Data processing agreement

In accordance with article 28 of the General Data Protection Regulation (GDPR)

This agreement sets out how Noraina Limited processes personal data on behalf of a customer when it provides services under the services agreement between them. The customer is the controller; Noraina is the processor.

Parties

Customer (controller)	_____ hereafter the "Customer"
Supplier (processor)	Noraina Limited, a private company limited by shares incorporated in Ireland under registration number 614532, having its registered office at Unit 3D North Point House, North Point Business Park, New Mallow Road, Cork T23 AT2P, Ireland hereafter the "Supplier"
Services agreement	The agreement for services between the Customer and the Supplier dated _____ (the "Services Agreement")

1. Subject matter and duration

1.1 The subject matter and duration of the processing are determined by the Services Agreement. The Supplier processes personal data on behalf of the Customer within the meaning of article 4(2) and article 28 GDPR on the basis of this agreement.

2. Nature and purpose of the processing

2.1 The nature and purpose of the processing, the types of personal data and the categories of data subjects are described in Appendix 1, as completed by the Customer, insofar as they are not already set out in the Services Agreement.

2.2 The Supplier processes the personal data exclusively in a member state of the European Union or of the European Economic Area. Any transfer to a third country requires the prior consent of the Customer and may only take place if the conditions of articles 44 to 49 GDPR are met.

3. Technical and organisational measures (article 32 GDPR)

3.1 Before processing begins, the Supplier documents the technical and organisational measures it applies to the services and makes that documentation available to the Customer for review (Appendix 2). Once accepted by the Customer, the documented

measures form part of this agreement. If the Customer's review shows that changes are needed, they are made by mutual agreement.

3.2 The Supplier ensures the security of the data in accordance with article 28(3)(c) and article 32 GDPR, in particular in conjunction with article 5(1) and 5(2) GDPR. The measures ensure a level of security appropriate to the risk for the confidentiality, integrity, availability and resilience of the systems, taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of the processing, and the likelihood and severity of the risk to the rights and freedoms of natural persons.

3.3 The technical and organisational measures follow technical progress. The Supplier may implement alternative measures provided that they do not reduce the level of security of the documented measures. Substantial changes are documented.

4. Rectification, restriction and erasure

4.1 The Supplier does not rectify, erase or restrict the processing of the personal data on its own authority, but only on the documented instructions of the Customer. If a data subject contacts the Supplier directly with such a request, the Supplier forwards it to the Customer without undue delay.

4.2 Insofar as it is within the scope of the services, the Supplier carries out without undue delay, on the documented instructions of the Customer, the Customer's deletion policy and requests for erasure, rectification, data portability and access.

5. Obligations of the Supplier

5.1 In addition to this agreement, the Supplier complies with its obligations under articles 28 to 33 GDPR. In particular, the Supplier:

a. has appointed a Data Protection Officer, who can be reached at dpo@noraina.cloud, notifies the Customer of any change without undue delay and keeps the Data Protection Officer's contact details on its website;

b. entrusts the processing only to employees who are bound to confidentiality and have been made familiar with the data protection provisions relevant to their work (articles 28(3)(b), 29 and 32(4) GDPR). The Supplier and any person acting under its authority who has access to the personal data process it only on the instructions of the Customer, including the powers granted in this agreement, unless required to do so by law;

c. implements and maintains the technical and organisational measures described in Appendix 2;

d. cooperates, on request, with the supervisory authority in the performance of its tasks;

e. informs the Customer without undue delay of any inspection or measure by a supervisory authority insofar as it relates to this agreement, including any investigation of the Supplier by a competent authority for an infringement of law relating to the processing of personal data under this agreement;

f. supports the Customer to the best of its ability if the Customer is subject to an inspection by a supervisory authority, administrative or criminal proceedings, or a claim by a data subject or third party relating to the processing under this agreement;

g. regularly monitors its internal processes and its technical and organisational measures to ensure that the processing in its area of responsibility meets the requirements of data protection law and protects the rights of data subjects;

h. provides, on request through the Customer's account manager, documentation showing that the technical and organisational measures in clause 3 are in place.

6. Sub-processors

6.1 Sub-processing, for the purposes of this agreement, means services that relate directly to the provision of the services. It does not include ancillary services the Supplier uses, such as telecommunications, postal and transport services, maintenance and user support, or other measures to ensure the confidentiality, availability, integrity and resilience of hardware and software. The Supplier nevertheless puts in place appropriate and legally binding contractual arrangements and inspection measures to protect the Customer's data when it uses ancillary services.

6.2 The Customer gives the Supplier general authorisation to engage the sub-processors listed in Appendix 3. By signing this agreement, the Customer also gives the prior consent required by clause 2.2 for any transfer outside the European Economic Area that Appendix 3 describes, under the safeguards it names. The Supplier informs the Customer in advance of any intended addition or replacement of a sub-processor, and the Customer may object on reasonable data protection grounds within 15 days of that notice.

6.3 The Supplier imposes on each sub-processor, by contract, the same data protection obligations as those in this agreement, and remains responsible to the Customer for the performance of the sub-processor's obligations (article 28(2) and 28(4) GDPR).

7. Audits and inspections

7.1 The Customer may carry out inspections in consultation with the Supplier, or have them carried out by an auditor it appoints. The Customer may verify the Supplier's compliance with this agreement in its business operations by spot checks, which as a rule are announced in good time.

7.2 The Supplier makes available to the Customer the information needed to demonstrate compliance with its obligations under article 28 GDPR and, in particular, evidence of the technical and organisational measures in place.

7.3 Evidence of measures that are not specific to this agreement may be provided through adherence to an approved code of conduct (article 40 GDPR), a certification under an approved certification mechanism (article 42 GDPR), current certificates, reports or report extracts from independent bodies (such as auditors, data protection officers, IT security departments or quality auditors), or a suitable IT security or data protection certification. The Supplier's information security management system is certified to ISO/IEC 27001:2022 by Iscertia Evaluación & Certificación (certificate ES20240003).

7.4 The Supplier may charge for its time in supporting the Customer's inspections, as set out in clause 11.1.

8. Assistance and personal data breaches

8.1 The Supplier assists the Customer in meeting its obligations regarding the security of personal data, the notification of personal data breaches, data protection impact assessments and prior consultation under articles 32 to 36 GDPR. This includes:

a. ensuring an appropriate level of protection through technical and organisational measures that take into account the circumstances and purposes of the processing and the likelihood and severity of a breach, and that allow breaches to be detected promptly;

b. notifying the Customer of any personal data breach without undue delay after becoming aware of it;

c. assisting the Customer in informing the data subjects concerned, and providing the Customer without undue delay with the information it needs to do so;

d. assisting the Customer with its data protection impact assessments;

e. assisting the Customer with prior consultation of the supervisory authority.

8.2 The Supplier may charge for assistance that is not included in the description of the services and is not required because of a failure of the Supplier.

9. Instructions from the Customer

9.1 The Customer confirms oral instructions without delay, at least in text form.

9.2 The Supplier informs the Customer without undue delay if it considers that an instruction infringes data protection law. The Supplier may suspend the instruction until the Customer confirms or changes it.

10. Deletion and return of personal data

10.1 No copies or duplicates of the data are made without the Customer's knowledge, except backups needed to ensure proper processing and data that must be kept to meet statutory retention obligations.

10.2 When the contracted work is completed, or earlier at the Customer's request, and at the latest when the Services Agreement ends, the Supplier returns to the Customer, or with the Customer's prior consent destroys in accordance with data protection law, all documents, processing results and data sets relating to the services that have come into its possession, including test and discarded material. On request, the Supplier tells the Customer how and when the data was deleted.

10.3 The Supplier keeps the documentation that shows the data was processed properly and in accordance with this agreement for the applicable retention periods after the agreement ends, or hands it over to the Customer when the agreement ends.

11. Other provisions

11.1 **Charges.** No fee is payable for this agreement. The Customer reimburses the Supplier for assistance with data subject requests under clause 4, for supporting inspections under clause 7 (at the hourly rate of the Supplier's employee who accompanies the auditor), and for any costs arising from instructions under clause 9.

11.2 **Duration.** This agreement depends on the existence of the Services Agreement and ends automatically when the Services Agreement ends. The right to terminate for cause and statutory rights of rescission are not affected.

11.3 **Precedence.** In the event of a conflict between this agreement and the Services Agreement regarding the processing of personal data, this agreement prevails.

11.4 **Governing law and jurisdiction.** This agreement is governed by the laws of Ireland. The courts of Cork, Ireland, have jurisdiction.

By signing, the parties agree to this data processing agreement and its appendices:

Customer	**Supplier**

Name: _____

For and on behalf of _____

Date: _____

Name: _____

For and on behalf of Noraina Limited

Date: _____

Appendix 1: Personal data and purposes of processing

Completed by the Customer.

Purpose of the processing	
Types of personal data	
Categories of data subjects	
Special categories of data (article 9 GDPR), if any	

Appendix 2: Technical and organisational measures

The Supplier applies the measures of its information security management system, certified to ISO/IEC 27001:2022. Policies and procedures are approved by management and reviewed at least once a year. The Customer can request the detailed documentation through its account manager.

Area	Measures
Access control	Access is granted on business need, on need-to-know and least-privilege principles, and is reviewed periodically. User accounts are managed centrally and require multi-factor authentication. Privileged access to production systems is restricted, temporary and logged. Accounts are disabled when a person leaves.
Encryption	Personal data on the Supplier's infrastructure is encrypted in transit over external networks and at rest, using current industry-standard algorithms. Cryptographic keys are managed through their whole life cycle.
Separation	Customer environments are logically isolated from each other. Production and non-production environments are separated, as is customer traffic from management traffic.
Logging and monitoring	Security-relevant events are logged centrally, with access to logs restricted by role, and monitored by a central system with alerting and escalation.
Vulnerability and change management	Systems are regularly scanned for vulnerabilities and patched according to risk, and are periodically tested by independent assessors. Changes to production follow a documented change management process.

Area	Measures
Backup and continuity	Services that include backup are backed up regularly to a separate location, encrypted, and restores are tested. Business continuity and disaster recovery plans are documented, reviewed and tested at least once a year.
Physical security	The Supplier's infrastructure is hosted in third-party datacentres with ISO/IEC 27001-certified physical security, including controlled and logged access, surveillance, redundant power and environmental controls.
Disposal of media	Storage media are securely wiped before reuse or disposal, or physically destroyed when they cannot be wiped.
Staff	Employees and contractors are bound by confidentiality agreements and receive regular security and privacy training.
Incident management	A documented incident response process covers detection, classification, escalation, containment, evidence preservation and root cause analysis. Customers are notified of personal data breaches as set out in clause 8.
Suppliers	Suppliers are risk assessed before they are engaged and reviewed periodically. Security and privacy requirements are part of their contracts.

Appendix 3: Authorised sub-processors

Sub-processor	Service	Location and transfer safeguards
Equinix	Datacentres hosting the Supplier's servers (DB3 Dublin, PA2 Paris)	Ireland and France. Data is encrypted and Equinix has no access to the keys.
Telehouse	Datacentre hosting the Supplier's servers (TH3 Paris)	France. Data is encrypted and Telehouse has no access to the keys.
Templus	Datacentre hosting the Customer's own equipment (Barcelona)	Spain. Only when the Customer chooses this location for its equipment and the Supplier manages that equipment on the Customer's instructions.
Equinix	Datacentre hosting the Customer's own equipment (LD5 London)	United Kingdom, covered by an adequacy decision of the European Commission. Only when the Customer chooses this location for its equipment and the Supplier manages that equipment on the Customer's instructions.

Sub-processor	Service	Location and transfer safeguards
Wasabi	Storage of backups	Amsterdam, the Netherlands. Data is encrypted and Wasabi has no access to the keys.
Cloudflare	Network, security and edge services	Configured to process data in its European region. Cloudflare is part of a group based in the United States; any access from outside the EEA relies on the EU–U.S. Data Privacy Framework or the Standard Contractual Clauses.
Google (Google Workspace)	Email, calendar and documents	European Union and other locations of the Google group; transfers rely on the EU–U.S. Data Privacy Framework or the Standard Contractual Clauses.
HubSpot	Customer relationship management and support	European Union datacentre. HubSpot is part of a group based in the United States; any access from outside the EEA relies on the EU–U.S. Data Privacy Framework or the Standard Contractual Clauses.
Xero	Accounting and invoicing	Xero group based in New Zealand, which is covered by an adequacy decision of the European Commission; its own sub-processors include providers in the United States and other countries. Transfers rely on the Standard Contractual Clauses included in Xero's data processing terms.
Anthropic	AI assistant used by the Supplier's staff	Contracted with Anthropic Ireland, Limited. Data is processed by the Anthropic group and its sub-processors, including in the United States. Transfers rely on the Standard Contractual Clauses included in Anthropic's data processing addendum.