DATA PROCESSING AGREEMENT

Controller-Processor / Processor - Processor or Sub-processor

Last updated: August 18, 2026

This Data Processing Agreement ("DPA") forms part of the agreement between **The Data Company Technologies Inc.** (or, if applicable, the other *Nimble* entity specified in the Order or a master agreement, "**Company**") and the undersigned service provider ("**Vendor**"), each a "Party" and collectively, the "Parties". This DPA forms an integral part of the binding agreement signed by the parties ("**Agreement**") and reflects the parties' agreement with regard to the Processing of Personal Data by Vendor on behalf of Company and/or Company's clients (also, "Controller").

By engaging with Company in the framework of the Agreement, Vendor accepts this DPA and represents and warrants that it has full authority to bind itself to this DPA and comply with its terms and conditions.

When Vendor is based outside the European Union (EU) or the European Economic Area (EEA), or the United Kingdom (UK), accesses or allows access to Personal Data from non-EU (or EEA) countries, or the UK, or otherwise transfers data to non-EU (or EEA/UK) countries, the Parties will add to this DPA an adequate mechanism that qualifies as a legal basis for restricted cross-border data transfers, as further detailed in Section 10.

I. Capitalized terms not defined herein shall have the meanings assigned to such terms in the Agreement.

II. In the event of any conflict between the provisions of this DPA and the provisions of the Agreement, the provisions of this DPA shall prevail over the conflicting provisions of the Agreement with respect to the Processing and securing of Personal Data.

1. SCOPE AND APPLICABILITY

1.1. This DPA applies to the extent that the Applicable Data Protection Law governs the Processing of Personal Data under the Agreement, or, when Vendor is likely to Process Company Data, including Company's Customer Data. This icludes any in the following circumstances:

(a) the Processing is in the context of the activities of an establishment of either Party in the EU, EEA or the UK; or

(b) the Personal Data relates to Data Subjects who are in the EU, EEA or UK and the Processing relates to the offering to them of goods or services or the monitoring of their behavior on behalf of Company.

1.2. Notwithstanding the above, this DPA and the obligations hereunder do **not** apply to aggregated or fully and irreversibly anonymized information that cannot, by any means reasonably likely to be used, be attributed to an identified or identifiable natural person, and the burden of demonstrating that information is anonymized rests with Vendor.

1.3. This DPA sets forth the Parties' responsibilities and obligations regarding the Processing of Personal Data during the Parties' Agreement and thereafter.

2. DEFINITIONS

2.1. **Affiliated Company** means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. “Control” for purposes of this definition means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

2.2. **Data Protection Law** means all applicable and binding privacy and data protection laws and regulations, including such laws and regulations of the European Union (EU), the European Economic Area (EEA) and their Member States, Switzerland, the United Kingdom, Canada, Israel and the United States of America, as applicable to the Processing of Personal Data under the Agreement, including, without limitation, the GDPR, the UK GDPR, the CCPA, the CPRA and any other comprehensive US state privacy law, the Israeli Privacy Protection Law, 5741-1981 (including Amendment No. 13) and the Privacy Protection (Data Security) Regulations, 5777-2017, Quebec Law 25, and, where Vendor provides or deploys an AI System, Regulation (EU) 2024/1689 (the EU AI Act), in each case as amended or replaced from time to time and as applicable to the Processing of Personal Data hereunder and in effect at the time of Processor’s performance hereunder.

2.3. **“CCPA**” and/or “**CPRA**” means, respectively, the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 et. seq. and the California Privacy Rights Act, expanding and amending the CCPA.

2.4. The terms "**Controller**", "**Processor**", “**Sub-Processor**”, "**Data Subject**", "**Personal Data**", "**Processing**" (and/or "**Process**"), “**Personal Data Breach**”, the **“Union**”, “**Member State**” and "**Special Categories of Personal Data**" shall have the meanings given in the EU Data Protection Law. The terms “**Business**”, “**Business Purpose**”, “**Consumer**” and “**Service Provider**” shall have the same meaning as in the CCPA. To the extent that CCPA applies, the term “Controller” shall also mean “Business”, and “Processor” shall also mean “Service Provider”.

2.5. **Company Data** means any and all Personal Data shared with Vendor by Company or its Affiliated Companies or customers, or otherwise Processed by Vendor on behalf of the Company for the purposes stipulated in the Agreement and this DPA, whether provided by Company or directly by its customers. The Personal Data categories, elements and the authorized purposes for Personal Data Processing are detailed in **Annex A** of this DPA.

2.6. **Data Transfers** means either one or both of (a) a transfer of Company Data from the Company or Data Subjects to Vendor; or (b) an onward transfer of any of Company Data from Vendor to a contracted and authorized Sub-Processor.

2.7. **"Restricted Country"** means any country: (i) which is not a member of the European Economic Area; or (ii) which has not been approved by the European Commission or the UK Government pursuant to Article 45 of the GDPR or the UK GDPR (as applicable), as ensuring an adequate level of data protection in relation to Personal Data;

2.8. **"Restricted Transfer"** means a transfer of Personal Data between the Parties which in the absence of an Adequacy Decision, or any other lawful mechanism (such as, without limitation SCC), would be unlawful under Data Protection Laws;

2.9. **EU Data Protection Law** means the (i) the EU GDPR or the UK GDPR; (ii) the EU e-Privacy Directive (Directive 2002/58/EC), as amended and updated from time to time (“**e-Privacy Law”**); (iii) any national data protection laws made under, pursuant to, replacing or succeeding (i) and (ii); and (iv) any legislation replacing or updating any of the foregoing.

2.10. **GDPR** means 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).

2.11. **Personal Data** or **Personal Information** means any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, to or with an identified or identifiable natural person or Consumer, which is processed by Vendor on behalf of Company, under this DPA and the Agreement.

2.12. **Security Incident** means any accidental or unlawful destruction, loss, alteration, unauthorized use, or disclosure of, or access to, Personal Data of the other party or to facilities hosting such Personal Data. For the avoidance of doubt, any Personal Data Breach of the other party's Personal Data will comprise a Security Incident.

2.13. **Services** means the services provided to the Company by Vendor in accordance with the Agreement and this DPA.

2.14. **Standard Contractual Clauses** or **SCC** means the Standard Contractual Clauses between controllers and processors, and between processors and processors, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, including all Annexes thereto, as currently located at Standard Contractual Clauses.

2.15. **UK GDPR** means the Data Protection Act 2018, as well as the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (SI 2019/419).

3. RELATIONSHIP OF THE PARTIES

3.1. **Roles.** The Parties agree and acknowledge that between the Parties, and under the performance of their obligations set forth in the Agreement and with respect to the Processing of Personal Data, specifically the Company Data, the Company is the **Controller** and the Vendor is the **Processor** on behalf of Company. Vendor acknowledges that in some instances, Company acts as the Processor of its Client's Personal Data, in which case, Processor acts as the Company's Sub-processor.

3.2. **Compliance**. Each Party shall be individually and separately responsible for complying with the obligations that apply to it subject to the Data Protection Law. The subject matter and duration of the Processing carried out by the Processor in connection with the Agreement, the nature and purpose of the Processing, the type of Personal Data and the categories of Data Subjects are described in **Annex A** of this DPA.

3.3. Without limiting the generality of the above, Vendor shall: (a) comply with all applicable Data Protection Laws in the Processing of Company Data; and (b) not Process Company Data other than as **required** for the purpose defined in the Agreement and this DPA, (c) not Process Company Data other than instructed by Company; (d) not acquire, and shall not be deemed to acquire, any right, title or interest in Company Data, all of which remains the exclusive property of Company or its clients; and (e) not exercise any independent discretion as to the purposes or means of Processing Company Data.

4. PROCESSING AND PROTECTION OF PERSONAL DATA

4.1. When Processing on Company's behalf under the Agreement, Vendor shall Process Personal Data **solely** for the following purposes: (i) Processing in accordance with the Agreement and this DPA; (ii) Processing in accordance with Company's documented instructions, where such instructions are consistent with the terms of the Agreement; (iii) Processing as required under Data Protection Laws applicable to Vendor as a Processor, provided that Vendor shall inform Company of the legal

requirement in advance unless such law or order prohibits such information on important grounds of public interest.

4.2. Vendor shall inform Company without undue delay if, in Vendor's opinion, an instruction for the Processing of Personal Data given by Company infringes upon applicable Data Protection Laws. In such event, Vendor shall (a) inform Company, providing relevant details of the issue, (b) upon request of Company, temporarily cease all Processing of the affected Personal Data (other than securely storing such data), and (c) if the Parties do not agree on a resolution to the issue in question and the costs thereof, Company may terminate the Agreement and/or this DPA with respect to the affected Processing.

4.3. Without derogating from the above or any specific section in this DPA, with respect to Processing activities of Personal Data by Vendor, Vendor represents and warrants that it: (a) will treat all Company Data Processed by it on behalf of the Company as confidential and ensure that persons authorized to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, as further detailed in Section 7 hereunder; (b) has implemented appropriate technical and organizational measures to ensure the privacy of Data Subjects and the security of Company Data, and that Vendor has implemented a mechanism to exercise rights by a Data Subject under applicable Data Protection Law, as further detailed in Sections 5 and 6 hereunder; (c) will not access, Process or transfer Company Data in any Restricted Country, or permit any Sub-Processor or Vendor Personnel to do so, without the prior written consent of the Company and without implementing appropriate lawful measures, including demonstrating a lawful basis for Data Transfers, as further detailed in Section 10 hereunder, and including, without limitation, demonstrating upon request, a proper transfer impact assessment and, where applicable, a Data Protection Impact Assessment, as required by applicable Data Protection Law; (d) provide Company with reasonable resources and assistance as are required by the Company pursuant to Articles 32 to 36 of the GDPR, as detailed in section 6 herein; (e) subject to Company's sole instructions, delete all the Company Data following the completion of the Processing, and delete existing copies unless the Union or Member State law requires longer storage of such, as further detailed in Section 11 hereunder; (f) make available to the Company at its request all information necessary to demonstrate compliance with the obligations herein and under Article 28 of the GDPR, including without limitation, provide the Company with a written description of the technical and organizational methods employed by Vendor and its authorized Sub-Processors (if any) for the Processing of Personal Data, as further detailed in Section 6.3 hereunder; (g) will not use, and will not permit any Sub-Processor, Vendor Personnel or third party to use, any Company Data to train, fine-tune, retrain, ground, evaluate, benchmark or otherwise develop or improve any artificial intelligence or machine learning system, model, algorithm or data set, whether for Vendor's own benefit, for the benefit of another customer or for any third party, and this prohibition applies equally to Personal Data, to derived and inferred data, and to prompts, queries, logs, telemetry and any output generated from Company Data; (h) will not input, upload, paste or otherwise make Company Data available to any generative artificial intelligence tool, including any hosted service, API, browser extension, coding assistant or embedded product feature, without Company's prior written approval, such approval being conditional on enterprise-tier terms with training disabled, minimum available retention, no provider-side human review of Company Data and no cross-customer model improvement, and Company may withdraw approval at any time on written notice, in which case Vendor shall cease the relevant use within five (5) business days; (i) acknowledges that where it Processes Company Data in breach of paragraphs (g) or (h), all right, title and interest in any resulting model weights, embeddings, data sets, derivative data and outputs shall vest exclusively in Company to the extent permitted by law, and Vendor shall, at Company's election and at Vendor's cost, delete or retrain the affected model and

certify the result in writing; (j) will disclose in Annex B, before use, each artificial intelligence system and generative artificial intelligence tool used in connection with the Services, together with its provider, hosting location, model and retention and training configuration; (k) will not use any artificial intelligence system to take decisions producing legal or similarly significant effects concerning a Data Subject, or to profile Data Subjects, without Company's prior written instruction; (l) will notify Company within twenty-four (24) hours of any exposure or suspected exposure of Company Data through an artificial intelligence system, including through prompts, logs, caches, embeddings, model memory or provider-side retention, each such event constituting a Security Incident for the purposes of Section 9; and (m) where Vendor provides or deploys an artificial intelligence system in connection with the Services, will identify its risk classification under Regulation (EU) 2024/1689, confirm whether Vendor acts as provider or deployer, not cause Company to become a provider without written notice, and supply the documentation Company reasonably requires to meet its own obligations under that Regulation.

4.4. **CCPA Standard of Care; No Sale of Personal Information**.

4.4.1. Vendor acknowledges and confirms that it does not receive or Process any Personal Information as consideration for any services or other items that Vendor provides to Company under the Agreement. Vendor shall not have, derive, or exercise any rights or benefits regarding Personal Information Processed on Company's behalf, and may use and disclose Personal Information solely for the purposes for which such Personal Information was provided to it, as stipulated in the Agreement and this DPA.

4.4.2. Vendor certifies that it understands the rules, requirements and definitions of the CCPA and CPRA and agrees to refrain from selling (as such term is defined in the CCPA and CPRA) any Personal Information Processed hereunder, nor taking any action that would cause any transfer of Personal Information to or from Vendor under the Agreement or this DPA to qualify as "selling" such Personal Information under the CCPA. Vendor shall not (a) retain, use or disclose Personal Information for any purpose other than the business purposes set out in the Agreement and Annex A, including any commercial purpose of Vendor; (b) retain, use or disclose Personal Information outside the direct business relationship between Vendor and Company; or (c) combine Personal Information received from or on behalf of Company with Personal Information received from or on behalf of any third party, or collected from Vendor's own interactions with consumers, except as permitted by Applicable Data Protection Law. Vendor shall notify Company within five (5) business days if it determines that it can no longer meet its obligations under Applicable Data Protection Law, and Company may take reasonable and appropriate steps to stop and remediate any unauthorized use of Personal Information.

5. DATA SUBJECTS RIGHTS AND ONLINE DATA REQUESTS (ODR)

5.1. Vendor shall assist Company in responding to requests to exercise Data Subject rights or Consumer rights (including any complaints regarding the Processing of Personal Data) under Data Protection Laws, including, without limitation, EU Data Protection Laws and the CCPA/CPRA ("**Data Subject Request(s)**"). This obligation includes Vendor to (i) promptly notify Company, and in any event within two (2) business days, if it receives a Data Subject Request in respect of Personal Data, and shall not alter, delete, restrict or otherwise Process Company Data in response to a Data Subject Request, regulatory inquiry or complaint unless instructed by Company in writing; (ii) providing full cooperation and assistance to Company in relation to any Data Subject Request within the time frame stipulated by Data Protection Law; (iii) ensuring that it does not respond to Data Subject Requests except as per the documented instructions of Company or as strictly required

by the applicable Data Protection Laws to which the Vendor and the Data Subject are subject, and (iv) maintain electronic records of Data Subject Requests and the accommodation of which.

6. SECURITY, TECHNICAL AND ORGANIZATIONAL MEASURES

6.1. **Controls for the Protection of Personal Data**. Vendor represents and warrants that it has implemented and will maintain all appropriate technical and organizational measures for the protection of Personal Data Processed hereunder, including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data, confidentiality and integrity of Personal Data, including measures of assessing risks and protecting against such risks. This includes, but is not limited to, conducting penetration tests or similar security audits, the implementation of certification schemes such as ISO/IEC 27001 or a current SOC 2 Type II attestation, encryption of Personal Data in transit (TLS 1.2 or higher) and at rest (AES-256 or equivalent), multi-factor authentication for all remote and privileged access, and remediation of critical vulnerabilities within seven (7) days and high vulnerabilities within thirty (30) days, and including those measures that may be instructed from time to time by the Company or applicable Data Protection Law. Upon Company's request, Vendor shall (a) provide Company with any report indicating the performance of such penetration tests and/or other organizational and technical measures implemented by Vendor; and (b) assist Company, in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR. Where the Processing is subject to the Israeli Privacy Protection Law, 5741-1981 (including Amendment No. 13) and the Privacy Protection (Data Security) Regulations, 5777-2017, Vendor shall additionally: (i) determine and apply the security level applicable to the database (basic, medium or high) and implement the corresponding controls, including a database definition document, access permission management, access logging, periodic risk surveys and, where a high security level applies, penetration testing and annual internal audits; (ii) appoint a Data Protection Officer where required and provide the contact details to Company; (iii) notify Company within twenty-four (24) hours of a severe security incident as defined in those Regulations and support Company's notification to the Privacy Protection Authority and to affected individuals; (iv) not engage any holder or sub-holder of the database without Company's prior written approval; and (v) return or destroy the data on termination and certify destruction in writing.

6.2. **Records of Processing Activities**. Vendor shall keep records of its Processing activities performed on behalf of Company, in compliance with Article 30 of the GDPR, which shall include at least: (i) the details of the Vendor as a Processor of Personal Data, any representatives, Sub-Processors, data protection officers and Vendor Personnel having access to Personal Data; (ii) the categories of Processing activities performed; (iii) information regarding cross-border Data Transfers, if any; and (iv) a description of the technical and organizational security measures implemented in respect of the Processed Personal Data. Without derogating from Company's Audit Rights under Section 6.3 below, Company reserves the right to inspect the records maintained by Processor under this Section 6.2 at any time.

6.3. **Audits and Inspections**. Upon prior written request, and subject to confidentiality undertakings by Company, Vendor shall make available to Company (or Company's independent third-party auditor subject to their confidentiality undertakings) all information necessary to demonstrate compliance with this DPA, and shall permit Company or such auditor to audit and inspect Vendor's Processing of Company Data once in any twelve (12) month period on thirty (30) days written notice, and at any time on five (5) business days notice following a Security Incident, a material change to the Services or to Sub-Processors, a finding of non-compliance, or a documented request from a Supervisory Authority or from a client of

Company. Vendor shall respond to security and privacy questionnaires and evidence requests within ten (10) business days, shall remediate critical findings within thirty (30) days, and shall bear Company's reasonable audit costs where the audit identifies a material breach of this DPA or of Applicable Data Protection Law. In the event of an audit or inspection, as set forth above, Company shall take reasonable steps to avoid causing (or, if it cannot avoid, minimize) any disruption to Vendor's operations while conducting such audit or inspection.

7. VENDOR PERSONNEL

7.1. To the extent permissible under applicable Data Protection Law, Vendor shall conduct an appropriate background investigation of Vendor's employees or contractors who may have access to Personal Data ("**Vendor Personnel**"), before allowing them such access. If a background investigation reveals that an individual is not suited to access Personal Data, then Vendor shall not provide such individual with access to Personal Data.

7.2. Vendor shall ensure that all Vendor Personnel: (i) has such access only as necessary for the purposes of providing Company with the Services (as defined in the Agreement and this DPA) and complying with Applicable Data Protection Laws; (ii) is contractually bound to confidentiality requirements no less onerous than in this DPA and the Agreement; (iii) is provided with appropriate privacy and security training, at least annually; (iv) is informed of the confidential nature of Personal Data, and required to keep it confidential; and (v) is aware of Vendor's duties and obligations under this DPA and the Agreement; (vi) has access revoked within twenty-four (24) hours of termination of engagement or change of role, with all Company Data returned or securely deleted from personal or local devices; (vii) does not access, store or Process Company Data on unmanaged personal devices, or transmit Company Data through personal accounts, personal messaging applications or unapproved cloud storage; and (viii) does not use any generative artificial intelligence tool with Company Data except as approved by Company in writing.

8. SUB-PROCESSORS

8.1. **Authorized Sub-Processors.** Vendor shall not appoint (or disclose any Company Data to) any Sub-Processor unless authorized in writing and in advance by the Company. The current authorized Sub-Processors are listed and stipulated in **Annex B**. In the event where Vendor requires to engage with additional or replace an existing Sub-Processor to process Personal Data, it shall first ensure such Sub-Processor's compliance with the applicable Data Protection Law, and this DPA, then Vendor shall notify the Company in writing of any intended use or replacement of a Sub-Processor and will include the legal name, address and jurisdiction of the proposed Sub-Processor, the Processing locations (including any remote access locations), a description of the Processing activities and the categories of Company Data involved, the transfer mechanism relied on for any Restricted Transfer, a summary of its technical and organizational measures and any certifications or attestations held, and whether the Sub-Processor provides, embeds or relies on any AI System or Generative AI Tool, by email notification to the DPO at: privacy@nimbleway.com. Company reserves the rights to objects in writing (including by way of an email exchange) to the proposed use or replacement of the relevant Sub-Processor within thirty (30) days of receipt of the email notification, in which case Vendor shall not use or replace the Sub-Processor concerned in relation with the Company Data. Authorization of a Sub-Processor by Company does not mean confirmation of the Sub-Processor's compliance.

8.2. Vendor shall (i) only use a Sub-Processor that has provided sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR and this DPA and ensure the protection of the rights of Data Subjects; and (ii) impose, through a legally binding contract between Vendor and Sub-Processor, the same data protection obligations as set out in this DPA. Vendor acknowledges and agrees that if any Sub-Processor fails to fulfill its obligations in the contract between the Vendor and Sub-Processor, Vendor shall remain fully liable to the Company for the performance of the Sub-Processor's obligations.

8.3. **Contracts with Sub-processors**. Vendor represents and warrants that it has entered into a written agreement with each Sub-processor containing appropriate safeguards to the protection of Personal Data. Where Vendor engages a Sub-processor for carrying out specific Processing activities on behalf of Company, the same or materially similar data protection obligations as set out in the Agreement and this DPA shall be imposed on such new Sub-processor by way of a contract, in particular, obligations to implement appropriate technical and organizational measures for the protection of Personal Data Processed hereunder and in such a manner that the Processing will meet the requirements of the GDPR. Processor shall review and validate at least annually, and certify to Company upon request, that each of its Sub-processors is able to fulfill its duties as applicable to its performance of its obligations hereunder. If any review reveals any compliance deficiencies by such Sub-processor, Processor shall promptly find a solution, mitigation and/or remedy such issue; however, if such is not possible, Company may instruct Processor to not continue using such Sub-processor and Company may terminate this DPA and/or the Agreement to the extent Processor can no longer provide the Services without use of such Sub-processor and, if applicable, shall be entitled to a refund of the pro-rata portion of any prepaid fees for the remaining term.

9. NOTIFICATION AND SECURITY INCIDENT

9.1. Vendor represents and warrants that it maintains Security Incident management policies and procedures and will notify Company without undue delay (but in any event no later than twenty-four (24) hours) after becoming aware of any actual or suspected Security Incident, or any request for disclosure of Personal Data by a Supervisory Authority and/or any other law enforcement authority or court unless prohibited under criminal law specifically requiring Vendor as a Processor to preserve the confidentiality of a law enforcement investigation against Company.

9.2. Vendor shall provide Company with all information on the nature of the Security Incident, including the categories of Data Subjects concerned and the categories of Personal Data and data records concerned. Vendor shall take all necessary steps to identify and take those steps necessary to remediate and/or mitigate the cause of such a Security Incident as well as fully cooperate with Company in the investigation, mitigation, and remediation of a Security Incident. The initial notice shall include, to the extent known, the nature and suspected cause of the Security Incident, the date and time of occurrence and of discovery, the categories and approximate number of Data Subjects and records concerned, the likely consequences, the measures taken or proposed, and the contact details of Vendor's incident lead. Vendor shall provide updates at least every twenty-four (24) hours until containment, deliver a written root cause analysis and remediation plan within ten (10) business days of containment, preserve all logs and forensic evidence for at least twelve (12) months, and reimburse Company's reasonable costs of forensic investigation, regulatory notification and notification to affected

Data Subjects where the Security Incident is caused by Vendor, its Sub-Processors or Vendor Personnel.

9.3. Upon request of Company, Vendor shall provide Company with sufficient information to allow Company to meet any obligations under Applicable Data Protection Laws to report or inform Data Subjects or data protection authorities of the Security Incident.

9.4. Vendor will not make, disclose, release or publish any finding, admission of liability, communication, notice, press release or report concerning any Security Incident or disclosure request which directly or indirectly identifies Company (including in any legal proceeding or in any notification to regulatory or supervisory authorities or affected individuals) without Company's prior written approval, unless, and solely to the extent that, Vendor is compelled to do so pursuant to Applicable Data Protection Laws. In which case, unless prohibited by such laws, Vendor shall provide Company with reasonable prior written notice to provide Company with the opportunity to object to such disclosure and in any case, Vendor shall limit the disclosure to the minimum scope required.

10. DATA TRANSFER

10.1. **Data Transfers from the EU, EEA, Switzerland and the UK to countries that offer an adequate level of data protection** ("**Third Countries**"). Personal Data may be transferred from an EU Member State, the EEA member countries (Norway, Liechtenstein and Iceland) (collectively, "**EEA**"), Switzerland and the UK to countries that offer an adequate level of data protection under or pursuant to the adequacy decisions published by the relevant data protection authorities of the EEA, the European Union, the Member States or the European Commission, Switzerland, and/or the UK as relevant ("**Adequacy Decisions**"), as applicable, without any further safeguard being necessary. Where Vendor is established in the United States and self-certifies under the EU-US Data Privacy Framework, the UK Extension to it, or the Swiss-US Data Privacy Framework (together, the DPF), transfers of Company Data may rely on the relevant DPF adequacy decision, provided that Vendor maintains an active certification covering the categories of Company Data Processed (including HR data where applicable), notifies Company within five (5) business days if its certification lapses, is withdrawn or is placed on the ineligible list, and agrees that if the certification ceases to be valid or the relevant adequacy decision is annulled, suspended or amended, the Standard Contractual Clauses in Annex C shall apply automatically and without further action from the date of that event. Before any Restricted Transfer, and on request thereafter, Vendor shall provide Company with a transfer impact assessment covering the laws and practices of the destination country, any government access requests received in the preceding twelve (12) months, and the supplementary measures applied.

10.2. **Data Transfers from the EU, EEA, Switzerland and the UK to other countries.** If the Processing of Personal Data by Processor includes any Restricted Transfer, including without limitation the following Data Transfers (either directly or via onward transfer), the respective SCC shall apply:

10.2.1. From the EU, EEA or Switzerland to other countries which have not been subject to a relevant Adequacy Decision ("**EEA Transfer**"), the terms set forth in the Standard Contractual Clauses (SCC) in **Annex C** shall apply.

10.2.2. From the UK to other countries which have not been subject to a relevant Adequacy Decision, ("**UK Transfers**"), the terms set forth in the Standard Contractual Clauses (SCC), in accordance with the UK data protection authority shall apply.

10.2.3. The terms set forth in Annex C to this DPA (Additional Safeguards), and the technical and organizational measures set forth in Annex D, shall apply to any or both EEA Transfer and a UK Transfer.

11. DELETION OR RETURN OF COMPANY DATA

11.1. Without undue delay, and in any event within thirty (30) days, following termination of the Agreement, Processor shall, at the choice of Company, delete or return to Company all the Personal Data it Processes on behalf of Company, in the manner described in the Agreement or as otherwise reasonably requested by Company.

11.2. Notwithstanding the above, Vendor shall automatically permanently delete within thirty (30) days following termination or expiration of the Agreement and/or DPA any Personal Data, including existing copies of such Personal Data, unless Applicable Data Protection Laws require otherwise. Vendor warrants that it will guarantee the confidentiality of Personal Data. Deletion shall be performed using a method consistent with NIST SP 800-88 or an equivalent standard, and shall extend to backups, archives, disaster recovery copies, ticketing and support systems, logs, and any cache or retained content held by a Sub-Processor or by any approved Generative AI Tool. Where a backup cannot be deleted immediately, Vendor shall isolate it, cease all Processing other than storage, and delete it on expiry of its retention cycle, which shall not exceed ninety (90) days. Upon Company's written request, the Processor's authorized officer shall provide written certification to Company, stating that Processor has fully complied with this section.

12. LIABILITY

12.1. Vendor is solely and exclusively liable for all actions, omissions and Processing activities that it or its directors, officers, employees, representatives and agents take in respect of Processing the Company Data. The limitations and exclusions of liability set out in the Agreement shall not apply to (a) Vendor's breach of this DPA; (b) any unauthorized or unlawful Processing of Company Data; (c) any Security Incident caused by Vendor, its Sub-Processors or Vendor Personnel; (d) Vendor's indemnity obligations under Section 13; or (e) Vendor's fraud, gross negligence or willful misconduct. Nothing in this DPA limits either Party's liability where such limitation is prohibited by Applicable Data Protection Law, including liability to Data Subjects under Article 82 GDPR.

12.2. Vendor shall indemnify, defend, and hold harmless Company, its Affiliated Companies, its clients, and their respective officers, directors, and employees from and against all claims and proceedings and all liability, loss, costs, fines, and expenses (including reasonable legal fees) arising in connection with (i) Vendor's unlawful or unauthorized Processing, destruction of, or damage to any Personal Data; and/or (ii) Vendor's (including the Vendor Personnel and Sub-Processors) failure to comply with its obligations under this DPA, the Agreement or any further written Processing instructions given by Company in accordance with this DPA; (iii) any Security Incident affecting Company Data caused by Vendor, its Sub-Processors or Vendor Personnel; and/or (iv) any claim brought by a client of Company arising from Vendor's breach of this DPA.

13. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

Upon Company's request, Processor shall provide Company, at no additional charge and within ten (10) business days of request, with the cooperation, information and assistance needed to fulfill Company's obligations under the Applicable Data Protection Laws to carry out a data protection impact assessment related to Company's use of the Services. Vendor shall provide the necessary assistance to Company in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this Section 13.

14. INDURANCE

Vendor shall maintain, at its own cost, throughout the term of the Agreement and for two (2) years thereafter, Cyber and Privacy Liability insurance of not less than USD 2,000,000 per occurrence and USD 3,000,000 in the aggregate, and Professional Liability or Technology Errors and Omissions insurance of not less than USD 1,000,000 per occurrence, with reputable insurers, shall provide certificates of insurance on request, and shall notify Company at least thirty (30) days before any cancellation or material reduction in coverage. Where Vendor Processes Special Categories of Personal Data or sensitive personal information, holds persistent, privileged or administrative access to Company production systems, collection infrastructure or Company Data at scale, provides security services, or has experienced a high severity Security Incident in the preceding twelve (12) months, Vendor shall be classified as a high-risk vendor and shall additionally undergo annual independent penetration testing and provide the full report, vulnerability list and remediation plan within ten (10) business days of completion, maintain ISO/IEC 27001 certification or a SOC 2 Type II report, maintain strict environment segregation with no co-mingling of Company Data, give sixty (60) days notice of any Sub-Processor change, and maintain Cyber and Privacy Liability insurance of not less than USD 5,000,000 per occurrence and USD 10,000,000 in the aggregate. Company may suspend all or part of the Processing and Vendor's access to Company Data and Company systems with immediate effect on written notice where Company reasonably believes a Security Incident has occurred or is occurring, where Vendor is in breach of its obligations relating to artificial intelligence, Sub-Processors or international transfers, where an instruction from a Supervisory Authority or from a client of Company requires it, or where continued Processing would place Company in breach of Applicable Data Protection Law. A material breach of this DPA is a material breach of the Agreement, and where the breach is not capable of remedy, or involves unauthorized Processing, a breach of the artificial intelligence obligations or an unauthorized Restricted Transfer, Company may terminate with immediate effect. Company may amend this DPA where required to comply with new or amended Data Protection Law, or with a decision, guidance or enforcement action of a Supervisory Authority, by giving Vendor thirty (30) days written notice.

ANNEX A | DETAILS OF PROCESSING ACTIVITIES

Subject Matter - Nature and purpose of the Processing

1. *Processing and executing a service agreement*
2. *Providing the Services*
3. *[Adding the exact purpose and nature by vendor or Company]*

Categories of data subjects and types of Personal Data

	Categories of data subjects	Categories of personal data
☐	Company's personnel/employees	
☐	Company's customers	
☐	Web users (making their data publicly available)	
☐	Company's vendors/suppliers	
☐	Job Candidates	
☐	Prospective customers	
☐	Website visitors	=

The parties to select the relevant categories of data subjects and respective Personal Data involved (or potentially be involved.

The parties to attach/add Data Flow.

Duration of Processing

For as long as the contract between the parties is effective, **unless** specifically instructed otherwise by Company, by a Data Subject, or, requested for deletion by Data Subject, or required by the nature of the data (e.g. web tracking). Any request of ZDR (Zero Data Retention) shall prevail this section.

Special categories of Personal Data

Vendor declares that it will not Process any Special Categories of Personal Data or sensitive personal information. If any such data is to be Processed, Vendor must list it here and obtain Company's written approval before Processing begins, and shall apply the enhanced controls in Annex D and the high-risk vendor requirements in Section 14.

Location of Processing (including accessing)

[*Vendor to list all location of processing, including hosting, accessing, viewing and more*]

Vendor shall not Process, store or access Company Data in, or transfer Company Data to, the following jurisdictions, and shall implement geo-blocking or equivalent controls to enforce this: Cuba, Iran, North Korea, Sudan, Syria, Russia, Belarus, the occupied regions of Ukraine including Crimea, and any jurisdiction subject to comprehensive sanctions by the EU, the UK, the US or Israel.

ANNEX B | AUTHORIZED SUB-PROCESSORS

The Processor may engage the following entities to carry out specific Processing activities on behalf of Company or data center facility management activities.

[*Processor to complete and submit PRIOR to finalizing and signing the DPA*]

Entity	**Data Involved in processing**	**Processing Location**	**Purpose**	**Lawful basis for cross-border data transfer**

ANNEX C | DATA TRANSFERS – Standard Contractual Clauses

Preamble

According to the GDPR, Standard Contractual Clauses ensure appropriate data protection safeguards can be used as a ground for data transfers from the EU or the EEA to Third Countries. This includes model contract clauses, so-called Standard Contractual Clauses (SCC) pre-approved by the European Commission.

On 4 June 2021, the European Commission issued modernized Standard Contractual Clauses under the GDPR for data transfers from Controllers or Processors in the EU/EEA (or otherwise subject to the GDPR) to Controllers or Processors established outside the EU/EEA (and not subject to the GDPR), those available here.

Applicability of SCC to this DPA and Agreement

1. In the absence of Adequacy Decision, as per Section 10 of the DPA, the following modules of the Standard Contractual Clauses shall apply to Processor:

   [please select the applicable modules]:

   - ☐ Module one: Controller – Controller (C2C).
   - ☑ Module two: Controller – Processor (C2P).
   - ☑ Module three: Processor – Processor (P2P)
   - ☐ Module four: Processor - Controller (P2C)

2. Vendor shall not Process the Company Data nor permit any Authorised Sub-processor to Process Company Data in a Restricted Country, other than recipients in the countries (if any) listed in Annex A, unless authorized in writing by Company in advance via an amendment to this DPA.
3. In respect of any Restricted Transfer, Vendor and each Vendor Affiliate (as "**data importer**") and the Company and each Company Affiliate (as "**data exporter**") with effect from the commencement of the relevant transfer hereby enter into the Standard Contractual Clauses in respect of any transfer from the Company or any Company Affiliate to Vendor and each Vendor Affiliate (or any onward transfer). Module 2 of the Standard Contractual Clauses shall apply between the Company (or each Company Affiliate) and Vendor(or each Vendor Affiliate) and Module 3 of the Standard Contractual Clauses shall apply between Vendor and each Sub-processor and the following:
   - Clause 7- Docking clause of the Standard Contractual Clauses shall apply;
   - Clause 9 - Use of sub-processors of the Standard Contractual Clauses Option 2 (general written authorisation) shall apply and the "time period" shall be thirty (30) days;
   - Clause 11(a) - Redress of the Standard Contractual Clauses, the optional language shall not apply;
   - Clause 13(a) - Supervision of Standard Contractual Clauses, the following shall be inserted: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex C1.C, shall act as a competent supervisory authority.
   - Clause 17 - Governing law of the Standard Contractual Clauses Option 1 shall apply and the "Member State" shall be Ireland;

- Clause 18 - Choice of forum and jurisdiction of the Standard Contractual Clauses the Member State shall be Ireland;

- Annex I of the Standard Contractual Clauses shall be deemed to be pre-populated with the relevant sections of Annex A, and C1 to this DPA and the processing operations are deemed to be those described in the Agreement;

- Annex II of the Standard Contractual Clauses shall be deemed to be pre-populated with the relevant sections of Annex D to this DPA.

4. Where a Restricted Transfer is subject to the UK GDPR, the Standard Contractual Clauses shall be read in accordance with, and deemed amended by, the provisions of Part 2 (Mandatory Clauses) of the UK IDTA, and the parties confirm that the information required for the purposes of Part 1 (Tables) of the UK IDTA is set out in Annexes A and C1 to this Addendum and the Agreement.
5. In the case of conflict between the terms of the Standard Contractual Clauses and the Agreement, the terms of the Standard Contractual Clauses shall take precedence.
6. Nothing in this DPA shall prevent Company from imposing any further conditions in respect of any transfer of Personal Data, including requiring the Vendor and each Vendor Affiliate to enter into and comply with any further agreements, in order to legitimize such transfer of Company Data.
7. If Vendor, any Vendor Affiliate or Sub-processor receives a Legal Process requiring disclosure of Company Data to a Public Body, Company shall: (i) promptly notify Company, unless legally prohibited from doing so; (ii) use all reasonable efforts to redirect the Public Body issuing such Legal Process to request that Company Data directly from Company or the relevant Company Affiliate; and (iii) where (ii) is not possible, use all reasonable efforts to challenge the Legal Process (where there are grounds for doing so) and to minimize the amount of any Company Data which Vendor, any VendorAffiliate or Sub-processor is compelled to disclose.

[Vendor may submit its own applicable SCC. In the absence of such submission, this Annex C shall apply]

Annex C.1

A. LIST OF PARTIES

Data Importer: Identity and contact details of the data importer(s) and, where applicable, of its/their data protection officer and/or representative in the European Union.

Name: Vendor's name as stipulated in the applicable Agreement/Order.
Address: Vendor's address as stipulated in the applicable Agreement/Order.
Contact person's name, position and contact details: as stipulated in the applicable Agreement/Order.
Role (controller/processor): Processor / Sub-Processor

Data Exporter: Identity and contact details of the data exporter(s), including any contact person with responsibility for data protection

Name: The Data Company Technologies Inc.
Address: 1007 N. Orange St., 10th Fl., Wilmington, Delaware 19801
Contact person's name, position and contact details: as stipulated in the applicable Order.

Role (controller/processor): Controller / Processor

B. DESCRIPTION OF TRANSFER

1 Categories of data subjects whose personal data is transferred

1.1 The personnel/employees/staff at Company or Company's Affiliate

1.2 The personnel at Company's business clients / end user of Company's products

1.3 The general public (Data made manifestly publicly available)

2 Categories of personal data transferred

1.1 Company Data which may include certain identification data of Company's personnel and Company's clients such as names, phone numbers and business email addresses.

1.2 Publicly available data which may be collected/streamed/communicated via Company on behalf of Company's clients and which may include names of individuals, email addresses, public profiles in social media and any other personal data that an individual chooses to display publicly.

3 Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

No sensitive data shall be transferred.

4 **The frequency of the transfer** (e.g. whether the data is transferred on a one-off or continuous basis). Personal Data is transferred on a continuous basis, under the terms of the Agreement, and the applicable DPA.

5 Nature of the processing

The personal data transferred will be subject to the following processing activities: (i) retrieval, consultation or use of the personal data and (ii) alignment, combination, blocking, erasure or destruction of the personal data; (iii) as otherwise provided in the Agreement, the DPA or required by applicable law.

6 Purpose(s) of the data transfer and further processing

The data importer shall process the Personal Data for the purposes set out in the Agreement, and as set out in Annex A

7 The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period.

Personal data of category number 3 is not retained by Company and shall not be retained by Vendor or Vendor Affiliate whatsoever. Personal data of categories number 1 and 2, is retained for the Term of the Agreement, or longer if required by applicable law.

8 For transfers to (sub-) processors, also specify the subject matter, nature and duration of the processing

8.1 Subject matter: the subject matter of the processing of the Personal Data is as set out in the Agreement.

8.2 The personal data transferred will be subject to the following processing activities: (i) retrieval, consultation or use of the personal data and (ii) alignment, combination, blocking, erasure or destruction of the personal data; (iii) as otherwise provided in the Agreement, this DPA or required by applicable law.

8.3 Duration of processing: Personal data of category number 3 is not retained by Company and shall not be retained by Vendor or Vendor Affiliate whatsoever. Personal data of categories number 1 and 2, is retained for the Term of the Agreement, or longer if required by applicable law.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13 of the SCCs

The Irish Data Protection Authority

ANNEX D | APPROPRIATE SAFEGUARDS IMPLEMENTED BY PROCESSOR

TECHNICAL AND ORGANISATIONAL (TOM) MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Vendor and each Vendors Affiliate or authorized Sub-Processors shall implement appropriate technical and organizational measures, policies and controls to maintain the adequate security of all physical, computer or network systems accessing, storing, transmitting, processing or otherwise supporting the Processing of Personal Data in accordance with this DPA and to ensure that such Personal Data is protected from accidental, unauthorized or unlawful processing, access, disclosure, loss, alteration, damage or destruction.

At a minimum, Vendor and each Vendors Affiliate shall ensure compliance with the requirements described at: https://mvsp.dev/mvsp.en/index.html. Vendors shall inform Company in case of any material non-compliance with the requirements set out herein and will provide evidence of alternative or compensating controls implemented to protect Personal Data.

The measures set out below apply in addition to the baseline referenced above. Where this Annex and the baseline differ, the stricter requirement applies.

D.1 Scope and maintenance. These measures apply to all systems, environments, networks, applications, devices and facilities used to access, store, transmit or otherwise Process Company Data, including those operated by Sub-Processors. Vendor shall implement them at its own cost, shall not degrade them during the term, and shall notify Company at least thirty (30) days before any material change that reduces the level of protection. Vendor warrants that this Annex accurately describes its measures as at the effective date, and shall review and update it at least annually and on any material change.

D.2 Security governance and accountability. (a) a documented information security policy set, approved by management and reviewed at least annually; (b) a named individual accountable for information security, and a Data Protection Officer where required, with contact details provided to Company; (c) defined security roles and responsibilities across the organisation; (d) a security awareness programme covering phishing, social engineering and the secure handling of Company Data; (e) an annual management review of the security programme, with findings and remediation status made available to Company on request.

D.3 Risk management. (a) a documented risk assessment methodology covering confidentiality, integrity, availability and resilience; (b) risk assessment of the systems used to Process Company Data at least annually and on material change; (c) a risk register recording owners, treatment plans and target dates; (d) assessment of privacy risk and support for Company's data protection impact assessments under Section 14.

D.4 Personnel security. (a) background screening to the extent permitted by applicable law before access to Company Data, and re-screening of privileged users at defined intervals; (b) written confidentiality

undertakings that survive termination of employment or engagement; (c) security and data protection training before first access and at least annually thereafter, with completion records retained and produced to Company on request; (d) documented joiner, mover and leaver processes, with all access revoked within twenty-four (24) hours of termination or role change; (e) a disciplinary process for security policy violations; (f) equivalent controls applied to contractors, temporary staff and outsourced personnel.

D.5 Access control. (a) role-based access granted on the principles of least privilege and need to know; (b) unique named accounts, with no shared or generic accounts and no interactive use of service accounts; (c) a formal access request, approval and revocation workflow, with records retained for at least twelve (12) months; (d) access reviews at least quarterly for privileged access and at least semi-annually for all other access to Company Data; (e) privileged access management with session monitoring or recording where feasible; (f) segregation of duties between development, deployment and production administration where team size permits; (g) automatic session timeout and account lockout after a defined number of failed authentication attempts.

D.6 Authentication and credential management. (a) multi-factor authentication, preferably phishing-resistant, for all remote, administrative, privileged and cloud console access and for any system holding Company Data; (b) centralised identity management and single sign-on where available; (c) a password policy consistent with NIST SP 800-63B or equivalent; (d) secrets, API keys and certificates held in a managed secrets store and never in source code, tickets, spreadsheets or chat tools; (e) rotation of credentials on personnel change and immediately on suspected compromise.

D.7 Encryption and key management. (a) TLS 1.2 or higher with strong cipher suites for data in transit, including service-to-service traffic where feasible; (b) AES-256 or equivalent for data at rest, covering databases, object storage, backups and portable media; (c) documented key management covering generation, storage, rotation, escrow and destruction, with key material held separately from the data it protects; (d) no Company Data on removable media unless encrypted and expressly approved by Company; (e) certificate lifecycle management with monitoring of expiry and revocation.

D.8 Network security. (a) network segmentation separating production, corporate, development and management environments; (b) firewalls and security groups operating on a default-deny basis, with rule sets reviewed at least annually; (c) intrusion detection or prevention at the perimeter and on critical internal segments; (d) protection against denial of service attacks for internet-facing services; (e) secure remote access through VPN or a zero trust broker, with no direct exposure of administrative protocols to the internet; (f) DNS and egress filtering; (g) wireless networks secured to WPA2-Enterprise or better and segregated from systems Processing Company Data.

D.9 Endpoint security. (a) centrally managed endpoints with full disk encryption, enforced screen lock and automated patching; (b) endpoint detection and response with centralised alerting on every device capable of accessing Company Data; (c) mobile device management with remote wipe for any mobile access; (d) prohibition on Processing Company Data on unmanaged or personal devices; (e) removable media controls including blocking or encryption enforcement; (f) local administrator rights restricted, justified and time-bound.

D.10 Secure development and change security. (a) a documented secure development lifecycle including security requirements, threat modelling for material changes and peer code review; (b) static and dynamic application security testing and software composition analysis integrated into the pipeline; (c) secret scanning on commit; (d) separation of development, test, staging and production environments with distinct credentials; (e) no production Company Data in non-production environments, and where test data derives from production it shall be anonymized or pseudonymized and used only with Company's prior written approval; (f) infrastructure as code with peer review and version control; (g) OWASP ASVS or an equivalent standard as the baseline for internet-facing applications.

D.11 Data segregation, minimisation and handling. (a) logical or physical segregation of Company Data from Vendor's own data and from the data of other customers, with a documented tenancy model provided to Company on request; (b) collection and retention limited to what is necessary for the Services; (c) pseudonymisation or tokenisation where the purpose can be achieved without direct

identifiers; (d) a documented data flow diagram for Company Data, updated on material change; (e) technical controls preventing Company Data from being copied into ad hoc locations such as personal drives, local spreadsheets, ticket attachments, chat tools or unapproved cloud storage.

D.12 Logging, monitoring and detection. (a) logging of authentication, authorisation, administrative actions, configuration changes and access to Company Data; (b) centralised, time-synchronised and tamper-resistant log storage with access restricted to authorised personnel; (c) retention of security logs for at least twelve (12) months, of which at least three (3) months shall be immediately searchable; (d) alerting on anomalous access, privilege escalation, bulk export and abnormal authentication patterns; (e) continuous monitoring capability or a documented on-call rota covering out of hours; (f) provision to Company of logs relating to Company Data on request during an investigation or audit.

D.13 Vulnerability and patch management. (a) authenticated vulnerability scanning of infrastructure and applications at least monthly; (b) continuous dependency and container image scanning; (c) documented remediation timelines of seven (7) days for critical, thirty (30) days for high and ninety (90) days for medium severity findings, measured from identification; (d) emergency patching without undue delay for vulnerabilities under active exploitation; (e) a documented exception process with compensating controls and expiry dates, with any exception affecting Company Data notified to Company; (f) monitoring of supplier advisories and known exploited vulnerability catalogues relevant to the technology stack.

D.14 Testing and independent assurance. (a) independent third-party penetration testing of the systems and applications used to Process Company Data at least once every twelve (12) months and after any material architectural change or Security Incident; (b) provision to Company on request of the executive summary, the findings list by severity and the remediation plan, and for a high-risk vendor the full report within ten (10) business days of completion; (c) evidence of closure or retest for critical and high severity findings; (d) red team or scenario-based exercises where proportionate to the risk profile.

D.15 Change and configuration management. (a) documented change management covering risk assessment, testing, approval and rollback; (b) hardened baseline configurations aligned to CIS Benchmarks or equivalent, with drift detection; (c) continuous cloud configuration monitoring covering public exposure of storage buckets, databases and management interfaces; (d) separation between the author and the approver of production changes.

D.16 Asset and data classification management. (a) an inventory of hardware, software, cloud services and data stores that hold or can access Company Data, reviewed at least annually; (b) a named owner for each asset; (c) a data classification scheme under which Company Data is classified at the highest applicable tier and handled accordingly; (d) a decommissioning process ensuring data removal before disposal, reassignment or return of equipment.

D.17 Physical and environmental security. (a) Processing only in facilities with access control, visitor logging, monitoring and, where lawful, video surveillance; (b) use of data centres certified to ISO/IEC 27001, SOC 2 or equivalent, with the list provided to Company on request; (c) clear desk and clear screen practices; (d) environmental controls including fire detection and suppression, power redundancy and climate control; (e) equivalent expectations for home and remote working, including a private working space and a prohibition on using public or untrusted networks without VPN.

D.18 Resilience, backup and business continuity. (a) documented business continuity and disaster recovery plans, reviewed and tested at least annually; (b) recovery time and recovery point objectives defined, disclosed to Company and consistent with the criticality of the Services; (c) backups taken at least daily for production systems, encrypted, access-controlled and, where feasible, immutable or write-once; (d) restoration testing at least annually with records retained; (e) geographic redundancy consistent with the permitted Processing locations in Annex A and the restrictions in Section 10; (f) ransomware resilience including offline or logically isolated backup copies.

D.19 Supply chain and Sub-Processor security. (a) a security and privacy assessment of each Sub-Processor before engagement and at least annually thereafter; (b) contractual flow-down of the measures in this Annex; (c) a maintained register of Sub-Processors and third-party services with access

to Company Data; (d) monitoring of Sub-Processor certifications, attestations and publicly reported incidents; (e) an exit and transition plan for critical Sub-Processors; (f) no onward disclosure of Company Data without Company's prior written authorisation under Section 8.

D.20 Artificial intelligence controls. (a) a maintained inventory of AI systems and generative AI tools used in connection with the Services or with any access to Company Data; (b) enterprise-tier configuration with model training disabled, minimum available retention and no provider-side human review of Company Data; (c) a prohibition on entering Company Data into unapproved tools, enforced technically where feasible through data loss prevention, egress filtering or managed browser controls; (d) logging and periodic review of AI tool usage in workflows that touch Company Data; (e) controls against prompt injection, model abuse and data poisoning for any AI feature exposed to untrusted input; (f) human review of AI-generated output before it is relied upon in any deliverable provided to Company.

D.21 Incident detection and response. (a) a documented incident response plan defining roles, severity classification, escalation paths and the notification timelines in Section 9; (b) testing of the plan at least annually through tabletop or simulation exercises, with records retained; (c) forensic readiness including log preservation, chain of custody and evidence handling; (d) a documented post-incident review identifying root cause and corrective actions; (e) a named security contact and an out-of-hours escalation route provided to Company and kept current.

D.22 Secure disposal and destruction. (a) media sanitisation consistent with NIST SP 800-88 or an equivalent standard; (b) cryptographic erasure accepted where the keys are destroyed and the method is documented; (c) certificates of destruction provided on request; (d) secure destruction of physical records containing Company Data; (e) deletion extending to backups, archives, caches, logs, ticketing systems and any retention held by an approved AI tool, in accordance with Section 11.

D.23 Certification, evidence and cooperation. (a) maintain ISO/IEC 27001 certification or a current SOC 2 Type II report covering the systems used to Process Company Data, or an equivalent independent third-party attestation; (b) provide the certificate or report, including the scope statement and any qualifications or exceptions, on request and at least annually; (c) notify Company within ten (10) business days if a certification or attestation lapses, is withdrawn, is qualified or has its scope reduced; (d) complete Company's security and privacy questionnaires and evidence requests within ten (10) business days; (e) cooperate with Company's audits under Section 6.3.

D.24 Exceptions and compensating controls. Where Vendor does not implement a measure set out in this Annex, it shall record below the measure concerned, the reason, the compensating control applied and the target remediation date, and shall obtain Company's written acceptance. Failure to implement a measure without recording it here is a breach of this DPA.

Measure not implemented / Reason / Compensating control / Target remediation date:

D.25 Vendor declaration. Vendor confirms that the measures described in this Annex are implemented as at the effective date, save for the exceptions recorded in D.24, and that it will notify Company of any material change.

Name: _____ Title: _____ Date: _____