Note to copy:

For Clients that would like to receive a pdf copy of the Workzoom Terms of Service, we have made this copy available to you. No changes made to this copy are agreed to by Nortek Solutions Inc. (dba Workzoom) or its affiliates. If you require a signed copy, please contact your Workzoom representative.

Please note that we update the Data Processing Agreement as we describe in the 'General Provisions' section below. Current Data Processing Agreement terms are available at https://www.workzoom.com/legal/dpa and archived Data Processing Agreement terms are available at https://www.workzoom.com/legal/archive.

If you would like to receive an email notification when we update the Workzoom Data Processing Agreement, please complete the form found at https://www.workzoom.com/legal/subscribe-to-updates.

If you have any questions, please contact your Workzoom representative.

This Workzoom Data Processing Agreement and its Annexes ("DPA") reflects the parties' agreement with respect to the Processing of Personal Data by us on your behalf in connection with the Workzoom Subscription Services.

This DPA is supplemental to, and forms an integral part of, the Agreement as defined in your Order Form and is effective upon its incorporation into the Agreement. In case of any conflict or inconsistency with the terms of the Agreement, this DPA will take precedence over the terms of the Agreement to the extent of such conflict or inconsistency.

We update these terms from time to time. We will update you of changes if you have an active Workzoom subscription and have subscribed to receive email notifications at https://www.workzoom.com/legal/subscribe-to-updates.

Terms not otherwise defined in this DPA will have the meaning as set forth in the Agreement.

1. DEFINITIONS

"California Personal Information" means Personal Data that is subject to the protection of the CCPA.

"CCPA" means California Civil Code Sec. 1798.100 et seq. (also known as the California Consumer Privacy Act of 2018).

"Consumer", **"Business"**, **"Sell"** and **"Service Provider"** will have the meanings given to them in the CCPA.

"Controller" means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

“Data Protection Laws” means all applicable worldwide legislation relating to data protection and privacy which applies to the respective party in the role of Processing Personal Data in question under the Agreement, including without limitation European Data Protection Laws, the CCPA and the data protection and privacy laws of Australia and Singapore; in each case as amended, repealed, consolidated, or replaced from time to time.

“Data Subject” means the individual to whom Personal Data relates.

"Europe" means the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom.

“European Data” means Personal Data that is subject to the protection of European Data Protection Laws.

"European Data Protection Laws" means data protection laws applicable in Europe, including: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ("GDPR"); (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; and (iii) applicable national implementations of (i) and (ii); or (iii) GDPR as it forms parts of the United Kingdom domestic law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 ("UK GDPR"); and (iv) Swiss Federal Data Protection Act on 19 June 1992 and its Ordinance ("Swiss DPA"); in each case, as may be amended, superseded or replaced.

“Instructions” means the written, documented instructions issued by a Controller to a Processor, and directing the same to perform a specific or general action with regard to Personal Data (including, but not limited to, depersonalizing, blocking, deletion, making available).

"Permitted Affiliates" means any of your Affiliates that (i) are permitted to use the Subscription Services pursuant to the Agreement but have not signed their own separate agreement with us and are not a “Client” as defined under the Agreement, (ii) qualify as a Controller of Personal Data Processed by us, and (iii) are subject to European Data Protection Laws.

“Personal Data” means any information relating to an identified or identifiable individual where such information is contained within Client Data and is protected similarly as personal data, personal information, or personally identifiable information under applicable Data Protection Laws.

“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 transmitted, stored, or otherwise Processed by us and/or our Sub-Processors in connection with the provision of the Subscription Services. "Personal Data Breach" will not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

“Processing” means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available,

alignment or combination, restriction, or erasure of Personal Data. The terms **"Process"**, **"Processes"** and **"Processed"** will be construed accordingly.

"Processor" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

"Standard Contractual Clauses" means the standard contractual clauses for Processors annexed to the European Commission's Decision (EU) 2021/914 of 4 June 2021, in the form set out at Annex 4; as may be amended, superseded or replaced.

"Sub-Processor" means any Processor engaged by us or our Affiliates to assist in fulfilling our obligations with respect to the provision of the Subscription Services under the Agreement. Sub-Processors may include third parties or our Affiliates but will exclude any Workzoom employee or consultant.

2. CLIENT RESPONSIBILITIES

2.1 Compliance with Laws. Within the scope of the Agreement and in its use of the services, you will be responsible for complying with all requirements that apply to it under applicable Data Protection Laws with respect to its Processing of Personal Data and the Instructions it issues to us.

2.2 In particular but without prejudice to the generality of the foregoing, you acknowledge and agree that you will be solely responsible for: (i) the accuracy, quality, and legality of Client Data and the means by which you acquired Personal Data; (ii) complying with all necessary transparency and lawfulness requirements under applicable Data Protection Laws for the collection and use of the Personal Data, including obtaining any necessary consents and authorizations (particularly for use by Client for marketing purposes); (iii) ensuring you have the right to transfer, or provide access to, the Personal Data to us for Processing in accordance with the terms of the Agreement; (iv) ensuring that your Instructions to us regarding the Processing of Personal Data comply with applicable laws, including Data Protection Laws; and (v) complying with all laws (including Data Protection Laws) applicable to any emails or other content created, sent or managed through the Subscription Services, including those relating to obtaining consents (where required) to send emails, the content of the emails and its email deployment practices. You will inform us without undue delay if you are not able to comply with your responsibilities under this 'Compliance with Laws' section or applicable Data Protection Laws.

2.3 Controller Instructions. The parties agree that the Agreement, together with your use of the Subscription Service in accordance with the Agreement, constitute your complete Instructions to us in relation to the Processing of Personal Data, so long as you may provide additional instructions during the subscription term that are consistent with the Agreement, the nature and lawful use of the Subscription Service.

2.4 Security. You are responsible for independently determining whether the data security provided for in the Subscription Service adequately meets your obligations under applicable Data Protection Laws. You are also responsible for your secure use of the Subscription Service, including

protecting the security of Personal Data in transit to and from the Subscription Service (including to securely backup or encrypt any such Personal Data).

3. WORKZOOM OBLIGATIONS

3.1 Compliance with Instructions. We will only Process Personal Data for the purposes described in this DPA or as otherwise agreed within the scope of your lawful Instructions, except where and to the extent otherwise required by applicable law. We are not responsible for compliance with any Data Protection Laws applicable to you or your industry that are not generally applicable to us.

3.2 Conflict of Laws. If we become aware that we cannot Process Personal Data in accordance with your Instructions due to a legal requirement under any applicable law, we will (i) promptly notify you of that legal requirement to the extent permitted by the applicable law; and (ii) where necessary, cease all Processing (other than merely storing and maintaining the security of the affected Personal Data) until such time as you issue new Instructions with which we are able to comply. If this provision is invoked, we will not be liable to you under the Agreement for any failure to perform the applicable Subscription Services until such time as you issue new lawful Instructions with regard to the Processing.

3.3 Security. We will implement and maintain appropriate technical and organizational measures to protect Personal Data from Personal Data Breaches, as described under Annex 2 to this DPA ("Security Measures"). Notwithstanding any provision to the contrary, we may modify or update the Security Measures at our discretion provided that such modification or update does not result in a material degradation in the protection offered by the Security Measures.

3.4 Confidentiality. We will ensure that any personnel whom we authorize to Process Personal Data on our behalf is subject to appropriate confidentiality obligations (whether a contractual or statutory duty) with respect to that Personal Data.

3.5 Personal Data Breaches. We will notify you without undue delay after we become aware of any Personal Data Breach and will provide timely information relating to the Personal Data Breach as it becomes known or reasonably requested by you. At your request, we will promptly provide you with such reasonable assistance as necessary to enable you to notify relevant Personal Data Breaches to competent authorities and/or affected Data Subjects, if you are required to do so under Data Protection Laws.

3.6 Deletion or Return of Personal Data. We will delete all Client Data, including Personal Data (including copies thereof) Processed pursuant to this DPA, on termination or expiration of your Subscription Service in accordance with the procedures set out in the Workzoom Terms of Service. This term shall apply except where we are required by applicable law to retain some or all of the Client Data, or where we have archived Client Data on back-up systems, which data we will securely isolate and protect from any further Processing and delete in accordance with our deletion practices. You may retrieve your Client Data from your account in accordance with the Workzoom Terms of Service.

4. DATA SUBJECT REQUESTS

The Subscription Service provides you with a number of controls that you can use to retrieve, correct, delete or restrict Personal Data, which you can use to assist it in connection with its obligations under Data Protection Laws, including your obligations relating to responding to requests from Data Subjects to exercise their rights under applicable Data Protection Laws ("Data Subject Requests").

To the extent that you are unable to independently address a Data Subject Request through the Subscription Service, then upon your written request we will provide reasonable assistance to you to respond to any Data Subject Requests or requests from data protection authorities relating to the Processing of Personal Data under the Agreement. You shall reimburse us for the commercially reasonable costs arising from this assistance.

If a Data Subject Request or other communication regarding the Processing of Personal Data under the Agreement is made directly to us, we will promptly inform you and will advise the Data Subject to submit their request to you. You will be solely responsible for responding substantively to any such Data Subject Requests or communications involving Personal Data.

5. SUB-PROCESSORS

You agree that we may engage Sub-Processors to Process Personal Data on your behalf. We have currently appointed, as Sub-Processors, the Workzoom Affiliates and third parties listed in Annex 3 to this DPA. We will notify you if we add or replace any Sub-Processors listed in Annex 3 at least 30 days prior to any such changes.

Where we engage Sub-Processors, we will impose data protection terms on the Sub-Processors that provide at least the same level of protection for Personal Data as those in this DPA (including, where appropriate, the Standard Contractual Clauses), to the extent applicable to the nature of the services provided by such Sub-Processors. We will remain responsible for each Sub-Processor's compliance with the obligations of this DPA and for any acts or omissions of such Sub-Processor that cause us to breach any of its obligations under this DPA.

6. DATA TRANSFERS

You acknowledge and agree that we may access and Process Personal Data on a global basis as necessary to provide the Subscription Service in accordance with the Agreement, and in particular that Personal Data may be transferred to and Processed by Workzoom in Canada, the United States and to other jurisdictions where Workzoom Affiliates and Sub-Processors have operations. Wherever Personal Data is transferred outside its country of origin, each party will ensure such transfers are made in compliance with the requirements of Data Protection Laws.

7. ADDITIONAL PROVISIONS FOR EUROPEAN DATA

7.1 Scope. This 'Additional Provisions for European Data' section shall apply only with respect to European Data.

7.2 Roles of the Parties. When Processing European Data in accordance with your Instructions, the parties acknowledge and agree that you are the Controller of European Data and we are the Processor.

7.3 Instructions. If we believe that your Instruction infringes European Data Protection Laws (where applicable), we will inform you without delay.

7.4 Objection to New Sub-Processors. We will give you the opportunity to object to the engagement of new Sub-Processors on reasonable grounds relating to the protection of Personal Data within 30 days of notifying you in accordance with the 'Sub-Processors' section. If you do notify us of such an objection, the parties will discuss your concerns in good faith with a view to achieving a commercially reasonable resolution. If no such resolution can be reached, we will, at our sole discretion, either not appoint the new Sub-Processor, or permit you to suspend or terminate the affected Subscription Service in accordance with the termination provisions of the Agreement without liability to either party (but without prejudice to any fees incurred by you prior to suspension or termination). The parties agree that by complying with this sub-section (d), Workzoom fulfils its obligations under Sections 9 of the Standard Contractual Clauses.

7.5 Sub-Processor Agreements. For the purposes of Clause 9(c) of the Standard Contractual Clauses, you acknowledge that we may be restricted from disclosing Sub-Processor agreements but we shall use reasonable efforts to require any Sub-Processor we appoint to permit it to disclose the Sub-Processor agreement to you and shall provide (on a confidential basis) all information we reasonably can.

7.6 Data Protection Impact Assessments and Consultation with Supervisory Authorities. To the extent that the required information is reasonably available to us, and you do not otherwise have access to the required information, we will provide reasonable assistance to you with any data protection impact assessments, and prior consultations with supervisory authorities or other competent data privacy authorities to the extent required by European Data Protection Laws.

7.7 Transfer Mechanisms for Data Transfers.

(a) Workzoom shall not transfer European Data to any country or recipient not recognized as providing an adequate level of protection for Personal Data (within the meaning of applicable European Data Protection Laws), unless it first takes all such measures as are necessary to ensure the transfer is in compliance with applicable European Data Protection Laws. Such measures may include (without limitation) transferring such data to a recipient that is covered by a suitable framework or other legally adequate transfer mechanism recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Data, to a recipient that has achieved binding corporate rules authorization in accordance with European Data Protection Laws, or to a recipient that has executed appropriate standard contractual clauses in each case as adopted or approved in accordance with applicable European Data Protection Laws.

(b) You acknowledge that in connection with the performance of the Subscription Services, Workzoom is a recipient of European Data in Canada. The parties agree to abide by and process European Data in compliance with the Standard Contractual Clauses.

(c) The parties agree that for the purposes of the Standard Contractual Clauses, (i) Workzoom will be the "data importer" and Client will be the "data exporter" (on behalf of itself and Permitted Affiliates); (ii) the Annexes of the Standard Contractual Clauses shall be populated with the relevant information set out in Annex 1 and Annex 2 of this DPA; (iii) if and to the extent the Standard Contractual Clauses conflict with any provision of this DPA, the Standard Contractual Clauses will prevail to the extent of such conflict.

(d) To the extent that and for so long as the Standard Contractual Clauses as implemented in accordance with this DPA cannot be relied on by the parties to lawfully transfer Personal Data in compliance with the UK GDPR, the applicable standard data protection clauses issued, adopted or permitted under the UK GDPR shall be incorporated by reference, and the annexes, appendices or tables of such clauses shall be deemed populated with the relevant information set out in Annex 1 and Annex 2 of this DPA.

(e) If for any reason Workzoom cannot comply with its obligations under the Standard Contractual Clauses or is in breach of any warranties under the Standard Contractual Clauses, and you intend to suspend the transfer of European Data to Workzoom or terminate the Standard Contractual Clauses, you agree to provide us with reasonable notice to enable us to cure such non-compliance and reasonably cooperate with us to identify what additional safeguards, if any, may be implemented to remedy such non-compliance. If we have not or cannot cure the non-compliance, you may suspend or terminate the affected part of the Subscription Service in accordance with the Agreement without liability to either party (but without prejudice to any fees you have incurred prior to such suspension or termination).

7.8 Demonstration of Compliance. We will make all information reasonably necessary to demonstrate compliance with this DPA available to you and allow for and contribute to audits, including inspections conducted by your auditor in order to assess compliance with this DPA. You acknowledge and agree that you will exercise your audit rights under this DPA and Clause 8.9 of the Standard Contractual Clauses by instructing us to comply with the audit measures described in this 'Demonstration of Compliance' section. You acknowledge that the Subscription Service is hosted by our data center partners who maintain independently validated security programs (including SOC 2 and ISO 27001) and that our systems are regularly tested by independent third-party penetration testing firms. Upon request, we will supply (on a confidential basis) a summary copy of its penetration testing report(s) to you so that you can verify our compliance with this DPA. Further, at your written request, we will provide written responses (on a confidential basis) to all reasonable requests for information made by you necessary to confirm our compliance with this DPA, provided that you will not exercise this right more than once per calendar year unless you have reasonable grounds to suspect non-compliance with the DPA.

8. ADDITIONAL PROVISIONS FOR CALIFORNIA PERSONAL INFORMATION

8.1 Scope. The 'Additional Provisions for California Personal Information' section of the DPA will apply only with respect to California Personal Information.

8.2 Roles of the Parties. When processing California Personal Information in accordance with your Instructions, the parties acknowledge and agree that you are a Business and we are a Service Provider for the purposes of the CCPA.

8.3 Responsibilities. The parties agree that we will Process California Personal Information as a Service Provider strictly for the purpose of performing the Subscription Services and Consulting Services under the Agreement (the "Business Purpose") or as otherwise permitted by the CCPA, including as described in the 'Data Practices and Service Data' section of our Product Privacy Policy.

9. GENERAL PROVISIONS

9.1 Amendments. Notwithstanding anything else to the contrary in the Agreement and without prejudice to the 'Compliance with Instructions' or 'Security' sections of this DPA, we reserve the right to make any updates and changes to this DPA and the terms that apply in the 'Amendment; No Waiver' section of the Workzoom Terms of Service will apply.

9.2 Severability. If any individual provisions of this DPA are determined to be invalid or unenforceable, the validity and enforceability of the other provisions of this DPA will not be affected.

9.3 Limitation of Liability. Each party and each of their Affiliates' liability, taken in aggregate, arising out of or related to this DPA (and any other DPAs between the parties) and the Standard Contractual Clauses (where applicable), whether in contract, tort or under any other theory of liability, will be subject to the limitations and exclusions of liability set out in the 'Limitation of Liability' section of the Workzoom Terms of Service and any reference in such section to the liability of a party means aggregate liability of that party and all of its Affiliates under the Agreement. For the avoidance of doubt, if Workzoom is not a party to the Agreement, the 'Limitation of Liability' section of the Workzoom Terms of Service will apply as between you and Workzoom.

9.4 Governing Law. This DPA will be governed by and construed in accordance with the laws of the Province of Ontario and the federal laws of Canada applicable in the Province of Ontario, unless required otherwise by Data Protection Laws.

10. PARTIES TO THIS DPA

10.1 Permitted Affiliates. By signing the Agreement, you enter into this DPA (including, where applicable, the Standard Contractual Clauses) on behalf of yourself and in the name and on behalf of your Permitted Affiliates. For the purposes of this DPA only, and except where indicated otherwise, the terms "Client", "you" and "your" will include you and such Permitted Affiliates.

10.2 Authorization. The legal entity agreeing to this DPA as Client represents that it is authorized to agree to and enter into this DPA for and on behalf of itself and, as applicable, each of its Permitted Affiliates.

10.3 Remedies. The parties agree that (i) solely the Client entity that is the contracting party to the Agreement will exercise any right or seek any remedy any Permitted Affiliate may have under this DPA on behalf of its Affiliates, and (ii) the Client entity that is the contracting party to the Agreement will exercise any such rights under this DPA not separately for each Permitted Affiliate individually but in a combined manner for itself and all of its Permitted Affiliates together. The Client entity that is the contracting entity is responsible for coordinating all Instructions, authorizations and communications with us under the DPA and will be entitled to make and receive any communications related to this DPA on behalf of its Permitted Affiliates.

10.4 Other rights. The parties agree that you will, when reviewing our compliance with this DPA pursuant to the 'Demonstration of Compliance' section, take all reasonable measures to limit any impact on us and our Affiliates by combining several audit requests carried out on behalf of the Client entity that is the contracting party to the Agreement and all of its Permitted Affiliates in one single audit.

(Remainder of page intentionally left blank)

Annex 1 - Details of Processing

1. LIST OF PARTIES

Data exporter:
Name: The Client, as defined in the Order Form (on behalf of itself and Permitted Affiliates)

Address: The Client's address, as set out in the Order Form

Contact person's name, position and contact details: The Client's contact details, as set out in the Order Form.

Activities relevant to the data transferred under these Clauses: Processing of Personal Data in connection with Client's use of the Workzoom Subscription Services governed by the Workzoom Terms of Service.

Role (controller/processor): Controller

Data importer:
Name: Nortek Solutions Inc. (dba Workzoom)

Address: 150 King St. West, Suite 200, Toronto, Ontario, M5H 1J9, Canada

Contact person's name, position and contact details: Ted Glendening, VP of Corporate Development, Workzoom, 150 King St. West, Suite 200, Toronto, Ontario, M5H 1J9, Canada

Activities relevant to the data transferred under these Clauses: Processing of Personal Data in connection with Client's use of the Workzoom Subscription Services governed by the Workzoom Terms of Service

Role (controller/processor): Processor

2. DESCRIPTION OF TRANSFER

Categories of Data Subjects whose Personal Data is Transferred
Employees - including, past, potential, present and future staff (including directors/board members, agents, independent contractors, volunteers, interns, part time/full time/temporary/ casual workers, retirees, and benefit recipients) of Client.

Candidates – past, potential, present and future candidates of Client who are being considered or have been selected for placement for a role with Client (including candidate information sourced from publicly available sources).

Referees / References – past, present, potential and future employment referees for a particular candidate of Client.

Employee Associates – including emergency contacts, guardians, parents, siblings, spouse/partner, children, other relatives, beneficiaries, dependents and personal contacts

Supplier/Vendor Associates - Business Contacts

Categories of Personal Data Transferred
Employees and Candidates: Personal information (including, but not limited to, name, identification number(s), photograph(s), address, birth date, gender, marital status, number of children, emergency contact, telephone number(s), academic and professional qualifications, CV/resume, employment history, language proficiency, etc.); Information in connection with the employee's job (including, but not limited to, title, grade, location, reporting lines, team affiliation, hire date, working hours, contract details, performance and evaluation data, employee discipline information, work history, benefits and insurance, assets assigned, training, time-off documentation, etc.); Payroll related information (including, but not limited to, salary and compensation information, tax and social security information, bank details, pensions, share options, bonuses, other benefits, etc.).

Referees / References / Associates: Contact details: name, address, telephone number (fixed and mobile), email address, fax number.

Sensitive Data transferred and applied restrictions or safeguards
Health and disability information.

Frequency of the transfer
Continuous

Nature of the Processing
Personal Data will be Processed in accordance with the Agreement and may be subject to the following Processing activities:

1. Storage and other Processing necessary to provide, maintain and improve the Subscription Services provided to you; and/or
2. Disclosure in accordance with the Agreement and/or as compelled by applicable laws.

Purpose of the transfer and further processing
We will Process Personal Data as necessary to provide the Subscription Services pursuant to the Agreement, as further specified in the Order Form, and as further instructed by you in your use of the Subscription Services.

Period for which Personal Data will be retained
Subject to the 'Deletion or Return of Personal Data' section of this DPA, we will Process Personal Data for the duration of the Agreement, unless otherwise agreed in writing.

3. COMPETENT SUPERVISORY AUTHORITY

For the purposes of the Standard Contractual Clauses, the supervisory authority that shall act as competent supervisory authority is either (i) where Client is established in an EU Member State, the supervisory authority responsible for ensuring Client's compliance with the GDPR; (ii) where Client is not established in an EU Member State but falls within the extra-territorial scope of the GDPR and has appointed a representative, the supervisory authority of the EU Member State in which Client's representative is established; or (iii) where Client is not established in an EU Member State but falls within the extra-territorial scope of the GDPR without having to appoint a representative, the

supervisory authority of the EU Member State in which the Data Subjects are predominantly located. In relation to Personal Data that is subject to the UK GDPR or Swiss DPA, the competent supervisory authority is the UK Information Commissioner or the Swiss Federal Data Protection and Information Commissioner (as applicable).

(Remainder of page intentionally left blank)

Annex 2 - Security Measures

We currently observe the Security Measures described in this Annex 2. All capitalized terms not otherwise defined herein shall have the meanings as set forth in the Workzoom Terms of Service.

1. ACCESS CONTROL

1.1 Preventing Unauthorized Product Access

Outsourced processing: We host our Service with outsourced cloud infrastructure providers. Additionally, we maintain contractual relationships with vendors in order to provide the Service in accordance with our DPA. We rely on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors.

Physical and environmental security: We host our product infrastructure with multi-tenant, outsourced infrastructure providers. The physical and environmental security controls are audited for SOC 2 Type II and ISO 27001 compliance, among other certifications.

Authentication: We implement a uniform password policy for our customer products. Clients and authorized users must authenticate before accessing the application or any non-public client data.

Authorization: Client Data is stored in multi-tenant storage systems accessible to Clients via only application user interfaces and application programming interfaces. Clients are not allowed direct access to the underlying application infrastructure. The authorization model in each of our products is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customization options. Authorization to data sets is performed through validating the user's permissions against the attributes associated with each data set.

Application Programming Interface (API) access: Public product APIs may be accessed using an API key or through Oauth authorization.

1.2 Preventing Unauthorized Product Use

We implement industry standard access controls and detection capabilities for the internal networks that support its products.

Access controls: Network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure. The technical measures implemented include Virtual Private Cloud (VPC) implementations, security group assignment, and traditional firewall rules.

Intrusion detection and prevention: We implement a Web Application Firewall (WAF) solution to protect hosted customer websites and other internet-accessible applications. The WAF is designed to identify and prevent attacks against publicly available network services.

Static code analysis: Security reviews of code stored in our source code repositories is performed, checking for coding best practices and identifiable software flaws.

Penetration testing: We maintain relationships with industry recognized penetration testing service providers for annual penetration tests. The intent of the penetration tests is to identify and resolve foreseeable attack vectors and potential abuse scenarios.

1.3 Limitations of Privilege & Authorization Requirements

Workzoom ensures that the persons entitled to use its data processing systems are only able to access the data within the scope and to the extent covered by their respective access permission (authorization) and that Personal Data cannot be read, copied or modified or removed without authorization. This is accomplished by:

- employee policies and training in respect of each employee's access rights to Personal Data;
- protecting data against unauthorized access by means of encryption or pseudonymization (as appropriate);
- effective and measured disciplinary action against individuals who access Personal Data without authorization;
- release of data to only authorized persons; and
- policies controlling the retention of back-up copies.

Product access: A subset of our employees have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support and to troubleshoot potential problems. Employees are granted access by role, and roles are reviewed at least once every six months.

Background checks: All Workzoom employees sign a non-disclosure agreement and code of ethics and undergo a third-party background check as part of the new-hire process in accordance with and as permitted by the applicable laws. All Workzoom employees are required to conduct themselves in a manner consistent with company guidelines, non-disclosure requirements, and ethical standards.

2. TRANSMISSION CONTROL

In-transit: All data in transit is encrypted using 128-bit+ TLS 1.2 over TCP/IP using a 2048-bit certificate and strong cipher suites.

At-rest: Passwords are encrypted with the "PBKDF2WithHmacSHA1" algorithm which includes salted password hashing with key stretching. This method ensures best of class protection against dictionary, rainbow table and brute force attacks.

Data at rest is encrypted using the Advanced Encryption Standard (AES 256).

3. INPUT CONTROL

Detection: We designed our infrastructure to log extensive information about the system behavior, traffic received, system authentication, and other application requests. Internal systems aggregated log data and alert authorized technical personnel of malicious, unintended, or anomalous activities. Our personnel, including security, operations, and support personnel, are responsive to known incidents.

Response and tracking: We maintain a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, operations, or technical support personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, we will take appropriate steps to minimize product and Client damage or unauthorized disclosure. Notification to you will be in accordance with the terms of the Agreement.

4. AVAILABILITY CONTROL

Infrastructure availability: Workzoom is powered by intelligent clustering infrastructure that utilizes auto scaling and self-healing capabilities to ensure maximum availability, resiliency, and speed, while maintaining strict control over client data via a central database.

Workzoom utilizes Amazon Web Services' global network infrastructure with Global Accelerators and Edge Computing to ensure absolute minimal latency by routing Workzoom traffic to endpoints nearest to the client.

The infrastructure providers use commercially reasonable efforts to ensure a minimum of 99.95% uptime. The providers maintain a minimum of N+1 redundancy to power, network, and HVAC services.

Fault tolerance: Workzoom uses real-time replication for client data, across different availability zones with a minimum distance of 60 miles / 100 km to mitigate environmental and/or infrastructure-related failures. Encrypted back-ups are also taken daily (more frequent back-up options are available based on client requirements) and stored securely off-site at a minimum distance of 60 miles / 100 km from the primary server locations. Daily backups are held using a WORM system (Write Once Read Many) utilizing Object Locking. Therefore, once a backup is taken, no one can modify it (not even us). Removing any data requires MFA. We also take entire server images weekly to ensure we can restore not just data, but configurations as well. All of this protects client data against sophisticated hacking targeting back-up and recovery resources.

In the event of an incident or server failure, clients are switched to the replication environment and in the worst case, data is recovered from the last daily backups. Because Workzoom application servers use intelligent clustering infrastructure that covers a multitude of availability zones at all times, no application downtime will occur in the event of an incident at a single data centre. However, in the event of a major incident, the maximum data exposure is 24 hours and recovery time would normally be between 5 minutes and 8 hours, depending on the size and volume of restoration required.

(Remainder of page intentionally left blank)

Annex 3 - List of Sub-Processors

1. Amazon Web Services, Inc.

Mia Dakic
dakicm@amazon.com

Amazon Web Services is used as our infrastructure partner for the hosting of Personal Data for the performance of the Services provided by Workzoom to the Client pursuant to the Agreement and for the duration of the performance of those Services.

2. HireAbility.com, LLC

Shane Chubb, Vice President, Sales & Integration
+1 603-432-6653
schubb@hireability.com

HireAbility services are used to provide candidate resume parsing as part of the recruiting module of the Workzoom application.

(Remainder of page intentionally left blank)

Annex 4 – Standard Contractual Clauses

Module Two: Transfer Controller to Processor (C2P)

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

> (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex 1.A. (hereinafter each "data exporter"), and
>
> (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex 1.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex 1.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9 - Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex 1.B.

Clause 7

Docking clause

a) [Intentionally omitted]

SECTION II - OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex 1.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex 2 and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex 1.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration,

unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex 1.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) 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 30 business 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.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data

importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex 1.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III - LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination- including those requiring the disclosure of data to public authorities or authorising access by such authorities - relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent

supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authorities, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until

required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV - FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

> (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
>
> (ii) the data importer is in substantial or persistent breach of these Clauses; or
>
> (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without

prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

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 EU member state that Client's primary office and/or headquarters is located in.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the jurisdiction specified in Clause 17.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

UK AND SWISS ADDENDUM TO THE STANDARD CONTRACTUAL CLAUSES

(a) This Addendum amends the Standard Contractual Clauses to the extent necessary so they operate for transfers made by the data exporter to the data importer, to the extent that the UK GDPR or Swiss DPA (as defined in the Workzoom Data Processing Addendum) apply to the data exporter's processing when making that transfer.

(b) The Standard Contractual Clauses shall be amended with the following modifications:

(i) references to "Regulation (EU) 2016/679" shall be interpreted as references to the UK GDPR or Swiss DPA (as applicable);

(ii) references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of the UK GDPR or Swiss DPA (as applicable);

(iii) references to Regulation (EU) 2018/1725 shall be removed;

(iv) references to "EU", "Union" and "Member State" shall be replaced with references to the "UK" or "Switzerland" (as applicable);

(v) Clause 13(a) and Part C of Annex II are not used and the "competent supervisory authority" shall be the United Kingdom Information Commissioner or Swiss Federal Data Protection Information Commissioner (as applicable);

(vi) references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Information Commissioner" and the "courts of England and Wales" or the "Swiss Federal Data Protection Information Commissioner" and "applicable courts of Switzerland" (as applicable);

(vii) in Clause 17, the Standard Contractual Clauses shall be governed by the laws of England and Wales or Switzerland (as applicable); and

(viii) to the extent the UK GDPR applies to the processing, Clause 18 shall be replaced to state: "Any dispute arising from these Clauses shall be resolved by the courts of England and

Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts"; and

(ix) to the extent the Swiss DPA applies to the processing, Clause 18 shall be replaced to state: "Any dispute arising from these Clauses shall be resolved by the competent courts of Switzerland. The Parties agree to submit themselves to the jurisdiction of such courts".

(Remainder of page intentionally left blank)