DATA PROCESSING AGREEMENT (GDPR)

UPDATED:

This Data Processing Agreement ("DPA") is between Playbook UX, LLC, a New Hampshire Limited Liability Corporation ("Playbook UX") and the Client ("the Client").

The Client's details are as follows:
Name: _____
Address: _____
Contact person's name, position and contact details: _____
_____
___
Role: Controller

Playbook UX's details are as follows:
Name: Playbook UX LLC
Address: 14 Ferry Road Hanover, New Hampshire, 03755, United States
Lindsey Allarrd
Co-Founder & CEO
Role: Processor

This DPA forms part of the Service Contract (the "Contract"), between the Client and Playbook UX, pursuant to which the Client has purchased Playbook UX's services ("Services"). It is applicable to Personal Data that is Processed by Playbook UX on behalf of the Client. The Client and Playbook UX may be referred to individually as a "Party" and collectively as the "Parties".

1. Definitions

For the purpose of this DPA, the following definitions apply:

1. "Controller" means the entity that determines the purposes and means of the Processing of Personal Data.

2. "Data Breach" means a Breach of privacy leading to the destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data. Examples of Personal Data Breaches include:

- access by an unauthorized third party;
- deliberate or accidental action (or inaction) by a Controller or Processor;
- sending Personal Data to an incorrect recipient;
- computing devices containing Personal Data being lost or stolen;
- alteration of Personal Data without permission;
- loss of availability of Personal Data.

3. “Data Subject” means any identified or identifiable natural person whose Personal Data is Processed.

4. “GDPR” means: (i) the EU General Data Protection Regulation (2016/679) and any implementing laws in each EU member state as they may be amended from time to time, and (ii) the United Kingdom’s Data Protection Act 2018 (or “UK GDPR”) and any implementing laws in the United Kingdom when the Client is based in the UK.

5. "Personal Data" means data that may be connected, directly or indirectly to individuals, such as unique personal identifiers, account names purchasing history, internet activity, which is provided by the Client to Playbook UX or collected, accessed, stored or otherwise processed by Playbook UX in connection with the Services.

6. “Processing” means collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, combining, restricting, erasing or destroying Personal Data.

7. “Processor” means the entity that is responsible for Processing Personal Data on behalf of a Controller.

8. “Services” means the services that Playbook UX provides to the Client through the online platform https://www.playbookxux.com, namely, feedback gathering services from targeted audiences;

9. “Special categories of data” or “Sensitive data” means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a

person's sex life or sexual orientation, or data relating to criminal convictions and offences.

10. "Standard Contractual Clauses" means the European standard contractual clauses (controllers to processors modules) for the transfer of Personal Data to third countries set out in the EU Commission Decision of 4 June 2021.

11. "Subprocessor" means any third-party appointed by Playbook UX to process the Personal Data on behalf of the Client in connection with the Services.

12. "Supervisory Authority" is an independent public authority tasked with ensuring Personal Data is handled appropriately, and with monitoring compliance with the GDPR.

2. Processing of Personal Data

2.1. Processing under the exclusive instructions of the Client

The Parties acknowledge and agree that the Client is the Controller and Playbook UX is the Processor.

The Agreement shall apply to all activities within the scope of the Service Contract in the context of which Playbook UX or any Subprocessor may process the Personal Data.

Playbook UX shall only Process Personal Data on behalf of and in accordance with the Client's documented instructions. In other words, all Processing activities carried out by Playbook UX for the Client will aim at:

- providing the Services defined in this Contract;
- complying with other documented reasonable instructions provided by the Client (e.g., via contacting Playbook UX's customer chat and email support) where such instructions are consistent with the terms of the Contract; and
- complying with the GDPR.

Should Playbook UX wish to use the Client's Personal Data for the purposes that are not specified in this DPA, Playbook UX shall request the Client to provide prior authorization in writing and conclude relevant agreements with the Client.

When the Personal Data is transmitted by the Client to Playbook UX, the Client shall have sole responsibility for the accuracy and quality of Personal Data and for the means

by which the Client acquired Personal Data, including compliance with any lawfulness requirements.

2.2. Details on the Processing of Personal Data

The general objective of the Processing is to enable the Client to receive and Playbook UX to facilitate the provision of the Services by Playbook UX to the Client.

The nature of the Processing activities is to record audio and video of Data Subjects' screen and voice (during unmoderated studies), as well as their faces (during moderated studies) whenever they take part in a test, as well as collecting survey question data points.

The Client determines under its responsibility the purposes of the Processing activities, which are to (i) allow the Client to watch videos of Data Subjects interacting with their products as they speak their thoughts aloud, (ii) to view transcripts alongside video recordings and clips of important moments in the use of the Client's products by Data Subjects, and (iii) to be provided with comprehensive dashboards that streamline qualitative and quantitative synthesis.

The sources of collection the Personal Data by Playbook UX may be Personal Data that has been previously collected by the Client and that is transferred to Playbook UX in the context of the Services ("Bring your own Participants scenario"). In addition, the sources of collection may also consist in Personal Data that Playbook UX has previously collected from non-EU residents ("Playbook UX Participants scenario").

The personal Data or categories of Personal Data that is Processed in the "Bring your own Participants" is the following: (a) first name, (b) screen images, (c) sound and video recordings, (d) answer to Clients' questions, I device and operating system,, and other content or data in electronic form stored or transmitted by the Client to Playbook UX).

The Personal Data or categories of Personal Data that is Processed in the "Playbook UX Participants scenario" is (a) first name, (b) gender, (c) age, (d) location, I ethnicity, (f) household income, (g) job title, (h) industry, (i) company size, (j) seniority, (k) device & operating system, (l) answer to Clients' questions, (m) screen images, and (n) sound and video recordings

Special categories of Personal Data may be Processed according to this Agreement, including, information about the Data Subject's religious beliefs and ethnicity.

The categories of Data Subjects are the individuals that are the Clients' customers and/or subscribers, and whose Personal Data have been supplied by the Client to Playbook UX. Furthermore, categories of Data Subjects may also include non-EU individuals that have subscribed to Playbook UX's platform to become a tester in the Playbook UX Participants scenario.

The duration of the Processing is the Term of this Contract, and an additional period of 30 days after the Client and Playbook UX have terminated their contract ("Duration of Processing").

Playbook UX shall not be liable for any claim brought by the Client or any third party arising from Playbook UX's compliance with the Client's instructions.

3. Safeguards deployed by Playbook UX

3.1. Playbook UX' organizational safeguards

Playbook UX considers, with regard to its tools, products, applications or services, the principles of privacy by design and privacy by default. It also strives to offer services that respect the principles of proportionality, minimization and limitation of Personal Data, ensuring that only relevant Personal Data is Processed.

If Playbook UX becomes aware that the Personal Data that is Processed is inaccurate, or has become outdated, it shall inform the Client without undue delay. In this case, Playbook UX shall cooperate with the Client to erase or rectify the data.

Playbook UX shall take reasonable steps to ensure the reliability of any employee, agent or contractor engaged by Playbook UX in the Processing of Personal Data. In this sense, Playbook UX shall ensure that its staff will not access, use or modify Personal Data, except when this is strictly necessary for the purposes of providing the Services, or for the prevention or handling of technical issues.

Playbook UX's staff members accessing the Personal Data are informed of the confidential nature of the Personal Data and have entered into written confidentiality agreements.

3.2. Security and technical safeguards

Playbook UX shall maintain appropriate technical and security measures ("Security Measures"), having regard to the state of technological development and cost of implementation for protection of the security, confidentiality and integrity of Personal Data (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss, theft or alteration or damage, unauthorized disclosure of, or access to, Personal Data).

The Security Measures employed by Playbook UX are at the minimum the following:

1. Data Access Control: Access is granted on a least privilege, need-to-have and must-know basis to prevent disclosure. Users and their activities are uniquely identifiable and segregated by role. Administrative privileges are restricted to only those who need them.

2. Information System Access Control: Access is strictly controlled by a formal provisioning process. Information systems are password protected and have an owner responsible for managing and controlling access.
3. Multi-factor Authentication: Playbook UX' personnel are only granted access to Personal Data and critical technology after successfully presenting multiple, separate pieces of evidence.
4. Physical Access Control: Unauthorized persons are prevented from gaining physical access to premises, buildings or rooms where Personal Data and critical technology are located.
5. Transmission Control: All Personal Data transmitted through a public network (e.g., the internet) must be encrypted or sent via a secure channel.
6. Separation Control: Network services, systems, workstations, and servers are separated based on business purpose.
7. Availability Control: To protect against loss of data, information systems are subject to backup and built-in redundancy.
8. Patch Management Control: System patches are implemented in a reasonable, risk-based timeframe.
9. Security Awareness Training: Persons who may have access to Personal Data or critical systems are trained annually on topics related to the importance of information security and safeguards against data loss, misuse or breach through physical, logical and social engineering mechanisms.

Playbook UX and the Client use, whenever possible, encryption or pseudonymization, including during the transmission of Personal Data. In case of pseudonymization, the additional information for attributing the Personal Data to a specific Data Subject remains, where possible, under the exclusive control of the Client.

In addition, Playbook UX does not purposefully create back doors or similar programming that could be used to access the system and/or Personal Data and does not purposefully create or change its business processes in a manner that facilitates access to Personal Data or systems.

Furthermore, where the Processing involves Sensitive Data, additional technical safeguards are used.

Finally, Playbook UX regularly monitors compliance with the Security Measures and Playbook UX will not materially decrease the overall security of the Services during the Duration of Processing. Playbook UX shall implement regular checks to ensure that these measures continue to provide an appropriate level of security.

In this context, the Client agrees that the Security Measures are appropriate for the categories of Personal Data being Processed.

4. Sub-Processing

The Client acknowledges and agrees that Playbook UX may appoint third parties to assist in providing the Services and Processing of Personal Data ("Sub-processors"), provided that such Sub-processors:

- agree to act only on Playbook UX's instructions when Processing Personal Data (which instructions shall be consistent with the Client's Processing instructions to Playbook UX); and
- have entered into a written agreement with Playbook UX containing data protection obligations not less protective than those in this DPA with respect to the protection of Personal Data.

The current list of Sub-processors used by Playbook UX for the Processing of Personal Data to the Client is available here: https://www.playbookux.com/data-subprocessors

Playbook UX shall also provide, at the Client's request, a copy of a sub-processor agreement and any subsequent amendments to the Client. To the extent necessary to protect business secrets or other confidential information, including Personal Data, Playbook UX may redact the text of the agreement prior to sharing a copy.

When any new Sub-processor is appointed that will Process Personal Data, Playbook UX will, at least thirty (30) days before the new Sub-processor processes any Personal

Data, notify the Client of the future appointment via email at hello@playbookux.com. In the event that the Client reasonably objects to the Processing of its Personal Data by any Sub-processor, it shall inform Playbook UX immediately by emailing its objection at hello@playbookux.com, within fourteen (14) days after receipt of Playbook UX's notice. If the Client does not object, during this time period, the new Sub-processors shall be deemed accepted by the Client.

In such event, Playbook UX will do one of the following at Playbook UX's option:

- instruct the Sub-processor to cease any further Processing of the Client's Personal Data, in which event this DPA shall continue unaffected; or
- allow the Client to terminate this DPA and the Contract and related Services immediately, in which case Playbook UX will provide the Client with a pro rata refund of any payment paid in advance for Services but not yet received by the Client.

Playbook UX shall be liable for the acts and omissions of its Sub-processors to the same extent Playbook UX would be liable if performing the services of each Sub-processor directly under the terms of this DPA. Playbook UX shall notify the Client of any failure by the Sub-processor to fulfill its obligations under that contract.

Finally, Playbook UX is not liable for any damage or loss caused or alleged to be caused by or in connection with the Client's enablement, access or use of any third-party services, or the Client's reliance on the privacy practices, data security processes or other policies of such third-party services.

5. Data Transfers

Playbook UX and the Client hereby agree that the 2021 Standard Contractual Clauses attached in Annexes 1 and 2 will apply to the transfer of Personal Data, provided that:

- such transfers are subject to the GDPR; and
- the Personal Data is being transferred to a country that the relevant regulatory authorities in the EEA or Switzerland, as applicable, do not recognize as providing an adequate level of protection for Personal Data; and that
- the Personal Data is not covered by a suitable alternative framework deemed by relevant authorities as providing an adequate level of protection of Personal Data.

6. EU Data Subjects' Rights

In the “Bring your own Participants” scenario, the Client is responsible for:

- providing the appropriate information to EU Data Subjects on the Processing activities; and for
- responding to any EU Data Subjects’ Rights Requests (“Data Subject Request”) on the Personal Data Processed by Playbook UX.

In the event that Playbook UX receives any EU Data Subject complaint, inquiry, or request to exercise their rights regarding Personal Data (including right of access, right to rectification, restriction of Processing, erasure, data portability, object to the Processing, or its right not to be subject to an automated individual decision making), Playbook UX will redirect the Data Subject to make their request to the Client and will promptly notify the Client of the same in the “Bring your own Participants” scenario.

In addition,to the extent that the Client does not have the ability to address a EU Data Subject Request, Playbook UX shall, upon the Client's request, provide commercially reasonable efforts to assist the Client in fulfilling its obligation to respond to EU Data Subject Requests.

7. Privacy and security audits

During the execution of the services, Playbook UX shall be ready, upon request of the Client, to report and demonstrate the compliance of all the procedures and systems established to ensure the protection of the Personal Data. In particular, Playbook UX shall keep appropriate documentation on the Processing activities carried out on behalf of the Client.

Upon the Client's request with not less than thirty (30) days' notice, Playbook UX agrees (at the Client's expense) to permit the Client to perform reviews of Playbook UX's compliance with its obligations set forth under the DPA (the “Client Audits"). The Client Audits may be performed at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the Client may take into account relevant certifications held by Playbook UX.

The Client Audits may be conducted by the internal and external auditors and personnel of the Client who have entered into Playbook UX's form of nondisclosure agreement (collectively, "Auditors"). Such Client Audits shall be conducted in accordance with Playbook UX's security policies and procedures, without undue disruption to Playbook UX’s operations, in a commercially reasonable manner.

Playbook UX agrees to cooperate in a commercially reasonable manner with the Auditors and provide the Auditors commercially reasonable assistance as they may reasonably request in connection with the Client Audit. Except in the case of a the Client Audit performed in response to a Data Breach, the Client Audit(s) will be performed at the Client's sole cost and the Client will reimburse Playbook UX for its reasonable costs associated with such additional the Client Audits.

The Client shall promptly notify Playbook UX with information regarding the results of the Client Audits.

8. Data Protection Impact Assessments

Playbook UX shall, considering the nature of the Processing and the information available to Playbook UX, provide reasonable assistance to the Client, with any data protection impact assessments and prior consultations with Supervisory Authorities or other competent regulatory authorities as required for the Client to fulfill its obligations under the GDPR.

9. Data Breaches

Playbook UX shall cooperate with the Client and take reasonable commercial steps as are directed by the Client to assist in the investigation, mitigation and remediation of each such Data Breach.

Playbook UX shall notify the Client without undue delay after becoming aware of a Data Breach and provide reasonable information and cooperation to the Client so that the Client can fulfill any data breach reporting obligations it may have under the GDPR.

The notification shall at least contain a description of the nature of the Data Breach, including, if possible, the categories and approximate number of affected EU Data Subjects, a description of the likely consequences of the Breach, and a description of the measures to be taken, as well as measures employed to manage it.

If it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay

If notification is required to be made to the competent Supervisory Authority or to affected EU Data Subjects, notification will be made by the Client, and not by Playbook UX.

10. End-of-contract provisions

Processing by Playbook UX shall only take place for the Duration of the Contract. After the end of the provision of the Processing services, Playbook UX shall, in the “Bring your own Participants” scenario, delete or archive all Personal Data Processed on behalf of the Client within ten (10) business days and certify in writing to the Client that it has done so. Until the Personal Data is deleted, Playbook UX shall continue to ensure compliance with this DPA.

However, this requirement shall not apply to the extent Playbook UX is required by US regulations to retain all or some of the Personal Data, which data Playbook UX shall securely isolate and protect from further Processing, until such time as the relevant backup archive is destroyed.

11. Final provisions

This DPA sets out all of the terms that have been agreed between the Parties. To the extent that any provision of this DPA conflicts with any provision of the Contract, the terms of the DPA shall, as to the specific subject matter of the DPA, take precedence over the conflicting provision in the Contract.

This DPA shall remain in place until the expiry or termination of the Contract, unless:

- one of the conditions laid out in Clause 16 of the Standard Contractual Clauses is fulfilled;
- the Parties agree in writing that this DPA is to be terminated.

This Agreement is governed by the laws of New York. Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of New York.

If any part of this DPA is held unenforceable, the validity of all remaining parts will not be affected.

Appendix 1 – Standard contractual clauses

Clause 1: Purpose and scope

The purpose of this Appendix is to ensure compliance with the requirements of the GDPR for the transfer of Personal Data of EU Data Subjects from the European Union (where the Client is located) to the United States, where Playbook UX is based in the "Bring your own Participants" scenario.

For the purposes of this Appendix, the Client is the Data Exporter (the "Data Exporter"), and Playbook UX is the importing party ("the Data Importer"). These standard contractual clauses ("Clauses"), along with Appendix 2, form part of the Data Processing Agreement ("DPA").

Clause 2 – Effect and invariability of the Clauses

These Clauses set out appropriate safeguards, including enforceable Data Subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of the GDPR, with respect to data transfers from Controllers to Processors.

These Clauses are without prejudice to obligations to which the Data Exporter is subject by virtue of the GDPR.

Clause–3 - Third-party beneficiaries

(a) Data Subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the Data Exporter and/or Data Importer, with the following exceptions:

- Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
- Clause 8.1(b), 8.9(a), (c), (d) and (e);
- Clause 9;
- Clause 12(a), (d) and (f);

- Clause 13;
- Clause 15.1(c), (d) and (e);
- Clause 16(e);
- Clause 18 first paragraph.

(b) Paragraph (a) is without prejudice to rights of Data Subjects under GDPR.

Clause 4 - Interpretation

Where these Clauses use terms that are defined in the GDPR, those terms shall have the same meaning as in that Regulation. These Clauses shall be read and interpreted in the light of the provisions of the GDPR. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in the GDPR.

Clause 5 - Hierarchy

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

Clause 6 - Description of the transfer(s)

The details of the transfer(s), and in particular the categories of Personal Data that are transferred and the purpose(s) for which they are transferred, are specified in Section 2.2. of the DPA. The transfers are carried out on a continuous basis.

Clause 7 - Docking clause

An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a Data Exporter or as a Data Importer, by signing this DPA and the Clauses.

Once it has signed the DPA and the Clauses, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a Data Exporter or Data Importer.

The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

Clause 8 - Data protection safeguards

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

8.1 Instructions

(a) The Data Importer shall process the personal data only on documented instructions from the Data Exporter, that are laid out in section 2.2 of this DPA.

(b) The Data Importer shall immediately inform the Data Exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The Data Importer shall process the personal data only for the specific purpose(s) of the transfer, unless on further instructions from the Data Exporter.

8.3 Transparency

On request, the Data Exporter shall make a copy of these Clauses, including the DPA and the Appendix, available to the Data Subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and Personal Data, the Data Exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights.

On request, the Parties shall provide the Data Subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the Data Exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

As laid out in section 3.2. of the DPA, if the Data Importer becomes aware that the Personal Data it has received is inaccurate, or has become outdated, it shall inform the Data Exporter without undue delay. In this case, the Data Importer shall cooperate with the Data Exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the Data Importer shall only take place for the duration specified in section 2.2 of the DPA. After the end of the provision of the Services, the Parties will follow the procedure laid out in section 10 of the DPA.

This is without prejudice to Clause 14, in particular the requirement for the Data Importer under Clause 14(e) to notify the Data Exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) With respect to the security of the Processing, the Data Importer shall comply with the measures laid out in section 3.2 of the DPA.

(b) The Data Importer shall grant access to the personal data to members of its personnel in the conditions laid oud in section 3.1. of the DPA.

(c) In the event of a personal data breach concerning personal data processed by the Data Importer under these Clauses, the Parties will follow the procedure laid out in section 9 of the DPA.

(d) The Data Importer shall cooperate with and assist the Data Exporter to enable the Data Exporter to comply with its obligations under the GDPR, as laid out in section 9 of the DPA.

8.7 Sensitive data

As provided in section 3.2. of the DPA, the Data Importer shall apply specific restrictions and/or additional safeguards if sensitive data is processed.

8.8 Onward transfers

The Data Importer shall only disclose the Personal Data to a third party, whether this third party is located in the same country as Playbook UX or in another third country (hereinafter “onward transfer”) if the third party is or agrees to be bound by these Clauses or if:

- the onward transfer is to a country benefiting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the Processing in question;
- the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- the onward transfer is necessary in order to protect the vital interests of the Data Subject or of another natural person.

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

8.9 Documentation and compliance

(a) The Data Importer shall promptly and adequately deal with enquiries from the Data Exporter that relate to the processing under these Clauses.

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

(c) The Data Importer shall make available to the Data Exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses. If the Data Exporter requests it, the Data Importer shall allow for and contribute to audits as laid out in section 7 of the DPA.

(d) As laid out in section 7 of the DPA, the Data Exporter may choose to conduct the audit by itself or mandate an independent auditor.

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

Clause 9 - Use of sub-processors

(a) The Data Importer shall only engage sub-processors following the procedure laid out in Section 4 of the DPA.

(b) Where the Data Importer engages a sub-processor to carry out specific processing activities (on behalf of the Data Exporter), it shall do so by way of a written contract, as laid out in section 4 of the DPA. The Parties agree that, by complying with this Clause, the Data Importer fulfils its obligations under Clause 8.8. The Data Importer shall ensure that the sub-processor complies with the obligations to which the Data Importer is subject pursuant to these Clauses.

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

Clause 10 – Data Subjects' rights

The Data Importer shall comply with the instructions given by the Data Exporter, as laid out in Section 6 of the DPA.

Clause 11- Redress

The Data Importer shall inform Data Subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a Data Subject.

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

The Data Importer shall accept the decision of the Data Subject to:

- lodge a complaint with the Supervisory authority in the Member State of his/her habitual residence or place of work, or the competent Supervisory authority pursuant to Clause 13;
- refer the dispute to the competent courts within the meaning of Clause 18.

The Parties accept that the Data Subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of the GDPR.

The Data Importer shall abide by a decision that is binding under the applicable EU or Member State law.

The Data Importer agrees that the choice made by the Data Subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12- Liability

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

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

(c) Notwithstanding paragraph (b), the Data Exporter shall be liable to the Data Subject, and the Data Subject shall be entitled to receive compensation, for any material or non-material damages the Data Exporter or the Data Importer (or its sub-processor) causes the Data Subject by breaching the third-party beneficiary

rights under these Clauses. This is without prejudice to the liability of the Data Exporter and, where the Data Exporter is a processor acting on behalf of a controller, to the liability of the controller under the GDPR.

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

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

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

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

Clause 13 – Supervision

The Supervisory authority of New Hampshire shall act as competent Supervisory authority.

The Data Importer agrees to submit itself to the jurisdiction of and cooperate with the competent Supervisory authority in any procedures aimed at ensuring compliance with these Clauses.

In particular, the Data Importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the Supervisory authority, including remedial and

compensatory measures. It shall provide the Supervisory authority with written confirmation that the necessary actions have been taken.

Clause 14 - Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices of the United States applicable to the Processing of Personal Data by the Data Importer, including any requirements to disclose Personal Data or measures authorizing access by public authorities, prevent the Data Importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of the GDPR, are not in contradiction with these Clauses.

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

- the specific circumstances of the transfer, including the length of the Processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of Processing; the categories and format of the transferred Personal Data; the economic sector in which the transfer occurs; the storage location of the data transferred;

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

- the measures applied during transmission and to the Processing of the Personal Data in the United States;

- the technical safeguards put in place to supplement the safeguards as laid out under section 3 of this DPA; and

- the relevant contractual or organisational measures laid out in Annex I of the Clauses.

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

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

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

(f) Following a notification pursuant to paragraph (e), or if the Data Exporter otherwise has reason to believe that the Data Importer can no longer fulfil its obligations under these Clauses, the Data Exporter shall promptly identify appropriate measures (e.g., technical or organisational measures to ensure security and confidentiality) to be adopted by the Data Exporter and/or Data Importer to address the situation. The Data Exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent Supervisory authority to do so. In this case, the Data Exporter shall be entitled to terminate the contract, insofar as it concerns the Processing of Personal Data under these Clauses. If the contract involves more than two Parties, the Data Exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15 - Obligations of the Data Importer in case of access by public authorities

15.1. Notification

(a) Before any access is granted to the Personal Data, the Data Importer agrees to notify the Data Exporter and, where possible, the Data Subject promptly (if necessary, with the help of the Data Exporter) if it:

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

- becomes aware of any direct access by public authorities to Personal Data transferred pursuant to these Clauses in accordance with the laws of the US; such notification shall include all information available to the importer.

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

(c) Where permissible under the US laws, the Data Importer agrees to provide the Data Exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

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

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

15.2. Review of legality and data minimization

(a) The Data Importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the US laws, applicable obligations under international law and principles of international comity. The Data Importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the Data Importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the Personal Data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the Data Importer under Clause 14(e).

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

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

Clause 16 - Non-compliance with the Clauses and termination

(a) The Data Importer shall promptly inform the Data Exporter if it is unable to comply with these Clauses, for whatever reason.

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

(c) The Data Exporter shall be entitled to terminate the contract, insofar as it concerns the Processing of Personal Data under these Clauses, where:

- the Data Exporter has suspended the transfer of Personal Data to the Data Importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

- the Data Importer is in substantial or persistent breach of these Clauses; or

- the Data Importer fails to comply with a binding decision of a competent court or Supervisory authority regarding its obligations under these Clauses.

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

Parties will follow the procedure laid out in section 10 of the DPA with respect of the deletion and/or return of the Personal Data.

(d) Either Party may revoke its agreement to be bound by these Clauses where:

- the European Commission adopts a decision pursuant to Article 45(3) of the GDPR that covers the transfer of Personal Data to which these Clauses apply; or

- the GDPR becomes part of the legal framework of the country to which the Personal Data is transferred. This is without prejudice to other obligations applying to the Processing in question under the GDPR.

Clause 17 - Governing law

These Clauses shall be governed by the law of the country set forth in DPA, or if such law does not allow for third-party beneficiary rights, then the law of New Hampshire.

Clause 18 - Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State. The Parties agree that those shall be the courts of Austria.

(b) A Data Subject may also bring legal proceedings against the Data Exporter and/or Data Importer before the courts of the Member State in which he/she has his/her habitual residence. The Parties agree to submit themselves to the jurisdiction of such courts.

Appendix 2 - Supplementary Contractual and Organisational Measures

This Appendix forms part of the Clauses. In addition to the measures laid out in the Clauses and in the DPA, including the technical measures listed in section 4 of the DPA, the Parties have agreed to put in place the following contractual measures.

- Contractual measures:

The Data Importer agrees to monitor any legal or policy developments that might lead to its inability to comply with its obligations, and promptly inform the Data Exporter of any such changes and developments, and if possible, ahead of their implementation to enable the Data Exporter to recover the data from the Data Importer.

In case the Data Importer receives a request from public authorities to cooperated on a voluntary basis, the Data Importer will first seek the express or implied consent of the exporter and/or the Data Subject.

To the extent permissible under the US law, the Data Importer will notify promptly the Data Subject of the request or order received from the US public authorities, or of the importer's inability to comply with the contractual commitments, to enable the Data Subject to seek information and an effective redress

- Organizational measures:

The Data Importer has adopted internal policies with clear allocation of responsibilities for data transfers, reporting channels and standard operating procedures for cases of covert or official requests from public authorities to access the data.

It has also developed specific training procedures for personnel in charge of managing requests for access to Personal Data from public authorities

Finally, the Data Importer agrees to document and record the requests for access received from public authorities and the response provided, alongside the legal reasoning and the actors involved (e.g., if the exporter has been notified and its reply, the assessment of the team in charge of dealing with such requests, etc.). These records are made available to the Data Exporter.

The Parties hereby agree to be bound by the terms of this Agreement as set forth above and as of the completion of signing this Agreement.

Name:

Signature:

Title:

Date

Email:

Playbook UX, LLC

Signature:

Title: CEO

Email: hello@playbookux.com