses, as independent controllers, and may request additional information directly or through Leve; Remote Leverage

transmits the data they require for that purpose. Payment Partners make their own compliance decisions under their own legal obligations.

6B.3 Sanctions and restricted jurisdictions

Remote Leverage does not contract with, transmit payment instructions for, or provide Services to any Sanctioned Person or any person located in, ordinarily resident in, or organized under the laws of a jurisdiction subject to comprehensive United States sanctions, and does not provide Services to nationals of a sanctioned jurisdiction where sanctions law prohibits or restricts it, as Terms Section 31.2 provides. Remote Leverage may restrict access by Placement Candidates and Contractor Users who are covered persons under 28 C.F.R. Part 202 to government-related data or bulk United States sensitive personal data. Remote Leverage may refuse, suspend, or terminate an Account or a payment instruction, and may retain, block, and disclose Personal Data, as sanctions, export-control, and anti-money-laundering laws require or permit, without liability to the affected User to the extent permitted by law.

6B.4 Contracts and electronic signatures

Direct Contracts, each COR Contractor's independent contractor agreement with Remote Leverage, offers made through Leve, statements of work, tax forms, and other documents may be presented and executed electronically through the electronic-signature provider listed in Annex G, as Terms Section 9 provides. Each signatory consents to conduct the transaction by electronic means and agrees that electronic signatures and records have the same legal effect as handwritten signatures and paper records under applicable electronic-signature law. The electronic-signature audit trail, including signer identity, email address, IP address, and timestamps, is a Leve Record and is retained as evidence of execution with the related document.

6B.5 Tax documents and information reporting

Leve collects Forms W-9, W-8BEN, and W-8BEN-E and local equivalents, may validate taxpayer identification numbers where validation is available, and stores and transmits them, as Terms Sections 6, 11.11, and 31.3 describe. In the Self Serve: Direct Pay Services, the Direct Pay Client is the payer for tax purposes, Leve may transmit the forms to the Client as a convenience only, and the Client is solely responsible for any withholding, information returns, and other filings. In the Managed: Contractor of Record Services, where Remote Leverage itself is the payer, Remote Leverage uses the information to meet the withholding and information-reporting duties that law imposes on it as payer, such as Forms 1099-NEC or 1042-S and equivalent local filings, and to furnish statements to payees, which Users consent to receive electronically under Terms Section 17.5. Payment Partners may separately file Forms 1099-K. Remote Leverage does not determine any other User's classification, withholding, treaty eligibility, or reporting obligations. Taxpayer identification numbers are Processed as required by 26 U.S.C. section 6109 and equivalent laws, are treated as Sensitive Personal Data, and are disclosed only to tax authorities, the Client that is the payer, Payment Partners, accountants, and advisers who need them. Tax and payment records are retained as set out in Section 1.8.

6B.6 Chargebacks, collections, and disputes

Where a payment is disputed, reversed, charged back, or unpaid, Remote Leverage may Process and disclose the relevant Account, contract, invoice, Timesheet, Work-Verification Data, Leve Records, communication, and payment records, including Messages under Section 6A, to Payment Partners, card networks, financial institutions, collection agencies, commercial credit reporting agencies where Terms Section 10.6 permits, legal counsel, courts, and arbitral bodies, to the extent necessary to respond to the dispute and to establish, exercise, or defend its legal claims, as Terms Section 10.7 contemplates.

6B.7 Currency conversion and exchange-rate records

Leve records the exchange rate shown and applied to each conversion, the amounts, and the related payment instruction as Leve Records, and Remote Leverage Processes those records to administer invoicing and payment instructions, respond to disputes, and meet recordkeeping obligations.

SECTION 6C. SMS AND RCS MESSAGING PROGRAM

These are the terms of the SMS/RCS Program. For Prospects and other participants who are not Users, they operate as the program terms and, together with Section 1, as the privacy notice for the SMS/RCS Program. For Users, they supplement Terms Section 17.5. The current text of this Section is available on the Published Page.

6C.1 Program description and message types

Remote Leverage Inc. operates a recurring SMS and RCS messaging program. A person can join the SMS/RCS Program in three ways: (a) by checking the unchecked SMS consent box on a form on Remote Leverage's website that is not a Leve registration or acceptance form; (b) by giving consent during a consultation, which is completed when the person replies with an affirmative keyword to the confirmation text that Remote Leverage then sends; or (c) by texting Remote Leverage first, in which case consent to Promotional Messages is completed only when the person replies with an affirmative keyword, such as YES or JOIN, to the confirmation message described in Section 6C.3(c). By joining in one of these ways, you consent to receive recurring automated text and RCS messages from Remote Leverage at the mobile phone number you provided or texted from. These messages may include appointment reminders and scheduling confirmations; Account, placement, and Placement Candidate status updates; customer service and support messages; and promotional offers, news, and information about our virtual assistant placement services and other Services.

6C.2 Consent and revocation

Consent to receive these messages is not required to purchase any goods or services from Remote Leverage. Consent to Promotional Messages is never given by accepting the Terms or this Privacy Agreement, and a User may revoke it at any time, as Section 6C.7 describes, without affecting the User's Account or any Service.

6C.3 How consent is given and recorded

(a) **Web forms.** A form on Remote Leverage's website that offers the SMS/RCS Program presents a separate, unchecked checkbox, apart from any acceptance of the Terms or this Privacy Agreement, next to this disclosure, or a disclosure to the same effect: "By checking this box, I agree to receive recurring automated marketing and informational text messages (SMS and RCS) from Remote Leverage at the mobile number provided, including messages sent using an automated system. Consent is not a condition of any purchase. Msg frequency varies. Msg & data rates may apply. Reply HELP for help, STOP to cancel. See the SMS Program terms and Privacy Agreement at https://remoteleverage.com/privacy-policy/." Checking the box is the person's electronic signature on that agreement.

(b) **Consultations.** Where a person agrees during a consultation to receive Program Messages, Remote Leverage notes the oral agreement in the Consent Record and sends one confirmation message containing the disclosures in paragraph (c). Promotional Messages begin only after the person replies with an affirmative keyword to that confirmation message.

(c) **Text-in confirmation (double opt-in).** When a person texts Remote Leverage first, by keyword or by a free-form message, Remote Leverage may send a single reply that answers the person's inquiry and asks for consent. That reply states, in substance: "Remote Leverage: Thanks for your message. Reply YES to receive recurring automated texts from Remote Leverage at this number, including promotional offers and texts sent using an automated system. Consent is not a condition of purchase. Msg frequency varies. Msg & data rates may apply. Reply HELP for help, STOP to cancel. Terms and Privacy: https://remoteleverage.com/privacy-policy/". Until the person replies with an affirmative keyword, Remote Leverage sends only messages responsive to the person's own inquiry, which are Informational Messages, and sends no promotional content on the strength of the inbound text alone.

(d) **Effect of the affirmative reply or checkbox.** The person's affirmative reply under paragraph (b) or (c), or the checked box under paragraph (a), is the person's electronic signature under applicable electronic-signature law and constitutes the person's prior express written consent, within the meaning of 47 C.F.R. section 64.1200(f)(9) and

Fla. Stat. section 501.059(1)(g), to receive automated Promotional Messages and Informational Messages at that number.

(e) **Users' Account messages.** A User that provides a mobile number on Leve consents to receive Informational Messages about its Account and the Services, including automated messages, as Terms Section 17.5 provides. Remote Leverage does not send Promotional Messages to a User on that basis alone; it sends them only after consent given under paragraph (a), (b), or (c).

6C.4 Message frequency and message and data rates

Message frequency varies. Message and data rates may apply. Remote Leverage does not charge you for these messages, but your mobile carrier's standard message and data rates apply and Remote Leverage is not responsible for those charges.

6C.5 Consent records

Remote Leverage keeps a Consent Record for each number, including the telephone number; the channel of consent; the date and time; the disclosure text shown or sent; the checked box, the noted oral agreement and the affirmative reply, or the affirmative text reply; the IP address, form identifier, or message identifier; and each HELP request, opt-out, and opt-back-in, with its date, time, and channel. Consent Records are Leve Records, are retained as Section 1.8 provides and are used to evidence consent and opt-outs and to honor them.

6C.6 Help and customer care

Reply HELP to any message for help. You may also contact our customer care team at paula@remoteleverage.com or by phone at +1 (650) 668-0728.

6C.7 Opting out and revoking consent

Reply STOP to any message to cancel at any time. After you reply STOP, you will receive one final confirmation message and will not receive further messages from that program. Remote Leverage also treats the words QUIT, END, REVOKE, OPT OUT, CANCEL, and UNSUBSCRIBE, and any other reasonable means by which you clearly express a desire not to receive further messages, including a reply in another language, an email to paula@remoteleverage.com, or a call to +1 (650) 668-0728, as an opt-out. Remote Leverage does not designate an exclusive opt-out method. Remote Leverage honors each opt-out promptly and in any event within ten business days after receipt, or any shorter period that Applicable Data Protection Law requires. A revocation of consent to Promotional Messages applies to all Promotional Messages from Remote Leverage. An opt-out sent in response to an Informational Message ends the Program Messages from that program, other than the single confirmation message, and Remote Leverage does not send Promotional Messages after any opt-out unless the person later opts back in. To resume messages, reply START or opt in again through Leve.

6C.8 Time-of-day and frequency limits

Remote Leverage sends Promotional Messages only between 8:00 a.m. and 8:00 p.m. in the recipient's local time, or any narrower window that applicable law sets. For recipients in Colombia, Remote Leverage sends Promotional Messages only from Monday to Friday between 7:00 a.m. and 7:00 p.m. and on Saturday between 8:00 a.m. and 3:00 p.m., and not on Sundays or public holidays, consistently with Ley 2300 de 2023. Remote Leverage does not send more than three Promotional Messages on the same subject to the same number in any 24-hour period. Where a recipient's time zone cannot be determined reliably, Remote Leverage applies the window that is most restrictive for the time zones associated with the number's area code and any address on record.

6C.9 Changed or reassigned phone numbers

If your mobile phone number changes or is reassigned to another person, you will not be held liable or responsible for any messages sent to that number, and your failure to notify us of the change will not constitute a breach of the Terms or of this Privacy Agreement or a waiver of any of your rights. You may notify us at

paula@remoteleverage.com so that we can update our records, but you are under no obligation to do so. Remote Leverage may query the Reassigned Numbers Database established by the Federal Communications Commission, as 47 C.F.R. section 64.1200(m) contemplates, and stops messaging a number that the database reports as permanently disconnected since consent was given.

6C.10 Delivery and supported devices

Delivery of messages is subject to effective transmission by your mobile carrier, and carriers are not liable for delayed or undelivered messages. Not all mobile devices or carriers support RCS; where RCS is unavailable, messages may be delivered as SMS or MMS. Program Messages are delivered through messaging service providers and carriers that act on Remote Leverage's behalf and are identified on the Subprocessor Page.

6C.11 Eligibility

You must be at least 18 years of age and the authorized subscriber or customary user of the mobile phone number you provide.

6C.12 Privacy

Information collected in connection with this messaging program is handled in accordance with this Privacy Agreement, published at https://remoteleverage.com/privacy-policy/, including the categories, purposes, and retention described in Sections 1.2(Z), 1.3, and 1.8. Mobile phone numbers and messaging consent are not sold, rented, or shared with third parties or Affiliates for marketing purposes. Text messaging originator opt-in data and consent are not shared with any third party, except the messaging service providers and carriers that deliver Program Messages on Remote Leverage's behalf, and as law requires.

6C.13 Compliance with telephone and messaging laws

Remote Leverage operates the SMS/RCS Program in accordance with the Telephone Consumer Protection Act, 47 U.S.C. section 227, and 47 C.F.R. section 64.1200, including the revocation-of-consent rules in effect from time to time; the state telephone-solicitation and messaging laws that apply to it; the CTIA Messaging Principles and Best Practices; and the requirements of mobile carriers and their registration systems for application-to-person messaging.

6C.14 Recipients outside the United States

Remote Leverage sends Promotional Messages to a mobile number outside the United States only where the consent obtained, the content, the timing, and any do-not-contact registry check satisfy the law of the recipient's country, including, where applicable, the authorization requirements of Colombia's Ley Estatutaria 1581 de 2012 and the contact rules of Ley 2300 de 2023, Mexico's Registro Público para Evitar Publicidad, and Argentina's Registro Nacional No Llame under Ley 26.951. Informational Messages to recipients outside the United States are sent on the basis described in the applicable Annex.

SECTION 7. INTERNATIONAL DATA TRANSFERS

7.1 Data flows and mechanisms

Remote Leverage receives Personal Data from Placement Candidates and Contractor Users located principally in the Americas (Canada, the United States, Mexico, Central America, South America, and the Caribbean) and, from time to time, in other regions, including Europe and Asia-Pacific, and transfers it to infrastructure in the United States and in the other countries where its Subprocessors operate, as listed in Annex G, to Payment Partners, and to Clients, which are principally located in the United States. Personal Data that Remote Leverage collects directly from a data subject located abroad is Processed under the law that applies to that collection, and where that law

treats the movement of the data to Remote Leverage or onward as a transfer, the transfer is subject to the mechanism required by the origin country's Applicable Data Protection Law:

(a) **United States.** Transfers of Personal Data between Remote Leverage and Clients within the United States are not restricted under United States federal law. Such transfers remain subject to applicable United States state privacy laws as set out in Annex B.

(b) **Canada.** For Personal Data originating in Canada, Remote Leverage relies on contractual safeguards ensuring comparable protection consistent with PIPEDA and, where applicable, Quebec Law 25, as set out in Annex C.

(c) **Mexico and Latin America.** For Personal Data originating in Mexico and Latin American countries, Remote Leverage relies on:

(i) the data subject's authorization where that country's data protection law requires it (for example, the Colombian autorización and the Argentine consentimiento), obtained under Section 0.4A, or another transfer basis that law provides, such as the standard contractual clauses of the Brazilian Agência Nacional de Proteção de Dados, the model contractual clauses of the Ibero-American Data Protection Network that the competent authority has approved, a transmission contract with a processor, or the necessity of the transfer for a contract with the data subject;

(ii) contractual safeguards (data processing terms, confidentiality, and security requirements set out in this Privacy Agreement and Annex G); and

(iii) where the country's law requires it, notice to or authorization from the competent data-protection authority before transfer, and supplementary measures (for example, a transfer impact assessment or data protection impact assessment).

(d) **European Economic Area, United Kingdom, and Switzerland.** For Personal Data originating in the European Economic Area, the United Kingdom, or Switzerland, Remote Leverage relies on the mechanisms in Annex A.

(e) **All other transfers.** For Personal Data originating in any other jurisdiction, and as a general rule for every transfer under this Section, Remote Leverage relies on the first of the following mechanisms that is available and sufficient under the origin country's Applicable Data Protection Law: (i) an adequacy decision, list of adequate countries, or equivalent finding for the destination country or recipient, including, for a recipient certified under it, the Data Privacy Framework; (ii) Standard Contractual Clauses; (iii) the binding contractual safeguards in this Privacy Agreement and in Remote Leverage's agreements with Clients and Subprocessors; (iv) the data subject's authorization or consent to the transfer, obtained under Section 0.4A; (v) the necessity of the transfer for the performance of a contract with, or in the interest of, the data subject, or for pre-contractual steps taken at the data subject's request; (vi) the necessity of the transfer for the establishment, exercise, or defence of legal claims; and (vii) any other mechanism that the origin country's Applicable Data Protection Law recognizes, together with any notice to or authorization by the competent authority, transfer impact assessment, and supplementary measures that it requires.

7.2 Contractual safeguards

For all transfers under Section 7.1(b) to (e), Remote Leverage imposes data-protection obligations on the recipient (including Clients, through the Terms and this Privacy Agreement) no less protective than those in this Privacy Agreement, covering confidentiality, security, data-subject rights, breach notification, and compliance with Applicable Data Protection Law. Payment Partners receive Personal Data subject to their own legal obligations and privacy notices as independent controllers, as Section 6B.1 describes.

7.3 Controller responsibility (Managed: Contractor of Record Services)

For Processing under Section 5A, Remote Leverage is responsible for ensuring that transfers of COR Contractor data from Remote Leverage's receipt into the United States comply with this Section 7. The COR Client is responsible for compliance with its own transfer obligations regarding any onward transfers it undertakes, including exports of

Messages and Work-Verification Data. The parties cooperate to maintain valid transfer mechanisms for COR Contractor data.

7.4 Transfer documentation

Remote Leverage maintains documentation demonstrating compliance with this Section 7 (including transfer mechanism selections, authorization copies, and transfer impact assessments where required). Upon request, and subject to reasonable notice and confidentiality restrictions, Remote Leverage will provide information to the Client or a Supervisory Authority demonstrating that transfers comply with Applicable Data Protection Law.

SECTION 8. DATA-SUBJECT RIGHTS MECHANICS

We accept requests by email to privacy@remoteleverage.com and through any request functionality made available on Leve. We verify the requester's identity proportionately, acknowledge and respond within the timeline each regime sets, and, where we cannot fulfill a request, explain why and how to appeal or complain. We keep records of requests and responses. Regime-specific rights and timelines are in the Annexes; where multiple regimes apply to one data subject, we apply the most protective right and shortest reasonable timeline.

Channels by role. Placement Candidates, Contractor Users, Authorized Users, Account Administrators, Visitors, and Prospects may use privacy@remoteleverage.com for any request, and Users may also use the request functionality on Leve and, for routine corrections, the profile and Account settings described in Terms Section 7.6. A COR Contractor may direct a request to Remote Leverage as the primary point of contact under Section 5A.2, even where it concerns Processing by the COR Client. A Direct Contractor's request about Processing that the Direct Pay Client controls is handled as described below under "Requests concerning Client-controlled data." Participants in the SMS/RCS Program may also opt out as Section 6C.7 describes, and Visitors may manage Tracking Technologies as Annex H describes.

Authorized agents. Where Applicable Data Protection Law permits a request through an authorized agent, we may require the agent to provide signed written permission from the data subject or a valid power of attorney, and may require the data subject to verify his or her identity directly with us.

Appeals. Where a regime provides a right to appeal, a data subject may appeal our decision on a request by replying to it or by writing to privacy@remoteleverage.com with the subject "Privacy Request Appeal" within a reasonable period after receiving it. We respond within the period the regime sets and, if we deny the appeal, explain how to contact the competent authority, such as a state Attorney General.

Requests concerning Client-controlled data. Where a request concerns Personal Data that Remote Leverage Processes as processor for a Client, including in the Self Serve: Direct Pay Services, or Messages or Work-Verification Data that a Client has exported, we may refer the request to the Client and assist it under Section 5.6, and we tell the requester that we have done so.

Limits. To the extent Applicable Data Protection Law permits, we may decline, or charge a reasonable fee for, requests that are manifestly unfounded or excessive, and may restrict a response where necessary to protect the rights of others, including the content of other participants' Messages, to comply with law, or to establish, exercise, or defend legal claims.

SECTION 9. SECURITY

We maintain an information-security program with technical and organizational measures appropriate to the risk, addressing access control and authorization management, encryption in transit and at rest for appropriate data, network and endpoint security, logging and monitoring of security events, secure development and change management, vendor review, personnel confidentiality, backup and resilience, and incident response, and we take reasonable measures to protect and secure Personal Data in electronic form. A current summary is in Annex G.

When records containing Personal Data are no longer to be retained, we dispose of them, or arrange for their disposal, by shredding, erasing, or otherwise modifying the Personal Data to make it unreadable or undecipherable. No method of transmission over the internet or of electronic storage is completely secure, and we cannot guarantee absolute security. Users are responsible for keeping their credentials confidential, for using multi-factor authentication where offered, for the security of their own devices and networks, and for promptly reporting any suspected unauthorized access to their Account to security@remoteleverage.com or the Support Email, as Terms Section 7.4 provides.

SECTION 10. PERSONAL DATA BREACH RESPONSE

We assess Security Incidents and notify Personal Data Breaches as follows. Where we are controller or joint controller, we assess each incident against each applicable regime's threshold and notify the competent authority and affected individuals within the required timelines, including without limitation: without undue delay and, where feasible, within 72 hours of awareness under the European Union and United Kingdom GDPR and under regimes that adopt the same window; within the timelines set by United States state breach-notification statutes; and within the timelines set by the other applicable regimes named in the Annexes. Where we are processor, we notify the controller without undue delay under Section 5.7. Security Incidents that do not amount to a Personal Data Breach are investigated and documented but are not notified.

SECTION 11. RECORDS OF PROCESSING AND GOVERNANCE

We maintain records of Processing activities as required, conduct data protection impact assessments for high-risk Processing, including monitoring and work verification and Client access to Messages, where required by Applicable Data Protection Law, appoint a Data Protection Officer and Article 27 or equivalent representatives and publish or provide their contact details as that law requires, conduct the risk assessments that United States state privacy laws require maintain the controller-arrangement and processor documentation required by Sections 5 and 5A, and maintain the governance needed to demonstrate accountability.

SECTION 11A. ARTIFICIAL INTELLIGENCE AND AUTOMATED DECISION TOOLS

11A.1 Use of automated tools

Remote Leverage may use automated tools, including tools that use machine learning or artificial intelligence, to help source, parse, match, rank, and assess Placement Candidates, to verify identity, and to detect fraud and falsification, as Terms Section 8.2 describes. Automated outputs assist the people who make decisions and do not replace them. Where a decision that produces legal or similarly significant effects would be based solely on automated Processing, Remote Leverage provides human review on request and the other safeguards described in Section 1.11. This includes the Talent Marketplace search and ordering function described in Section 1.11 and the automated Processing of Video Introductions permitted by Section 1.9B(d).

11A.2 Notice and jurisdiction-specific requirements

Where Applicable Data Protection Law or another law requires it, Remote Leverage, or the Client where the Client makes the relevant decision, gives prior notice of the use of automated decision tools, explains their role, and provides any required means to request human review, an alternative process, or reasonable accommodation. This includes, where they apply, the bias-audit, notice, opt-out, explanation, correction, appeal, and human-review requirements of state and local laws on automated decision tools and on the use of artificial intelligence in hiring and engagement decisions. Any obligation those laws place on the person making the decision rests on the Client where the Client makes it. It also includes, where they apply, the Illinois Artificial Intelligence Video Interview Act, 820 ILCS 42, and Section 3-717 of the Labor and Employment Article of the Annotated Code of Maryland, as Section 1.9B(i) describes.

11A.3 Non-discrimination

Automated tools may not be configured or used, by Remote Leverage or by a Client, to make or support decisions on the basis of characteristics protected by applicable anti-discrimination law, or of proxies for them such as postal codes, and a Client must not instruct Remote Leverage, or use Leve outputs, to do so, as Terms Sections 8.2 and 19(g) provide. No Marketplace Viewer may search for, filter, or select Placement Candidates by a protected characteristic or an evident proxy for one, including the appearance or voice of a Placement Candidate in a Video Introduction.

11A.4 Client decisions

Where a Client uses Leve outputs to make its own selection, engagement, or termination decisions, the Client is responsible for those decisions and for compliance with the laws that govern them, including any notice, audit, accommodation, and record-keeping obligations that apply to the Client as the engaging party.

11A.5 Third-party artificial-intelligence services

Where Remote Leverage uses a third-party artificial-intelligence service to Process Personal Data, the provider acts as a Subprocessor or service provider, is listed on the Subprocessor Page when engaged, and is engaged on terms that limit its use of that Personal Data to providing the service and prohibit it from using the Personal Data to train or improve its own models.

11A.6 Use of Personal Data to improve tools and models

Remote Leverage may use Personal Data that it controls, and De-Identified Data, to evaluate and improve the tools and models it uses to operate the Services, subject to Section 1.4 and any opt-in, opt-out, or objection right that Applicable Data Protection Law provides. Remote Leverage does not use the content of Messages, Work-Verification Data screenshots, identity documents, biometric data, or taxpayer identification numbers to train artificial-intelligence models, and uses Client Personal Data to improve tools and models only to the extent Section 5 and Applicable Data Protection Law permit a processor or service provider to do so. Users must not enter Regulated Data or Sensitive Personal Data into any automated feature not designated for it, as Terms Section 8.2 provides. Remote Leverage does not use Video Introductions, or the image or voice they contain, to train artificial-intelligence models, and uses transcripts generated from them for that purpose only as De-Identified Data under Section 4.2.

SECTION 12. GENERAL

Severability and read-down apply per Section 4.3. Provisions that by their nature should survive termination survive, including confidentiality, data-protection, and liability terms. This Privacy Agreement does not create an attorney-client relationship with any User and is not legal advice to any person, consistently with Terms Section 6. Contact: privacy@remoteleverage.com.

Limitation of liability. To the maximum extent permitted by law, Remote Leverage's aggregate liability arising out of or in connection with this Privacy Agreement, whether in contract, tort, or otherwise, is subject to the limitations and exclusions of liability in Terms Section 26 and, for claims within its scope, the COR MSA, and Remote Leverage is not liable for any indirect, incidental, special, consequential, exemplary, or punitive damages, or for loss of profits, revenue, goodwill, or data, except to the extent a signed Commercial Agreement expressly provides otherwise. To the extent permitted by law, Remote Leverage is not liable for the acts or omissions of third parties it has not engaged, for integrations, onward transfers, exports, or services that a User selects or directs, or for a Security Incident that occurs despite Remote Leverage's maintenance of the measures described in Section 9. Nothing in this Privacy Agreement limits liability that cannot be limited under applicable law, including liability to a data subject that Applicable Data Protection Law does not permit to be excluded.

User responsibilities. Each User must provide accurate and current Personal Data and keep it updated, as Terms Section 7.1 provides; keep Account credentials, one-time passcodes, and trusted devices secure and not share them; provide Personal Data of third parties, such as Client personnel, emergency contacts, and references, only where the User has the right to do so and has informed them as Applicable Data Protection Law requires; and not upload Sensitive Personal Data or Regulated Data that the Services do not require.

Suspension. Where a User withdraws an authorization or consent, objects to Processing, or requests restriction or deletion of Personal Data that is necessary to provide a Service, Remote Leverage may suspend or end the affected Service, without liability to the extent permitted by law, and Processing necessary to comply with law or to establish, exercise, or defend legal claims continues.

Legal requests and legal holds. Remote Leverage may preserve and disclose Personal Data where it believes in good faith that doing so is required by law, regulation, legal process, or an enforceable governmental request, or is necessary to protect the rights, property, or safety of Remote Leverage, its Users, or others, and may suspend deletion of Personal Data that is subject to a legal hold. Where legally permitted and reasonably practicable, Remote Leverage informs the affected Client before disclosing Client Personal Data in response to a governmental request.

Business transfers. Personal Data may be disclosed and transferred, subject to appropriate confidentiality protections, in connection with an actual or proposed merger, acquisition, financing, reorganization, sale of all or part of Remote Leverage's business or assets, or insolvency or similar proceeding, and the successor may continue to Process it in accordance with this Privacy Agreement.

Third-party sites and integrations. Leve may contain links to, or integrations with, third-party websites, products, and services, including Payment Partners and integrations that a Client enables. Their Processing is governed by their own terms and privacy notices, and Remote Leverage is not responsible for them, except to the extent this Privacy Agreement makes Remote Leverage responsible for a Subprocessor it engaged, as Terms Section 23 provides.

Language. This Privacy Agreement is written in English, and the English version governs, consistently with Terms Section 17.5. Any translation is provided for convenience, except where applicable law makes a local-language version mandatory or binding, in which case that version governs to the extent the law requires.

Third-party beneficiaries. No person other than Remote Leverage, the Remote Leverage Parties, and the Users who accept this Privacy Agreement has any right to enforce it, except that data subjects may enforce the provisions that Applicable Data Protection Law requires to be enforceable by them, including as third-party beneficiaries of Standard Contractual Clauses incorporated under Section 7.

ANNEX A. EUROPEAN ECONOMIC AREA, UNITED KINGDOM, AND SWITZERLAND

Applicability. This Annex applies to the Personal Data of data subjects located in the European Economic Area, the United Kingdom, or Switzerland, including Placement Candidates and Contractor Users engaged or monitored there, to the extent the GDPR, the UK GDPR and the Data Protection Act 2018 (as amended by the Data (Use and Access) Act 2025), or the Swiss Federal Act on Data Protection applies to the Processing, including where Remote Leverage offers Services to, or monitors the behaviour of, those data subjects. References in this Annex to the GDPR include the UK GDPR and, with the necessary adaptations, the Swiss Federal Act on Data Protection.

Controller and representative. The controller is Remote Leverage, which has no establishment in the European Economic Area, the United Kingdom, or Switzerland. The Services are directed principally to Clients in the United States and to Placement Candidates and Contractor Users in the Americas and Asia-Pacific, so these laws apply to Remote Leverage only where it offers the Services to, or monitors the behaviour of, a data subject located in those territories (Article 3(2) GDPR). That Processing is occasional, does not include large-scale Processing of special categories of data, and is unlikely to result in a risk to data subjects, so Remote Leverage has not designated a representative under Article 27(2)(a) of the GDPR or of the UK GDPR, or under Article 14 of the Swiss Federal Act

on Data Protection, and is not required to appoint a Data Protection Officer under Article 37. Remote Leverage reviews this position at least once a year and will designate a representative, and publish the representative's details on the Published Page, if it begins to direct the Services to those territories or to engage Contractor Users located there on a regular basis. Data subjects and Supervisory Authorities may contact Remote Leverage at privacy@remoteleverage.com.

Information provided under Articles 13 and 14. The information that Articles 13 and 14 require is in Section 0.1 (controller and contact), Sections 1.2 and 1.3 (categories, sources, and purposes), Section 1.5 and this Annex (legal bases and legitimate interests), Section 1.6 (recipients), Section 7 and this Annex (transfers and safeguards; a copy of the safeguard is available from privacy@remoteleverage.com), Section 1.8 (retention), Sections 1.11 and 11A (automated decision-making), and Sections 1.12 and 1.13 and this Annex (rights and complaints). Providing the Personal Data that Leve marks as required is a contractual requirement and a condition of the Service concerned, and Remote Leverage cannot provide that Service without it; tax and identity data is also a statutory requirement where Remote Leverage is the payer or must screen for sanctions. All other Personal Data is optional.

Legal bases. Remote Leverage relies on: performance of a contract or pre-contractual steps; compliance with a legal obligation; and legitimate interests, including the operation, security, and improvement of the Services, fraud and falsification prevention, proportionate monitoring and work verification under Section 6, and access to Messages under Section 6A. For special categories of Personal Data, Remote Leverage relies on an applicable Article 9 condition, including explicit consent where that is the applicable condition and the establishment, exercise, or defence of legal claims. Remote Leverage does not rely on the consent of Placement Candidates or Contractor Users as the basis for core Processing, for monitoring, or for access to Messages, as Sections 0.4A, 6.2, and 6A.10 explain. Non-essential Tracking Technologies are set only with prior consent, as Annex H describes. Where Remote Leverage relies on consent for data subjects in these territories, namely for non-essential Tracking Technologies, direct marketing, the Personal-Device Consent, biometric verification, and the Marketplace Display and Likeness Authorization, each is named separately in the acceptance box and in Section 0.4A and can be withdrawn at any time, with the consequences that Section 0.4A describes. Biometric verification is a condition of the Services, and the Marketplace Display and Likeness Authorization is a condition of the Talent Marketplace, because confirming that each Placement Candidate and Contractor User is the person shown in his or her identity document and video is necessary to prevent impersonation and identity fraud in a remote service.

Data-subject rights. Data subjects may exercise the rights of access, rectification, erasure, restriction, objection, portability, and, where applicable, the right not to be subject to a solely automated decision producing legal or similarly significant effects. Requests are made to privacy@remoteleverage.com and are answered without undue delay and within one month, extendable by two further months for complex or numerous requests. Data subjects in the United Kingdom may first raise a complaint with Remote Leverage at privacy@remoteleverage.com, which Remote Leverage acknowledges within 30 days and answers without undue delay; this does not affect the right to complain to the Information Commissioner. Data subjects may lodge a complaint with the supervisory authority of their habitual residence, place of work, or place of the alleged infringement in the European Economic Area, with the Information Commissioner's Office in the United Kingdom, or with the Federal Data Protection and Information Commissioner in Switzerland.

International transfers. Remote Leverage's collection of Personal Data directly from a data subject in the European Economic Area, the United Kingdom, or Switzerland is not a transfer under Chapter V of the GDPR, consistently with the European Data Protection Board's Guidelines 05/2021, and Remote Leverage applies this Privacy Agreement to that data. Where Remote Leverage receives Personal Data from an exporter in those territories, such as a Client established there for which it acts as processor under Section 5, or makes an onward transfer, it relies, in this order, on an adequacy decision (including the Data Privacy Framework for a certified recipient), on the Standard Contractual Clauses with the UK Addendum or Swiss adaptations as Section 5.10 provides, or on a derogation under Article 49, such as the necessity of the transfer for a contract with the data subject, together with a transfer impact assessment where required. Remote Leverage is not itself certified under the Data Privacy Framework.

ANNEX B. UNITED STATES (FEDERAL AND STATE)

Applicability. This Annex applies to United States residents whose Personal Data Remote Leverage Processes, including Authorized Users and Account Administrators, Visitors, Prospects, and Placement Candidates and Contractor Users resident in the United States. It reflects the comprehensive state privacy laws in effect and the applicable federal sectoral laws.

Comprehensive state laws. Remote Leverage Processes Personal Data consistently with the comprehensive state privacy laws in effect from time to time, to the extent each applies to Remote Leverage. California is the only one of these states whose law extends to individuals acting as job applicants, independent contractors, or business contacts; the other states' laws exclude individuals acting in a commercial or employment context. To the extent the California law applies to Remote Leverage, it therefore governs Personal Data of Placement Candidates, Contractor Users, Authorized Users, and business contacts resident in California, while the other states' laws apply principally to Visitors and Prospects acting in a personal capacity. Puerto Rico and other United States territories are Processed under applicable federal and local law.

Notice at collection. At or before collection, Remote Leverage discloses the categories of Personal Information and of sensitive Personal Information collected, the purposes of use, whether the information is sold or shared, the categories of sources and of recipients, and the retention period or the criteria used to set it, through this Privacy Agreement and the notices on Leve that link to it.

Consumer rights. Subject to the applicable state law, residents may request to know and access their Personal Information, to correct it, to delete it, and to obtain a portable copy; may opt out of the sale or sharing of Personal Information and of targeted advertising; may limit the use and disclosure of sensitive Personal Information; and, where the state law provides, may exercise rights regarding profiling and automated decision-making. Remote Leverage treats a Global Privacy Control signal, and any other universal opt-out mechanism that a state law recognizes, as a valid request to opt out of sale, sharing, and targeted advertising for the browser or device that sends it, for every United States Visitor and User, including in the states whose laws require it, as Annex H describes. Remote Leverage does not discriminate against a consumer for exercising a right. Requests are made to privacy@remoteleverage.com or through any request functionality made available on Leve and are verified and answered within the statutory period. Residents may use an authorized agent and may appeal a decision on a request as described in Section 8. Complaints may be directed to the California Privacy Protection Agency, the Attorney General of the resident's state, or the Federal Trade Commission.

Sale and sharing. Remote Leverage does not sell Personal Information for monetary consideration. Where any disclosure, including through advertising Tracking Technologies, constitutes a sale or sharing under a state law, Remote Leverage provides and honors the required opt-out, including through the "Your Privacy Choices" link and the preference center described in Annex H.

Sensitive Personal Information. Use and disclosure of sensitive Personal Information, including precise geolocation, government identifiers, financial account information, and biometric information, are limited to the purposes the applicable state law permits, and the limitation right is honored.

Background checks. Remote Leverage does not run criminal background checks unless agreed in a signed writing, as Terms Section 13.3 provides. Where an Engagement or placement involves a consumer report, the person that procures the report, whether Remote Leverage or the Client, complies with the federal Fair Credit Reporting Act and stricter state analogs, including a clear and conspicuous written disclosure, made before the report is procured in a document that consists solely of the disclosure, the consumer's written authorization, which may be given on that document, and the pre-adverse-action and adverse-action process. Whether the employment-purpose provisions of that Act apply to independent contractors is unsettled, and they are followed where a consumer report is obtained in connection with an Engagement or placement; doing so does not imply that any person is an employee.

Biometric information. Where biometric identifiers are Processed, Remote Leverage complies with applicable state biometric laws, including the Illinois Biometric Information Privacy Act, the Texas Capture or Use of Biometric

Identifier Act, and the Washington biometric statute, including informed written consent, a public retention and destruction schedule, and the prohibition on sale where those laws apply. The retention and destruction schedule is in Section 1.9A.

Talent Marketplace, likeness, and video. Remote Leverage displays a Placement Candidate's name, image, or likeness in the Talent Marketplace only on the express consent in Section 0.4A(i), consistently with Section 540.08 of the Florida Statutes and comparable state right-of-publicity laws. Video Introductions are not used to create biometric identifiers or biometric information within the meaning of the Illinois Biometric Information Privacy Act, 740 ILCS 14/10, or comparable state laws, as Section 1.9B(d) provides. Remote Leverage is not engaged in the business of renting, selling, or delivering prerecorded audiovisual material within the meaning of the Video Privacy Protection Act, 18 U.S.C. section 2710, and in any event does not disclose to any third party information identifying a Marketplace Viewer as having requested or obtained a specific Video Introduction, as Section 1.9B(h) provides. For Placement Candidates resident in California, the notice at collection for Video Introductions is the notice described in Section 1.9B(c).

Communications and marketing. Remote Leverage complies with the CAN-SPAM Act for commercial email, and with the Telephone Consumer Protection Act and other applicable state telephone-solicitation and messaging laws for calls and text messages, as Section 6C describes.

California Shine the Light, Nevada, and recording. Remote Leverage does not disclose Personal Information to third parties for their own direct-marketing purposes within the meaning of California Civil Code section 1798.83. Remote Leverage does not sell covered information as defined in Nevada Revised Statutes section 603A.333, and Nevada residents may nonetheless submit a request under section 603A.345 to privacy@remoteleverage.com. Where an all-party-consent law applies, Messages and calls are accessed and recorded only as described in Section 6A, and session replay and chat Tracking Technologies are used only as described in Annex H.

Children and countries of concern. Leve is limited to Users who are 18 or older, and Remote Leverage does not knowingly collect Personal Information from children under 13 within the meaning of the Children’s Online Privacy Protection Act. Remote Leverage does not engage in data brokerage of bulk United States sensitive personal data or government-related data with a country of concern or covered person within the meaning of 28 C.F.R. Part 202, and Sections 3.4 and 6B.3 address access by covered persons.

ANNEX C. CANADA (FEDERAL AND PROVINCIAL)

Applicability. This Annex applies to Personal Data of individuals in Canada, including Placement Candidates and Contractor Users located there. Remote Leverage complies with the federal Personal Information Protection and Electronic Documents Act for commercial activity across provincial or national borders, and with the substantially similar private-sector laws of Quebec, Alberta, and British Columbia for individuals in those provinces.

Accountability and purposes. Remote Leverage identifies the purposes for collection at or before the time of collection, limits collection, use, disclosure, and retention to those purposes and to what a reasonable person would consider appropriate in the circumstances, and is accountable for Personal Data in its custody, including data transferred to service providers for Processing.

Consent and other bases. Remote Leverage obtains meaningful consent where the law requires it, and otherwise relies on the permitted grounds for the collection, use, and disclosure of Personal Data, including the purposes reasonably necessary to establish, manage, or end an Engagement or placement. For sensitive information, including in Quebec, express consent is obtained where required. Commercial electronic messages are sent only as Canada’s Anti-Spam Legislation permits.

Quebec Law 25. For individuals in Quebec, Remote Leverage provides the transparency the Act respecting the protection of personal information in the private sector requires, including notice of the purposes, the categories of third parties, and any transfer outside Quebec, completes a privacy impact assessment before certain projects and transfers, provides notice where a decision is based exclusively on automated Processing, and honors the rights of

access, rectification, de-indexing, portability, and cessation of dissemination. Where that Act requires it, the title and contact information of the person in charge of the protection of personal information are published on the Published Page, and where the Charter of the French Language requires it, a French version of this Privacy Agreement is provided to persons in Quebec before acceptance.

Data-subject rights. Individuals may request access to and correction of their Personal Data, and, where applicable, portability, deletion, and withdrawal of consent. Requests are made to privacy@remoteleverage.com. Complaints may be brought to the Office of the Privacy Commissioner of Canada or, in Quebec, Alberta, or British Columbia, to the Commission d'accès à l'information du Québec or the provincial Information and Privacy Commissioner.

International transfers. Transfers to Remote Leverage in the United States and to service providers are made with comparable protection through contractual and organizational measures, and, in Quebec, following the required assessment.

ANNEX D. PHILIPPINES

This Annex applies to the Processing of Personal Data of data subjects in the Philippines, including Placement Candidates, Contractor Users, and Authorized Users located there, to the extent the Data Privacy Act of 2012 (Republic Act No. 10173), its Implementing Rules and Regulations, and the issuances of the National Privacy Commission apply, including under Section 6 of that Act where the Processing relates to a Philippine citizen or resident and Remote Leverage has a link with the Philippines; in this Annex, "personal information," "sensitive personal information," "personal information controller," and "personal information processor" have the meanings that Act gives them, and Remote Leverage is a personal information controller for the Processing it controls and a personal information processor where it acts under Section 5. Because that Act treats age, marital status, education, health, and government-issued identifiers as sensitive personal information, the dates of birth, education history, identity documents, and taxpayer identification numbers described in Section 1.2 are Processed only on a criterion in Section 13 of that Act, principally the data subject's consent specific to the purpose and given before the Processing, obtained under Sections 0.4A(b) and 0.4A(c) and given freely, specifically, and in an informed manner, evidenced by written, electronic, or recorded means and withdrawable as easily as given, consistently with NPC Circular No. 2023-04, or where a law provides for the Processing or it is necessary for the establishment, exercise, or defense of legal claims; other personal information is Processed on the criteria in Section 12 of that Act, namely contract, legal obligation, and legitimate interests, including for monitoring under Section 6 and access to Messages under Section 6A, applied proportionately and with the prior notice described in those Sections, and, because Republic Act No. 4200 prohibits recording a private communication without the authorization of all the parties, calls and meetings are recorded only after every participant has been notified and has authorized the recording under Sections 6A.5 and 6A.6, never covertly. Remote Leverage designates a Data Protection Officer, contactable at privacy@remoteleverage.com, and registers its Data Protection Officer and data processing systems with the National Privacy Commission where NPC Circular No. 2022-04 requires it; maintains the security measures that Section 20 of that Act and NPC Circular No. 2023-06 require and conducts privacy impact assessments where the Commission's issuances require them; notifies the Commission and affected data subjects within 72 hours of a personal data breach that Section 20(f) of that Act and NPC Circular No. 16-03 make notifiable, and submits the full report within five days unless the Commission grants more time, without treating any request for postponement as suspending those obligations; remains accountable under Section 21 of that Act for personal information transferred to third parties in or outside the Philippines, using this Privacy Agreement, its Subprocessor agreements, Section 5, and, where appropriate, the model contractual clauses that NPC Advisory No. 2024-01 recognizes to provide comparable protection; sends Promotional Messages to Philippine numbers only to persons who opted in under Section 6C.3, with sender identification and an opt-out, never between 9:00 p.m. and 7:00 a.m. Philippine time under National Telecommunications Commission Memorandum Circular No. 03-03-2005 and in any event within the window in Section 6C.8; and sets non-essential Tracking Technologies for Visitors in the Philippines only after consent through the cookie banner in Annex H. Data subjects in the Philippines have the rights in Sections 16 to 18 of that Act, including to be informed, to object (including to direct marketing), to access, to rectification, to erasure or blocking, to damages, and to portability, exercisable by their lawful heirs and assigns,

through privacy@remoteleverage.com or the request functionality on Leve, and may complain to the National Privacy Commission (https://privacy.gov.ph), which generally expects the data subject first to raise the concern with Remote Leverage in writing; nothing in the Terms or this Privacy Agreement limits those rights or the remedies the Act provides before Philippine courts.

ANNEX E. LATIN AMERICA

Applicability and scope. This Annex applies to Personal Data of data subjects located in the Latin American countries below, including Placement Candidates and Contractor Users engaged or monitored there. For each country, Remote Leverage provides notice and honors the rights set out for that country, and, where that country's law requires notice in a local language, makes a Spanish-language or, for Brazil, a Portuguese-language version of the applicable notice available. Where a country requires a prior, express authorization before Processing, that authorization is given through the authorizations in Section 0.4A. Countries of Latin America and the Caribbean that are not listed below are addressed in Annex F.

Shared rights and protections. In every country in this Annex, data subjects may exercise, at minimum, the rights to access their Personal Data, to rectify inaccurate or incomplete data, to request cancellation or deletion, to object to Processing, and to revoke any authorization given, together with any additional right the country's law confers. Requests are made to privacy@remoteleverage.com and through any request functionality made available on Leve. Sensitive Personal Data and the Personal Data of children and adolescents are Processed only on the heightened basis the country's law requires. International transfers of Personal Data to Remote Leverage in the United States and to service providers are made under the transfer basis the country's law provides, supported by contractual safeguards. The statements in the Terms about the absence of an expectation of privacy in monitored activity and in Messages do not limit the rights in this Annex, as Section 6A.10(f) provides.

Legal basis for Placement Candidate and Contractor User data. For the core Processing of Placement Candidate and Contractor User data, for monitoring, and for access to Messages, Remote Leverage relies on contractual necessity, legal obligation, and the legitimate or locally authorized interest basis where the country's law provides one, except where the country's law requires the data subject's authorization or consent for that Processing, in which case it is obtained under Section 0.4A, and otherwise reserves authorization for genuinely optional and separable Processing, in recognition of the power imbalance in the engagement relationship.

Image and voice. Several countries in this Annex protect a person's image and voice independently of data-protection law, including Article 53 of the Código Civil y Comercial de la Nación of Argentina, Article 20 of the Código Civil of Brazil, Article 87 of the Ley Federal del Derecho de Autor of Mexico, and the right to one's own image that the Constitutional Court of Colombia derives from the Constitution. Remote Leverage records, displays, and uses a Placement Candidate's image and voice in the Talent Marketplace only on the authorization in Section 0.4A(i), only for the purposes in Section 1.9B, and stops doing so on withdrawal. In Colombia, Marketplace Profiles are made available only under the access controls in Section 1.9B(c), consistently with the principle of restricted access and circulation in Article 4(f) of Ley Estatutaria 1581 de 2012. In Brazil, where Remote Leverage relies on legitimate interests for the display of Marketplace Profiles under the Lei Geral de Proteção de Dados Pessoais, it relies on the authorization in Section 0.4A(i) for the use of image under Article 20 of the Código Civil, and the Placement Candidate may oppose the display at any time under Section 1.9B(f).

E.1 Argentina

Governed by the Ley de Protección de los Datos Personales (Ley 25.326) and administered by the Agencia de Acceso a la Información Pública. Data subjects have the rights of information, access, rectification, update, and suppression of their Personal Data. Sensitive data is Processed only on the grounds the law permits. Complaints may be brought to the Agencia de Acceso a la Información Pública. Data subjects may exercise the right of access free of charge at intervals of not less than six months, unless a legitimate interest is shown, as provided in Article 14(3) of Ley 25.326. International transfers to countries that the Agencia has not recognized as providing adequate protection, including the United States, are made with the data subject's express consent under Section 0.4A,

under model contractual clauses approved by the Agencia, or under another exception the law provides. Promotional Messages are not sent to numbers registered in the Registro Nacional No Llame under Ley 26.951.

E.2 Brazil

Governed by the Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018) and administered by the Agência Nacional de Proteção de Dados (ANPD). Processing rests on a legal basis under Articles 7 and 11, including the performance of a contract, compliance with a legal obligation, the regular exercise of rights in judicial, administrative, or arbitral proceedings, and the legitimate interests of the controller, and Remote Leverage does not rely on the consent of Placement Candidates or Contractor Users for core Processing. Data subjects have the rights to confirmation and access, correction, anonymization, blocking or deletion of unnecessary or excessive data, portability, deletion of data Processed with consent, information about sharing and about the consequences of refusing consent, and revocation of consent. Notice and rights content is provided in Portuguese where required. International transfers rest on a mechanism in Article 33 of the LGPD and Resolution CD/ANPD No. 19/2024, including the standard contractual clauses adopted by the ANPD, which must be incorporated without alteration where they are the mechanism used, or the necessity of the transfer for the performance of a contract with the data subject, and the transfer information that the Resolution requires is made available. Collection of Personal Data directly from a data subject by Remote Leverage, as a foreign controller subject to the LGPD, is Processed under the LGPD whether or not it is also characterized as an international transfer. Complaints may be brought to the ANPD. Biometric identity verification rests on Article 11, II, g of the LGPD, for fraud prevention and the security of the data subject in identification and authentication processes, and not on consent.

E.3 Chile

Governed by Ley 19.628 on the protection of private life and, from the date on which Ley 21.719 enters into force, by Ley 19.628 as amended by Ley 21.719, under which the Agencia de Protección de Datos Personales is the supervisory authority. Until that date, Processing requires the data subject's authorization unless an exception applies, which Remote Leverage obtains under Section 0.4A, and data subjects may exercise their rights under Ley 19.628, including before the courts. From that date, Processing rests on a lawful basis, including the performance of a contract, compliance with a legal obligation, and the legitimate interests of the controller; data subjects have the rights of access, rectification, deletion or cancellation, objection, portability, and blocking, and rights in relation to automated decisions; sensitive data and the data of minors are Processed on the heightened basis the law requires; and complaints may be brought to the Agencia de Protección de Datos Personales.

E.4 Colombia

Governed by the Ley Estatutaria 1581 de 2012 and Decreto 1377 de 2013 (compiled in Decreto 1074 de 2015) and administered by the Superintendencia de Industria y Comercio. This Privacy Agreement is Remote Leverage's personal data processing policy (política de tratamiento de la información) for data subjects in Colombia. Processing of Personal Data requires the prior, express, and informed authorization of the data subject, given through the authorizations in Section 0.4A by checking the acceptance box in Section 0.4, a means that can be consulted later, as Ley Estatutaria 1581 de 2012 and Decreto 1377 de 2013 permit, except where the law permits Processing without authorization. The purposes of Processing are those in Sections 1.3, 6.1, 6A.2, and 6A.3. Data subjects have the rights to know, update, and rectify their data, to request proof of the authorization, to be informed of the use of their data, to lodge complaints, to revoke the authorization, and to request deletion where Processing does not respect constitutional and legal principles. Inquiries (consultas) are answered within ten business days after receipt, extendable once by up to five business days with notice of the reason, and claims (reclamos) within fifteen business days after receipt, extendable once by up to eight business days with notice of the reason, as Articles 14 and 15 of Ley 1581 de 2012 provide; both are submitted to privacy@remoteleverage.com, which is the channel responsible for attending them. Sensitive data is Processed only with explicit authorization and on the grounds the law permits, and no data subject is obliged to authorize the Processing of sensitive data. Complaints may be brought to the Superintendencia de Industria y Comercio after the claim procedure with Remote Leverage has been exhausted. International transfers to the United States are made to a country that the Superintendencia de Industria y Comercio lists as providing an adequate level of protection,

and are also covered by the data subject's express authorization; transmissions to processors (encargados) outside Colombia are covered by a transmission contract or by the data subject's authorization, and Remote Leverage may also use the model contractual clauses of the Ibero-American Data Protection Network that the Superintendencia has approved as an optional mechanism. Promotional Messages to recipients in Colombia observe the contact rules of Ley 2300 de 2023, as Section 6C.8 provides.

E.5 Costa Rica

Governed by the Ley de Protección de la Persona frente al tratamiento de sus datos personales (Ley 8968) and administered by the Agencia de Protección de Datos de los Habitantes. Data subjects have the rights of access, rectification, deletion, and objection, and the right to informational self-determination. Sensitive data is Processed only on the grounds the law permits. Complaints may be brought to the Agencia de Protección de Datos de los Habitantes. Transfers of Personal Data rest on the data subject's informed consent, obtained under Section 0.4A, or on another ground the law permits.

E.6 Dominican Republic

Governed by the Ley Orgánica sobre Protección de Datos de Carácter Personal (Ley 172-13) and the constitutional guarantee of habeas data. Data subjects have the rights of access, rectification, cancellation, and objection. Sensitive data is Processed only on the grounds the law permits. Data subjects may seek relief through the habeas data guarantee and the competent authority.

E.7 Ecuador

Governed by the Ley Orgánica de Protección de Datos Personales and its General Regulation and administered by the Superintendencia de Protección de Datos Personales. Processing rests on a lawful basis, including the performance of a contract, compliance with a legal obligation, and the legitimate interests of the controller. Data subjects have the rights of information, access, rectification and update, deletion, opposition, portability, and the right not to be subject to automated decisions, and the right to suspend Processing. Complaints may be brought to the Superintendencia de Protección de Datos Personales. International transfers to countries that the Superintendencia has not declared adequate rest on the safeguards it recognizes, including the model clauses of the Ibero-American Data Protection Network, or on another mechanism that the Ley Orgánica and the Superintendencia's transfer rules recognize.

E.8 El Salvador

Governed by the Ley para la Protección de Datos Personales (Decreto Legislativo 144 of 2024, in force since November 2024) and administered by the Agencia de Ciberseguridad del Estado. Processing rests on the data subject's free, specific, informed, and express consent, obtained under Section 0.4A, or on another ground the law permits, and international transfers require the data subject's prior authorization and a contract that guarantees equivalent protection. Data subjects have the rights of access, rectification, cancellation or deletion, objection, and portability. Sensitive data and the data of minors are Processed on the heightened basis the law requires. Complaints may be brought to the Agencia de Ciberseguridad del Estado.

E.9 Mexico

Governed by the Ley Federal de Protección de Datos Personales en Posesión de los Particulares published on March 20, 2025, which replaced the 2010 law, and administered by the Secretaría Anticorrupción y Buen Gobierno, which assumed the functions of the dissolved Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Remote Leverage provides a privacy notice, in comprehensive and simplified forms, that identifies any sensitive data and distinguishes the purposes that require consent from those that do not, and Processes Personal Data on the principles and grounds the law establishes. Data subjects have the rights of access, rectification (including of outdated data), cancellation, and opposition, which must be exercised by indicating the specific right or request, the right to revoke consent, and the right to object to Processing that produces adverse legal effects or significantly affects their rights or freedoms through solely automated means. Sensitive data is

Processed only with the express consent the law requires. Transfers to Clients and other third parties rest on consent under Section 0.4A or on an exception the law provides, such as the necessity of the transfer for a contract in the data subject's interest, and communications to processors do not require consent. Promotional Messages are not sent to numbers registered in the Registro Público para Evitar Publicidad. Complaints may be brought to the Secretaría Anticorrupción y Buen Gobierno.

E.10 Panama

Governed by the Ley 81 de 2019 on the protection of Personal Data and administered by the Autoridad Nacional de Transparencia y Acceso a la Información. Data subjects have the rights of access, rectification, cancellation, opposition, and portability. Sensitive data and the data of minors are Processed on the heightened basis the law requires. Complaints may be brought to the Autoridad Nacional de Transparencia y Acceso a la Información.

E.11 Paraguay

Governed by the Ley de Protección de Datos Personales (Ley 7593/2025), promulgated on November 27, 2025, whose obligations apply from the end of its transition period, expected in November 2027; until then, the constitutional guarantee of habeas data and applicable sectoral rules apply. From that date, Processing rests on a lawful basis, including the performance of a contract, compliance with a legal obligation, and the legitimate interests of the controller. Data subjects have the rights of access, rectification, deletion, objection, and portability, and rights in relation to automated decisions. Sensitive data and the data of children and adolescents are Processed on the heightened basis the law requires. Complaints may be brought to the control authority designated under the law.

E.12 Peru

Governed by the Ley de Protección de Datos Personales (Ley 29733) and its Regulation approved by Decreto Supremo 016-2024-JUS, in force since March 30, 2025, and administered by the Autoridad Nacional de Protección de Datos Personales. Data subjects have the rights of information, access, rectification, cancellation, and opposition, and the right to portability. Sensitive data is Processed only on the grounds the law permits. Complaints may be brought to the Autoridad Nacional de Protección de Datos Personales. Cross-border transfers are made to recipients that assume adequate protection obligations, or with the data subject's consent obtained under Section 0.4A or under another exception the law provides.

E.13 Uruguay

Governed by the Ley de Protección de Datos Personales (Ley 18.331) and administered by the Unidad Reguladora y de Control de Datos Personales. Data subjects have the rights of access, rectification, update, inclusion, and deletion. Sensitive data is Processed only on the grounds the law permits. Complaints may be brought to the Unidad Reguladora y de Control de Datos Personales. Transfers to countries that are not recognized as providing adequate protection, including the United States, are made with the data subject's consent obtained under Section 0.4A, under contractual safeguards, or under another exception in Article 23 of Ley 18.331.

ANNEX F. OTHER JURISDICTIONS

Applicability. This Annex applies to the Personal Data of any data subject located in a country, state, province, or territory that is not separately addressed in Annexes A through E (the Philippines being addressed in Annex D). It covers, without limitation, the other states and territories of the Americas, including Bolivia, Guatemala, Haiti, Honduras, Nicaragua, Belize, Guyana, Suriname, and the Caribbean states, the jurisdictions of Asia-Pacific other than the Philippines, and every other jurisdiction worldwide from which Remote Leverage sources Placement Candidates, in which a Contractor User performs services or is monitored, in which a Client or its Authorized Users are located, or from which Leve is accessed. Where a jurisdiction later enacts or is found to have a comprehensive

data-protection statute, Remote Leverage applies that statute and, where appropriate, adds a dedicated annex. This Annex does not extend to any jurisdiction, person, or engagement excluded by Section 6B.3.

Application of the global baseline. The global baseline in Section 1 and the protections of this Privacy Agreement apply in full to every data subject covered by this Annex. No data subject covered by this Annex receives less than the baseline, and where the local law confers a stronger right, that stronger right applies. Only the mandatory requirements of local law apply in addition to the baseline, and any provision of this Privacy Agreement that would be unlawful under local law is read down under Section 4.3.

Authorization and consent. Where the local law requires a prior, express, or informed authorization or consent, or a specific notice, before Personal Data is Processed, before sensitive Personal Data or the data of children or adolescents is Processed, or before Personal Data is transferred internationally, Remote Leverage obtains that authorization, consent, or provides that notice before the Processing or transfer begins, through the authorizations in Section 0.4A, given electronically by checking the acceptance box in Section 0.4. For the core Processing of Placement Candidate and Contractor User data, for monitoring, and for access to Messages, Remote Leverage relies on contractual necessity, legal obligation, and the legitimate or locally authorized-purpose basis where the local law provides one, and otherwise reserves authorization for genuinely optional and separable Processing, in recognition of the power imbalance in the engagement relationship.

Respect for habeas data and data-subject rights. Remote Leverage respects the constitutional and statutory habeas-data guarantees and any other data-subject rights recognized in the jurisdiction, including, at minimum, the rights to be informed, to access, to rectify inaccurate or incomplete data, to request cancellation or deletion, to object to Processing, and to revoke any authorization given, together with any additional right the local law confers. Data subjects exercise these rights at privacy@remoteleverage.com or through any request functionality made available on Leve, and Remote Leverage verifies and responds within the period the local law requires or, absent a stated period, within a reasonable time.

Residual standard where no comprehensive statute exists. Where a jurisdiction has no comprehensive data-protection statute, Remote Leverage relies on the constitutional protection of privacy and habeas data, on any sectoral rules that apply, and, as a residual standard, on the protections of the global baseline and this Privacy Agreement, and it defaults to the higher common standard reflected in this Privacy Agreement so that a single document remains defensible across jurisdictions.

Sensitive data and minors. Sensitive Personal Data and the Personal Data of children and adolescents are Processed only on the heightened basis the local law requires and, absent a stated basis, only where strictly necessary and subject to enhanced safeguards.

Local language, registration, authorities, and representatives. Where local law mandatorily requires a notice or instrument in a local language, the registration of a database or Processing activity, notice to or authorization by the local authority, or the appointment of a local representative or data protection officer, Remote Leverage meets that requirement where it applies to Remote Leverage.

Personal data breaches. Where local law requires notice of a personal data breach to a local authority or to data subjects, Remote Leverage gives that notice within the period local law requires, as described in Section 10.

Laws modeled on the GDPR. Where local law follows the structure of the GDPR, including the Digital Personal Data Protection Act, 2023 of India and its rules, Remote Leverage applies the corresponding provisions of Annex A with the necessary adaptations, to the extent that local law applies to the Processing.

International transfers. International transfers of Personal Data to Remote Leverage and to service providers in the United States and elsewhere are made under the transfer basis the local law provides, applying the mechanisms in Section 7.1(e) in the order stated there, including any notice to or authorization by the local authority that the local law requires, and are supported by contractual and organizational safeguards.

ANNEX G. SUBPROCESSORS, IDENTITY-VERIFICATION AND MONITORING TOOLS, AND SECURITY MEASURES

G.1 Subprocessors and service providers

The following table lists, as at the version date of this Privacy Agreement, the Subprocessors, Payment Partners, and other service providers that Process Personal Data in connection with Leve and the Services, whether as Subprocessors of Client Personal Data under Section 5 or as service providers to Remote Leverage as controller. The current list, including the messaging service providers that deliver Program Messages under Section 6C and any provider of an optional artificial-intelligence feature, is maintained on the Subprocessor Page, which is incorporated by reference and prevails over this table if they differ, and changes are notified as described in Section 5.5. Payment Partners execute debits, charges, currency conversions, and payouts on payment instructions transmitted through Leve and hold any funds under their own licenses; they act as independent controllers for their own know-your-customer, anti-money-laundering, sanctions, fraud-prevention, and regulatory recordkeeping Processing under their own privacy notices, as Section 6B.1 describes. Providers that are provisioned but do not Process Personal Data are not listed.

Subprocessor (legal entity)	Service and role	Location (headquarters and processing region)	Processing activity	Categories of data
Supabase Pte. Ltd. and its affiliate Supabase, Inc.	Database, authentication, and file-storage provider (Subprocessor)	Singapore and United States (headquarters); processing in the United States or other region as configured	Hosts the Leve application database, including User, Engagement, and Client records, Messages and their metadata, Leve Records, documents, and payment-instruction metadata; provides User authentication, including sign-in with Google; and stores uploaded files, such as identity documents and signed contracts, in encrypted storage accessed through short-lived signed links. Messages are encrypted in transit and at rest but are not end-to-end encrypted.	Identity, contact, Engagement, tax, payment-instruction, Messaging Service, and Account data; uploaded documents (categories A, D, E, Q, R, S, T, V)
Vercel Inc.	Application hosting and content-delivery network (Subprocessor)	United States (San Francisco, California); compute in Portland, Oregon, United States, with a global edge network	Hosts and serves Leve; terminates encrypted connections, protects against denial-of-service attacks, and delivers content for all User traffic.	All Leve data in transit; IP addresses and request logs (category W)
Veriff OÜ	Identity and biometric verification (Subprocessor)	Estonia (Tallinn); processing locations as set out in Veriff's terms	Verifies government identity documents and performs biometric liveness and face-matching checks during onboarding of Placement Candidates and Contractor Users	Identity-document images and data, selfie or video images, biometric identifiers,

Subprocessor (legal entity)	Service and role	Location (headquarters and processing region)	Processing activity	Categories of data
			and, where required, Account Administrator verification. Identity documents and verification media submitted in the verification flow are processed by Veriff and are not intended to be retained on Remote Leverage's systems.	verification results (categories A, B)
Stripe, Inc. and, where applicable, its affiliates, including Stripe Payments Europe, Limited	Payment execution: card payments (licensed Payment Partner; independent controller for its own regulatory purposes)	United States (South San Francisco, California); Ireland for European Economic Area processing where applicable	Executes card payments through Stripe Connect on payment data submitted through Leve. Remote Leverage does not see or store full card numbers, which are handled within Stripe's PCI DSS Level 1 environment.	Payment-card, billing-contact, and transaction data (categories J, T)
Wise US Inc. and its affiliates, including Wise Payments Limited	Payment execution and payouts, including currency conversion (licensed Payment Partner; independent controller for its own regulatory purposes)	United States (New York) and United Kingdom (London)	Executes international payouts to Contractor Users, including quotes, conversions, and transfers, on payment instructions transmitted through Leve, using payout details submitted by the Contractor User.	Name, contact, bank-account, and payout data (categories A, T)
Cadana Inc. and its affiliates	Payment execution and payouts (licensed Payment Partner; independent controller for its own regulatory purposes)	United States (Bethesda, Maryland) and other countries where Cadana operates	Executes payouts to Contractor Users through Cadana's payment network on payment instructions transmitted through Leve, and processes payout destination data.	Name, contact, payout-destination, and payment data (categories A, T)
Corpay Cross-Border Solutions	Payment execution and payouts,	United States (Atlanta, Georgia)	Executes mass and cross-border payouts to Contractor Users on payment instructions transmitted	Name, bank-account, payout, and

Subprocessor (legal entity)	Service and role	Location (headquarters and processing region)	Processing activity	Categories of data
(Corpay, Inc. group)	including currency conversion (licensed Payment Partner; independent controller for its own regulatory purposes)		through Leve and returns payment-status updates, including booking and batch-release status.	payment-status data (categories A, T)
DocuSeal, LLC	Electronic signature and document processing (Subprocessor)	United States (Chicago, Illinois); hosting in the United States or the European Union as configured	Hosts and processes COR Contractors' independent contractor agreements with Remote Leverage, Direct Contracts, offers made through Leve, and Forms W-8 and W-9, including signer names, tax identification numbers, signatures, and the signing audit trail.	Identity, contact, tax, signature, and audit-trail data (categories A, R, S)
JotForm Inc.	Onboarding form collection (Subprocessor)	United States (San Francisco, California)	Collects onboarding information that Contractor Users and Placement Candidates submit through forms, including identity, address, payout-account, and emergency-contact details.	Identity, contact, banking, and emergency-contact data (categories A, E, T)
Time Doctor, LLC	Monitoring Tool: time tracking and work verification (Subprocessor)	United States	Where monitoring has been activated and authorized under Section 6, records time and collects Work-Verification Data for Contractor Users; the data is reconciled into Leve Timesheets.	Time, Work-Verification Data, and device-usage data (categories F, U)
Workforce Cloud Tech, Inc. (trading as Recruit CRM)	Applicant-tracking and placement-pipeline system (Subprocessor and service provider)	United States (Norwood, New Jersey); hosting in the United States or the European Union as configured	Supplies deal, job, and recruiter and salesperson data for commission reconciliation; receives a placed Placement Candidate's name, email address, telephone number, city, and country when the placement is marked as completed; and records an Engagement-end status and audit note on the Placement Candidate's record.	Placement Candidate identity and contact data; placement and commission data (categories A, C, X)

Subprocessor (legal entity)	Service and role	Location (headquarters and processing region)	Processing activity	Categories of data
Google LLC (Google Workspace: Calendar, Sheets, Admin Directory)	Scheduling and productivity suite (Subprocessor)	United States (Mountain View, California)	Creates and manages onboarding, interview, and consultation calendar events with User and organizer email addresses as attendees; reads Contractor User names, hourly rates, and hours recorded from Timesheet spreadsheets; and looks up or resets passwords for Google Workspace accounts that Remote Leverage administers for Contractor Users, by email address.	Name, email, rate, hours, and account data (categories A, E, Q, U)
Zoom Communications, Inc.	Video conferencing (Subprocessor and service provider)	United States (San Jose, California)	Hosts video meetings, including onboarding meetings that Leve creates, updates, and deletes under a Remote Leverage staff host account. The Leve integration transmits no Placement Candidate or Contractor User Personal Data to Zoom, but participants' names, images, and voices are processed by Zoom when they join a meeting.	Staff host-account data and meeting details; participant name, image, and voice during meetings (category V)
Intuit Inc. (QuickBooks and QuickBooks Payments)	Accounting (service provider) and ACH debit execution (licensed Payment Partner; independent controller for its own regulatory purposes)	United States (Mountain View, California)	Receives Contractor User names, email addresses, countries, and payout amounts to record contractor payments in Remote Leverage's accounting records; receives Client organization names, email addresses, and per-Contractor User invoice line items for billing; and receives Client bank routing and account numbers, which are tokenized immediately and are not stored in raw form, to execute ACH debits.	Name, email, country, payment, invoice, and tokenized bank data (categories A, G, J, T)
Slack Technologies, LLC (a Salesforce company)	Internal team communications (Subprocessor and service provider)	United States (San Francisco, California)	Receives Contractor User first and last names, roles, Client organization names, and start dates for internal announcements of new	Name, email, role, Client name, and start date (categories A, D, V)

Subprocessor (legal entity)	Service and role	Location (headquarters and processing region)	Processing activity	Categories of data
			Engagements and placements; receives Contractor User email addresses to check workspace membership; and receives internal staff names and email addresses and aggregate payout totals in operational notifications. Payout data for any individual is not transmitted.	
Twilio Inc. (SendGrid)	Transactional email delivery (Subprocessor)	United States (San Francisco, California)	Delivers all transactional email, including the recipient address, sender identity, subject line, and full message body, which for onboarding and offer emails includes the recipient's name, role, rate, Payment Arrangement, currency, and start date, and attachments such as offers, signed documents, and calendar invitations.	Contact, rate, Engagement, and document data (categories A, D, S, V)
PostHog Inc.	Product analytics (Subprocessor and service provider)	United States (San Francisco, California); hosting in the United States or the European Union as configured	Receives standard browser analytics events, including page views, automatically captured interface interactions, and session and device metadata. Leve does not deliberately send User names, email addresses, or payment data, but automatically captured events may incidentally include text displayed on screen.	Usage, device, and session data; incidental on-screen text (category W)
Freshworks Inc. (Freshdesk)	Customer-support ticketing (Subprocessor and service provider)	United States (San Mateo, California); data-center region as configured	Receives requester names and email addresses and the names of the tools requested when Contractor Users submit tool-access requests, and the name, email address, role, ticket content, and attachments of Users who submit support requests.	Name, email, role, support content, and attachments (categories H, V)
Functional Software, Inc. (doing business as Sentry)	Error tracking and application monitoring (Subprocessor)	United States (San Francisco, California); hosting in the United States or	Receives application error events and stack traces, the content of application log messages, some of which may contain user email addresses, and masked	Diagnostic data, email addresses in logs, masked session

Subprocessor (legal entity)	Service and role	Location (headquarters and processing region)	Processing activity	Categories of data
		the European Union as configured	recordings of user sessions, with media blocked, when an error occurs. No user identity profile is attached to these events.	recordings (category W)
Arcjet	Bot protection and rate limiting (Subprocessor)	Multiple regions (global infrastructure)	Receives the requester's IP address and request headers on authenticated page loads to detect bots and enforce rate limits. No User or Remote Leverage personnel account data is transmitted.	IP address and request headers (category W)
ZeroBounce	Email-address validation (Subprocessor and service provider)	United States; processing in the European Union or the United States depending on the service endpoint used	Receives the email address entered at sign-up or when a User is invited to a Workspace, and returns a deliverability and validity result used to block invalid or disposable addresses before an account is created.	Email address and validation result (category W)

G.2 Identity-verification and monitoring tools

Identity and biometric verification is performed by Veriff OÜ under Sections 1.2, 1.9A, and 6B.2. Time tracking and work verification are performed only through the Monitoring Tool, currently Time Doctor, under Section 6 and only where activated and authorized. Where Remote Leverage deploys mobile-device-management, endpoint-detection-and-response, or other security tooling on devices under Section 6.4, the provider is identified to the affected Contractor User in the Monitoring Authorization or Personal-Device Consent given under Section 6.8.

G.3 Technical and organizational measures

Remote Leverage maintains the following technical and organizational measures for Leve and may update them from time to time, provided that the overall level of protection is not materially reduced.

Measure	Description
Access control and authorization management	Role-based access control, with roles for super administrators, administrators, managers, bookkeepers, virtual assistants, members, and contractors, is enforced on the server for every request. Every server action re-validates the User's session and organization scope before it executes, and the multi-tenant architecture isolates the data of each Client organization. Identity verification is required for Account Administrators. Sign-in uses one-time passcodes with trusted-device management, and sessions time out automatically after a period of inactivity.
Encryption in transit and at rest	TLS 1.2 or higher is enforced on all connections, with HTTP Strict Transport Security and preloading. The database and file storage are encrypted at rest using AES-256. Payment-card data is handled within the Payment Partner's PCI DSS Level 1

Measure	Description
	environment and is not seen or stored by Remote Leverage. Identity documents submitted through the identity-verification flow are processed by the identity-verification provider and are not intended to be persisted on Remote Leverage's infrastructure. Sensitive files, such as identity documents and signed contracts, are stored in encrypted object storage and served only through short-lived signed links.
Network and endpoint security	Leve is served from its hosting provider's edge network with automatic TLS certificate management, a global content-delivery network, and infrastructure-level protection against denial-of-service attacks. Security headers, including Content-Security-Policy, X-Frame-Options set to DENY, X-Content-Type-Options set to nosniff, and Strict-Transport-Security with preload, are applied to all routes. Adaptive rate limiting and bot protection are enforced. Security controls for devices used by Remote Leverage personnel are outside Leve and are not described in this Annex; controls for devices used by Contractor Users are addressed in Section 6.
Logging and monitoring	Every action on Leve is recorded as a Leve Record, and every data-changing action is recorded in an audit trail with the actor, timestamp, and change detail. Client access to and export of Messages, and human access to Messages by Remote Leverage personnel, are logged. Application errors are captured by an error-monitoring service. Dependency and code-level scanning runs continuously, including dependency-vulnerability scanning on every code change (Snyk), static analysis for SQL injection, cross-site scripting, and related vulnerability classes (GitHub CodeQL), automated dependency-update alerts (Dependabot), and supply-chain checks on every build (pnpm audit).
Secure development and change management	Parameterized database queries are used across all data access to prevent SQL injection, and the database schema enforces referential integrity through foreign-key constraints. Webhooks from external integrations, such as payment, identity-verification, and electronic-signature providers, are signature-verified before they are processed. Changes are deployed through code review and continuous-integration checks, including type checking, unit tests, and deployment-configuration validation, before release.
Vendor review	Section 5.5 sets out the data-protection obligations that Remote Leverage imposes on Subprocessors. Additions and replacements are reflected on the Subprocessor Page and notified as described in that Section.
Personnel confidentiality and training	The confidentiality obligations of persons authorized to Process Personal Data are set out in Sections 4.4(a) and 5.3. Access to Leve, and to Messages and Work-Verification Data, is granted according to role and need to know.
Backup and resilience	The production database uses point-in-time recovery, which allows restoration to a specific point in time within the configured recovery window.
Incident response	Suspected security vulnerabilities may be reported to security@remoteleverage.com or the Support Email. Remote Leverage's published targets are to acknowledge a report within 48 hours and to provide an initial assessment within five business days. Personal Data Breaches are assessed and notified as described in Section 10 and Section 5.7.

ANNEX H. COOKIE AND TRACKING TECHNOLOGIES NOTICE

H.1 What we use

Leve and remoteleverage.com use Tracking Technologies in four categories: (a) strictly necessary, for sign-in, security, bot protection, load balancing, and remembering consent choices; (b) preferences, such as language and search filters; (c) analytics and diagnostics, including product analytics and masked session recordings associated with errors, provided by the services listed in Annex G; and (d) advertising, including the Meta pixel and similar tags, which measure the effectiveness of Remote Leverage's advertising and may let the advertising provider link a visit to its own user. First-party technologies are set by Remote Leverage; third-party technologies are set by their providers under their own privacy notices.

H.2 Your choices

Strictly necessary technologies are always active. For Visitors and Users in the European Economic Area, the United Kingdom, Switzerland, the Philippines, and any other jurisdiction that requires prior consent, other technologies are set only after consent through the cookie banner. Elsewhere they are active by default and can be switched off at any time through Cookie Settings, the preference center, or browser and device settings. Refusing or withdrawing consent does not affect access to Leve.

H.3 United States opt-outs

Where an advertising technology is a sale or sharing under United States state law, Visitors and Users may opt out through the "Your Privacy Choices" link or the preference center. Remote Leverage treats a Global Privacy Control signal as a valid opt-out for the browser or device that sends it. Remote Leverage does not respond to Do Not Track signals, for which no common standard exists.

H.4 Talent Marketplace pages and duration

Section 1.9B(h) limits the data that advertising technologies may receive on Talent Marketplace pages. Session technologies expire when the browser closes. Persistent technologies last for the period shown in the preference center, generally no more than 13 months, after which consent is requested again where consent is the basis.