EthonAI Master Service Agreement (As of February 2026)

1 Introduction

For all orders placed with the provider (the **Provider**) by the client (the **Client**) this Agreement applies exclusively. It shall also apply to future business with the Client. Provider does not accept opposing terms and conditions of the Client that deviate from this Agreement unless agreed in writing.

The Client's use of the Service without signing the Order Form is considered an acceptance of these Terms and Conditions and the terms laid out in the Order Form submitted to the Client.

2 Definitions

Affiliate means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "**Control**," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

Agreement means this Master Service Agreement including its Terms and Conditions, annexes, and the Order Form.

Confidential Information means any information (a) disclosed by the disclosing Party regarding any aspects of its business which is (i) clearly labelled as confidential by the disclosing Party at the time of disclosure or (ii) which is evidently of a confidential nature; and (b) the terms of this Agreement.

Factory means the Client's factories for which the Client purchases the Services and which are specified in the Order Form.

Fees means the fees specified in the Order Form.

Force Majeure Event means an event, or a series of related events, that is outside the reasonable control of the Party affected which render the fulfilment of the affected Party's obligation under this Agreement legally impossible or would lead to such Party's insolvency.

Initial Term means the fixed term for a given order as specified in the Order Form.

Malicious Code means code, files, scripts, agents or programs intended to do harm.

Order Form means an ordering document specifying the Services to be provided hereunder that is entered into between the Provider and the Client. By entering into an Order Form, a Client Affiliate agrees to be bound by the terms of this Agreement as if it were an original party hereto.

Services means the Provider's proprietary products and services ordered by Client under an Order Form and made available online.

Term means the Initial Term and any extension thereof.

Terms and Conditions means these terms and conditions.

Upgrade means new versions of, and updates to the Services, whether for the purposes of fixing an error, bug or other issue or enhancing the functionality of the Services.

3 Scope

Subject to the terms of this Agreement and payment of the Fees Provider will make the Services available to the Client as specified in the applicable Order Form for each Service ordered, and provide Client with reasonable technical support services in accordance with the terms set out in the Service Level Terms as specified in Annex 1.

4 Client's Rights and Responsibilities

4.1 Use Rights

Subject to the terms of this Agreement Provider grants Client a limited, Factory-specific, non-exclusive, non-sublicensable, non-transferable and revocable right and license to access and use the Services during the Term solely for Client's internal purposes as specified in the Order Form.

The Services may be accessed solely by Client's employees or service providers who are explicitly authorized by Client to access and use the Services (each, a "**User**"). Client shall immediately report any unauthorized access or use of the Services to Provider. In order to access the Services, Client and/or its Users may be required to set up an administrative account with Provider ("**Account**").

4.2 Use Restrictions

Client shall not, during the Term and thereafter:

- **a.** make any Services available to anyone other than Client, or use any Services for the benefit of anyone other than Client or its Affiliates;
- **b.** sell, resell, license, sublicense, distribute, rent, lease, assign, transfer or pledge any Services or include any Services in a service bureau or outsourcing offering;
- **c.** use a Service to store or transmit Malicious Code;
- **d.** use the Services to develop any services or products that are the same or substantially similar;
- **e.** interfere with or disrupt the integrity or performance of any Service or third-party data contained therein;
- **f.** use the Service other than in accordance with the Provider's instructions;
- **g.** use the Service in any way that is unlawful, illegal, fraudulent or harmful or use it in connection with any unlawful, illegal, fraudulent or harmful purpose or activity;
- **h.** use the Service in any way that causes, or may cause, damage to the Service or impairment of the availability or accessibility of it, or any of the areas of, or services on, the Service;
- **i.** attempt to gain unauthorized access to any Service or its related systems or networks;
- **j.** remove or alter any trademarks or other proprietary right notices displayed on or in the Service;
- **k.** circumvent, disable or otherwise interfere with security-related features of the Service or features that enforce use limitations;
- **l.** modify, adapt, copy, translate, edit or create derivative works of a Service or any part, feature, function or user interface thereof;
- **m.** frame or mirror any part of any Service;

n. except to the extent permitted by mandatory law, disassemble, reverse engineer, or decompile a Service or otherwise attempt to discover the source code, object code or underlying structure, ideas, know-how or algorithms relevant to the Service.

4.3 Other Client's Responsibilities

It is the Client's responsibility to ensure compliance with internal policies, union contracts as well as legal requirements of the respective countries regarding the privacy protection of individual employees.

It is the Client's sole responsibility to provide the IT systems required to process data with the Services. The Client must report any change in the number of used Service deployments (i.e., the number of camera stations and production lines) to the Provider within thirty (30) days.

All instructions to the Provider in relation to the Agreement and Client's use of the Service shall only be valid if given by the Client's representative indicated in the Order Form.

5 Fees and payment

The Fees and payment terms for the Initial Term are specified in the Order Form.

If the term for a given order renews , the Provider may increase the Fees payable in the renewal term from the Fees charged in the immediately preceding term provided that the Provider has given notice of such increase at least thirty (30) days before the expiration of the preceding term.

Under exceptional circumstances, the Provider reserves the right to notify the Client of an increase in Fees after the period for the termination notification has expired, in which case the Client shall be entitled to terminate the Agreement by giving the Provider notice of termination upon five (5) days after the receipt of the fee increase notification from the Provider. Failure to terminate within this period shall be deemed acceptance of the new Fees.

If the Client does not pay any amount when due, the Provider may charge the Client interest on the overdue amount at the rate of 5% per year (which interest will accrue daily and be compounded quarterly).

Provider may suspend the provision of the Services if any amounts due to be paid by the Client to the Provider are overdue by more than thirty (30) days. In the case of a suspension of Services, Client remains fully obligated to pay the Fees and the Client is not entitled to claim any refunds or damages.

6 Intellectual Property

Company shall own and retain all right, title and interest in and to (a) the Services, all improvements, enhancements, customizations or modifications thereto, (b) any software, applications, inventions or other technology developed in connection with implementation services or support, and (c) all intellectual property rights related to any of the foregoing.

Any anonymous information, which is derived from the use of the Services (i.e., metadata, aggregated and/or analytics information and/or intelligence relating to the operation, support, Client‘s use of the Services) which is not personally identifiable information and which does not identify Client may be used for providing the Services, for development of the Services, and/or for statistical purposes. Such analytics information is Provider’s exclusive property.

As between the Parties, Client is, and shall be, the sole and exclusive owner of all data and information inputted or uploaded using the Services by or on behalf of Client or otherwise integrated (“**Client Data**”). Client hereby grants Provider a worldwide, non-exclusive, non-assignable, non-sublicensable (except to Provider’s subcontractors, if applicable), non-transferable, royalty-free, irrevocable right and license to access and use the Client Data, including for Provider to (i) provide the Services (ii) fulfil its obligations under this Agreement and (iii) create derivative works and aggregated anonymized data derived from Client Data, including comparative data sets, statistical analyses, reports and related services (“**Provider Data**”). Provider is free to use and dispose of such Provider Data for any purpose.

Client grants Provider a worldwide, irrevocable, royalty-free license to use, distribute, disclose, and make and incorporate into its services any suggestion, enhancement request, recommendation, correction or other feedback provided by Client or Users relating to the operation of Provider’s services and software.

7 Data Retention and Deletion

The Provider can choose to archive Client Data six months after reception, and can choose to delete Client Data three years after reception, unless otherwise required by applicable law or agreed upon in writing by both parties.

8 Representations and Warranties

8.1 Mutual Representation and Warranties

Each party represents that it has the legal right and authority to enter into and perform its obligations under the Agreement.

8.2 Provider Representation and Warranties

Provider represents and warrants that:

a. it uses reasonable efforts consistent with prevailing industry standards to maintain the Services in a manner which minimizes errors and interruptions in the Service and shall perform the Service with due care;

b. under normal authorized use, the Services shall substantially perform in conformance with the performance and functional specifications set out in the Order Form;

c. the Services are compatible with the latest version of Microsoft Edge, Google Chrome, Mozilla Firefox.

As Client's sole and exclusive remedy and Provider's sole liability for breach of this warranty, Provider shall use commercially reasonable efforts to fix the Services. The warranty set forth herein shall not apply if the failure of the Services results from or is otherwise attributable to: (i) repair, maintenance or modification of the Services by persons other than Provider or its authorized contractors; (ii) accident, negligence, abuse or misuse of theServices; (iii) use of the Services other than in accordance with this Agreement; or (iv) the combination of the Services with equipment or software not authorized or provided by Provider.

8.3 Client Acknowledgement

Client acknowledges and agrees that:

a. Provider is not providing any consulting or advisory services to the Client in connection with the Services. The evaluation of the AI models' or Services performance is the sole responsibility of the Client. The Provider does not give any performance guarantees for AI models trained by the Client, nor does it guarantee that correlations and statistics computed using the Services represent real-world causal relationships. Taking actions on production lines and operations based on findings surfaced through the Services is the sole responsibility of the Client. Provider only provides the Services and supports the Client in its use, including by running custom data analytics as appropriate when requested. The Provider does not provide hardware to run the Services;

b. the Provider may from time to time, in its sole discretion, apply Upgrades to the Services which may result in changes to the appearance and/or functionality of the Services;

c. complex software is never wholly free from defects, errors and bugs, and Provider gives no warranty or representation that the Services will be wholly free from such defects, errors and bugs;

d. complex software is never entirely free from security vulnerabilities; and subject to the other provisions of the Agreement, Provider gives no warranty or representation that the Services will be entirely secure.

To the maximum extent permitted by applicable law, the Parties do not make or imply any warranties or representations concerning the subject matter of the Agreement other than those expressly set out in this Agreement.

9 Limitations and Exclusion of Liability

To the extent permitted by applicable law, all liability of either Party is explicitly excluded, including, liability for simple negligence and for acts or omissions of auxiliary persons. Mandatory statutory liabilities, including liability for death, personal injury, and fraud, remain unaffected.

Neither Party shall be liable for any:

a. loss of profits, income, revenue, use, production interruption or anticipated savings;

b. loss of business, contracts or commercial opportunities;

c. loss of or damage to goodwill or reputation;
loss or corruption of any data, database or software, except where the obligation under this Agreement explicitly requires the protection of such loss;
d. special, indirect or consequential loss or damage; and
e. losses arising out of a Force Majeure Event.

The aggregate liability of Provider under this Agreement shall be limited to the fees Client paid to Provider for the Services during the 12-month period immediately preceding the first event giving rise to the relevant claim.

10 Data Protection

Provider and Client shall comply with the applicable data protection legislation in relation to the processing of personal data.

The Client warrants that it has the legal right to disclose all data protected by any applicable data protection legislation that it does in fact disclose to the Provider under or in connection with the Agreement.

Insofar as Provider acts as a processor within the meaning of the applicable data protection law, it shall do so in accordance with the Data Processing Agreement attached as Annex 2.

11 Confidentiality

The Parties acknowledge that during the Term they may provide each other with Confidential Information. The Parties agree to

a. receive, treat and keep Confidential Information in confidence;
b. refrain from using it otherwise than for the purpose of and in compliance with this Agreement;
c. limit the disclosure of Confidential Information to employees, professional advisors, directors, or Affiliates who, having a need to know said Confidential Information for the purpose of this Agreement, will be obligated to maintain such information confidential;
d. to take all reasonably required steps to prevent unauthorized access to Confidential Information;
e. not to disclose such Confidential Information to any other person, organization or entity without the prior written consent of the disclosing Party.

Nothing in this Section 11 shall restrict the Provider in engaging third party providers for the delivery of the Services (for example third party internet service providers).

The obligations set out in this Section 11 shall not apply to:

a. Confidential Information that is publicly known (other than through a breach of an obligation of confidence);
b. Confidential Information that was in possession of the receiving Party prior to disclosure by the other Party;

c. Confidential Information that is received from an independent third party who, to the best knowledge of the receiving Party, has a right to disclose the relevant Confidential Information;

d. was independently developed by the receiving Party without reference to the Confidential Information disclosed to the receiving Party; or

e. Confidential Information to the extent necessary to comply with legal requirements or enforceable court or administrative orders, provided that the receiving Party provides the disclosing Party with notice of such requirements and its intent to make the disclosure without undue delay to give the disclosing Party a reasonable opportunity to obtain a suitable protective order.

Each Party shall immediately notify the other Party if it becomes aware of

a. Any potential disclosure, access to or use of any Confidential Information in breach of this Agreement;

b. Any unauthorized intrusion into systems containing Confidential Information; and

c. Any disclosure of any Confidential Information where the purpose of such disclosure does not have any apparent correlation with the execution of this Agreement.

Unless otherwise agreed, each Party will upon request return to the other Party or destroy all tangible and intangible copies of the Confidential Information in its possession or in the possession of its subcontractors or its staff upon expiration or termination of the Agreement. In addition, each Party will upon request delete all Confidential Information of the other Party in electronic format from its information systems and the information systems of its subcontractors, with the exception of any automatically generated backup copies, which will remain subject to the confidentiality obligations under the Agreement and/or under applicable law.

12 Publicity

Each Party will make any public disclosure relating to the conditions of the Agreement (including press releases, public announcements, and marketing materials) only with the prior written consent of the other Party.

13 Use of Client's name and logo

The Client grants the Provider an unlimited, worldwide, non-exclusive, royalty-free right to use its logo for sales and marketing purposes (including but not limited to use on the Provider's website, presentations, and promotional materials). In addition, the Client agrees to support the Provider with one client announcement on social media, and development of one client success case study.

14 Term and Termination

14.1 Term

This Agreement applies during the Initial Term agreed for each given order individually as specified in the Order Form, and shall automatically renew for additional periods of the same duration as the Initial Term, unless either Party requests in writing non-renewal at least thirty (30) days prior to the end of the the-current term.

14.2 Termination

Either Party may terminate the Agreement immediately by giving written notice to the other Party if the other Party:

a. commits any material breach of this Agreement, and:

(i) that breach is not remediable; or

(ii) that breach is remediable, but the other Party fails to remedy the breach within thirty (30) days of receipt of a written notice requiring it to do so; or

(iii) persistently breaches the terms of the Agreement (irrespective of whether such breaches collectively constitute a material breach)

b. is dissolved;

c. ceases to conduct all (or substantially all) of its business;

d. is or becomes unable to pay its debts as they fall due;

e. is or becomes insolvent or is declared insolvent; or

f. an order is made for the winding up of the other Party, or the other Party passes a resolution for its winding up (other than for the purpose of a solvent company reorganization where the resulting entity will assume all the obligations of the other Party under this Agreement).

g. is subject to a Force Majeure Event that continues for at least sixty(60) days.

15 Effect of Termination

Upon termination of the Agreement, all the provisions of the Agreement will cease to have effect, save that the following provisions of the Agreement will survive and continue to have effect (in accordance with their terms or otherwise indefinitely): Section 11 and 16.

Termination of the Agreement will not affect either Party's accrued liabilities and rights as at the date of termination.

16 Force Majeure Event

Where a Force Majeure Event gives rise to a failure or delay in either Party performing its obligations under the Agreement (other than obligations to make payment), those obligations will be suspended for the duration of the Force Majeure Event.

Neither Party shall be liable for any delay or non-performance under this Agreement caused by any event beyond its reasonable control provided that the Party affected gives prompt notice in writing to the other Party of such Force Majeure Event and uses all reasonable endeavors to continue to perform its obligations under this Agreement.

A Party who becomes aware of a Force Majeure Event which gives rise to, or which is likely to give rise to, any failure or delay in performing its obligations under the Agreement, will:

a. immediately notify the other Party; and

b. will inform the other Party of the period for which it is estimated that such failure or delay will continue.

The affected Party will take commercially reasonable steps to mitigate the effects of the Force Majeure Event.

17 Miscellaneous

No breach of any provision of the Agreement will be waived except with the express written consent of the Party not in breach.

Unless specifically provided otherwise in this Agreement, any notice required or permitted to be given by either Party under this Agreement shall be in writing and shall only be deemed to have been duly served if hand delivered or sent by e-mail with the original to be forwarded by registered mail to the address of the other Party set out in the Order Form or such other address as may be notified by that Party.

If a provision of this Agreement or a portion thereof is or becomes invalid and/or unenforceable, the other provisions of the Agreement will continue in effect. The Parties commit themselves to negotiate in good faith to substitute the ineffective provision with one that most closely reflects the economic intention of the ineffective provision. The same applies to unintentional gaps in the Agreement.

Nothing in the Agreement constitutes a partnership, agency relationship or contract of employment between the Parties.

This Agreement may not be varied except by a written document signed (including by using industry standard electronic signature tools) by or on behalf of each of the Parties.

The Client may not assign any or all of its contractual rights and/or obligations under this Agreement without the prior written consent of the Provider. The Client hereby agrees that the Provider may assign any or all of its contractual rights and/or obligations under this Agreement to any Affiliate or any successor to all or a substantial part of the business of the Provider from time to time.

This Agreement constitutes the entire agreement between the Parties in relation to the Services ordered in the relevant Order Form, and supersedes all previous agreements, arrangements and understandings between the Parties in respect of that subject matter.

This Agreement will be governed by and construed in accordance with the substantive laws of Switzerland excluding its conflict of law provisions and excluding the United Nations Convention on the International Sale of Goods (CISG). Exclusive place of jurisdiction is Zurich (City), Zurich 1, Switzerland.

Annex 1 - Service Level Terms

Provider reserves the right to change the terms of these Service Level Terms by providing Client with at least thirty (30) days prior written notice.

1.1 Service Availability

Provider shall use commercially reasonable efforts to make the Services available 99%, measured monthly using the Provider's systems, excluding holidays and weekends, updates and other system changes at the Client, and scheduled maintenance. Any downtime calculation shall only be based on malfunction of the Provider's software and exclude any downtime resulting from other software installed, outages of third-party connections or utilities or other reasons beyond Provider's control will also be excluded from any such calculation.

Uptime is measured using the Provider's systems over each month. It is calculated to the nearest minute, based on the number of minutes in the given month (e.g., a month with 31 days contains 44'640 minutes).

1.1 Support Terms

Provider will use commercially reasonable efforts to make available a 365/24/7 e-mail helpdesk facility (**"Helpdesk"**).

The Client must make all requests for support services through the Helpdesk at **support@ethon.ai**.

1.1.1. Response Times

Provider will use reasonable endeavors to respond to requests for support services made through the Helpdesk as swiftly as possible and within the following response times. All requests with respect to the Services shall be prioritized based upon the severity of the problem:

Severity Level	Definition	First Response Time
1	a) A Service is down; or b) Key component(s) of the Service functionality is/are not working and no workaround available	8 business hours*
2	a) The main functionality of a Service is not working, but a workaround exists	16 business hours*
3	a) A secondary functionality of a Service is not working (i.e., the effect of the incident or problem does not directly impact the Client's ability to use the Service)	24 business hours*
4	a) The Client experiences an incident or problem, which is not Level 1, 2 or 3 classified; or b) Non-EthonAI device/browser-specific problem	30 business hours*

*Business Hours: 9am – 6pm (CET) Monday-Friday except Swiss public national holidays and holidays in the municipality of Zurich City.

1.1.2. **Resolution Times**

Provider will use reasonable endeavors to resolve issues raised by the Client through the Helpdesk as swiftly as possible considering the severity of the incident, it being understood, however, that the Provider cannot guarantee resolution times.

1.2 **Limitations of Support Service**

The Provider shall have no obligation under the Agreement to provide support services in respect of any fault or error caused by:

a) the improper use of the Services by the Client; or
b) the use of the Services otherwise than in accordance with the terms and conditions of the Agreement.

Annex 2 – Data Processing Agreement (DPA)

Parties

- Controller: Client
- Processor: EthonAI

Scope

1. This DPA governs the roles, responsibilities and obligations of Controller and Processor regarding the processing of personal data by Processor on behalf of Controller.
2. This DPA supplements the provisions of the EthonAI Master Service Agreement ("Main Agreement") without restricting the rights and obligations of the Parties with regard to the provision or use of the services as agreed in the Main Agreement. In case of conflict, the provisions of this DPA take precedence over the provisions of the Main Agreement (unless expressly agreed otherwise in the Main Agreement).

Subject matter, duration, nature and purpose, type of personal data and categories of data subjects

1. The subject matter of the processing is the provision of services as agreed in the Main Agreement by Processor for Controller. The processing consists in storage, keeping, and use of data.
2. Processor processes categories of personal data that Controller chooses to use Processor's services for. In particular, this may include data collected by the Controller or entered by its employees and customers. The categories of data subjects include employees and customers of Controller.
3. Personal data shall not be processed for a period longer than is necessary for serving its purpose. This DPA shall remain in force for as long as Processor processes personal data on behalf of Controller pursuant to the Main Agreement.

Roles

1. This DPA only applies in case that EthonAI acts as processor for Client according to applicable data protection laws. In cases where EthonAI arranges for Client to conclude a direct contract with a third-party service provider and the third-party service provider becomes Client's direct processor, Client itself shall be responsible for making any necessary agreements with the third-party service provider under applicable data protection laws.
2. Insofar as Processor is not subject to the European Union General Data Protection Regulation (EU GDPR), Processor shall assume this role only on the basis of its contractual obligations under this DPA and will not be subject to the GDPR solely for this reason.
3. This DPA does expressly not apply to the processing of personal data where EthonAI determines the purposes and means of the processing and therefore acts as controller. Such processing is carried out in accordance with EthonAI's Privacy Notice and the applicable data protection laws.

Duties of Processor

1. Subject to the following paragraph, Processor undertakes to process the personal data only as instructed by Controller, i.e. for the provision of Processor's services in accordance with the Main Agreement. The Main Agreement is deemed to be the exclusive instructions of Controller.
2. If Processor considers them to be unlawful, it shall inform Controller accordingly.
3. Client authorizes EthonAI

a. to create aggregated statistical, non-personal data from data containing pseudonymized identifiers (such as usage logs containing unique, pseudonymized identifiers); and
b. to calculate statistics related to Client's Data ("Client Data" means all data, including all text, sound, video, or image files, and software, that are provided to EthonAI by, or on behalf of, Client through use of the services)

in each case without accessing or analyzing the content of Client's Data and limited to achieving the purposes below, each as incident to providing the services to Client:

a. billing and account management;
b. compensation such as calculating employee commissions and partner incentives;
c. internal reporting and business modeling, such as forecasting, revenue, capacity planning, and product strategy; and
d. financial reporting.

When processing for these business operations, EthonAI will apply principles of data minimization and will not use or otherwise process Client's data for:

a. user profiling,
b. advertising or similar commercial purposes, or
c. any other purpose, other than for the purposes set out in this Section.

4. Processor shall oblige all auxiliary persons and employees to maintain confidentiality insofar as they are not already obliged to do so by law.
5. Processor shall always ensure appropriate data security in accordance with applicable data protection law, at least the agreed TOMs below.
6. Processor shall report any breach of data security without delay to Controller and provide all information necessary. Processor's obligation to report or respond to a security incident pursuant to this Section shall not be construed as an admission of fault or liability on the part of Processor with respect to the personal data breach.
7. Upon written request and against separate reasonable remuneration and within the scope of Processor's operational resources and possibilities, Processor undertakes to support Controller in accordance with the applicable data protection laws in the fulfillment of data subject rights by Controller, in conducting data protection impact assessment and consultations with supervisory authorities. Such support shall be provided upon written request, within reasonable timeframes, and against separate reasonable remuneration.
8. At the end of the DPA, Processor shall return all data and delete or anonymize it to the extent permitted.

Subprocessors

1. Processor shall only use subprocessors with the prior approval of Controller. Controller can only reject subprocessors for legitimate reasons under data protection law. Subprocessors shall be deemed approved by Controller if no written objection is received within 30 days of notification of the commission of such a subprocessor. The subprocessors approved at the time of the conclusion of this DPA are listed Annex 1 of this DPA.
2. Subprocessors shall be bound in the same way as Processor.

Transfer abroad

1. Processor shall not export any of Controller's data outside Switzerland, the EU or the European Economic Area (EEA), except:

a. To Controller itself, its affiliated companies or third parties in fulfillment of an instruction from Controller or as provided for in the Main Agreement;
b. Unless otherwise agreed in the Main Agreement, to a recipient in a country with an adequate level of data protection;
c. Unless otherwise agreed in the Main Agreement, to a recipient who is not in a country with an adequate level of data protection, provided that the conditions required under the applicable data protection law for such transfers have been met; or
d. This is agreed with Client in the Main Agreement or otherwise.

Duties of Controller

1. Controller must comply with all applicable data protection laws and is responsible for the lawfulness of the processing of the personal data, including the permissibility of (sub)processing and the transfer of personal data abroad.
2. Controller has the sole responsibility for the accuracy, quality, and legality of the personal data and the means by which it acquired the personal data.
3. Controller is obliged independently take appropriate technical and organizational measures to protect the personal data in its area of responsibility.
4. Controller must inform Processor immediately if it discovers violations of applicable data protection laws in the provision of services by Processor.
5. In the event of claims by a data subject or fines imposed by supervisory authorities or other competent authorities, Controller shall:
    a. promptly inform Processor in writing of any potential or pending claims or penalties;
    b. make reasonable efforts to reduce or avoid such claims or penalties;
    c. provide Processor with an opportunity to respond to any reply, settlement, defense or complaint with respect to such claim; and
    d. provide Processor with a reasonable amount of information in relation thereto. However, Controller shall not be bound by any recommendations made by Processor.
6. Within 30 days of termination of this DPA, Controller must inform Processor in writing whether Controller's data is to be returned or deleted. If no notification is given, Processor shall be entitled to delete Controller's data without prior notice.

Information and audit rights

1. Processor shall be obliged to provide Controller, upon written request, with all information that Controller reasonably requires to prove compliance with this DPA to data subjects or data protection or other supervisory authorities.
2. Processor shall enable Controller or an auditor commissioned by Controller and bound to confidentiality to check Processor's compliance with this DPA. If Processor is found to have violated the DPA after submitting corresponding evidence, Processor shall implement suitable corrective measures immediately and free of charge.
3. The aforementioned information and inspection rights of Controller shall only exist to the extent that the Main Agreement does not grant Controller any other information and inspection rights that meet the relevant requirements of the applicable data protection laws. Furthermore, these information and inspection rights are subject to the requirement of proportionality and the protection of Processor's legitimate interests (in particular security or confidentiality interests).

4. Audits shall be conducted during normal business hours, with minimal disruption to Processor's operations. Furthermore, audit requests shall be limited to once per calendar year unless a supervisory authority requests otherwise.

Unless otherwise agreed between the parties, Controller shall bear all costs of the information and examination, including proven internal costs of Processor.

Annex 1: Approved Subprocessors

Name	Address	Data Storage and Access	Function
auth0	100 1st St Suite 150, San Francisco, United States	Germany/Ireland.	Authentication and authorization platform.
AWS	38 Avenue John F. Kennedy, L-1855, Luxembourg	Germany. Service Provider will not intentionally store Customer Data outside the region(s) configured by Customer, except for transient processing, resiliency, security operations, and support as necessary to provide the Services.	Data storage and hosting.
Google Cloud Platform (GCP) (Google Cloud EMEA Limited)	70 Sir John Rogerson's Quay, Dublin 2, D02 R296, Ireland.	Customer-selected region(s) (incl. EU/EEA options) where the relevant GCP service is configured; customer data for common services is stored in the selected location/region.	Cloud infrastructure hosting (compute, storage, networking, managed services, backups, and related support services).
Microsoft Azure (Microsoft Ireland Operations Ltd)	One Microsoft Court, South County Business Park, Leopardstown, Dublin 18, Ireland (D18 DH6K).	For most Azure services, you can specify the region/geo where customer data is stored and processed; Microsoft may replicate for resiliency, but states it will not store/process outside the selected Geo for covered services.	Cloud infrastructure hosting (compute, storage, networking, managed services, backups, and related support services).
Sendgrid	25-28 North Wall Quay, Dublin 1, Ireland	Ireland	Sending emails.

Annex 2: Technical and Organizational Measures (TOMs)

Pseudonymization

- Authorization process or approval routines for authorizations to edit additional information for identification purposes

Measures for Encryption

- Encryption of mobile devices such as laptops, tablets and smartphones

- Encryption of files
- Encryption of systems/installations
- Encrypted storage of passwords
- Secure data transfer (e.g., SSL, FTPS, TLS)
- Secure WLAN

Measures to ensure confidentiality: Access Control

- Access control system, badge reader (magnetic/chip card)
- Door locks (electric door openers, combination locks, etc.)
- Key management/documentation of key allocation
- Special protective measures for the storage of back-ups and/or other data carriers
- Non-reversible destruction of data carriers
- Visitor regulations (e.g., pick-up at reception, documentation of visiting times, visitor badge, escort to the exit after the visit)

Measures to ensure confidentiality: Access control to use of system

- Personal and individual user log-in when logging into the system or company network
- Access control list for all systems containing Personal Data
- Authorization process for access authorizations
- Limitation of authorized users
- Use of passwords and multi-factor authorization
- Single Sign-On
- Password procedure (specification of password parameters with regard to complexity and update interval)
- Encrypted storage of passwords
- Electronic documentation of passwords and protection of this documentation against unauthorized access
- Personalized chip cards, tokens, PIN/TAN, etc.
- Logging of access
- Additional system log-in for certain applications
- Automatic locking of clients after a certain period of time without user activity (also password-protected screen saver or automatic pause)
- Automatic blocking of accounts after failed login
- Firewall

Measures to ensure confidentiality: Access Control to Personal Data

- Management and documentation of differentiated authorizations
- Evaluations/logging of data processing
- Authorization process for authorizations
- Approval routines
- Profiles/roles
- Encryption of CD/DVD ROM, external hard disks and/or lap-tops (e.g., via operating system, Safe Guard Easy, PGP)
- Measures to prevent unauthorized transfer of data to externally usable data carriers (e.g., copy protection, blocking of USB ports, data loss prevention (DLP) system)
- Mobile Device Management System
- Segregation of Duties
- Non-reversible deletion of data carriers
- Privacy films for mobile data processing systems

Measures to ensure the integrity of Personal Data

- System-based logging of access and changes to Personal Data
- Checking and monitoring access to/changes to Personal Data
- Configuration management
- Alarms for unauthorized changes
- Document Management System (DMS) with change history
- Security/logging software
- Organizationally defined responsibilities
- Multi-eye principle
- Logging of data transmission or data transport

Measures to ensure and restore the availability of Personal Data

- Security concept for software and IT applications
- Monitoring of security events/alert process(es) on servers, in networks and databases
- Security incident response process
- Back-up process
- Storage process for back-ups (fire-protected safe, separate fire compartment, etc.)
- Guarantee of data storage in the secure network
- Installing security updates as required
- Mirroring of hard disks
- Setting up an uninterruptible power supply (UPS)
- Suitable archiving facilities for paper documents
- Fire and/or extinguishing water protection for the server room
- Fire and/or extinguishing water protection for the archiving rooms
- Air-conditioned server room
- Virus protection
- Firewall
- Definition of roles and responsibilities
- Emergency plan
- Successful emergency drills

Measures to ensure Resilience of the System

- Emergency plan for machine breakdown
- Redundant power supply
- Sufficient capacity of IT systems and facilities
- Logistically controlled process to prevent power peaks
- Dynamic scanning of applications and/or static code analysis
- Redundant systems/plants
- Resilience and error management

Measures to ensure effectiveness

- Procedure for regular checks/audits
- Emergency tests