Exhibit C

Data Processing Addendum

DPA
This Data Processing Addendum (”DPA”), forming part of the Compa SaaS Customer Agreement (“Principal Agreement”), is made and entered into as of the Effective Date, by and between Compa Technologies, Inc., a Delaware corporation, with offices 2211 Michelson Dr., Suite 900, Irvine, CA US 92612 (“Compa”) and [_____] (the “Customer”). (each a “Party” and together, “Parties”)
WHEREAS (A) The Customer acts as a Data Controller. (B) Compa acts as Data Processor. (C) The Customer wishes to contract certain Services as set forth in the Principal Agreement, which involve the processing of personal data by the Data Processor. Further details of the Processing are set out in Schedule 1 to this DPA. (D) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (E) The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

1. DEFINITIONS. Capitalized terms shall have the meaning set forth in this Section 1 or as otherwise defined in other sections of this DPA. If not defined, Capitalized terms shall have the same meaning set forth in the Principal Agreement or the GDPR, as applicable:

1.1 "DPA" means this Data Processing Agreement and all Schedules.

1.2 "Customer Personal Data" means any Personal Data Processed by a Contracted Processor on behalf of Customer pursuant to or in connection with the Principal Agreement, including Personal Data provided as Customer Data as defined in the Principal Agreement.

1.3 "Contracted Processor" means Compa and any Subprocessor.

1.4 "Data Protection Laws" means all data protection legislation and regulations applicable to the processing of the Customer Personal Data under this DPA and the Principal Agreement, including without limitation as applicable Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data ("GDPR"), the California Consumer Privacy Act as amended by the California Privacy Rights Act, ("CCPA/CPRA") or equivalent other State laws, and supplementing national legislation, in each case as may be amended, repealed, consolidated, or replaced from time to time.

1.5 "EEA" means the European Economic Area.

1.6 "GDPR" has the meaning set forth in the definition of Data Protection Laws.

1.7 "Data Transfer" means:

(a) a transfer of Customer Personal Data from the Customer to Compa; or

(b) an onward transfer of Customer Personal Data from Compa to a Subprocessor.

1.8 "Standard Contractual Clauses" means (i) the agreement pursuant to the European Commission's Implementing Decision of 2021/914 published on 4 June 2021 and as adopted by the Swiss Federal Data Protection and Information Commissioner ("Swiss FDPIC") on standard contractual clauses ("SCCs") for the transfer of personal data to Third Countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, and any replacement, amendment or restatement of the foregoing issued by the European Commission (the "EU Model Clauses"); (ii) the international data transfer addendum ("UK Transfer Addendum") adopted by the UK Information Commissioner's Office ("UK ICO") for data transfers from the UK to Third Countries; or (iii) any similar such clauses adopted by a data protection regulator relating to Personal Data transfers to Third Countries, including without limitation any successor clauses thereto .

1.9 "Services" means the services the Customer is provided pursuant to the Principal Agreement.

1.10 "Subprocessor" means any person appointed by or on behalf of Data Processor to process Customer Personal Data on behalf of the Customer in connection with the DPA.

2. PROCESSING OF CUSTOMER PERSONAL DATA.

2.1 Compa, as Data Processor, shall be responsible for:

(a) Complying with applicable Data Protection Laws in respect of its processing of Personal Data, in conformance with any processing instructions it receives from Customer

(b) Retaining, using, disclosing, or otherwise processing the Personal Data only for the purposes described in the Agreement and the Business Purpose specified in Schedule 1 and in accordance with the lawful, documented instructions of Customer (including the instructions of any of Customer's authorized

Users accessing the Services on Customer's behalf), as set out in the Agreement, this DPA or otherwise in writing;

(c) Ensuring it shall not Sell or Share Customer's Personal Data, nor use, retain, disclose, or otherwise process Customer's Personal Data outside of its business relationship with Customer or for any other Business Purpose or Commercial Purpose except as required by law.

(d) Informing Customer if Compa determines that it is no longer able to meet its obligations under Data Protection Laws or where in Compa's reasonable opinion, any of Customer's instructions infringes any Data Protection Laws;

(e) Customer reserves the right to take reasonable and appropriate steps to: (i) ensure Compa's processing of Personal Data is consistent with Customer's obligations under Data Protection Law; and (ii) discontinue and remediate unauthorized use of Personal Data;

(f) Ensuring it will not combine Personal Data which it Processes on Customer's behalf, with Personal Data which it receives from or on behalf of another person or persons, or collects from its own interaction with any individual, provided that Compa may combine Personal Data to perform any Business Purpose permitted or required under the Agreement to perform the Services; and

(g) Compa may pseudonymize Personal Data and to the extent such data is capable of being re-identified it shall remain protected as Personal Data hereunder; and Personal Data which has been pseudonymized, and is not reasonably expected to be re-identified, is deemed de-identified. Compa agrees that any pseudonymized or aggregated data used for Compa's internal purposes (i.e., other than Processing) is conditioned upon Compa's commitment to not re-identify such data and further commitment that in no event shall any such data be published unless pseudonymized in a manner that does not identify, and cannot be re-identified to, Customer or any individual Data Subject.

2.2 Compa intends to Process and store Customer Personal Data in the United States, but reserves the right to lawfully Process and store data elsewhere, to the extent not prohibited under the Principal Agreement and this DPA.

3. DATA PROCESSOR PERSONNEL. Compa shall take commercially reasonable steps to ensure that any employee, agent, or contractor of Compa, who may have access to the Customer Personal Data, are subject to confidentiality undertakings or statutory obligations of confidentiality, ensuring in each case that access is limited to those individuals who need to know or access the relevant Customer Personal Data, as necessary for the purposes of the Principal Agreement.

4. SECURITY. Taking into account the state of the art, the costs of implementation and the nature, scope, context, and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Compa shall in relation to the Customer Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk in accordance with Article 32(1) of the GDPR as described in Schedule 3.

5. SUBPROCESSING.

5.1 The Customer generally agrees that Compa may engage Subprocessors to Process Customer Personal Data. The Customer authorizes Compa to appoint (and permit each Subprocessor appointed in accordance with this Section 5 to appoint) Subprocessors in accordance with this Section 5 and any restrictions in the Principal Agreement.

5.2 Compa may continue to use those Subprocessors already engaged by Compa as at the date of this DPA (as listed at Schedule 2 to this DPA).

5.3 If Compa engages a new Subprocessor, Compa shall inform the Customer of the engagement and the Customer may object to the engagement of such new Subprocessor by

notifying Compa within 7 (seven) days of Compa's notice, provided that such notification must be on reasonable grounds, directly related to the new Subprocessor's ability to comply with substantially similar obligations to those set out in this DPA. If the Customer does not object within the specified time period, the engagement of the new Subprocessor shall be deemed accepted by the Customer.

5.4 With respect to each Subprocessor (which, for the purposes of this Section 5.4 includes new Subprocessors engaged in accordance with Section 5.3), Compa shall ensure that the arrangement between Compa and the relevant Subprocessor is governed by a written contract including terms that offer at least the same level of protection for Customer Personal data as those set out in this DPA and meet the requirements of Article 28(3) of the GDPR.

6. DATA SUBJECT RIGHTS.

6.1 Taking into account the nature of the Processing, Compa shall reasonably assist the Customer, insofar as this is possible, in the fulfilment of the Customer's obligations to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 Compa shall:

(a) promptly notify Customer if it receives a request from a Data Subject under any Data Protection Law in respect of Customer Personal Data; and

(b) ensure that it does not respond to that request except on the documented instructions of Customer or as required by applicable laws to which Compa is subject, in which case Compa shall to the extent permitted by applicable laws inform Customer of that legal requirement before Compa responds to the request.

7. PERSONAL DATA BREACH AND NOTIFICATION.

7.1 Compa shall notify Customer without undue delay upon Compa becoming aware of a Personal Data Breach affecting Customer Personal Data, providing Customer with sufficient information to allow the Customer to meet any obligations to notify, report, or inform Data Subjects and Supervisory Authorities of the Personal Data Breach under the Data Protection Laws.

7.2 Compa shall co-operate with the Customer and take reasonable commercial steps as are directed by Customer to assist in the investigation, mitigation, and remediation of each such Personal Data Breach.

8. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION. Compa shall provide reasonable assistance to the Customer with any data protection impact assessments, and prior consultations with Supervisory Authorities or other competent data privacy authorities, to the extent required by Articles 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Customer Personal Data by, and taking into account the nature of the processing and information available to, the Contracted Processors.

9. DELETION OR RETURN OF CUSTOMER PERSONAL DATA. Compa shall promptly and in any event within 90 days of the date of cessation of any Services involving the processing of Customer Personal Data, delete and procure the deletion of all copies of the Customer Personal Data or return all Customer Personal Data to the Customer, at the Customer's choice.

10. AUDIT RIGHTS.

10.1 Subject to this Section 10, Compa shall make available to the Customer on request, no more frequently than annually unless in response to a request by a regulatory authority: (i) reasonable information necessary to demonstrate compliance with this DPA, and (ii) shall allow for and contribute to audits, including inspections, by the Customer or an auditor mandated by the Customer in relation to the Processing of the Customer Personal Data by the Contracted Processors. A Customer may only

mandate an auditor for the purposes of this Section 10.1 if the auditor is reasonably agreed to by Compa.

10.2 Information and audit rights of the Customer only arise under Section 10.1 to the extent that the DPA does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

10.3 Customer shall give Compa reasonable advance notice of any audit or inspection to be conducted under Section 10.1 and shall make (and ensure that each of its mandated auditors makes) reasonable endeavors to avoid causing (or, if it cannot avoid, to minimize) any damage, injury, or disruption to Compa's premises, equipment, personnel, and business while its personnel are on those premises in the course of such an audit or inspection. Compa need not give access to its premises for the purposes of such an audit or inspection:

(a) to any individual unless he or she produces reasonable evidence of identity and authority;

(b) outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and Customer undertaking an audit has given notice to Compa that this is the case before attendance outside those hours begins;

(c) for the purposes of more than one audit or inspection, in respect of Compa, in any calendar year, except for any additional audits or inspections which Customer is required to carry out by a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory, where the Customer has identified its concerns or the relevant requirement or request in its notice to Compa of the audit or inspection; or

(d) to a third party who is performing the audit on behalf of the Customer, unless such third party auditor executes a confidentiality agreement acceptable to Compa before the audit.

10.4 Customer shall reimburse Compa for any time expended for any such on-site audit, if applicable, at Compa's then-current professional services rate, which shall be made available to Customer upon request. Before commencement of any such on-site audit; Customer and Compa shall mutually agree on the scope, timing, and duration of the audit in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Compa. Customer shall promptly notify Compa with information regarding any non-compliance during the course of an audit.

10.5 The Customer must provide Compa with any audit reports generated in connection with any audit at no charge unless prohibited by applicable law. The Customer may use audit reports only for the purposes of meeting its audit requirements under the Data Protection laws and/or confirming compliance with the requirements of this DPA. The audit reports shall be confidential.

10.6 Nothing in this Section 10 shall require Compa to breach any confidentiality owed to any of its clients, employees, or Subprocessors, or to grant access to any multi-tenant systems.

11. DATA TRANSFER. Compa may process and transfer Personal Data originating from the European Area in and to the United States and third countries where its affiliates and its Sub-processors have operations. All data transfers and processing of Personal Data originating from the European Area shall be made in compliance with the applicable European Area Data Protection Law, and if a Contracted Processor is in a third country, then the Standard Contractual Clauses, Module Two ("Controller to Processor") shall apply as to such transfer. If Standard Contractual Clauses apply, it is not the intention of either party, nor the effect of this DPA, to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses. To the extent Company adopts an alternative data transfer mechanism (including any new version or replacement to the Standard Contractual Clauses adopted pursuant to Data Protection Laws) for the transfer of Personal

Data ("Alternative Transfer Mechanism"), the Alternative Transfer Mechanism shall upon notice to Compa apply instead (but only to the extent such Alternative Transfer Mechanism complies with Data Protection Law and extends to the third countries to which Personal Data is transferred). In the event that the Contracted Processor is self-certified under the Data Privacy Framework (DPF), such certification has been deemed adequate under European Area Data Protection Law for processors in the United States and the Standard Contractual Clauses shall not apply..

(i) EEA Personal Data Transfers. For the purposes of the descriptions in the Standard Contractual Clauses relating to Personal Data Transfers under GDPR: (i) Schedule 1- Details of Processing and Schedule 3 – Information Security of this DPA shall form Annex I and Annex II of the Standard Contractual Clauses, respectively, if applicable; (iii) Annex III of the Standard Contractual Clauses shall be subject to General Authorization; and (iv) The Standard Contractual Clauses shall be governed by the laws of Customer's member state.

(ii) Swiss Personal Data Transfers. Where Personal Data transfers are subject to the Swiss DPA: (i) References to "Regulation (EU) 2016/679" and any articles therefrom shall be interpreted to include references to the Swiss DPA; (ii) References to "EU", "Union" and "Member State" shall be interpreted to include references to "Switzerland"; (iii) Schedule 1- Details of Processing and Schedule 3 – Information Security of this DPA shall describe the applicable requirements for Annex I-III of the Standard Contractual Clauses.

(iii) UK Personal Data Transfers. Where Personal Data transfers are subject to the UK Data Protection Law, each party agrees to be bound by the terms and conditions set out in the UK Transfer Addendum, attached hereto and incorporated herein.

12. Law Enforcement Request

12.1 Authority Request. If Compa becomes aware that any law enforcement, regulatory, judicial or governmental authority (an "Authority") wishes to obtain access to or a copy of some or all of Customer's Personal Data, whether on a voluntary or a mandatory basis, then unless legally prohibited as part of a mandatory legal compulsion that requires disclosure of Personal Data to such Authority, Compa shall: (1) promptly, without undue delay, notify Customer of such Authority's data access request, to the extent legally permissible; (2) inform the Authority that any and all requests or demands for access to Personal Data should be notified to or served upon Customer in writing; and (3) not provide the Authority with access to Personal Data unless and until authorized by Customer. In the event Compa is under a legal prohibition or a mandatory legal compulsion that prevents it from complying with (1)-(3) in full, Compa shall use reasonable and lawful efforts to challenge such prohibition or compulsion (and Customer acknowledges that such challenge may not always be reasonable or possible in light of the nature, scope, context and purposes of the intended Authority access request). If Compa makes a disclosure of Personal Data to an Authority (whether with Customer's authorization or due to a mandatory legal compulsion) Compa shall use best efforts to only disclose such Personal Data to the extent Compa determines it is legally required to do so and in accordance with applicable lawful process.

12.2 Imminent Risk. Clause 12.1 shall not apply in the event that, taking into account the nature, scope, context and purposes of the intended Authority's access to the Personal Data, Compa has a reasonable and good-faith belief that urgent access is necessary to prevent an imminent risk of serious harm to any individual. In such event, Compa shall notify Customer as soon as possible following such Authority's access and provide Customer with full details of the same, unless and to the extent Compa is legally prohibited from doing so.

12.3 Authority Requests. Compa shall use good faith efforts to not knowingly disclose Personal Data to an Authority in excess of a request (e.g., a massive, disproportionate and indiscriminate manner that goes beyond what is necessary in a democratic society). Compa shall have in place,

maintain and comply with a process governing Personal Data access requests from Authorities which at minimum prohibits: (1) disclosure in excess of requested information (e.g., massive, disproportionate or indiscriminate disclosure of Personal Data) relating to data subjects in the EEA and the United Kingdom; and (2) disclosure of Personal Data relating to data subjects in the EEA and the United Kingdom to an Authority without a subpoena, warrant, writ, decree, summons or other legally binding order that compels disclosure of such Personal Data.

12.4 Interception Policy. Compa shall have in place and maintain in accordance with good industry practice measures to protect Personal Data from interception. This includes complying with industry best practices of having in place and maintaining network protection to deny attackers the ability to intercept data and the use encryption of Personal Data whilst in transit to deny attackers the ability to read Personal Data

13. MISCELLANEOUS.

Notices. All notices and communications given under this DPA shall be made in accordance with the notices section of the Principal Agreement.

13.2 Liability and Indemnification. The liability of each party to this DPA, arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, shall be subject to the limitations or exclusions of liability set out in the Principal Agreement. Furthermore, the terms of indemnification by both Parties shall be governed by the Principal Agreement.

13.3 Order of Precedence. In the event of inconsistencies between the provisions of this DPA and any other agreements between the Parties, including the Principal Agreement and agreements entered into or purported to be entered into after the date of this DPA (except where explicitly agreed otherwise in writing, signed on behalf of the parties), the provisions of this DPA shall prevail. In the event of any conflict or inconsistency between this DPA and the Standard Contractual Clauses set forth in Schedule 3, the Standard Contractual Clauses shall prevail.

13.4 Governing Law. Notwithstanding Sections 7 and 9 of the Standard Contractual Clauses, this DPA is governed by the laws of the country or territory stipulated for this purpose in the Principal Agreement.

13.5 Term and Termination. The term of this DPA shall commence on the Effective Date of this DPA and shall be coterminous with the Principal Agreement in accordance with Section 7 of the Principal Agreement.

13.6 Amendment. This DPA is subject to the applicable terms for amendment set forth in the Principal Agreement.

IN WITNESS WHEREOF, the parties hereto hereby execute this DPA effective as of the Effective Date.

SCHEDULE 1 - DETAILS OF THE PROCESSING

This Schedule includes certain details of the processing of Customer Personal Data as required by Article 28(3) GDPR.

1. **Data Exporter**

Company Name	Address	Contact name, position, and contact information	Role
Customer information as included in the Agreement or applicable Ordering Document			Controller

2. **Data Importer**

Company Name	Address	Contact name, position, and contact information	Role
Compa Technologies, Inc. 2211 Michelson Dr., Suite 900, Irvine CA US 92612 Privacy@trycompa.com			Processor

3. **Activities relevant to the data transferred under these Clauses**

The activities relevant to the data transferred are the Services more fully described in the Agreement and applicable ordering documents.

4. **Processing Information**

Categories of Data Subjects whose Personal Data is transferred	Customer may submit Personal Data to Compa for the provision of the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects: ● Customer's Users authorized by Customer to use the Services ● Employees, agents, advisors, freelancers of Customer (who are natural persons) ● Candidates and prospective candidates of Customer
Categories of Personal Data transferred	Customer may submit Customer Personal Data to Compa for the provision of the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data: • First and last name • Title • Position • Employer • Client ID

	• Physical addresses • Geolocation • Contact information (company, email, phone, physical business address)
Sensitive Personal Data transferred	N/A
Frequency of the transfer	Continuous
Nature of the processing	The nature of the processing is to enable use of Processor's cloud-hosted and related services as more fully described in the Agreement.
Purpose of the data transfer and further processing	
For processing involving California consumers, please select the Business Purpose(s) for processing Personal Data	☐ N/A ☒ Improving or building the quality of the Services. ☒ Preventing, detecting, or investigating data security incidents or protecting against malicious, deceptive, fraudulent or illegal activity. ☐ Auditing related to counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards. ☒ Helping to ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for these purposes.

	☒ Debugging to identify and repair errors that impair existing intended functionality. ☐ Short-term, transient use, including, but not limited to, non-personalized advertising shown as part of a consumer's current interaction with the business, provided that the consumer's personal information is not disclosed to another third party and is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business. ☒ Performing services on behalf of the business, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of the business. ☐ Providing advertising and marketing services, except for cross-context behavioral advertising, to the consumer provided that, for the purpose of advertising and marketing, a service provider or contractor shall not combine the personal information of opted-out consumers that the service provider or contractor receives from, or on behalf of, the business with personal information that the service provider or contractor receives from, or on behalf of, another person or persons or collects from its own interaction with consumers. ☒ Undertaking internal research for technological development and demonstration. ☒ Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.
Period for which the Personal Data will be retained or criteria used to determine that period	During the term of the Agreement. Once the contract expires or terminates, the retention and deletion periods are more fully described in the Agreement, DPA, and accompanying Order Form or SOW.
Subprocessor transfers –subject matter, nature, and duration of processing	The subject matter, nature, and duration of the Processing more fully described in the Agreement, DPA, and accompanying Order Form or SOW.

5. Signatures

Signatures	The Parties agree that to the extent required and applicable as set forth herein, the Standard Contractual Clauses and the UK Transfer Addendum are incorporated by reference and that by executing the DPA, each party is deemed to have executed the Standard Contractual Clauses and the UK Transfer Addendum.

6. **Processing operations**

7. **EEA, Swiss and UK Model Clause Information**:

SCC Clause	**GDPR**	**Swiss DPA**	**UK Data Protection Law**
Module in Operation **Module Two (Controller to Processor)**			
Clause 7- Docking Clause	An entity that is not a party to these clauses may, with the agreement of the parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex 1.A		
Clause 9(a)- Use of Sub-processors	GENERAL WRITTEN AUTHORISATION: The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 7 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.		
Clause 11 (Redress)	Optional language in Clause 11 shall not apply		
Clause 17- Governing Law	These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Member State of the Controller.	These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Switzerland.	These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of England and Wales.
Clause 18 – Choice of Forum and Jurisdiction	(b) The parties agree that those shall be the courts of the Member State of the Controller.	The parties agree that those shall be the competent courts of Switzerland.	The parties agree that those shall be the competent courts of England and Wales.

Annex 1A- List of Parties	The name, address, and contact person's name, position, and contact details, and each party's role in processing personal data are provided in Section 1, 2, and 3 above		
Annex 1B – Description of Transfer	This information can be found in Section 4 above. To the extent applicable, the descriptions of safeguards applied to the special categories of Personal Data can be found in Appendix 2 to the DPA.		
Clause 13 and Annex 1C – Competent Supervisory Authority	Identify the competent supervisory authority/ies in accordance with Clause 13: Irish Data Protection Commissioner	Identify the competent supervisory authority/ies in accordance with Clause 13: FDPIC	Identify the competent supervisory authority/ies in accordance with Clause 13: UK Informational Commissioner
Annex II – Technical and Organizational Measures	The description of technical and organization measures designed to ensure the security of Personal Data is described more fully in Schedule 3 to the DPA.		
Annex II – Technical and Organizational Measures – Subprocessors			
Annex III – List of Subprocessors	See Schedule 2 to the DPA		
Ending the UK Transfer Addendum when the Approved Addendum changes	N/A	N/A	Which Parties may end this Addendum as set out in Section 19: ☒ Importer ☒ Exporter

SCHEDULE 2 – APPROVED SUBPROCESSORS

Entity Name	**Secureframe**
Subprocessing Activity	Security scanning
Entity Country	United States

Amazon Web Services	**WorkOS**
Cloud service provider	SSO infrastructure
United States	United States

Google Workspace	**Textkernel**
Data room	Job description parsing
United States	United States

Mixpanel	**Sentry**
Cloud-based Analytics	Cloud-based logging
United States	United States

A current list is available at: https://www.trycompa.com/privacy

SCHEDULE 3 – INFORMATION SECURITY AND PRIVACY POLICY

Description of the technical and organizational security measures implemented by the data importer in accordance with the Standard Contractual Clauses:

See details at: https://www.trycompa.com/security in addition to the following privacy policy:

Privacy Policy
This Privacy Policy ("Policy") describes how Compa Technologies Inc. ("Compa," "we," "our," "us") collects, processes, uses, and discloses certain information obtained through your use of our website (the "Site"), which is available at https://www.trycompa.com/legal/privacy-policy, as well as information that we collect offline and in other contexts (collectively with the Site, the "Services").

Information We Collect and Maintain About You

We collect information from you directly when you provide it to us through the Services. We further automatically collect certain information about you and your smartphone or other device when you use, access, or interact with our Services.

Personal information provided directly by you through the Site. When you make an account with us or use other features on the Site (such as apply for a job with us), we may collect your personal information, including the following categories of information:

- Full name
- The password you create for your account
- Email address
- Phone number
- Organization name
- Information about the types of candidates you wish to pursue

Personal information about applicants. Through our Services, we collect information from our customers about applicants they are assessing. We may collect the following categories of information about applicants:

- Full name
- Contact information (email address and phone number)
- Education history
- Employment history
- Any other personal information you provide in your resume, cover letter, or application

Server logs. Server logs automatically record information and details about your online interactions with us. For example, server logs may record information about your visit to our Site on a particular time and day and collect information such as your device ID or IP address.

Cookies. We also use cookies on the Site. Cookies are small files that are stored on your mobile device through the Site. A cookie allows the Site to recognize whether you have visited before and may store user preferences and other information. For example, cookies can be used to collect or store information about your use of the Site during your current session and over time (including the pages you view and the files you download), your device's operating system, your device ID, IP address, and your general geographic location.

Pixel tags. A pixel tag (also known as a web beacon, clear GIF, pixel, or tag) is an image or a small string of code that may be placed in an advertisement or email. It allows companies to set or read cookies or transfer information to their servers when you load a webpage or interact with online content. For example, we or our service providers may use pixel tags to determine whether you have interacted with a specific part of our Services, viewed a particular advertisement, or opened a specific email.

SDKs and mobile advertising IDs. Our Services may include third-party software development kits ("SDKs") that allow us and our service providers to collect information about your activity. In addition, some mobile devices come with a resettable advertising ID (such as Apple's IDFA and Google's Advertising ID) that, like cookies and pixel tags, allow us and our service providers to identify your mobile device over time for advertising purposes.

Third-party plugins. Our Site may include plugins from other companies, including social media companies (e.g., the Facebook "Like" button). These plugins may collect information, such as information about the pages you visit, and share it with the company that created the plugin even if you do not click on the plugin. These third-party plugins are governed by the privacy policies and terms of the companies that created them.

Third-party online tracking. We also may partner with certain third parties to collect, analyze, and use some of the personal and other information described in this section. For example, we may allow third parties to set pixels and mobile advertising IDs through the Site. This information may be used for a variety of purposes, including analytics and interest-based advertising, as discussed below (see the section entitled "With Whom and Why We Share Your Information").

Aggregated or deidentified information. We may also share aggregated or deidentified information about users of the Services, such as by publishing a report on trends in the usage of the Services. Such aggregated or deidentified information will not identify you personally.

How We Use Your Information

We use the information that we collect for a variety of purposes. Our legal bases for processing your personal information are: 1) our legitimate interest in running and maintaining our business; 2) performance and fulfillment of our contracts; 3) your consent; and 4) compliance with our legal obligations. In many instances, more than one of these legal bases apply to the processing of your personal information.

The purposes for which we use your information include to:

- Provide you with our Services;
- Respond to your questions or requests concerning the Services;
- Fulfill the terms of any agreement you have with us;
- Fulfill your requests for our Services or otherwise complete a transaction that you initiate;

- Send you information about our Services and other topics that are likely to be of interest to you, including newsletters, updates, or other communications, including promotional emails;
- Improve our artificial intelligence and machine learning;
- Deliver confirmations, account information, notifications, and similar operational communications;
- Improve your user experience and the quality of our products and Services;
- Improve automated insights delivered to you while using our Services;
- Comply with legal and/or regulatory requirements;
- Aggregate and deidentify information;
- Serve advertisements;
- Analyze how visitors use the Services and various Services features, including to count and recognize visitors to the Services;
- Create new products and Services; and
- Manage our business.

With Whom and Why We Share Your Information

We share your information with third parties for a variety of purposes, as described below.

Third-party service providers. Compa uses third-party service providers that perform Services on our behalf, including web-hosting companies, and mailing vendors. These service providers may collect and/or use your information, including information that identifies you personally, to assist us in achieving the purposes discussed above.

We may also share your information with third parties when necessary to fulfill your requests for Services; to complete a transaction that you initiate; to meet the terms of any agreement that you have with us or our partners; or to manage our business.

Analytics. We partner with certain third parties to obtain the automatically collected information discussed above and to engage in analysis, auditing, research, and reporting. These third parties may use pixels or server logs, and they may set and access device IDs and IP addresses from your device.

Interest-based Advertising. The Services also enable third-party tracking mechanisms to collect information about you and your computing devices for use in online interest-based advertising. For example, third parties, such as Facebook, may use the fact that you visited our Site to target online ads to you about our Services. In addition, our third-party advertising networks might use information about your use of our Services to help target advertisements based on your mobile activity in general. For information about interest-based advertising practices, including privacy and confidentiality, visit the Network Advertising Initiative website or the Digital Advertising Alliance website.

The use of online tracking mechanisms by third parties is subject to those third parties' own privacy policies, and not this Policy. If you prefer to prevent third parties from setting and accessing cookies on your computer or other device, you may set your browser to block cookies. Additionally, you may remove yourself from the targeted advertising of companies within the Network Advertising Initiative by opting out here, or of companies participating in the Digital Advertising Alliance by opting out here. Although our Site currently does not respond to "do not track" browser headers, you can limit tracking through these third-party programs and by taking the other steps discussed above.

You may also opt-out of interest-based by adjusting the advertising preferences on your mobile device (for example, in iOS, visit Settings > Privacy > Advertising > Limit Ad Tracking, and in Android, visit

Settings > Google > Ads > Opt out of interest-based ads). Additionally, you may opt out for companies that participate in the Digital Advertising Alliance's AppChoices tool by downloading it here and following the instructions in the app.

Legal purposes. We also may use or share your information with third parties when we believe, in our sole discretion, that doing so is necessary:

- To comply with applicable law or a court order, subpoena, or other legal process;
- To investigate, prevent, or take action regarding illegal activities, suspected fraud, violations of our terms and conditions, or situations involving threats to our property or the property or physical safety of any person or third party;
- To establish, protect, or exercise our legal rights or defend against legal claims; or
- To facilitate the financing, securitization, insuring, sale, assignment, bankruptcy, or other disposal of all or part of our business or assets.

Your Choices

If you wish to access, correct, or delete the personal information we have on file, you may contact us at privacy@trycompa.com.

If you wish to opt-out of marketing emails you receive from us, you may do so by following the instructions in those emails or by contacting us at privacy@trycompa.com.

International Users

If you are a resident of the EU, UK, or another jurisdiction with an applicable privacy law, you may have certain rights available to you. These rights may include:

- The right to be informed about our data collection practices;
- The right to access and rectify your data;
- The right to erase or delete your data;
- The right to data portability;
- The right to restrict and object to the processing of your data (including for direct marketing purposes);
- The right to opt-out of marketing emails and text messages;
- The right to limit our use of any automated decision-making processes;
- The right to lodge a complaint to your local data protection authority; and
- The right to withdraw consent (to the extent applicable).

To exercise any of the rights listed above, please contact us via email at team@trycompa.com. We will respond to your request as soon as reasonably possible but no longer than 30 days.

External Links

The Site may contain links to third-party websites. If you use these links, you will leave the Site. We have not reviewed these third-party sites and do not control and are not responsible for any of these sites, their content, or their privacy policy. Thus, we do not endorse or make any representations about them, or any

information, software, or other products or materials found there, or any results that may be obtained from using them. If you decide to access any of the third-party sites listed on our website, you do so at your own risk.

Data Security

We employ physical, technical, and administrative procedures to safeguard the personal information we collect both online and offline. However, no website or platform is 100% secure, and we cannot ensure or warrant the security of any information you transmit to the Services or to us, and you transmit such information at your own risk.

For questions about information security, please contact us at security@trycompa.com.

Data Retention

We retain personal information about you necessary to fulfill the purpose for which that information was collected or as required or permitted by law. We do not retain personal information longer than is necessary for us to achieve the purposes for which we collected it. When we destroy your personal information, we do so in a way that prevents that information from being restored or reconstructed.

International Users

The information that we collect through or in connection with the Services is transferred to and processed in the United States for the purposes described above. We may also subcontract the processing of your data to, or otherwise share your data with, affiliates or third parties in countries other than your country of residence. The data-protection laws in these countries may be different from, and less stringent than, those in your country of residence. However, we comply with all applicable laws regarding international data transfers.

By using the Services or by providing any information to us, you expressly consent to such transfer and processing.

Children

Content on this Services is directed at individuals over the age of 18 and is not directed at children under the age of 13. We do not knowingly collect personally identifiable information from children under the age of 13.

Changes to this Policy

We may make changes to the Services in the future and as a consequence will need to revise this Policy to reflect those changes. We will post all such changes on the Services, so you should review this page periodically.

How to Contact Us

Should you have any questions or concerns about this Policy, you can contact us at by email at privacy@trycompa.com.

Cookie Policy

This Cookie Policy ("Policy") describes how Compa Technologies Inc. ("Compa," "we," "our," "us") collects, processes, uses, and discloses certain information obtained through your use of our website (the "Site"), which is available at https://www.trycompa.com. To learn more about our privacy practices in general, please review our Privacy Policy.

What are cookies?

Cookies are small files that are stored on your mobile device through the Site. A cookie allows the Site to recognize whether you have visited before and may store user preferences and other information. For example, cookies can be used to collect or store information about your use of the Site during your current session and over time (including the pages you view and the files you download), your device's operating system, your device ID, IP address, and your general geographic location.

What types of cookies do we use?

Necessary Cookies. Necessary cookies allow us to offer the best possible experience when accessing and navigating through our Site. For example, these cookies allow us to recognize that you have created an account with us and accessed the Site previously.

Functionality Cookies. Functionality cookies let us operate the Site in accordance with the choices you make. For example, we will remember your username and how you customized the Site during future visits.

Analytical Cookies. These cookies enable us and third-party services to collect aggregated data for statistical purposes on how your visitors use the Site. These cookies do not collect information such as your name or email address and are used to help us improve your user experience of the Site.

Advertising Cookies. These cookies allow us and third-party services to show more relevant advertising to people who visit the Site (and other websites) by showing you advertisements that are based on your browsing patterns and the way you interact with our Site and others. Please review the section below on interest-based advertising to learn more about third-party advertising cookies in particular.

How can you manage cookies?

You may stop your browser from accepting cookies altogether by changing your browser's cookie settings. You can usually find these settings in the "options" or "preferences" menu of your browser.

How does the Site use interest-based advertising?

The Site enables third-party tracking mechanisms (including cookies) to collect information about you and your computing devices for use in online interest-based advertising. For example, third parties, such as Facebook, may use the fact that you visited our Site to target online ads to you about our services. In addition, our third-party advertising networks might use information about your use of our services to help target advertisements based on your mobile activity in general. For information about interest-based advertising practices, including privacy and confidentiality, visit the Network Advertising Initiative website or the Digital Advertising Alliance website.

The use of online tracking mechanisms by third parties is subject to those third parties' own privacy policies, and not this policy. If you prefer to prevent third parties from setting and accessing cookies on your computer or other device, you may set your browser to block cookies. Additionally, you may remove yourself from the targeted advertising of companies within the Network Advertising Initiative by

opting out here, or of companies participating in the Digital Advertising Alliance by opting out here. Although our Site currently does not respond to “do not track” browser headers, you can limit tracking through these third-party programs and by taking the other steps discussed above.

You may also opt-out of interest-based by adjusting the advertising preferences on your mobile device (for example, in iOS, visit Settings > Privacy > Advertising > Limit Ad Tracking, and in Android, visit Settings > Google > Ads > Opt out of interest-based ads). Additionally, you may opt out for companies that participate in the Digital Advertising Alliance's AppChoices tool by downloading it here and following the instructions in the app.

How can you contact us?

If you have any questions about this Policy, you may contact us at team@trycompa.com. You may also visit our Privacy Policy to learn more about our privacy practices.