Data Processing and Sharing Agreement

PARTIES

(1) DORIS WORLDWIDE LTD incorporated and registered in England and Wales with company number 15895046 whose registered office is at 19 Astley Grove, Stalybridge, England, SK15 1NL ("**Doris**")

(2) You, the Customer, as defined in the Terms ("**Customer**")

BACKGROUND

(A) The Parties have entered into or shall enter into a separate Agreement that governs the provision to and receipt of the Doris Services by Doris to the Customer (the "**Terms**").

(B) This Data Processing and Sharing Agreement ("**Agreement**") is supplementary to the Terms and sets out the additional terms on which Doris and the Customer may process personal data, Doris (as Controller or Processor (as relevant)), as part of the provision of the Doris Services to the Customer (as Controller) under the Terms.

1. Definitions

1.1. Capitalised terms used but not defined in this Agreement have the meaning given to them in the Terms and all rules of interpretation as set out in the Terms shall apply in this Agreement.

1.2. The following additional definitions shall apply in this Agreement:

Appropriate Safeguards: means such legally enforceable mechanism(s) for transfers of Personal Data as may be permitted under the Data Protection Legislation from time to time, including the UK International Data Transfer Agreement, or the UK IDTA along with the EU Standard Contractual Clauses (as applicable), or any other mechanisms as set out in Article 46 of the EU GDPR and the UK GDPR (as applicable).

Business Purposes: the Doris Services to be provided by Doris to the Customer as described in the Terms and any other purposes specifically identified in Annex A.

Commissioner: the Information Commissioner (see Article 4(A3), UK GDPR and section 114, DPA 2018).

Controller, Processor, Data Subject, Personal Data, Personal Data Breach and Processing: have the meanings given to them in the Data Protection Legislation.

Data Protection Legislation: To the extent the UK GDPR applies, the law of the United Kingdom or of a part of the United Kingdom which relates to the protection of Personal Data. To the extent the EU GDPR applies, the law of the European Union or any member state of the European Union to which Doris or Customer is subject, which relates to the protection of Personal Data. And any applicable national implementing laws, regulations and secondary legislation relating to the processing of Personal Data and the privacy of electronic communications.

EEA: the European Economic Area.

EU GDPR: the General Data Protection Regulation 2016/679.

EU Standard Contractual Clauses: means the standard contractual clauses approved by the European Commission in Commission Decision 2021/914 dated 4 June 2021, for transfers of Personal Data to third countries not otherwise recognized as offering an adequate level of protection for Personal Data by the European Commission (as amended and updated from time to time).

Personal Data: means Personal Data (as defined under applicable Data Protection Legislation) shared between the Parties pursuant to the provisions of the Terms and this Agreement, including but not limited to that specified in Annex A.

Restricted Transfer: means a transfer of Personal Data between any Party to this Agreement in circumstances where in the absence of the obligations created by this Agreement the export of the Personal Data would be in breach of the applicable Data Protection Legislation.

SCCs: means: (i) where the EU GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries published at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0914&qid=1693902889407, ("**EU SCCs**"); and

(ii) where the UK GDPR applies standard data protection clauses adopted pursuant to Article 46(2)(c), ("**UK SCCs**").

Supervisory Authority: means a governmental or government chartered regulatory body having binding legal authority over a party.

Third Country: means a country or territory that is not part of the United Kingdom or the EEA.

UK DPA 2018: means the UK Data Protection Act 2018.

UK GDPR: means the EU GDPR as transposed into United Kingdom national law by operation of section 3 of the European Union (Withdrawal) Act 2018, together with the UK DPA 2018.

UK IDTA: means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under section 119A(1) UK DPA 2018, Version B1.0, in force as of 21 March 2022.

2. Data Protection Obligations

2.1. The parties envisage that under this Agreement:

2.1.1. Each Party is a separate independent Data Controller of the Personal Data processed for the provision and receipt of the Doris Services in respect of the Personal Data of prospective students and their guardians as specified in Annex A Part 1 ("**C2C Processing**"); and

2.1.2. Doris acts as a Data Processor on behalf of the Customer in respect of the Personal Data it processes of its members of staff, personnel, and educational institutions for the provision and receipt of the Doris Services (i.e. providing them with accounts to contact and be contacted by the prospective students and/or their prospective guardians, including via our platform) as specified in Annex A Part 2 ("**C2P Processing**").

2.2. Doris may process, transfer and disclose Personal Data as described in their relevant privacy notices in particular for (i) the delivery of the Doris Services, (ii) administration of engagement and general correspondence with the Customer and its personnel; (iii) screening of individuals associated with the other Party against international sanctioned parties lists, and (iv) aggregation, de-identification and, where feasible, full anonymisation of Personal Data for benchmarking, market research and data analysis purposes associated with the development of Doris' products and services. The Customer acknowledges and understands that Doris shall act as an independent Data Controller of any Personal Data which is processed pursuant to this Clause and shall comply with Data Protection Legislation in respect of such processing.

3. Controller Processing Obligations

3.1. Each Party agrees for its own part that, to the extent that it processes Personal Data under or in connection with the Terms and this Agreement as a separate independent Data Controller, including in respect of the C2C Processing:

3.1.1. It will observe all applicable requirements of the Data Protection Legislation and this Agreement in relation to its processing of Personal Data; and

3.1.2. All Personal Data collected or sourced by it or on its behalf for processing in connection with the Terms and/or this Agreement or which is otherwise provided or made available to the other Party shall have been collected or otherwise obtained in compliance with Data Protection Legislation, and may be processed, disclosed and transferred as described in or in connection with the Terms and this Agreement.

3.1.3. It shall implement appropriate technical and organisational measures to protect the Personal Data under or in connection with the Terms and this Agreement against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

3.1.4. Both Parties will work together in good faith to ensure the information prescribed by the Data Protection Legislation is made available to relevant data subjects.

3.1.5. If either Party receives any complaint, notice or communication from a supervisory authority which relates to the other Party's processing of Personal Data under or in connection with the Terms and this Agreement or potential failure to comply with the Data Protection Legislation in respect of that Personal Data, that Party shall direct the supervisory authority to the other Party.

3.1.6. If a data subject makes a written request to a Party to exercise any of their rights in relation to the Personal Data that concerns processing of the other Party, that Party, shall direct the data subject to the other Party.

3.1.7. If either Party becomes aware of a Personal Data Breach that requires notification to a Supervisory Authority, it shall notify the other Party without undue delay, and each Party shall co-operate with the other, to the extent reasonably requested, in relation to any notifications to supervisory authorities and/or to affected Data Subjects.

3.1.8. ANNEX AAnnex A Part 1 describes the subject matter, duration, nature and purpose of the processing and the Personal Data categories and Data Subject types in respect of which Doris may process the Personal Data to fulfil the Business Purposes in respect of the C2C Processing.

4. Processor Processing Obligations

4.1. Customer retains control of the C2P Processing of Personal Data and remains responsible for its compliance obligations under the Data Protection Legislation, including but not limited to, providing any required notices and obtaining any required consents, and for the written processing instructions it gives to Doris, as applicable.

4.2. To the extent that Doris processes Personal Data in the course of providing the Doris Services as a Data Processor, it will:

4.2.1. only process the Personal Data only for the purpose of providing the Doris Services or otherwise on the Customer's written instructions, which may be specific instructions or instructions of general nature, and including in order to comply with its obligations under the Terms;

4.2.2. implement and maintain appropriate technical and organizational measures to protect Personal Data against unauthorized or unlawful processing and accidental loss, destruction, damage, theft or disclosure, having regard to the harm which might result from any unauthorized or unlawful processing, accidental loss, destruction, damage or theft of the Personal Data and having regard to the nature of the Personal Data which is to be protected. Such security measures are further set out in Annex B;

4.2.3. at the Customer's request and choice, either deliver to the Customer or delete the Personal Data from its systems on termination of the Doris Services, unless Doris is required to retain such copies pursuant to applicable law;

4.2.4. take reasonable steps to ensure that any personnel, agents and/or contractors who process the Personal Data under the Terms for Doris are subject to appropriate contractual or statutory obligations

of confidentiality and understand their obligations when handling Personal Data in accordance with this Agreement;

4.2.5. provide reasonable assistance to the Customer to meet its obligations to: (i) respond to requests by data subjects exercising their rights under the Data Protection Legislation, (ii) in meeting its legal obligations in relation to the security of processing of Personal Data, (iii) notifying Personal Data breaches to supervisory authorities and data subjects upon the specific written request of the Customer in its role as a Data Controller or otherwise as required under applicable law (iv) in undertaking data protection impact assessments and the prior consultation with applicable Supervisory Authorities in relation to high risk processing, as applicable;

4.2.6. notify the Customer without undue delay of any Personal Data breaches and provide information when known as to the source and nature of the data breach, the type of data that was subject to the breach, and the identity of the affected data subjects;

4.2.7. maintain adequate records, and, on the Customer's written request, make available such information as the Customer may reasonably request to demonstrate Doris' compliance with its obligations under this Agreement and in relation to the Personal Data processed under the Terms only, and allow for and contribute to audits, including inspections, by the Customer or the Customer's designated auditor on a minimum of fifteen (15) working days' written notice, to demonstrate its compliance with Data Protection Legislation and this clause. Such audits shall be conducted at Customer's cost, during usual business hours and shall not be carried out more frequently than once in any twelve (12) month period; and

4.2.8. notify the Customer if, in Doris' reasonable opinion, the Customer's instructions in respect of any processing of Personal Data by Doris are unlawful.

4.3. ANNEX AAnnex A Part 2 describes the subject matter, duration, nature and purpose of the processing and the Personal Data categories and Data Subject types in respect of which Doris may process the Personal Data to fulfil the Business Purposes in respect of the C2P Processing.

4.4. Customer hereby (i) specifically authorises the Sub-Processors set out in Annex A to this Agreement, and (ii) generally authorises Doris to engage Sub-processors from time to time to process the Personal Data as part of the provision of the Doris Services.

4.5. Doris shall ensure in each case that it enters into a written contract with the Sub-processor that contains terms substantially the same as those set out in this Agreement, in particular, in relation to requiring appropriate technical and organisational data security measures, and remain liable to the Customer for the performance of that Sub-processor's performance of its obligations.

4.6. Doris shall provide the Customer with an opportunity to object to the appointment of each new Sub-processor, provided such objection is reasonable, within (10) working days after Doris supplies the Customer with full details in writing regarding such Sub-processor, after which the Sub-processor change shall be deemed approved.

5. Transfers of Personal Data

5.1. The Parties agree that the Personal Data will not be transferred outside of the United Kingdom or the European Economic Area under this Agreement and/or the Terms unless:

5.1.1. It is to a Third Country that the United Kingdom and/or the EU has recognised as providing adequate protection under Chapter V of the EU GDPR or the UK GDPR as applicable; or

5.1.2. Appropriate Safeguards are in place, e.g. the Parties have executed an agreement with the importing third party incorporating the EU Standard Contractual Clauses and the UK International Data Transfer Addendum where necessary, importing Parties are registered with the data privacy framework; or

5.1.3. The transfer otherwise complies with the Data Protection Legislation.

5.1.4. In accordance with clause 5.1.2 the Parties agree that, where the transfer of Personal Data between the Parties is a Restricted Transfer, the following shall apply to the transfer and this Agreement:

5.1.4.1. Where the EU GDPR applies, and the transfer of Personal Data is from the EEA either directly or via onward transfer, to any country or recipient outside of the EEA not subject to an adequacy determination by the European Commission:

5.1.4.1.1. The parties agree that the EU Standard Contractual Clauses shall apply to Restricted Transfers from the EEA. The EU Standard Contractual Clauses shall be deemed entered into (and incorporated into this Agreement by reference) and completed as follows: (i) Module One (Controller to Controller) shall apply where both Parties are Data Controllers and Modules Two (Controller to Processor) and Four (Processor to Controller) shall apply when Customer is Data Controller and Doris is the Data Processor, and shall be completed with the following specifications where relevant to each Module; (ii) In Clause 7 of the EU Standard Contractual Clauses, the optional docking clause will apply; (iii) in Clause 9 of the EU Standard Contractual Clauses, Option 2 is selected and the timeframe shall be 10 days; (iv) In Clause 11 of the EU Standard Contractual Clauses, the optional language shall not apply; (v) In Clause 13(a) of the EU Standard Contractual Clauses the Supervisory Authority shall be determined by the place of establishment of the data exporter, (vi) In Clause 17 of the EU Standard Contractual Clauses, Option 1 applies and the EU Standard Contractual Clauses shall be governed by Irish law; (vii) In Clause 18(b) of the EU Standard Contractual Clauses, disputes shall be resolved by the courts of Ireland; (viii) Annex I of the EU Standard Contractual Clauses shall be deemed completed with the information set out in Annex A of this Agreement; (ix) Annex II of the EU Standard Contractual Clauses shall be deemed completed with the information and requirements of Annex B of this Agreement. The frequency of the transfer shall be continuous, as necessary to deliver the Services, and retention shall be determined by the Customer in relation to C2P Processing only, and each independent Data Controller otherwise, except where such Party is required by applicable laws to retain Personal Data in accordance with its record retention schedules and policies, or as otherwise specified in the definition of Personal Data.

5.1.4.2. Where the UK GDPR applies, and the transfer of Personal Data is from the United Kingdom either directly or via onward transfer, to any country or recipient outside of the UK not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018;

5.1.4.2.1. The parties agree that, with respect to Restricted Transfers subject to the UK GDPR, the EU Standard Contractual Clauses are hereby incorporated into this Agreement by reference as follows: incorporating the selections in 5.1.4.1 and shall be deemed amended by the provisions of Part 2 (Mandatory Clauses) of the UK IDTA and the Parties confirm that the information required for the purposes of Part 1 (Tables) of the UK IDTA is set out in Annex A and B of this Agreement, and shall be amended as follows:

5.1.4.2.2. For the purpose of Module 1 of the EU Standard Contractual Clauses where both Parties are Data Controllers (data importer and exporter): Appendices 1 and 2 of the EU Standard Contractual Clauses shall be deemed to incorporate respectively the data subjects, categories of personal data and processing operations set out in Annex A and in the Terms and this Agreement.

5.1.4.2.2.1. The parties agree that the governing law and choice of forum and jurisdiction shall be that of England and Wales.

5.1.4.2.2.2. The Parties agree that Annex I.A will be populated as follows: Data Exporter and Data Importer Contact details: as detailed in this Agreement (each Party being both Data Exporter and Data Importer).

5.1.4.2.2.3. The Parties agree that Annex I.B of the IDTA shall be completed as described in Annex A of this Agreement.

5.1.4.2.2.4. The Parties agree that Annex I.C of the IDTA shall be completed as follows: the competent supervisory authority is the ICO supervisory authority.

5.1.4.2.2.5. The Parties agree that Annex II of the IDTA shall be completed as described and agreed between the parties in the Terms and/or this Agreement.

5.1.4.2.3. For the purpose of Modules 2 and 4 of the EU Standard Contractual Clauses where Doris acts as Data Processor (data importer): Appendices 1 and 2 of the EU Standard Contractual Clauses shall be deemed to incorporate respectively the data subjects, categories of personal data and processing operations set out in Annex A and the organisational and technical measures as described in Annex B of this Agreement.

5.1.4.2.3.1. The parties agree that the governing law and choice of forum and jurisdiction shall be that of England and Wales.

5.1.4.2.3.2. The Parties agree that Annex I.A will be populated as follows: With respect to Module 2: Data Exporter is Customer and Data Importer is Doris as a Data Processor. With respect to Module 4: Data Exporter is Doris as Data Processor and Data Importer is Customer as Data Controller. Data Exporter and Data Importer Contact details: as detailed in this Agreement.

5.1.4.2.3.3. The Parties agree that Annex I.B of the IDTA shall be completed as described in Annex A of this Agreement..

5.1.4.2.3.4. The Parties agree that Annex I.C of the IDTA shall be completed as follows: the competent supervisory authority is the ICO supervisory authority.

5.1.4.2.3.5. The Parties agree that Annex II of the IDTA shall be completed as described and agreed between the parties in the Terms and/or this Agreement.

5.1.4.2.3.6. The Parties agree that Annex III of the IDTA shall be completed with the Authorised Sub-Processors detailed in Annex A of this Agreement.

6. Term and Termination

6.1. This Agreement will remain in full force and effect so long as:

6.1.1. the Terms remain in effect; or

6.1.2. Doris retains any of the Personal Data related to the Terms in its possession or control.

7. Liability

Liability for breach of this Agreement shall be subject to the relevant clauses of the Terms.

8. General

8.1. Any provision of this Agreement that expressly or by implication should come into or continue in force on or after termination of the Terms in order to protect the Personal Data will remain in full force and effect.

8.2. If a change in any Data Protection Legislation prevents either Party from fulfilling all or part of its obligations under the Terms, the Parties may agree to suspend the processing of the Personal Data until that processing complies with the new requirements. If the Parties are unable to bring the Personal Data processing into compliance with the Data Protection Legislation within sixty (60) days, either Party may terminate the Terms on not less than thirty (30) working days on written notice to the other Party.

8.3. Any notice or other communication given to a Party under or in connection with this Agreement shall comply with the relevant terms of the Terms.

9. Precedence

If there is an inconsistency between any of the provisions of this Agreement and the provisions of the Terms, the provisions of this Agreement shall prevail.

10. Variation

No variation of this agreement shall be effective unless it is in writing and signed by the parties (or their authorised representatives).

11. Notices

11.1. Any notice given to a party under or in connection with this agreement shall be in writing and shall be:

11.1.1. for Doris, the email specified in the Documentation (as defined in the Terms) for legal notices from time to time; and

11.1.2. for the Customer, the contact email provided in connection with the Customer's account from time to time or via in-Services messaging functionality.

11.1.3. **Third Party Rights**

This Agreement does not confer any rights on any person or party (other than the parties to this agreement and, where applicable, their successors and permitted assigns) pursuant to the Contracts (Rights of Third Parties) Act 1999.

12. Governing Law

This agreement and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the law of England and Wales.

13. Jurisdiction

Each party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with this agreement or its subject matter or formation.

ANNEX A ANNEX A: Personal Data Processing Purposes and Details

Part 1: C2C Processing

Subject matter of Processing: provision of the personal data of the end-users of the Doris Services (i.e. the prospective students and their guardians) under the Terms and this Agreement.

Duration of Processing: the duration of the Terms and this Agreement**.**

Nature of Processing: collecting, displaying, using, transferring, analysing, contacting, publishing and/or presenting the Personal Data as part of the delivery of the Services.

Business Purposes: provision of the Personal Data by Doris to the Customer pursuant to the Terms and this Agreement.

Personal Data Categories (including Special Category Data):

1 Identity data of parents/guardians: (including first name, surname, username or similar identifier, title, date of birth, email address, gender, location, contact details (email and phone number), nationality, country of residence);

2 Individual Needs of Students (e.g. special educational needs, language support, health data); and

3 IP address, login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, device ID.

Data Subject Types: end-users, prospective students and their guardians.

Part 2: C2P Processing

Subject matter of Processing: provision of the personal data of the end-users of the Doris Services (i.e. the nominated personnel by the Customer to have accounts to use the Doris Services and be contacted by the prospective students and their guardians) under the Terms and this Agreement.

Duration of Processing: the duration of the Terms and this Agreement.

Nature of Processing: collecting, displaying, using, transferring, analysing, contacting, publishing and/or presenting the Personal Data as part of the delivery of the Services.

Business Purposes: provision of the Personal Data by the Customer to Doris (and in return) as part of the delivery and use of the Services pursuant to the Terms and this Agreement.

Personal Data Categories (including Special Category Data):

4 Identity data: (including first name, surname, username or similar identifier, title, date of birth, work email address, LinkedIn profile, job title, employment information (limited to that relevant to showcase in profile on the platform), location); and

5 IP address, login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, device ID.

Data Subject Types: customer personnel who are to have accounts and/or use the Doris Services.

Approved Sub-processors:

Sub-processor	Location	Purpose/service
Open AI	USA	Use of Open AI's API to power the chat/ recommendations

Cloudflare	USA	Content delivery and security
Heroku	EU	Server hosting + data storage
Datadog	EU	Monitoring
Sentry	EU	Monitoring
Hotjar	EU	Monitoring
GTM	EU	Marketing and Analytics
Meta	EU	Marketing and Analytics
Hubspot	EU (Germany)	CRM systems and marketing automation
Google	Europe	Business operations
Xero	USA	Financial record management
Saint & Co	EU	Accountancy services (e.g. invoicing)

ANNEX B: Security measures

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Examples of possible measures:
Measures of pseudonymisation and encryption of personal data
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing
Measures for user identification and authorisation
Measures for the protection of data during transmission
Measures for the protection of data during storage
Measures for ensuring physical security of locations at which personal data are processed
Measures for ensuring events logging
Measures for ensuring system configuration, including default configuration
Measures for internal IT and IT security governance and management
Measures for certification/assurance of processes and products
Measures for ensuring data minimisation
Measures for ensuring data quality
Measures for ensuring limited data retention
Measures for ensuring accountability
Measures for allowing data portability and ensuring erasure