DATA PROCESSING AGREEMENT

In connection with the services provided by NeuIntel, LLC ("PRICESPIDER") under the Master Services Agreement (or equivalent agreement) (the "AGREEMENT") between PRICESPIDER and ▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮ ("CLIENT") intends to transfer certain Personal Data to PRICESPIDER, so that PRICESPIDER is able to perform the services under the Agreement. This Data Processing Agreement ("DPA") shall govern the Parties' rights and obligations with respect to the processing of such Personal Data.

For purposes of this DPA, CLIENT may act as a Controller, or it may act as a Processor of one of its customers. PRICESPIDER therefore acknowledges that it may act as a Processor of CLIENT or a Sub-processor of CLIENT. Where CLIENT acts as a Processor, CLIENT is obligated contractually and / or under Applicable Data Protection Laws to flow down certain data protection related obligations to its appointed Sub-processors. Therefore all obligations placed on Processors in this DPA shall apply to PRICESPIDER regardless of whether PRICESPIDER acts as a Processor or Sub-processor.

Where PRICESPIDER is acting as CLIENT's Processor, Module Two of the Standard Contractual Clauses shall apply. Where CLIENTS Sub-processor, Module Three of the Standard Contractual Clauses shall apply.

1. **DEFINITIONS**:

    (a)   "APPLICABLE DATA PROTECTION LAW" shall mean Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, or "GDPR"); as well as any other data protection law that governs the processing of Personal Data (or its equivalent as defined therein)

    (b)   "CONTROLLER", "DATA SUBJECT", "PERSONAL DATA", "PROCESSING", "PROCESS", "PROCESSOR", and "SUB-PROCESSOR" shall have the meanings given in Applicable Data Protection Law; and

    (c)   "STANDARD CONTRACTUAL CLAUSES" means the agreement executed by and between Processor and sub-processor and attached hereto as Schedule 1 regarding the transfer of Personal Data to sub-processors established in countries which do not ensure an adequate level of data protection.

    (d)   "TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES" means measures to ensure a level of security that is appropriate to the level of risk, with respect to the confidentiality, integrity, availability and resilience of the systems and services by protecting the Personal Data: (i) against accidental or unlawful destruction, or accidental loss, alteration, unauthorized disclosure or access, in particular where processing involves the transmission of the Personal Data over a network; and (ii) against all other unlawful forms of processing of the Personal Data. The summary of the Technical and Organizational Security Measures to be undertaken by sub-processor, as part of its provision of services, are described in Schedule 1, Annex II.

2. **RELATIONSHIP OF THE PARTIES**: CLIENT appoints PRICESPIDER to process the Personal Data that is the subject of the Agreement by and between the parties (the "DATA"). Each Party shall comply with the obligations that apply to it under Applicable Data Protection Laws.

3. **PROHIBITED DATA**: CLIENT shall not disclose (and shall not request any Data Subject to disclose) any special categories of Data to PRICESPIDER for processing that is not expressly disclosed in Schedule 1, Annex I.

4. **PURPOSE LIMITATION**: PRICESPIDER shall process the Data for the purposes described in Annex I and strictly in accordance with the instructions of CLIENT (the "PERMITTED PURPOSE"), except where otherwise required by any EU (or any EU Member State) law applicable to CLIENT. In no event shall PRICESPIDER process the Data for its own purposes or those of any third party. PRICESPIDER shall immediately inform CLIENT if it becomes aware that CLIENT's processing instructions infringe Applicable Data Protection Law (but without obligation to actively monitor CLIENT's compliance with Applicable Data Protection Law).

5. **INTERNATIONAL TRANSFERS**: If Personal Data is stored at third-party hosting facilities within the European Economic Area ("EEA"). PRICESPIDER shall not transfer the Data (nor permit the Data to be transferred) outside of the EEA unless (i) it has first obtained CLIENT's prior written consent; and (ii) it takes such measures as are necessary to ensure the transfer is in compliance with Applicable Data Protection Law. Such measures may include (without limitation) transferring the Data to a recipient in a country that the European Commission has decided provides adequate protection for Personal Data, to a recipient that has achieved binding corporate rules authorization in accordance with Applicable Data Protection Law, or to a recipient that has executed Standard Contractual Clauses adopted or approved by the European Commission, as shown in Schedule 1.

6. **CONFIDENTIALITY OF PROCESSING**: PRICESPIDER shall ensure that any person that it authorizes to process the Data (including PRICESPIDER staff, agents and subcontractors) (an "AUTHORIZED PERSON") shall be subject to a strict duty of confidentiality (whether a contractual duty or a statutory duty), and shall not permit any person to process the Data who is not under such a duty of confidentiality. PRICESPIDER shall ensure that all Authorized Persons process the Data only as necessary for the Permitted Purpose.

7. **TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES**: PRICESPIDER shall implement appropriate technical and organizational measures to protect the Data (a) from accidental or unlawful destruction, and (b) loss, alteration, unauthorized disclosure of, or access to the Data (a "SECURITY INCIDENT"). Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of processing. Such measures shall include those measure set forth in Schedule 1, Annex II.

8. **SUBPROCESSING**: PRICESPIDER shall not subcontract any processing of the Data to a third party sub-processor without the prior written consent of CLIENT. Notwithstanding this, CLIENT consents to PRICESPIDER engaging third party sub-processors to process the Data provided that: (a) Processor provides at least 90 days' prior notice of the addition of any sub-processor (including details of the processing it performs or will perform), and obtains CLIENT's prior written consent; (b) PRICESPIDER imposes data protection terms on any sub-processor it appoints that protect the Data to the same standard provided for by this DPA; and (c) PRICESPIDER remains fully liable for any breach of this DPA that is caused by an act, error or omission of its sub-processor. A list of approved sub-processors as at the date of this DPA is attached hereto as Schedule 1, Annex III. If CLIENT refuses to consent to PRICESPIDER's appointment of a third party sub-processor on reasonable grounds relating to the protection of the Data, then PRICESPIDER will not appoint the sub-processor.

9. **COOPERATION AND DATA SUBJECTS' RIGHTS**: PRICESPIDER shall provide all reasonable and timely assistance (including by appropriate technical and organizational measures) to CLIENT to enable CLIENT to respond to: (a) any request from a data subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable); and (b) any other correspondence, enquiry or complaint received from a data subject, regulator or other third party in connection with the processing of the Data. In the event that any such request, correspondence, enquiry or complaint is made directly to PRICESPIDER, PRICESPIDER shall promptly inform CLIENT providing full details of the same.

10. **DATA PROTECTION IMPACT ASSESSMENT**: If PRICESPIDER believes or becomes aware that its processing of the Data is likely to result in a high risk to the data protection rights and freedoms of data subjects, it shall promptly inform CLIENT and provide CLIENT with all such reasonable and timely assistance as CLIENT may require in order to conduct a data protection impact assessment and, if necessary, consult with its relevant data protection authority.

11. **SECURITY INCIDENTS**: Upon becoming aware of a Security Incident, PRICESPIDER shall inform CLIENT without undue delay and shall provide all such timely information and cooperation as CLIENT may require in order for CLIENT to fulfil its data breach reporting obligations under (and in accordance with the timescales required by) Applicable Data Protection Law. PRICESPIDER shall further take all such measures and actions as are necessary to remedy or mitigate the effects of the Security Incident and shall keep CLIENT of all developments in connection with the Security Incident.

12. **DELETION OR RETURN OF DATA:** Upon termination or expiration of the Agreement, PRICESPIDER shall (at CLIENT's election) destroy or return to CLIENT all Data (including all copies of the Data) in its possession or control (including any Data subcontracted to a third party for processing). This requirement shall not apply to the extent that PRICESPIDER is required by any EU (or any EU Member State) law to retain some or all of the Data, in which event PRICESPIDER shall isolate and protect the Data from any further processing except to the extent required by such law.

13. **AUDIT**: PRICESPIDER shall make available to CLIENT all information necessary to demonstrate compliance with the obligations laid down in this DPA.

CLIENT	NeuIntel, LLC
Authorized Signature:	Authorized Signature:
Name:	Name: Lucas Baerg
Title:	Title: CFO
Date:	Date: 1/3/2023
Email:	Email: lucas.baerg@pricespider.com

SCHEDULE 1: STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1: Purpose and Scope

(a)   The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b)   The Parties:

(i)   the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I (A) (hereinafter each "data exporter"), and

(ii)   the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I (A) (hereinafter each "data importer")

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

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

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

Clause 2: Effect and Invariability of Clauses

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

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

Clause 3: Third-party beneficiaries

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

(i)   Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
(ii)   Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
(iii)   Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
(iv)   Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
(v)   Clause 13;
(vi)   Clause 15.1(c), (d) and (e);
(vii)   Clause 16(e);
(viii)   Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

---

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

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

Clause 4: Interpretation

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

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

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

Clause 5: Hierarchy

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

Clause 6: Description of the transfers

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

Clause 7: **Docking Clause**

(a)   An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b)   Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

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

SECTION II - OBLIGATIONS OF THE PARTIES

Clause 8: Data protection safeguards

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

MODULE TWO: Transfer controller to processor

8.1   Instructions

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

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

8.2   Purpose limitation

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

8.3   **Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex 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 content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4   **Accuracy**

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

8.5   **Duration of processing and erasure or return of data**

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

8.6   **Security of processing**

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

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

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

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

8.7   **Sensitive data**

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

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

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

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

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

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

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

8.9 Documentation and compliance

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

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

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

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

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

MODULE THREE: Transfer processor to processor

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b)　　　　The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c)　　　　The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d)　　　　The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter[2].

8.2　　　　Purpose limitation

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

8.3　　　　Transparency

　　　　On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4　　　　Accuracy

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

8.5　　　　Duration of processing and erasure or return of data

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

8.6　　　　Security of processing

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

---

[2] See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

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

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

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

8.7   Sensitive data

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

8.8   Onward transfers

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

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

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

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

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

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

8.9   Documentation and compliance

(a)   The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller 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 controller.

(c)   The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d)   The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e)   Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

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

(g)   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

MODULE TWO: Transfer controller to processor

(a)   GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorization for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b)   Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfills its obligations under Clause 8.8[3]. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

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

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

MODULE THREE: Transfer processor to processor

(a)   GENERAL WRITTEN AUTHORISATION The data importer has the controller's general authorization for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

---

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(b)   the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[5] The Parties agree that, by complying with this Clause, the data importer fulfills its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

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

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

Clause 10: Data subject rights

MODULE TWO: Transfer controller to processor

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

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

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

MODULE THREE: Transfer processor to processor

(a)   The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorized to do so by the controller.

(b)   The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organizational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

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

Clause 11: Redress

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

MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

(a)   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.

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

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

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

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

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

(e)   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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

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

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

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

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

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

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

Clause 13: Supervision

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a)   The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as a competent supervisory authority.

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

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

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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a)   The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures 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 Regulation (EU) 2016/679, are not in contradiction with these Clauses.

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

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

    (ii)   the laws and practices of the third country of destination- including those requiring the disclosure of data to public authorities or authorising access by such authorities - relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[4]

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

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

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

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

(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 fulfill its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organizational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three:, if appropriate in consultation with the controller]. 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 [for Module Three: the controller or] 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

MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

15.1   Notification

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

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

    (ii)   becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance

---

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

with the laws of the country of destination; such notification shall include all information available to the importer. [For Module Three: The data exporter shall forward the notification to the controller.]

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

(c)   Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter shall forward the information to the controller.]

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

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

15.2   Review of legality and data minimisation

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

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

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

SECTION IV - FINAL PROVISIONS
Clause 16: Non-compliance with the Clauses and termination

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

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

(c)   The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
   (i)   the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
   (ii)   the data importer is in substantial or persistent breach of these Clauses; or
   (iii)   the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

   In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] 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.

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

(e)   Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation

(EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17: Governing law

MODULE TWO: Transfer controller to processor

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights.

MODULE THREE: Transfer processor to processor

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights.

Clause 18: **Choice of forum and jurisdiction**

MODULE TWO: Transfer controller to processor

(a)	Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
(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.
(c)	The Parties agree to submit themselves to the jurisdiction of such courts.

MODULE THREE: Transfer processor to processor

|	
(a)	Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
(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.
(c)	The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX
ANNEX I

A.   LIST OF PARTIES

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Data exporter(s): *[Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name ▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒

Address: ▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒

Contact person's name, position and contact details: ▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒

Activities relevant to the data transferred under these Clauses: *Obtaining the Services from Data Importer*

Signature and date: X▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒

Role (controller/processor): *Controller/Processor*

Data importer(s): *[Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: NeuIntel, LLC

Address: 20 Pacifica, Suite 1000, Irvine, California, 92618

Contact person's name, position and contact details: Lucas Baerg, CFO (lucas.baerg@pricespider.com)

Activities relevant to the data transferred under these Clauses: *Provision of Services to the Data Exporter*

Signature and date: X▒▒▒▒▒▒▒▒▒▒▒   1/3/2023

Role (controller/processor): *Processor/sub-processor*

B.   DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred

- CLIENT employees and contractors
- Customers of CLIENT
- Customers of the customers of CLIENT.
- Any other individuals whose Personal Data is uploaded or transmitted via the services provided under the Agreement.

Categories of personal data transferred

- Identification data (including, for example, name, email address, IP address, localization data);
- Electronic identification data (including, for example, login details; connection data);
- Any other Personal Data uploaded or transmitted via the services provided under the Agreement.

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

- None anticipated

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

- Continuously, for the length of the Agreement between the parties.

Nature of the processing

- Personal Data will be processed for purposes of fulfilling PRICESPIDER'S obligations to CLIENT under the Agreement and the DPA.

Purpose(s) of the data transfer and further processing

- For PRICESPIDER to provide the Services to CLIENT pursuant to the Agreement.

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

- Personal Data shall be retained for the length of time necessary to provide the Services under the Agreement, or as otherwise required by applicable law.

MODULE THREE: Transfer processor to processor

Categories of data subjects whose personal data is transferred
- CLIENT employees and contractors
- Customers of CLIENT
- Customers of the customers of CLIENT.
- Any other individuals whose Personal Data is uploaded or transmitted via the services provided under the Agreement.

Categories of personal data transferred
- Identification data (including, for example, name, email address, IP address, localization data);
- Electronic identification data (including, for example, login details; connection data);
- Any other Personal Data uploaded or transmitted via the services provided under the Agreement.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.
- None anticipated

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).
- Continuously, for the length of the Agreement between the parties.

Nature of the processing
- Personal Data will be processed for purposes of fulfilling PRICESPIDER'S obligations to CLIENT under the Agreement and the DPA.

Purpose(s) of the data transfer and further processing
- For PRICESPIDER to provide the Services to CLIENT pursuant to the Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period
- Personal Data shall be retained for the length of time necessary to provide the Services under the Agreement, or as otherwise required by applicable law.

C.   COMPETENT SUPERVISORY AUTHORITY

- Identify the competent supervisory authority/ies in accordance with Clause 13: Commerce Connector, GmbH.

ANNEX II - TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

Cloud Provider for Platform

The software that comprises the Platform is located on Amazon Web Services (AWS) services located in the United States of America, and in Germany. The AWS data centers are managed and operated by Amazon Web Services EMEA SARL for data centers EMEA (Europe, Middle East, Africa). These data centers comply with key industry standards, such as ISO,IEC 27001:2013, for security and reliability. The data centers are managed, monitored, and administered by AWS operations staff that have years of experience in delivering online services with 24x7 continuity.   Detailed information about AWS security, can be found on the AWS Cloud Security site at https://aws.amazon.com/security/.

1. **Admission Controls.** Measures to bar unauthorized persons from access to Data Processing facilities and systems where Data is Processed or used:

> Automatic access control system
> Chip cards / Transponder systems
> Protection of building
> Reception/Doorman
> Security Cameras/Video Surveillance
> Visitors Book/Visitors Log
> Visitors accompanied by employees
> Diligence in section of security personnel

2. **Access Control to Systems.** Measures to prevent unauthorized persons from being able to use the Data Processing systems:

Login with username + password

> Anti-virus software clients
> Firewalls
> Intrusion detection systems
> Mobile device management
> Use VPN for remote access
> Encryption of Laptops/Tablets
> Manage User Permissions
> Creating User Profiles
> Secure Password Policy
> "Delete/Destroy" Policy
> Data Security Policy

3. **Access Control to Data.** Measures to guarantee that the persons authorized to use the data processing systems can only access the data for which they have access authorization, and that following the processing, use and storage, the data cannot be read, copied, changed or removed without authorization:

> Use of authorization concepts ("need to know basis")
> Minimum number of administrators
> Administration of user rights through administrators
> Logging of accesses to applications, specifically during input, amendment and deletion of data.

4. **Data Transmission Control.** Measures to guarantee that the data cannot be read, copied, changed or removed without authorization in their electronic transmission, during their transport or during their storage on data carriers, and that it can be checked and determined where the data should be communicated by means of data transmission devices:

> Email Encryption

Use of VPN

Logging of accesses and retrievals

Provision via encrypted connections like sftp, https

Passing data in anonymized or pseudonymized form

5.   **Input Control.**   Measures to guarantee that it can be checked and determined after the fact whether and by whom data have been entered into data processing systems, changed, modified or removed from the data processing systems:

Technical logging of the input, amendment and deletion of data

Manual or automated control of the protocols

Overview with which programs in which data was entered, changed or can deleted

6.   **Availability Control.**   Measures to guarantee that the data is protected against accidental destruction or loss including measures to ensure the ability to restore availability and access to the data in a timely manner in the event of a physical or technical incident:

Fire and smoke detection systems

Fire extinguisher Server room

Server room monitoring temperature and humidity

Server Room Air Conditioned

Backup & Recovery Concept (formulated)

Control of the backup process

Regular tests for data recovery and logging of results

Storage of the backup media on a safe place outside the server room

Separate partitions for operational systems and data

7.   **Separation Control.**   Measures to guarantee that data gathered for different purposes can be processed separately from each other:

Separation of production and test environments

Physical separation (systems/databases/data carriers)

RBACL (Role Based Access Control List)

Control Via Authorization Concept

Definition of Database Rights.

8.   **Job Control.**   Measures to ensure that data processed on behalf of Controller is only processed in compliance with Controller's instructions:

Communication of contract terms to authorized persons, and ongoing communication of any new Controller instructions to authorized persons.

9.   **Data Protection Officer / Representative.**   Processor's officer or representative who is responsible for the data protection under this Exhibit:

Lucas Baerg, CFO (lucas.baerg@pricespider.com).

Dennis Voigt, Melchers Rechtsanwaelte (d.voigt@melchers-law.com)

10.   **Encryption and/or Pseudonymisation.**   Measures to ensure that data is encrypted and/or processed in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the data is not attributed to an identified or identifiable natural person:

In the case of pseudonymization, separation of allocation data and breakdown storage in separate secured system (encrypted).

Internal instruction to anonymize/pseudonymize Personal Data if possible in the event of disclosure or even after expiry of the statutory deletion period.

11.   **Data Protection Management.** Measures to ensure a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of processing:

> Central documentation of all procedures and regulations on data protection with access possibility for employees according to need.
>
> A Data Protection Impact Assessment will be carried out if necessary
>
> Compliance with the information obligations according to Art 13 and 14 of the GDPR.
>
> Formalized process for the processing of requests for information from data subjects are available.

ANNEX III - LIST OF SUB-PROCESSORS

https://www.pricespider.com/wp-content/uploads/2022/12/DPA-subprocessors-customers.pdf