DEALROOM

PRIVATE & CONFIDENTIAL

DATA PROCESSING AGREEMENT

CONTROLLER

Trackingplan Inc.

PROCESSOR

[_____]

EFFECTIVE DATE

June 4, 2026

GOVERNING LAW

Kingdom of Spain

This Data Processing Agreement ("DPA") is entered into as of June 4, 2026 ("Effective Date") and forms part of any existing service agreement between the parties listed below.

DATA CONTROLLER:

[_____], a company with its principal place of business at [_____] ("Controller")

DATA PROCESSOR:

Trackingplan Inc., a company with its principal place of business at 2093 Philadelphia Pike #1638, Claymont, Delaware 2093, USA ("Processor")

BACKGROUND

The Controller has engaged the Processor to provide certain services. In providing those services, the Processor will process Personal Data on behalf of the Controller. This DPA sets out the terms on which the Processor will process Personal Data on behalf of the Controller, as required by: (a) Article 28 of the EU General Data Protection Regulation (Regulation (EU) 2016/679) ("EU GDPR"); (b) the UK General Data Protection Regulation as incorporated into UK law and the Data Protection Act 2018, in each case as amended by the Data (Use and Access) Act 2025 (together, the "UK GDPR"); and (c) The California Consumer Privacy Act of 2018 and the California Privacy Rights Act of 2020 ("CCPA/CPRA"), where applicable.

1. DEFINITIONS

In this Agreement:

“Data Protection Laws”	means all applicable laws relating to data protection and privacy, including: (a) EU GDPR; (b) UK GDPR and the Data Protection Act 2018, in each case as amended by the Data (Use and Access) Act 2025; (c) CCPA/CPRA; and (d) any other applicable national implementing legislation.
“Personal Data”	means any information relating to an identified or identifiable natural person that the Processor processes on behalf of the Controller.
“Processing”	means any operation performed on Personal Data, including collection, recording, organization, storage, adaptation, retrieval, consultation, use, disclosure, combination, restriction, erasure, or destruction.

“Personal Data Breach”	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.
“Sub-processor”	means any third party engaged by the Processor to process Personal Data on behalf of the Controller.
“Data Subject”	means an identified or identifiable natural person whose Personal Data is processed.
“Supervisory Authority”	means an independent public authority responsible for monitoring the application of Data Protection Laws.

2. Assistance with compliance

Taking into account the nature of the processing and the information available to it, the Processor shall assist the Controller in ensuring compliance with the Controller's obligations to carry out data protection impact assessments and, where required, to consult the competent supervisory authority prior to processing, under Articles 35 and 36 of the GDPR. The Processor's obligations to assist the Controller with security of processing, personal data breaches, and data subject requests are set out in the negotiated terms of this DPA.

3. Controller obligations

The Controller warrants that:

(a) It has obtained all necessary consents, provided all necessary notices, and otherwise has a lawful basis to transfer Personal Data to the Processor for processing under this DPA;

(b) Its instructions to the Processor will comply with Data Protection Laws;

(c) It will provide the Processor with accurate and complete information regarding the processing.

4. NEGOTIATED TERMS

4.1 Scope of processing

The Processor shall process Personal Data as reasonably necessary to perform the Services described in the Principal Agreement. The categories of data subjects, types of Personal Data, and purposes of processing are described in Annex 1, which may be updated by mutual agreement to reflect changes in the Services.

4.2 Processing instructions

The Processor shall process Personal Data in accordance with the Controller's documented instructions. The Processor may exercise reasonable technical discretion in routine operational matters (such as infrastructure maintenance, security updates, and backup operations) provided such actions do not alter the nature, scope, or purposes of processing. The Processor shall inform the Controller if any instruction would, in the Processor's reasonable opinion, infringe applicable data protection law.

4.3 Sub-processors

The Controller provides general written authorization for the Processor to engage Sub-processors. The Processor shall notify the Controller at least thirty (30) days in advance of any intended changes to Sub-processors, providing sufficient detail for the Controller to assess the change. The Controller may object to such changes on reasonable data protection grounds within the notice period. If the Controller objects, the parties shall negotiate in good faith to resolve the concern. The Processor shall ensure each Sub-processor is bound by data protection obligations no less protective than those in this Agreement.

4.4 International data transfers

Transfers outside the EEA or UK are permitted where: (a) the destination country has an adequacy decision; or (b) Standard Contractual Clauses are in place with supplementary measures where required.

4.5 Security measures (TOMs)

The Processor shall implement appropriate technical and organizational measures to protect Personal Data, taking into account the state of the art, costs, and nature of processing. Measures shall be documented in Annex 2.

4.6 Data breach notification

The Processor shall notify the Controller without undue delay and in any event within seventy-two (72) hours of becoming aware of a Personal Data breach. The notification shall include all information required under Article 33(3) of the GDPR or equivalent applicable law. The Processor shall cooperate with the Controller in investigating and

remediating the breach and in fulfilling the Controller's notification obligations to supervisory authorities and data subjects.

4.7 Data subject rights assistance

The Processor shall assist the Controller, by appropriate technical and organizational measures, in fulfilling the Controller's obligations to respond to requests from data subjects exercising their rights under applicable data protection law. Upon receiving the Controller's written instructions, the Processor shall provide the requested information or execute the requested action within ten (10) business days. The Processor shall promptly redirect to the Controller any data subject request received directly. Reasonable costs for assistance beyond standard operations may be charged at agreed rates.

4.8 Audit rights

The Processor shall provide the Controller with an annual compliance report summarizing its data protection practices, security measures, sub-processor usage, and any incidents during the reporting period. The Processor shall also make available current certifications (ISO 27001, SOC 2, or equivalent). The Controller may request an on-site audit where there is reasonable cause, such as a data breach, regulatory investigation, or material compliance concern, upon thirty (30) days' prior written notice. The Processor shall bear the costs of producing reports; the Controller shall bear the costs of any on-site audit.

4.9 Data deletion/return

Upon termination or expiry of the Principal Agreement, the Processor shall securely delete all Personal Data within ninety (90) days, including all copies in production systems, backups, and archives. The Controller is responsible for exporting any required data prior to termination using the Processor's standard export tools. The Processor shall confirm deletion in writing upon request. Data retained pursuant to applicable legal requirements shall be isolated and protected.

4.10 Confidentiality

The Processor shall ensure that persons authorized to process Personal Data are bound by confidentiality obligations, whether through contractual terms of employment or statutory obligation. The Processor shall provide regular data protection training to all personnel who access Personal Data. The Processor shall implement access controls to ensure that Personal Data is accessible only to authorized personnel with a legitimate need.

4.11 Liability & indemnification

The Processor's total aggregate liability for all claims arising under or in connection with this Agreement, including data protection breaches, shall not exceed the total fees paid or payable by the Controller under the Principal Agreement in the twelve (12) months preceding the first event giving rise to the claim. This limitation does not apply to liability arising from the Processor's intentional misconduct or gross negligence.

4.12 Term & termination

This Agreement shall have an initial term of one (1) year from the effective date and shall automatically renew for successive one-year periods unless either party provides written notice of non-renewal at least ninety (90) days prior to the end of the then-current term. Either party may terminate immediately for material breach of data protection obligations that remains uncured for thirty (30) days after written notice. This Agreement shall in any event terminate upon termination of the Principal Agreement.

5. GENERAL PROVISIONS

5.1 Order of precedence

In the event of a conflict between this DPA and any principal agreement, this DPA will prevail with respect to data protection matters.

5.2 Amendments

This DPA may only be amended in writing signed by both parties.

5.3 Term

This DPA commences on the Effective Date and continues until all Personal Data is deleted or returned, or until any principal agreement terminates or expires.

5.4 Survival

The obligations regarding deletion/return of Personal Data, confidentiality, and any provisions that by their nature should survive, will continue after termination.

5.5 Entire agreement

This DPA, including its Annexes, constitutes the entire agreement between the parties regarding data processing matters.

6. GOVERNING LAW AND JURISDICTION

This Data Processing Agreement is governed by the EU General Data Protection Regulation (Regulation (EU) 2016/679) and the Spanish Ley Orgánica 3/2018, de Protección de Datos

Personales y garantía de los derechos digitales (LOPDGDD). The parties submit any dispute arising out of or in connection with this Agreement to the exclusive jurisdiction of the Courts and Tribunals of the city of Madrid (Spain), expressly waiving any other forum that may correspond to them.

7. JURISDICTION-SPECIFIC REGULATORY PROVISIONS

(a) The Agencia Española de Protección de Datos (AEPD) shall be the competent supervisory authority for matters arising under this DPA.

(b) Where applicable, the Processor will comply with the specific requirements of Spanish data protection law regarding the processing of special categories of data.

(c) Any ambiguity in this DPA will be interpreted in accordance with Spanish civil law principles.

(d) For any transfer of Personal Data originating in the EEA to a country not covered by an adequacy decision under Article 45 of the GDPR, the parties shall put in place appropriate safeguards under Article 46 of the GDPR. In the absence of another Article 46 safeguard agreed by the parties, the applicable safeguard shall be the European Commission's Standard Contractual Clauses (Implementing Decision (EU) 2021/914, or any successor decision), in the module corresponding to each party's role. The annexes to those Clauses shall be completed using the processing description and the technical and organisational measures set out in this DPA, and the Processor shall conduct a transfer impact assessment and implement supplementary measures where necessary to ensure an essentially equivalent level of protection.

SIGNED by the parties:

For and on behalf of [_____]:

Signature: _____

Name: [_____]

Title: [_____]

Date: _____

For and on behalf of Trackingplan Inc.:

Signature: _____

Name: Lorena Torres

Title: Operations

Date: _____

ANNEX I

Description of Processing

This Annex describes the processing carried out by the Processor on behalf of the Controller under this DPA.

1. SUBJECT MATTER AND DURATION

The Processor will process Personal Data for the duration of the principal service agreement between the parties, and until all Personal Data has been deleted or returned in accordance with this DPA.

2. PURPOSE AND NATURE OF PROCESSING

Data quality monitoring for analytics implementations.

For that purpose the processing may include the collection, recording, organisation, structuring, storage, retrieval, consultation, use, disclosure, restriction, erasure and destruction of Personal Data.

3. CATEGORIES OF PERSONAL DATA

The Personal Data processed comprises the following categories:

(a) Usage, device & technical data (incl. IP);

(b) Marketing & communications;

(c) High level signals;

4. CATEGORIES OF DATA SUBJECTS

The Data Subjects are the individuals whose Personal Data is submitted by or on behalf of the Controller through the services, which may include the Controller's employees, contractors, customers, end users and business contacts.

5. CONTROLLER'S OBLIGATIONS AND RIGHTS

The Controller retains all rights and obligations with respect to the Personal Data as set out in this DPA, including the right to issue binding processing instructions and to audit the Processor's compliance with this Annex.

ANNEX II

Technical and Organisational Measures

This Annex describes the technical and organisational security measures implemented by the Processor to protect Personal Data in accordance with Article 32 of the GDPR.

1. ENCRYPTION

(a) All Personal Data transmitted over public networks is encrypted in transit using TLS 1.2 or higher;

(b) Personal Data at rest is encrypted using AES-256 or equivalent industry-standard encryption;

(c) Encryption keys are managed through a dedicated key management system with regular key rotation.

2. ACCESS CONTROL

(a) Role-based access control (RBAC) is enforced, granting personnel access only to the Personal Data necessary for their specific function;

(b) Multi-factor authentication (MFA) is required for all personnel accessing systems that process Personal Data;

(c) Access rights are reviewed at least quarterly and promptly revoked upon termination of employment or change of role;

(d) Unique user credentials are assigned to each authorized individual; shared accounts are prohibited.

3. NETWORK SECURITY

(a) Firewalls and intrusion detection/prevention systems (IDS/IPS) are deployed at network boundaries;

(b) Network segmentation isolates systems processing Personal Data from other environments;

(c) Vulnerability scans are performed at least monthly and penetration tests at least annually;

(d) Security patches are applied in accordance with a documented patch management policy.

4. LOGGING AND MONITORING

(a)

Access to Personal Data, including reads, writes, and deletions, is logged with timestamps and user identifiers;

(b) Logs are retained for a minimum of twelve (12) months and are protected against tampering;

(c) Automated alerting is in place for anomalous access patterns or suspected security incidents;

(d) Logs are reviewed regularly as part of the Processor's security operations.

5. BUSINESS CONTINUITY AND DISASTER RECOVERY

(a) Personal Data is backed up regularly, with backups stored in geographically separate locations;

(b) Backup restoration procedures are tested at least annually;

(c) A documented disaster recovery plan exists with a defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO);

(d) Redundant infrastructure is maintained to ensure availability of processing systems.

6. PERSONNEL SECURITY

(a) All personnel with access to Personal Data receive data protection and information security training upon onboarding and at least annually thereafter;

(b) Personnel are bound by written confidentiality agreements or non-disclosure agreements (NDAs);

(c) Background checks are conducted on personnel with access to Personal Data, to the extent permitted by applicable law;

(d) Disciplinary procedures are in place for breaches of security policies.

7. PHYSICAL SECURITY

(a) Data centres and facilities housing systems that process Personal Data are protected by physical access controls, including badge access, visitor logs, and surveillance;

(b) Equipment is protected against environmental threats such as fire, flood, and power failure;

(c) Decommissioned hardware and storage media are securely destroyed or wiped before disposal.

8. REGULAR TESTING AND ASSESSMENT

(a) The effectiveness of the above measures is tested and evaluated on a regular basis, at least annually;

(b)

Data protection impact assessments are carried out where processing is likely to result in a high risk to Data Subjects;

(c) Findings from audits, tests, and assessments are documented and result in corrective action plans where deficiencies are identified;

(d) The Processor maintains a documented information security management programme that is reviewed and updated at least annually.