Data Processing Addendum

This Data Processing Addendum supplements and is incorporated into the Agreement between Featurely and Customer. The DPA is binding on both parties without further action or signature. By executing or otherwise entering into the Agreement, Customer agrees to the terms of this DPA.

Capitalized terms used and not defined in this DPA shall have the respective meanings set forth in the Agreement and/or applicable Data Protection Law.

1. Scope

1.1 This DPA serves as a written data processing agreement between Featurely and Customer (on its behalf and on behalf of each Controller referenced in this DPA) and shall apply to any Processing of Personal Data by Featurely or any of its Sub-processors in connection with services provided under the terms of the Agreement. This DPA shall be effective for the period Featurely provides services to Customer under the Agreement to which this DPA applies and for any period after which Featurely retains Personal Data.

1.2 The Parties agree that this DPA shall replace any existing data processing agreement or similar document that the parties may have previously entered into in connection with the Featurely Services. In the event of any conflict between the terms of the Agreement, including any previously or concurrently executed addendums, and the terms of this DPA, the relevant terms of this DPA shall take precedence. If any provision of this DPA is found by any court of competent jurisdiction to be invalid or unenforceable, the invalidity of such provision shall not affect the other provisions hereof, and all provisions not affected by such invalidity shall remain in full force and effect. The provisions of this DPA shall not affect the fundamental rights and freedoms of data subjects or the powers of supervisory authorities under data protection law.

2. Definitions

2.1 "**Customer Data**" means all data provided or otherwise made available by Customer to Featurely in the course of Featurely providing services pursuant to the Agreement.

2.2 "**Data Protection Law**" means laws and regulations applicable to the Processing of Personal Data under the Agreement, including (i) the General Data Protection Regulation, Regulation (EU) 2016/679 ("GDPR") and the UK GDPR, (ii) the Swiss Federal Act on Data Protection; and (iii) the UK Data Protection Act 2018; in each case, as updated, amended or replaced from time to time. The terms "Controller," Data Subject," "Processing," "Processor," and "supervisory authority" shall have the definitions set forth in the GDPR.

2.3 "**EEA**" means, for purposes of this DPA, the European Economic Area, Switzerland, and the United Kingdom.

2.4 "**Personal Data**" shall have the meaning set forth in the GDPR, to the extent such data is Customer Data.

2.5 "**Personal Data Breach**" means breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed by Featurely.

2.6 **"Instructions"** means documented instructions issued by Customer to Featurely, including via secure electronic means,

2.7 "**Standard Contractual Clauses**" means:

1. for UK Personal Data, the International Data Transfer Addendum to the EU SCCs, issued by the Information Commissioner in accordance with s. 119A of the UK Data Protection Act 2018, but, as permitted by clause 17 of such addendum, the Parties agree to change the format of the information set out in the addendum so that (i) the details of the parties in table 1 shall be set out in Annex 1 of the EU SCCs (with no requirement for further signature); (ii) for the purposes of table 2, the addendum shall be appended to the EU SCCs (including the modules and operational clauses noted below) and clause 10.5(b) selects the option and timescales for clause 9; and (iii) the appendix information listed in table 3 shall be set out in the Annexes to the EU SCCs ("UK SCCs"); and
2. for EU Personal Data, the standard contractual clauses adopted by the European Commission under Commission Implementing Decision (EU) 2021/914 including text from Module 2 (Controller to Processor) of such clauses, as modified in Section 10 ("EU SCCs"); and
3. for Swiss Personal Data, the EU SCCs.

2.8 "**Sub-processor**" means any Processor engaged by Featurely, including affiliates of Featurely acting as Processors.

3. Roles of the Parties

3.1 It is acknowledged and agreed that regarding the processing of Personal Data under this DPA, Customer is the Controller and Featurely is the Processor (whether acting itself or through Sub-processors pursuant to Section 8 (Sub-processors) below).

3.2 Both Parties shall, in their respective roles, comply with all Data Protection Laws regarding Personal Data Processed under this DPA.

3.3 The nature and purpose of the Processing, the types of Personal Data and categories of Data Subject Processed under this DPA are specified in **Schedule 1 – Part 1** hereto, as may be updated by the Parties as applicable from time to time.

3.4 Customer shall, in its use and receipt of the services provided or made available by Featurely pursuant to the Agreement ("Featurely Services"), Process Personal Data in accordance with the requirements of Data Protection Laws.

4. Customer Obligations

4.1 Customer acts as, and as between Customer and Featurely, will at all times remain, the Controller:

1. Concerning any Personal Data Processed by Featurely or its Sub-processors under this DPA; and
2. As applicable, on behalf of and in the name of its affiliates, end users, contractors and/or partners in their capacity as Controllers and whose Personal Data at any time is Processed by Featurely or its Sub-processors under this DPA.

4.2 Customer shall, in its use of the Featurely Services, process Personal Data in accordance with Data Protection Law, including any applicable requirements to provide notice to Data Subjects of the use of Featurely as a Processor.

4.3 Except as may be otherwise required under the applicable Data Protection Law, Customer shall serve as a single point of contact for Featurely in all matters under this DPA and shall be responsible for the internal coordination, review and submission of instructions or requests to Featurely as well as the onward distribution of any information, notifications and reports provided by Featurely hereunder.

4.4 In its capacity as Controller, Customer represents and warrants that it is entitled to provide access to Personal Data to Featurely for purposes hereof and, consequently, that it has a lawful basis and any necessary approvals from any relevant Data Subjects for Featurely's performance of the Featurely Services.

4.5 Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

5. Featurely Obligations and Limitations

5.1 Purposes for Processing: Subject to as legally permitted in its capacity as a Processor under this DPA, Featurely shall Process Personal Data hereunder solely in accordance with the documented instructions unless required to do so by Union or Member State law to which Featurely is subject for the Customer and for the following limited purposes:

1. performance of the Featurely Services under the terms of the Agreement;
2. Processing initiated by authorized users of Customer in their use of the Featurely Services;
3. Executing documented instructions of Customer provided such instructions relate to and are consistent with the services provided by Featurely;
4. Addressing service issues or technical problems, and/or

Meeting any express requirement under applicable law, in which case Featurely shall, unless it is prohibited by applicable law from doing so, inform Customer of the legal requirement before Processing.**5.2 Unauthorized Processing:** Featurely will promptly inform Customer if, in its determination, any instruction or request by Customer violates Data Protection Law. Featurely is entitled to suspend the execution of the relevant instruction until it is confirmed or amended by the controller.

5.3 Legal Requests: Featurely will report to Customer without undue delay any request, demand, or order received by Featurely from a competent supervisory authority or Data Subject relating to the Processing of Personal Data.

5.4 Assistance and Cooperation: Taking into account the nature of the Processing, Featurely will assist Customer in complying with its obligation to respond to requests of Data Subjects under Data Protection Law by appropriate technical and organizational measures, insofar as this is possible, provided that Featurely will provide such assistance to the extent:

1. The information is available to Featurely and such information is not otherwise available to Customer or the requested assistance cannot practicably be performed by Customer; and
2. Customer acknowledges that Featurely has no responsibility to interact directly with any Data Subject or supervisory authority in respect of any request, demand, or order (except as expressly provided under the applicable Data Protection Law or as otherwise agreed by the Parties in writing).

5.5 Retention and Destruction of Personal Data. Subject to applicable legal retention obligations, upon termination of the Agreement, Featurely will return to Customer or delete any Personal Data in its control, in accordance with the procedures and timeframes applied by Featurely from time to time, and, if requested, confirm such deletion to Customer in writing.

5.6 Confidentiality. Featurely will only rely on personnel in the Processing of Personal Data who are contractually or by statutory obligation bound to maintain confidentiality, ensure that access to Personal Data Processed is limited to those personnel who require such access to perform the applicable Featurely Services, and take commercially reasonable steps to ensure the reliability of personnel engaged in the Processing of Personal Data hereunder.

5.7 Non-Delegation. Featurely will not delegate the processing of Personal Data to a Sub-processor other than pursuant to section 8 (Sub-processors) below.

6. Security

6.1 Security Obligations. In connection with its Processing of Personal Data hereunder Featurely will provide for and maintain appropriate administrative, physical, technical and organizational security measures for such Processing, which measures are intended to protect Personal Data against accidental, illegal, or unauthorized loss, use, destruction, alteration, modification, disclosure or access, and to ensure a level of security appropriate to the particular risks involved in the Processing. In this connection:

1. It is acknowledged that further details on the administrative, physical and technical measures maintained by Featurely may be provided by Featurely to Customer upon reasonable request;
2. Featurely may update its security measures from time to time, provided such updates do not materially diminish the security of Featurely's Processing as compared to that provided immediately before the update; and
3. Customer is responsible for independently determining whether the security measures implemented by Featurely for processing by Featurely are sufficient to meet Customer's obligations under Data Protection Law. If Customer has reason to believe that Featurely's security practices are materially deficient, Customer must notify Featurely promptly upon such determination.

Details of Featurely’s technical and organizational measures (TOM) are set out in Schedule 1 – Part 2.

6.2 Security Incidents. Featurely will without undue delay after becoming aware of a Personal Data Breach affecting Personal Data notify Customer of such Personal Data Breach and take commercially reasonable steps to identify, mitigate and remediate the causes of such Personal Data Breach. At Customer's request, Featurely will cooperate with Customer in investigating and remedying any such Personal Data Breach.

7. Data Protection Impact Assessment

7.1 Taking into account the nature of the Processing and information available to Featurely, Featurely shall provide reasonable assistance to Customer with data protection impact assessments, and prior consultations with supervising authorities or other competent data privacy authorities as required under applicable Data Protection Law, including support for Customer's obligations under Articles 33 and 34 GDPR regarding Personal Data Breaches.

8. Sub-processors

8.1 General authorization. Featurely shall obtain the Customers general authorization to engage subcontractors listed in an agreed list(**Schedule 1 – Part 3)**.

8.2 Sub-processor Obligations. Featurely shall: (i) enter into a written agreement with each Sub-processor imposing data protection terms that require the Sub-processor to protect the Personal Data to the standard required by Data Protection Laws; and (ii) remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause Featurely to breach any of its obligations under this DPA**.** Featurely shall ensure an equivalent level of data protection for any data transfers to Sub-processors.

8.3 Notification of Changes. Featurely will notify the controller in writing at least four weeks in advance of any intended changes to this list by adding or replacing Sub-processors, thereby allowing the customer sufficient time to raise objections to these changes before the subcontractor in question is commissioned. The processor shall provide the controller with the necessary information to enable the controller to exercise its right to object.

9. Audits

9.1 Audit Rights. Featurely shall allow Customer or Customer's appointed third-party auditor to conduct audits, including inspections, to verify Featurely's compliance with its obligations under this DPA, subject to the following:

1. Customer may conduct such audits no more than once per year unless required by a supervisory authority;
2. Customer must provide Featurely with at least thirty (30) days' prior written notice of any intended audit;
3. Customer must ensure that all auditors are bound by confidentiality obligations; and
4. Audits must be conducted during regular business hours and in a manner that does not unreasonably interfere with Featurely's operations.

9.2 Audit Reports. Upon request and subject to confidentiality obligations, Featurely shall make available to Customer information reasonably necessary to demonstrate compliance with this DPA.

10. International Transfers

10.1 Standard Contractual Clauses. To the extent that Featurely Processes Personal Data that is protected by Data Protection Laws and originates from the EEA, and such Processing involves a restricted transfer of such Personal Data to a third country without an adequacy decision pursuant to Article 45 GDPR the Standard Contractual Clauses shall apply to such transfers (Annex II).

10.2 Alternative Transfer Mechanisms. To the extent Featurely adopts an alternative data export mechanism (including any new version of or successor to the Standard Contractual Clauses) for the transfer of Personal Data not described in this DPA ("Alternative Transfer Mechanism"), the Alternative Transfer Mechanism shall apply instead of any applicable transfer mechanism described in this DPA (but only to the extent such Alternative Transfer

Mechanism complies with Data Protection Laws and extends to the territories to which Personal Data is transferred).

11. Return or Deletion of Data

11.1 Upon termination or expiration of the Agreement, Featurely shall (at Customer's election) delete or return to Customer all Personal Data in its possession or control and provide written certification upon request. This requirement shall not apply to the extent Featurely is required by applicable law to retain some or all of the Personal Data, in which event Featurely shall isolate and protect the Personal Data from any further Processing except to the extent required by such law.

12. Liability

12.1 Each party's liability arising out of or related to this DPA shall be subject to the limitations and exclusions of liability set forth in the Agreement. This Section does not limit statutory liability under Article 82 GDPR or any mandatory provisions of Data Protection Law.

13. Term and Termination

13.1 This DPA shall remain in effect for so long as Featurely Processes Personal Data on behalf of Customer or until termination of the Agreement, whichever is later.

14. Governing Law and Jurisdiction

14.1 This DPA shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by Data Protection Laws. The rights of Data Subjects and supervisory authorities under the GDPR remain unaffected.

SCHEDULE 1

Part 1: Details of Processing

Subject matter of Processing:

The Processing of Personal Data as necessary to provide the Featurely Services under the Agreement.

Duration of Processing:

For the term of the Agreement and thereafter as required for data retention, return, or deletion.

Nature and purpose of Processing:

Featurely will Process Personal Data solely for the purpose of providing the Featurely Services as instructed by Customer, including: (i) providing synthetic user testing and behavioral simulation services; (ii) generating user insights, analytics, and feedback on Customer's products, designs, and content; (iii) facilitating experimentation and testing workflows including A/B testing and usability assessments; (iv) storing and managing Customer-uploaded content and test results; (v) enabling collaboration and sharing features within the Featurely platform as directed by Customer; and (vi) providing customer service, technical support, and related administrative functions necessary to deliver the Services.

Type of Personal Data:

The types of Personal Data Processed may include, depending on what Customer provides or generates through use of the Services: contact information (such as names and email addresses), account credentials and profile information, usage and behavioral data reflecting interactions with the Featurely platform, test responses and feedback, session data and analytics, device and browser information, and any other data that Customer uploads, submits, or directs Featurely to collect through the Services. Customer retains full control over what Personal Data is provided to Featurely.

Categories of Data Subjects:

Data Subjects may include Customer's employees, contractors, authorized users of the Featurely platform, end users of Customer's products or services that are being tested or analyzed, Customer's customers and prospects, and any other individuals whose Personal Data Customer chooses to Process through the Featurely Services.

Sensitive Data:

Customer shall not provide, and Featurely shall not knowingly Process, any special categories of Personal Data as defined in GDPR Article 9(1) (including data revealing racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic data, biometric data, health data, or data concerning sex life or sexual orientation) through the Featurely Services unless the Parties have entered into a separate written agreement specifically addressing such Processing.

Part 2: Technical and Organizational Measures

Featurely has implemented and maintains appropriate technical and organizational measures designed to protect Personal Data against unauthorized or unlawful Processing and against accidental loss, destruction, damage, alteration, or disclosure. These measures are designed to ensure a level of security appropriate to the risks presented by the Processing and the nature of the Personal Data to be protected. The measures include the following:

Access Control. Featurely employs role-based access control (RBAC) to restrict access to Personal Data based on job function and business need. Multi-factor authentication (MFA) is required for access to systems Processing Personal Data. Access rights are subject to regular review and audit to ensure ongoing appropriateness, and all access is granted in accordance with the principle of least privilege, limiting personnel access strictly to what is necessary to perform their designated responsibilities.

Data Security. Personal Data is protected through encryption both in transit and at rest. All data transmissions utilize industry-standard encryption protocols (TLS 1.2 or higher). Personal Data stored within Featurely's systems is encrypted using secure encryption standards. Featurely maintains secure key management practices to protect encryption keys and regularly applies security patches and updates to systems and software to address known vulnerabilities and maintain security posture.

Monitoring and Logging. Featurely maintains security event logging and monitoring capabilities to detect and respond to potential security incidents. Intrusion detection systems are deployed to identify suspicious activities and potential threats to Personal Data. Regular security assessments are conducted to evaluate the effectiveness of security controls and identify areas for improvement. Featurely maintains documented incident response procedures to ensure timely and appropriate response to any security incidents affecting Personal Data.

Organizational Measures. Featurely personnel with access to Personal Data receive regular security awareness training on data protection obligations and security best practices. All personnel are bound by confidentiality obligations, either through contractual agreements or statutory requirements. Where permitted by law, Featurely conducts background checks on personnel with access to Personal Data appropriate to their level of access and job responsibilities. Featurely maintains documented security policies and procedures governing the Processing of Personal Data and the operation of security controls.

Business Continuity. Featurely performs regular backups of systems containing Personal Data to enable recovery in the event of data loss or system failure. Documented disaster recovery procedures are maintained and tested to ensure Featurely's ability to restore access to Personal Data following a significant disruption. Business continuity planning ensures that critical Processing activities can continue or be resumed promptly following an incident. Incident response and recovery plans define processes and responsibilities for responding to and recovering from security incidents and system failures.

Additional Security Practices. Featurely undergoes regular third-party security audits to validate the effectiveness of its security controls and compliance with industry standards. Vulnerability scanning is conducted on a regular basis to identify and remediate potential security weaknesses in systems and applications. Featurely follows a secure software development lifecycle that incorporates security considerations throughout the design, development, testing, and deployment of software systems. Vendor security management processes ensure that Sub-processors and other third-party service providers maintain appropriate security standards and controls for any Personal Data they may Process on behalf of Featurely.

Part 3: List of Sub-Processors

Sub-processor	Type of Service	Location	More information (Security/Trust Link)
Amazon Web Services (AWS)	Cloud infrastructure and hosting	US	**https://aws.amazon.com/compliance/
Supabase	Database and authentication	US	**https://supabase.com/security
Stripe	Payment processing	US	**https://stripe.com/privacy
OpenAI	AI/ML services	US	**https://trust.openai.com/
Anthropic	AI/ML services	US	https://trust.anthropic.com/
Google Cloud (Gemini)	AI/ML and Cloud services	US	**https://cloud.google.com/trust-center
Resend	Email delivery service	US	**https://resend.com/security
Slack	Team collaboration	US	**https://slack.com/trust/security
Segment	Customer data platform	US	**https://segment.com/legal/security/
LogRocket	Session replay and monitoring	US	**https://logrocket.com/products/safety-security-performance
Datadog	Monitoring and analytics	US	**https://www.datadoghq.com/security/
Redis	Caching and data storage	US	https://trust.redis.io/
LangSmith	LLM tracing and monitoring	US	https://trust.langchain.com/
Mem0	AI memory management	US	https://mem0.ai/security
ZeroEntropy	Vector database and embeddings	US	https://trust.delve.co/zeroentropy
Dagster Cloud	Data orchestration	US	**https://dagster.io/security
Jina AI	Embeddings and search services	Germany	https://jina.ai/legal/
Anchor Browser	Browser automation services	US	https://trust.anchorbrowser.io/

Sub-processor	Type of Service	Location	More information (Security/Trust Link)
Apollo.io	Professional data enrichment	US	https://www.apollo.io/product/security

ANNEX I

LIST OF PARTIES

Data exporter(s): Customer

Role: Controller

Data importer(s):

Name: Featurely, Inc.

Contact details: privacy@featurely.ai

EU Representative (Germany):

Rickert Rechtsanwaltsgesellschaft mbH - FEATURELYAI
Colmantstraße 15
53115 Bonn
Germany
Email: FEATURELYAI@rickert.law

UK Representative:

Rickert Services Ltd UK - FEATURELYAI
PO Box 1487
Peterborough
PE1 9XX
United Kingdom
Email: FEATURELYAI@rickert-services.uk

Activities relevant to the data transferred under these Clauses: Provision of the Featurely Services as described in the Agreement.

Role: Processor

DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

The categories described in Schedule 1 of the DPA between the parties.

Categories of personal data transferred:

The categories described in Schedule 1 of the DPA between the parties.

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 specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.*****:**

The categories described in Schedule 1 of the DPA between the parties.

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

Continuous for the duration of the Processing under the DPA.

Nature of the processing/Purpose(s) of the data transfer and further processing:

The nature and purpose of processing is described in Schedule 1 of the DPA.

The period for which the personal data will be retained:

Personal Data to be retained during the performance of the Agreement and for a reasonable period of time following termination in order to effectuate the appropriate return and/or destruction of Personal Data in accordance with the Agreement and/or applicable law.

For transfers to (sub-) processors:

The subject matter and nature described in Schedule 1 of the DPA between the parties.

COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority in accordance with Clause 13 of these Standard Contractual Clauses.

ANNEX II

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.

(a) 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").

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

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

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix.

[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 […].

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:

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

(iii) 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);

(iv) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(v) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(vi) Clause 13;

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

(viii) Clause 16(e);

(ix) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(d) 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.

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7 - Optional

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.

(g) 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.

(h) 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 organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

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

(i) 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 its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

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

(k) 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.

(l) 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:

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

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

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

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

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

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

8.9 Documentation and compliance

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

(m) 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.

(n) 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.

(o) 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.

(p) 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

GENERAL WRITTEN AUTHORISATION The data importer has the data exporter’s general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 4 weeks 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.

(1) 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.[3] 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.

(b) 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.

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

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

Clause 10

Data subject rights

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

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

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

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

Clause 11

Redress

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

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

(g) 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.

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

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

(j) 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.

(k) 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.

(l) 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.

(m) 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.

(n) 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.

(o) 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.

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

Clause 13

Supervision

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: 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 competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(q) 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

(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

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

(r) 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.

(s) 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.

[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.

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

(u) 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).

(v) 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 [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

(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

15.1 Notification

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

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

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

(w) 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.

(x) 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.]

(y) 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.

(z) 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).

(aa) 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.]

(bb) 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.

(cc) 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).

(dd) 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.

(b) 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.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] 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.

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

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Germany.

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.

(d) The Parties agree that those shall be the courts of Germany.

(e) 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.

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

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

A. **LIST OF PARTIES**

Data Exporter: Customer (as defined in the Agreement)

Data Importer: Featurely (as defined in the Agreement)

Please see DPA Annex I.

B. **DESCRIPTION OF THE PROCESSING**

Please see DPA Schedule 1 Part 1

C. COMPETENT SUPERVISORY AUTHORITY

See Clause 13.

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

Please see DPA SCHEDULE 1 Part 3

ANNEX III – LIST OF SUB-PROCESSORS

Please see DPA SCHEDULE 1 Part 2