

DATA PROCESSING AGREEMENT (DPA)

English Language Version

J. Sallinger Ltd., trading as DNX360

Registered Address: 128 City Road, London, EC1V 2NX, United Kingdom

Company Registration Number: 12797704

Primary Notice Email: legal@DNX360.com

Main Website: www.DNX360.com

Version: 1.1

Effective Date: 22-May-2026

ENGLISH

Our Data Processing Agreement ("DPA") is drafted exclusively in the English language and constitutes the sole governing text with respect to the processing of personal data. Any use of DNX360's services involving the processing of personal data implies full and unconditional acceptance of the applicable DPA, as reproduced below.

By using the services, the professional client acknowledges that it has read, understood, and accepted this DPA.

FRANÇAIS

Notre Accord de Traitement des Données (le « DPA ») est rédigé exclusivement en langue anglaise et constitue le seul texte de référence applicable en matière de traitement des données à caractère personnel. Toute utilisation des services de DNX360 impliquant un traitement de données à caractère personnel emporte acceptation pleine et entière du DPA en vigueur, tel que reproduit ci-dessous.

En utilisant les services, le client professionnel reconnaît avoir lu, compris et accepté le présent DPA.

NEDERLANDS

Onze Data Processing Agreement ("DPA") is uitsluitend opgesteld in de Engelse taal en vormt de enige toepasselijke referentietekst met betrekking tot de verwerking van persoonsgegevens. Elk gebruik van de diensten van DNX360 waarbij persoonsgegevens worden verwerkt, houdt de volledige en onvoorwaardelijke aanvaarding in van de geldende DPA, zoals hieronder weergegeven. Door gebruik te maken van de diensten erkent de zakelijke klant dat hij deze DPA heeft gelezen, begrepen en aanvaard.

DEUTSCH

Unsere Data Processing Agreement („DPA“) ist ausschließlich in englischer Sprache abgefasst und stellt den einzigen maßgeblichen Referenztext im Hinblick auf die Verarbeitung personenbezogener Daten dar. Jede Nutzung der Dienstleistungen von DNX360, die eine Verarbeitung personenbezogener Daten umfasst, gilt als vollständige und vorbehaltlose Annahme der jeweils geltenden DPA, wie nachstehend wiedergegeben.

Mit der Nutzung der Dienstleistungen bestätigt der Geschäftskunde, dass er diese DPA gelesen, verstanden und akzeptiert hat.

ESPAÑOL

Nuestro Data Processing Agreement ("DPA") está redactado exclusivamente en inglés y constituye el único texto rector aplicable en materia de tratamiento de datos personales. Cualquier uso de los servicios de DNX360 que implique el tratamiento de datos personales conlleva la aceptación plena e incondicional del DPA vigente, tal como se reproduce a continuación.

Al utilizar los servicios, el cliente profesional reconoce haber leído, comprendido y aceptado el presente DPA.

ITALIANO

Il nostro Data Processing Agreement ("DPA") è redatto esclusivamente in lingua inglese e costituisce l'unico testo di riferimento applicabile in materia di trattamento dei dati personali. Qualsiasi utilizzo dei servizi di DNX360 che comporti il trattamento di dati personali implica l'accettazione piena e incondizionata del DPA vigente, come riportato di seguito.

Utilizzando i servizi, il cliente professionale dichiara di aver letto, compreso e accettato il presente DPA.

DANSK

Vores Data Processing Agreement ("DPA") er udelukkende udarbejdet på engelsk og udgør den eneste gældende referencetekst vedrørende behandling af personoplysninger. Enhver brug af DNX360's tjenester, som indebærer behandling af personoplysninger, medfører fuld og ubetinget accept af den gældende DPA, som gengivet nedenfor.

Ved at bruge tjenesterne bekræfter den erhvervskunde, at denne har læst, forstået og accepteret denne DPA.

SVENSKA

Vårt Data Processing Agreement ("DPA") är uteslutande upprättat på engelska och utgör den enda tillämpliga referenstexten avseende behandling av personuppgifter. Varje användning av DNX360:s tjänster som innebär behandling av personuppgifter medför ett fullständigt och villkorslöst godkännande av den gällande DPA:n, såsom den återges nedan.

Genom att använda tjänsterna bekräftar företagskunden att den har läst, förstått och accepterat denna DPA.

SLOVENČINA

Naša Data Processing Agreement („DPA“) je vypracovaná výlučne v anglickom jazyku a predstavuje jediný rozhodujúci referenčný text upravujúci spracúvanie osobných údajov. Každé používanie služieb DNX360, ktoré zahŕňa spracúvanie osobných údajov, znamená úplný a bezvýhradný súhlas s platným DPA, ako je uvedené nižšie.

Používaním služieb profesionálny zákazník vyhlasuje, že si tento DPA prečítal, porozumel mu a akceptoval ho.

This Data Processing Agreement ("DPA") is entered into between:

(1) **J. Sallinger Ltd.**, a company incorporated in England and Wales (company registration number 12797704), trading as **DNX360**, whose registered office is at 128 City Road, London, EC1V 2NX, United Kingdom (the "**Processor**" or "**DNX360**"); and

(2) The entity or individual identified in the applicable account registration or subscription confirmation (the "**Controller**" or "**Contractor**").

The Processor and the Controller are each a "**Party**" and together the "**Parties**".

1. INTRODUCTION AND SCOPE

1.1 This DPA governs the processing of Personal Data by DNX360 as Processor on behalf of the Contractor as Controller in connection with the DNX360 platform and services, as described in the Terms and Conditions between the Parties (the "**Master Agreement**" or "**Terms and Conditions**," as published on DNX360's website, and amended from time to time).

1.2 This DPA supplements and forms part of the Master Agreement. In the event of any inconsistency between this DPA and the Master Agreement, this DPA shall prevail solely with respect to the processing of Personal Data.

1.3 This DPA is a standalone agreement and may be executed, accepted, or incorporated independently of the Master Agreement where required by Applicable Data Protection Law, provided that both this DPA and the Master Agreement are in effect between the Parties.

1.4 This DPA does not govern any processing of Personal Data for which DNX360 acts as an independent Controller. Such processing is governed by the applicable DNX360 Privacy Policy.

2. DEFINITIONS AND INTERPRETATION

2.1 In this DPA, unless the context otherwise requires, the following terms shall have the meanings set out below. Capitalised terms not defined herein shall have the meanings ascribed to them in the Master Agreement.

(a) "**Applicable Data Protection Law**" means all applicable laws and regulations relating to data protection, privacy, and the processing of Personal Data, including (without limitation): (i) the UK General Data Protection Regulation (UK GDPR) as incorporated into United Kingdom law by virtue of Section 3 of the European Union (Withdrawal) Act 2018, together with the Data Protection Act 2018; (ii) Regulation (EU) 2016/679 (EU GDPR); (iii) the California Consumer Privacy Act, as amended by the California Privacy Rights Act (CCPA/CPRA); and (iv) any other applicable privacy or data protection legislation in any jurisdiction where Personal Data is collected, processed, or stored, in each case as amended, supplemented, or replaced from time to time.

(b) "**Data Subject**" means an identified or identifiable natural person to whom Personal Data relates.

(c) "**EEA**" means the European Economic Area.

(d) "**EU SCCs**" means the standard contractual clauses for the transfer of personal data to third countries approved by the European Commission pursuant to Decision 2021/914, as amended, supplemented, or replaced from time to time.

(e) "**Personal Data**" means any information relating to a Data Subject that is processed by the Processor on behalf of the Controller in connection with the Master Agreement, as further described in Schedule A to this DPA.

(f) "**Personal Data Breach**" means any confirmed breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed by the Processor.

(g) "**Processing**" (and its cognates "**Process**", "**Processed**", and "**Processes**") means any operation or set of operations performed on Personal Data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, destruction, anonymisation, and any other operation or set of operations contemplated by Applicable Data Protection Law.

(h) "**Sub-processor**" means any third party appointed by the Processor (or by any Sub-processor of the Processor) to Process Personal Data on behalf of the Controller in connection with the services provided under the Master Agreement.

(i) "**Supervisory Authority**" means any governmental, regulatory, or oversight body with competence over data protection matters, including (without limitation) the UK Information Commissioner's Office (ICO) and any competent supervisory authority within the EEA.

(j) "**UK Addendum**" means the International Data Transfer Addendum to the EU SCCs issued by the UK Information Commissioner under Section 119A of the Data Protection Act 2018, as may be amended, supplemented, or replaced from time to time.

(k) "**Sub-processor List**" means the then-current, up-to-date list maintained by DNX360 of all third-party Sub-processors engaged in the provision of the Services, including but not limited to any infrastructure providers, cloud hosting providers, security service providers, analytics providers, and artificial intelligence or machine learning model providers that may Process Customer Personal Data on behalf of DNX360 as mentioned in this DPA and available on www.DNX360.com/SubProcessorsList

The Sub-processor List forms an integral part of this DPA and is made available at the URL or other designated location specified by DNX360, as may be updated from time to time. The Sub-processor List may be amended by DNX360 in accordance with the Sub-processor update and notification provisions set out in this DPA.

(l) **“Sub-processor Engagement”** means the appointment or introduction of a new third-party Sub-processor not previously included in the Sub-processor List that is authorized to Process Customer Personal Data on behalf of DNX360.

For the avoidance of doubt, Sub-processor Engagement does not include any internal or operational changes in the allocation, routing, weighting, load balancing, failover, redundancy, or selection of Sub-processors already included in the Sub-processor List.

2.2 References to the EU GDPR, UK GDPR, or any specific provision thereof shall be interpreted to include the equivalent, corresponding, or analogous provisions under any Applicable Data Protection Law. Where different jurisdictions use different terminology for the same or substantially similar concepts, the terms used herein shall be interpreted to include their local equivalents.

2.3 The rules of interpretation set out in the Master Agreement shall apply to this DPA, mutatis mutandis.

3. ROLES AND RESPONSIBILITIES

3.1 The Contractor acts as Controller in relation to Personal Data submitted to or through the Platform by or on behalf of the Contractor or any SMB Client, or, where applicable, as processor, service provider, contractor, or other equivalent intermediary on behalf of the relevant controller, business, or other primary responsible party. DNX360 acts as Processor, Service Provider, Contractor, or sub-processor (as applicable) on behalf of the Contractor in relation to such Personal Data and shall Process such Personal Data solely in accordance with this DPA, the Master Agreement, and Applicable Data Protection Law.

3.2 Nothing in this DPA prevents DNX360 from Processing Personal Data as an independent Controller, Business, or other equivalent independent responsible party to the extent necessary for account administration, billing, payment processing, fraud prevention, security monitoring, incident response, legal and regulatory compliance, internal reporting, the establishment, exercise, or defence of legal claims, and the maintenance, reliability, security, and performance of the Platform and Services, in each case in accordance with Applicable Data Protection Law and the applicable DNX360 Privacy Policy.

3.3 For the avoidance of doubt, any use by DNX360 of anonymised data, or aggregated data that does not identify and cannot reasonably be used to identify any natural person, SMB Client, or Contractor, shall be governed by the Master Agreement and applicable law and shall fall outside the scope of this DPA to the extent such data is no longer Personal Data under Applicable Data Protection Law.

4. CONTROLLER OBLIGATIONS

4.1 The Contractor shall:

- (a) ensure that all Personal Data submitted to the Platform has been collected lawfully and that the Contractor has all necessary rights, permissions, consents, authorisations, and lawful bases to enable DNX360 to Process such Personal Data in accordance with this DPA and the Master Agreement;
- (b) provide all required privacy notices, disclosures, and transparency information to Data Subjects in accordance with Applicable Data Protection Law;
- (c) ensure the accuracy, relevance, and adequacy of Personal Data submitted to the Platform;
- (d) comply with all obligations incumbent upon it as a Controller under Applicable Data Protection Law, including (without limitation) all applicable data protection, privacy, artificial intelligence, employment, and sector-specific legislation; and
- (e) be solely responsible for its relationships with its own clients (including SMB Clients) and for any representations, warranties, or obligations made or undertaken by the Contractor in connection with the processing of their Personal Data.

4.2 The Contractor warrants and represents that it has and shall maintain throughout the term of this DPA all necessary rights, permissions, and authorisations for DNX360 to Process Personal Data as contemplated by this DPA, the Master Agreement, and Applicable Data Protection Law.

5. PROCESSOR OBLIGATIONS

5.1 DNX360 shall:

- (a) Process Personal Data only on the documented instructions of the Controller, unless required to do so by Applicable Data Protection Law to which DNX360 is subject, in which case DNX360 shall (to the extent permitted by such law) inform the Controller of that legal requirement

before carrying out the relevant Processing. The Master Agreement (including this DPA), any applicable Order Form, and the Contractor's use of the Platform shall constitute the Controller's documented instructions for the purposes of this clause;

(b) ensure that all persons authorised to Process Personal Data are subject to binding obligations of confidentiality (whether contractual or statutory);

(c) implement and maintain appropriate technical and organisational measures to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or unauthorised access, taking into account the state of the art, the costs of implementation, the nature, scope, context, and purposes of Processing, and the risks to Data Subjects, as further described in Schedule B to this DPA;

(d) take reasonable steps to ensure the reliability, integrity, and competence of any personnel who have access to Personal Data, including through appropriate training and authorisation; and

(e) taking into account the nature of the Processing, assist the Controller by appropriate technical and organisational measures, insofar as this is reasonably possible, with the fulfilment of the Controller's obligations to respond to Data Subject requests exercising their rights under Applicable Data Protection Law.

5A. US STATE PRIVACY LAW STATUS

5A.1 To the extent that the CCPA/CPRA or any analogous US state privacy law applies to the Processing of Personal Data under this DPA, the Parties acknowledge that DNX360 acts as a "service provider", "contractor", or analogous restricted recipient, as applicable, with respect to such Personal Data.

5A.2 DNX360 shall not:

(a) sell or share such Personal Data;

(b) retain, use, or disclose such Personal Data for any purpose other than for the specific business purposes and services described in the Master Agreement and this DPA, as otherwise permitted by applicable US state privacy law, or as otherwise instructed by the Controller; or

(c) combine such Personal Data with personal information received from another source, except as permitted by applicable US state privacy law.

5A.3 Nothing in this clause 5A restricts DNX360 from using anonymised or deidentified data, or aggregated data that does not identify any individual, to the extent permitted by applicable law.

6. SUB-PROCESSING

6.1 The Controller hereby provides DNX360 with a general written authorisation to engage Sub-processors in connection with the provision of the Services.

6.2 DNX360 may engage Sub-processors across categories including, without limitation, cloud hosting and infrastructure, storage, security, analytics, communications, payment processing, customer support, artificial intelligence and machine learning services, transcription, and related technical or operational service providers.

6.3 DNX360 shall maintain a current Sub-processor List (the "Sub-processor List"), identifying the Sub-processors authorised to Process Personal Data in connection with the Services. The Sub-processor List shall be made available at the URL designated by DNX360 from time to time and may additionally be made available through the Platform or upon written request. At the time of writing, this URL is www.DNX360.com/SubProcessorsList, but is provided for convenience only and may be subject to change.

6.4 DNX360 may update the Sub-processor List from time to time, including to add, replace, remove, suspend, or re-categorise Sub-processors. DNX360 may also dynamically route, allocate, or process Personal Data across listed Sub-processors as part of the normal operation of the Services, including for redundancy, resiliency, load balancing, latency optimisation, service quality, regional delivery, emergency substitution, or operational continuity.

6.5 DNX360 shall provide notice of any new Sub-processor Engagement by updating the Sub-processor List and, where reasonably practicable, by email, in-platform notification, or other reasonable written notice. Unless a shorter period is reasonably necessary for urgent security, legal, regulatory, operational continuity, or supplier-failure reasons, DNX360 shall use reasonable efforts to provide not less than thirty (30) days' prior notice of any new Sub-processor Engagement.

6.6 The Controller may object to a new Sub-processor Engagement on reasonable and substantiated data protection grounds by providing written notice to DNX360 within fourteen (14) days after the relevant notice under clause 6.5. Any objection must identify the specific Sub-processor concerned and the specific legal or data protection basis for the objection.

6.7 Any objection shall apply only to the relevant new Sub-processor Engagement and shall not affect the continued use of any other Sub-processors included on the Sub-processor List.

6.8 Following receipt of a valid objection, DNX360 may, in its sole discretion, use reasonable efforts to:

- (a) provide a commercially reasonable alternative;
- (b) recommend a change in the Controller's configuration or use of the Services to avoid the relevant Processing; or
- (c) decline to use the proposed Sub-processor for the Controller's relevant Processing.

6.9 If DNX360 is unable to resolve the objection through a commercially reasonable alternative within a reasonable period, either Party may terminate only the affected Services on written notice. In such case, DNX360 shall refund only any prepaid recurring subscription fees actually received by DNX360 covering the unused remainder of the then-current Subscription Period solely for the affected Services. No refund, compensation, or other payment shall be due in respect of any other amounts.

6.10 DNX360 shall impose on each Sub-processor, by way of a written agreement, data protection obligations that are no less protective in all material respects than those imposed on DNX360 under this DPA to the extent required by Applicable Data Protection Law.

6.11 DNX360 shall remain responsible for the acts and omissions of its Sub-processors to the extent required by Applicable Data Protection Law.

7. INTERNATIONAL DATA TRANSFERS

7.1 The Controller acknowledges that DNX360 operates across multiple jurisdictions, including the United Kingdom, the United States, and the European Economic Area, and that Personal Data may be transferred to, stored in, or accessed from any jurisdiction in which DNX360 or its Sub-processors maintain facilities or operations.

7.2 Where Personal Data is transferred to, stored in, or accessed from a country or territory outside the United Kingdom, the EEA, or any other jurisdiction from which such transfer is regulated under Applicable Data Protection Law, and where the destination has not been recognised as providing an adequate level of protection under Applicable Data Protection Law, DNX360 shall ensure that an appropriate transfer mechanism is in place to the extent required under Applicable Data Protection Law, which may include:

- (a) the EU SCCs;
- (b) the UK Addendum or the UK International Data Transfer Agreement;
- (c) an adequacy decision, adequacy regulation, adequacy finding, or equivalent recognition by a competent authority;
- (d) the EU-US Data Privacy Framework, the UK Extension thereto, the Swiss-US Data Privacy Framework, or any successor or equivalent mechanism, where applicable; or
- (e) any other lawful transfer mechanism recognised under Applicable Data Protection Law.

7.3 To the extent required under Applicable Data Protection Law, DNX360 shall carry out such transfer impact assessments, transfer risk assessments, or equivalent assessments as are reasonably necessary in connection with relevant international transfers of Personal Data.

7.4 References in this clause 7 to any transfer mechanism include any amended, replaced, successor, or equivalent mechanism recognised under Applicable Data Protection Law from time to time.

7.5 Nothing in this DPA requires DNX360 to adopt any transfer mechanism that is not legally required or otherwise commercially reasonable for DNX360 to implement, provided that DNX360 maintains an appropriate lawful basis for the relevant transfer where required under Applicable Data Protection Law.

8. DATA BREACH NOTIFICATION

8.1 To the extent required by Applicable Data Protection Law, DNX360 shall notify the Controller without undue delay after becoming aware of a confirmed Personal Data Breach affecting Personal Data Processed under this DPA and, where Applicable Data Protection Law requires a specific period, within the applicable required timeframe.

8.2 Such notification shall include, to the extent reasonably available at the time of notification:

- (a) a description of the nature of the Personal Data Breach, including (where possible) the categories and approximate number of Data Subjects and Personal Data records affected;
- (b) the contact details of the relevant DNX360 point of contact from whom further information may be obtained;
- (c) a description of the likely consequences of the Personal Data Breach; and
- (d) a description of the measures taken or proposed to be taken by DNX360 to address and mitigate the effects of the Personal Data Breach.

8.3 DNX360 shall cooperate with the Controller in the investigation, mitigation, and remediation of any Personal Data Breach, subject to (and without prejudice to) Applicable Data Protection Law, legal professional privilege, obligations of confidentiality owed to other customers, and system security considerations.

8.4 Nothing in this clause 8 requires DNX360 to provide notification where such notification is not required under Applicable Data Protection Law, including where the relevant incident is unlikely to result in a risk to individuals or where the affected data has been rendered unintelligible to unauthorised persons by appropriate technical measures, unless Applicable Data Protection Law requires notification notwithstanding those measures.

8.5 Nothing in this clause 8 shall be construed as an acknowledgement by DNX360 of any fault or liability with respect to a Personal Data Breach.

9. DATA SUBJECT RIGHTS

9.1 DNX360 shall, taking into account the nature of the Processing, assist the Controller by implementing appropriate technical and organisational measures, insofar as this is reasonably possible, for the fulfilment of the Controller's obligations to respond to requests from Data Subjects exercising their rights under Applicable Data Protection Law, including (without limitation) the rights of access, rectification, erasure, restriction, data portability, objection, and rights relating to automated decision-making.

9.2 DNX360 shall promptly notify the Controller of any request received directly from a Data Subject in respect of Personal Data Processed under this DPA. DNX360 shall not respond to any such request except on the Controller's documented instructions or as required by Applicable Data Protection Law.

9.3 The Controller acknowledges that DNX360's ability to assist with Data Subject requests may be limited by the technical architecture of the Platform and that compliance with certain requests may not be reasonably possible without disproportionate effort, particularly where Personal Data has been anonymised, aggregated, or incorporated into AI model training on an anonymised basis.

10. DATA PROTECTION IMPACT ASSESSMENTS AND PRIOR CONSULTATION

10.1 Taking into account the nature of the Processing and the information available to DNX360, DNX360 shall provide reasonable assistance to the Controller in connection with data protection impact assessments, transfer assessments, prior consultation with Supervisory Authorities, and equivalent obligations under Applicable Data Protection Law, to the extent that such assistance is:

- (a) required by Applicable Data Protection Law;
- (b) reasonably requested by the Controller in writing; and
- (c) reasonably technically and commercially feasible.

10.2 DNX360 may satisfy its obligations under this clause 10 by providing documentation, summaries, explanations, certifications, transfer mechanism information, security information, or other materials that DNX360 reasonably considers appropriate in the circumstances.

10.3 DNX360 may charge a reasonable fee for assistance under this clause 10 where the requested assistance exceeds DNX360's standard compliance or support obligations, provided that DNX360 informs the Controller of any such fee before providing the relevant assistance.

10.4 Nothing in this clause 10 requires DNX360 to disclose trade secrets, source code, algorithms, models, prompts, questionnaires, scoring methodologies, internal security materials, information relating to other customers, legally privileged material, or any other information protected from disclosure under this DPA, the Master Agreement, or Applicable Law.

11. AUDIT RIGHTS

11.1 DNX360 shall, upon written request, make available to the Controller such information as DNX360 reasonably determines is necessary to demonstrate compliance with its obligations under Article 28 of the EU GDPR and equivalent provisions under Applicable Data Protection Law.

11.2 DNX360 may satisfy its obligations under clause 11.1, in whole or in part, by providing current third-party certifications, attestations, audit reports, summaries, questionnaires, written responses, policies, procedures, or other equivalent compliance materials.

11.3 The Controller may request a direct audit or inspection only where:

- (a) the Controller has first requested and reviewed the materials made available under clause 11.2;
- (b) the Controller reasonably determines that such materials are insufficient to satisfy a specific legal obligation under Applicable Data Protection Law; and
- (c) the Controller provides DNX360 with a written request identifying the specific compliance concern, the legal basis for the request, the reason the materials already provided are insufficient, and the proposed scope, methodology, duration, and timetable.

11.4 Any direct audit or inspection shall be permitted only to the extent legally required and shall be subject to the following conditions:

- (a) no more than one (1) audit or inspection in any rolling twelve (12) month period unless a competent Supervisory Authority or mandatory Applicable Data Protection Law expressly requires otherwise;
- (b) not less than thirty (30) days' prior written notice;
- (c) the audit or inspection must be proportionate and strictly limited to Processing activities directly relevant to the Controller's Personal Data;
- (d) the audit or inspection must be conducted during normal business hours and in a manner that does not unreasonably disrupt DNX360's business, systems, personnel, security, or services to other customers;
- (e) DNX360 may require the audit or inspection to be conducted through document review, written responses, interviews, remote review, or other less intrusive means where reasonably sufficient;
- (f) any on-site visit shall be permitted only where less intrusive means are insufficient to satisfy a mandatory legal requirement identified by the Controller;

- (g) the audit or inspection must be conducted by an independent external auditor appointed by the Controller and approved in advance by DNX360, such approval not to be unreasonably withheld where Applicable Data Protection Law requires the audit;
- (h) DNX360 may reject a proposed auditor on reasonable grounds including confidentiality concerns, conflict of interest, competitive sensitivity, security concerns, lack of qualification, or prior misconduct; and
- (i) the auditor must be bound by written confidentiality obligations in a form acceptable to DNX360.

11.5 Nothing in this DPA requires DNX360 to disclose or permit access to:

- (a) source code, object code, algorithms, models, prompts, weights, training data, questionnaires, scoring methodologies, analytical frameworks, or other Protected IP;
- (b) trade secrets or commercially sensitive information;
- (c) information relating to other customers or third parties;
- (d) penetration-test materials, vulnerability details, forensic materials, internal security documentation, system configurations, or similar security-sensitive materials;
- (e) legally privileged material;
- (f) information subject to duties of confidentiality owed to third parties; or
- (g) information the disclosure of which would violate Applicable Law or materially increase security, legal, regulatory, operational, or commercial risk.

11.6 DNX360 may provide redacted, summarised, aggregated, excerpted, or otherwise limited materials where reasonably necessary to protect confidentiality, privilege, security, third-party rights, or DNX360's legitimate business interests, provided that such materials are sufficient to demonstrate compliance to the extent required by Applicable Data Protection Law.

11.7 The Controller shall bear its own costs and the costs of any audit or inspection, including DNX360's reasonable internal costs of facilitating the same, except to the extent Applicable Data Protection Law expressly prohibits such allocation.

11.8 All information disclosed or generated in connection with any audit or inspection shall constitute DNX360 Confidential Information and shall be subject to the confidentiality protections of the Master Agreement.

11.9 To the extent permitted by Applicable Data Protection Law, this clause 11 sets out the Controller's sole and exclusive contractual rights to audit, inspect, verify, or review DNX360 in relation to the subject matter of this DPA.

12. DATA RETENTION AND DELETION

12.1 Upon termination or expiry of the Master Agreement, and subject to clause 12.3, DNX360 shall, at the Controller's written request made within thirty (30) days of such termination or expiry:

- (a) return to the Controller all Personal Data in a commonly used, machine-readable format; or
- (b) securely delete all Personal Data in DNX360's possession or control,

as directed by the Controller. The Controller may request a combination of return and deletion for different categories of Personal Data.

12.2 If the Controller does not make a written request within the thirty (30) day period specified in clause 12.1, DNX360 may delete all Personal Data in accordance with its standard data retention and deletion policies.

12.3 DNX360 may retain Personal Data (or any part thereof) to the extent that retention is required or permitted by Applicable Data Protection Law, or is reasonably necessary for:

- (a) compliance with any legal, regulatory, tax, accounting, or reporting obligation;
- (b) the establishment, exercise, or defence of legal claims;
- (c) fraud prevention, security, or audit purposes;
- (d) insurance, indemnification, or dispute resolution;

- (e) backup, archival, and disaster recovery in accordance with standard business continuity practices; or
- (f) any other purpose for which retention is required or permitted under Applicable Data Protection Law.

12.4 Any Personal Data retained pursuant to clause 12.3 shall continue to be subject to the protections of this DPA and shall be Processed only for the specific purpose(s) for which it is retained. DNX360 shall delete such retained Personal Data once the applicable retention purpose has been fulfilled, subject to its standard retention, archival, overwrite, and deletion cycles.

13. SECURITY MEASURES

13.1 DNX360 shall implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risk of Processing, taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects.

13.2 Without prejudice to the generality of clause 13.1, such measures shall include, as appropriate:

- (a) the encryption of Personal Data in transit and at rest;
- (b) measures to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;
- (c) the ability to restore the availability of and access to Personal Data in a timely manner in the event of a physical or technical incident;
- (d) access controls and authentication mechanisms to prevent unauthorised access to Personal Data;
- (e) regular testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of Processing;
- (f) measures for the pseudonymisation and anonymisation of Personal Data, where appropriate;
- (g) incident detection, response, and management procedures; and
- (h) personnel security measures, including background checks, training, and binding confidentiality obligations.

13.3 The Controller acknowledges that security measures are subject to technical progress and development and that DNX360 may update or modify its security measures from time to time, provided that such updates or modifications do not materially decrease the overall level of protection afforded to Personal Data.

14. LIABILITY AND INDEMNIFICATION

14.1 The liability of each Party under or in connection with this DPA shall be subject to the limitation and exclusion of liability provisions set out in the Master Agreement, unless mandatory Applicable Data Protection Law requires otherwise.

14.2 The Contractor shall indemnify and hold harmless DNX360, its Affiliates, and their respective officers, directors, employees, and agents from and against any and all losses, damages, liabilities, costs, and expenses (including reasonable legal fees) arising from or in connection with:

- (a) the Contractor's breach of its obligations under this DPA or Applicable Data Protection Law;
- (b) any claim brought by a Data Subject or Supervisory Authority resulting from the Contractor's failure to comply with its obligations as Controller;
- (c) any Personal Data submitted to the Platform in breach of Applicable Data Protection Law or without the required consents, authorisations, or lawful bases;
- (d) any instructions provided by the Contractor that are contrary to Applicable Data Protection Law; and
- (e) any claim arising from the Contractor's failure to fulfil its obligations to Data Subjects or to provide adequate privacy notices or disclosures.

14.3 For the avoidance of doubt, DNX360's aggregate liability under this DPA shall not exceed the aggregate liability cap set out in the Master Agreement, and any liability incurred under this DPA shall count towards (and not be in addition to) such cap.

15. TERM AND TERMINATION

15.1 This DPA shall come into effect on the date on which the Contractor first accepts or becomes bound by the Master Agreement (or, where this DPA is executed separately, on the date of execution by both Parties) and shall remain in effect for the duration of DNX360's Processing of Personal Data on behalf of the Controller.

15.2 This DPA shall automatically terminate upon the later of: (a) the termination or expiry of the Master Agreement; and (b) the completion of all Processing activities and the deletion or return of all Personal Data in accordance with clause 12.

15.3 Clauses 2 (Definitions and Interpretation), 8 (Data Breach Notification), 11.5 (Confidentiality of Audit Findings), 12 (Data Retention and Deletion), 13 (Security Measures, to the extent Personal Data is retained), 14 (Liability and Indemnification), 16 (General Provisions), and this clause 15.3 shall survive the termination or expiry of this DPA.

16. GENERAL PROVISIONS

16.1 Governing Law. This DPA shall be governed by and construed in accordance with the laws of England and Wales, without regard to its conflict of law principles.

16.2 Jurisdiction. The courts of England and Wales shall have exclusive jurisdiction in relation to any dispute arising out of or in connection with this DPA, subject to DNX360's right to bring proceedings in any court of competent jurisdiction in accordance with the Master Agreement.

16.3 Amendments. DNX360 may amend this DPA from time to time by notice through the Platform, through the Controller's account or billing interface, by email to the registered account email address or other notified legal contact, by publication on DNX360's website, or by any combination of those methods, where reasonably necessary to:

- (a) comply with Applicable Data Protection Law, regulatory guidance, court orders, or transfer-mechanism requirements;
- (b) address security, fraud, abuse, misuse, technical integrity, operational continuity, or service architecture;
- (c) reflect updates to Sub-processors, transfer mechanisms, service features, or processing operations; or
- (d) make clarifications, corrections, or other changes that do not materially reduce the protections afforded to Personal Data under this DPA.

Any such amendment shall take effect on the date specified by DNX360 in the relevant notice. Updates to the Sub-processor List do not require a formal amendment to this DPA. Nothing in this clause limits any right of objection or other right available to the Controller under Applicable Data Protection Law or under clause 6 of this DPA.

16.4 Severability. If any provision of this DPA is held to be invalid, illegal, or unenforceable, the remaining provisions shall continue in full force and effect. The Parties shall negotiate in good faith a replacement provision that is valid, legal, and enforceable and that achieves, to the greatest extent possible, the economic, business, and other purposes of the invalid provision.

16.5 Entire Agreement. This DPA, together with the Master Agreement and any schedules, appendices, or annexes hereto, constitutes the entire agreement between the Parties with respect to the Processing of Personal Data and supersedes all prior agreements, representations, warranties, and understandings relating to the subject matter hereof.

16.6 No Waiver. No failure or delay by either Party in exercising any right, power, or remedy under this DPA shall operate as a waiver thereof, nor shall any single or partial exercise of any such right, power, or remedy preclude any other or further exercise thereof or the exercise of any other right, power, or remedy.

16.7 Third Party Rights. A person who is not a party to this DPA shall not have any rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this DPA.

16.8 Notices. All notices under this DPA shall be in writing and sent to the contact details specified in the Master Agreement, or to such other address as a Party may notify to the other in writing from time to time. Notices relating to data protection matters may be sent by email to legal@dnx360.com.

16.9 Counterparts. This DPA may be executed in counterparts, each of which shall be deemed an original, and all of which together shall constitute one and the same instrument.

17. CONTACT INFORMATION

For questions about this Data Processing Agreement, or to report a violation, please contact:

J. Sallinger Ltd.
128 City Road
London, EC1V 2NX
United Kingdom

Email: legal@dnx360.com

SCHEDULE A

Description of Processing Activities

A.1 Subject Matter and Duration of Processing

The Processing of Personal Data by DNX360 as Processor in connection with the provision of the DNX360 platform and services under the Master Agreement, for the duration of the Master Agreement and thereafter as reasonably necessary for backup cycles, audit trails, dispute management, legal compliance, regulatory requirements, and ongoing service improvement and security, subject to applicable retention limits.

A.2 Nature of Processing

Collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, deletion, erasure, anonymisation, and destruction of Personal Data, as necessary for the provision of the Platform and Services.

A.3 Purposes of Processing

Personal Data shall be Processed for the following purposes:

- (a) account setup, authentication, identity verification, and administration;
- (b) hosting, storage, transmission, backup, and organisation of submitted information;
- (c) operation of the Questionnaire Engine, AI Engine, and diagnostic analysis systems;
- (d) generation of analyses, reports, recommendations, Outputs, and interview guides;
- (e) voice transcription processing;
- (f) white-label branding and customisation;
- (g) customer support, troubleshooting, and onboarding;
- (h) monitoring, security, abuse prevention, and fraud detection;
- (i) product improvement, analytics, and model or service improvement only on anonymised data, or aggregated data that does not identify and cannot reasonably be used to identify any natural person;
- (j) billing, invoicing, payment processing, and tax compliance;
- (k) compliance with Applicable Data Protection Law and other applicable legislation; and
- (l) any other purpose reasonably necessary for the provision of the Platform and Services as described in the Master Agreement.

A.4 Categories of Data Subjects

The following categories of Data Subjects may be affected by the Processing:

- (a) the Contractor's employees, officers, directors, representatives, and agents;
- (b) SMB Clients and their employees, officers, representatives, agents, and authorised users;
- (c) Stakeholders assigned to complete questionnaires through the Platform; and
- (d) other business contacts whose Personal Data is submitted through the Platform by or on behalf of the Contractor.

A.5 Categories of Personal Data

The following categories of Personal Data may be Processed:

- (a) names, job titles, business email addresses, business telephone numbers, and other business contact details;
- (b) organisation names, department names, and organisational structure information;
- (c) account identifiers, login credentials (encrypted), and authentication data;
- (d) usage data, session data, access logs, IP addresses, device identifiers, and browser data;
- (e) questionnaire responses, including free-text and voice-transcribed responses;

- (f) business operational data submitted through the questionnaire (including processes, tools, workflows, team structures, business performance data, and strategic priorities);
- (g) billing data, payment-related identifiers, and transaction records;
- (h) communications data (including support tickets, emails, and in-platform messaging); and
- (i) any other Personal Data submitted by or on behalf of the Contractor or SMB Client through the Platform.

A.6 Special Categories of Data

The Processor shall not Process any special category data, sensitive personal information, criminal conviction data, or analogous restricted or heightened-risk data categories as defined under Applicable Data Protection Law, unless expressly permitted by the Platform, applicable supplemental terms, or DNX360's prior written approval, and all required notices, consents, and safeguards are in place.

SCHEDULE B

Technical and Organisational Security Measures

DNX360 implements and maintains technical and organisational measures designed to protect Personal Data, taking into account the nature of the Services, the state of the art, the costs of implementation, and the risks presented by the Processing. Such measures may include, as appropriate to the relevant environment, role, system, and risk profile, the following categories of controls:

B.1 Access Control and Authentication

- (a) Role-based access controls restricting access to Personal Data to authorised personnel on a need-to-know basis;
- (b) strong authentication mechanisms, including multi-factor authentication for administrative and privileged access;
- (c) unique user identification and credential management;
- (d) automatic session timeout and lockout policies; and
- (e) regular review and revocation of access rights, including upon personnel changes.

B.2 Encryption and Data Protection

- (a) Encryption of Personal Data in transit using industry-standard transport layer security protocols;
- (b) encryption of Personal Data at rest using industry-standard encryption algorithms;
- (c) secure key management practices; and
- (d) pseudonymisation and anonymisation measures, where appropriate.

B.3 Network and Infrastructure Security

- (a) Firewalls, intrusion detection, and intrusion prevention systems;
- (b) network segmentation and isolation of processing environments;
- (c) regular vulnerability scanning and patching;
- (d) distributed denial-of-service protection; and
- (e) secure configuration and hardening of systems and infrastructure components.

B.4 Availability and Resilience

- (a) Regular backups of Personal Data with tested restoration procedures;
- (b) redundancy and failover mechanisms for critical systems;
- (c) business continuity and disaster recovery planning and testing; and
- (d) monitoring of system availability and performance.

B.5 Incident Management

- (a) Documented incident detection, response, and escalation procedures;
- (b) incident classification and prioritisation frameworks;
- (c) post-incident review and lessons-learned processes; and
- (d) breach notification procedures in accordance with clause 8 of this DPA.

B.6 Organisational Measures

- (a) Information security policies and procedures, regularly reviewed and updated;
- (b) data protection and security awareness training for all personnel with access to Personal Data;
- (c) binding confidentiality obligations for all personnel and contractors;
- (d) vendor and sub-processor due diligence and security assessments;

- (e) data minimisation principles in system design and Processing activities; and
- (f) regular auditing and assessment of security controls.

B.7 Physical Security

- (a) Physical access controls to data centre facilities (where applicable);
- (b) environmental controls (fire suppression, climate control, power redundancy); and
- (c) secure disposal and destruction of physical media containing Personal Data.

END OF DATA PROCESSING AGREEMENT