fellow digitals

Processing Agreement

Parties:

<NAME CLIENT>,
<Street + no.>
(<Postal Code>) <Place>,
listed in the Companies House under number <registration numer>
and duly represented by <….>;

hereinafter referred to as: ***"Controller"*** on the one hand ",

and

FELLOW DIGITALS GMBH, with registered office at Brüsseler Straße 25 in 50674 Cologne (Germany), listed in the Commercial Registry at the Local Court of Cologne under the number HRB 78649 and duly represented by Mr. M.C.P. de Graaf;

hereinafter referred to as: ***"Processor"*** on the other hand;

joint referred as the ***"Parties"***;

Whereas:

- an agreement has been concluded between the Controller and the Processor with regard to the provision and management of the Fellow Digital software (Intranet and/or LMS) (hereinafter: the "**Agreement**");
- for the purpose of the fulfilment of its obligations under the Agreement, the Processor will be provided with personal data by the Controller and process these, or have these processed, for the Controller;
- the Parties regard EU Regulation 2016/679 of 27 April 2016 (hereinafter: the "**GDPR**") as the legal framework for privacy issues;
- terms in the GDPR that are used in this Processing Agreement, such as processing, personal data, controller and processor, have the meanings given to them in the GDPR;
- in accordance with article 28 GDPR, the Parties wish to describe the subject and duration of the processing, the nature and purpose of the processing, the type of personal data, the categories of data subjects and the rights and obligations of the Parties in this agreement (the "**Processing Agreement**").

Agree as follows:

Article 1 - General

1.1
The Processor processes the personal data only by order and for the benefit of the Controller during the term of the Agreement. The Processor will under no circumstance process the personal data for own purposes, unless statutory obligations dictate otherwise.

1.2
The Processor notifies the Controller immediately if the Processor has reason to believe that the Processor can no longer comply with the Processing Agreement.

1.3
The Controller provides personal data to the Processor. An overview of the categories of personal data that can be provided to the Processor is included in Annex 1. If necessary, the Parties will adjust Annex 1 during the term of the Processing Agreement.

1.4
The Processor processes personal data for the Controller in accordance with the written instructions and under the express responsibility of the Controller. The instructions of the Controller are detailed in the Processing Agreement and the Agreement.

1.5
The Controller has the control over the processing of the personal data and has defined the purpose of and the means for the processing of the personal data. The control over the processing will never rest with the Processor. The Parties record in Annex 1 what processing the Processor will carry out by order of the Controller.

1.6
In the event that a provision of the laws of the European Union or a Member State applicable to the Processor compels it to a processing that derogates from what is agreed in this Processing Agreement, the Processor will notify the Controller of this statutory provision prior to the processing, unless this provision prohibits such notification.

1.7
The Controller guarantees to the Processor that the content, the use and/or the processing of the personal data are not unlawful and do not infringe on any right of a third party.

1.8
The Controller will notify the Processor of any changes in the laws and regulations underlying the rights and obligations of the Parties in this Processing Agreement.

Article 2 – Security

2.1
The Parties will take technical and organizational security measures to protect the personal data against loss or any form of unlawful processing. The Processor will inform the Controller on request about measures in the field of security.

2.2
The security measures of the Processor will provide an appropriate level of protection, having regard to the state of the art, the costs of implementation as well as the risks associated with the processing and the nature of the personal data.

2.3
The measures taken on entry into this Processing Agreement as referred to in this article are listed in Annex 2.

2.4
The Processor cannot ensure that the security measures will be effective under all circumstances.

2.5
If the Controller deems that a change in security measures to be taken by the Processor is necessary to provide an appropriate level of protection, then the Parties will enter into consultations on the change in the security measures desired by the Controller.

Article 3 - Inspections and Audits

3.1
The Controller is entitled to have an annual inspection, including audits, of the performance of the Processing Agreement carried out by an independent expert who is bound to confidentiality.

3.2
The inspection initiated by the Controller takes place at least two weeks after prior written announcement by the Controller.

3.3
The Processor declares to be willing to cooperate in such an inspection and enter into consultations with the Controller on any recommendations for improvement made by the expert. The obligation to cooperate referred to here does not automatically imply the obligation to follow all recommendations.

3.4
The Controller can obviously not have an inspection carried out at other (sub-) processors. Regarding the part of the security for which sub-processors are responsible, the Processor can at the Controller's request provide the data security policy and any certificates of sub-processors.

3.5
The inspection referred to in paragraph 1 can be onerous for the business operations of the Processor. The Parties therefore agree that these inspections will only take place after the Controller has requested and assessed the similar inspection reports available at the Controller, and presents reasonable arguments why an inspection initiated by the Controller is nevertheless justified. An inspection is justified if the similar inspection reports available at the Controller do not give a definitive answer as to whether the Processor complies with this Processing Agreement.

3.6
The Controller will provide the Processor with a copy of the report of the inspection immediately on receipt.

3.7
The Parties agree that the costs of an audit shall be borne by the Controller, unless the audit reveals major defects that can be attributed to Processor. In that case, the Parties shall consult on the division of the costs of the audit.

Article 4 - Security incidents and data leaks

4.1
Taking into account the nature of the processing and the information available to the Processor, the Processor will support the Controller in complying with the obligations of the Controller pursuant to articles 33 and 34 GDPR on the notification of breaches to supervisory authorities and data subjects.

4.2
The Processor will inform the Controller of a breach as quickly as possible after the Processor has discovered the aforementioned breach.

4.3
The Processor will inform the Controller via the contact and the contact details of the Controller as included in Annex 3.

4.4
The notification of a breach to the supervisory authority and to the data subject will always remain the responsibility of the Controller. The Processor will never be obliged to notify a supervisory authority and/or data subject(s) of a breach.

4.5
The Processor keeps a register of all breaches and the measures taken in response to breaches. The Controller may inspect the register on request.

Article 5 - The Processor's obligation to cooperate

5.1
The Processor will assist the Controller, in so far as relating to the processing of personal data for the performance of the Agreement and in so far as possible given the nature of the processing, in:

a) fulfilling the statutory obligations of the Controller with respect to rights of data subjects by means of appropriate technical and organizational measures. The aforementioned obligations of the Controller are set out in articles 12 up to and including 23 GDPR and relate to, among other things, requests for (notification of) deletion or correction of personal data and the right to portability of data;
b) complying with the obligations of the Controller set out in articles 32 up to and including 36 GDPR, taking into account the information available to the Processor. The aforementioned obligations relate to the security of the processing, the data protection effect assessment and the prior consultation with a supervisory authority.

Article 6 - Engagement of other sub-processors

6.1
The Controller grants the Processor permission in advance to engage sub-processors to fulfil the obligations under the Agreement, subject to the condition that the Processor notifies the Controller of any intended changes regarding the addition or replacement of sub-processors. The Controller may object to an intended change within 10 working days after the notification. The Controller will not object on unreasonable grounds. If the Processor does not accept the Controller's objection, the Processor may terminate the Agreement without observing a notice period.

6.2
The sub-processors engaged by the Processor to perform the Agreement are listed in Annex 1.

6.3
If the Processor instructs another sub-processor to perform specific processing activities for the benefit of the Controller, then the Processor shall ensure that the same obligations regarding data protection are imposed on the sub-processor as are imposed in the present Processing Agreement. The obligations shall be agreed in written form. The Processor shall provide copies of the agreements between the Processor and sub-processors to the Controller on request, provided that commercially sensitive information may be deleted from such copies.

6.4
If the sub-processor fails to comply with its obligations regarding data protection, the Processor remains liable to the Controller for compliance with the obligations of the sub-processor.

Article 7 - Confidentiality

7.1
The Parties will not make the personal data available to others than their own employees and/or third parties that have a legitimate reason for inspection thereof. The Parties guarantee that the persons authorized to process the personal data have undertaken to observe confidentiality or are bound by an appropriate statutory duty of confidentiality. Personal data may only be processed to perform the Agreement and this Processing Agreement.

7.2
If a Processor receives a request or an order from a Dutch or foreign government authority in relation to personal data, including but not limited to a request from the supervisory authority, that Processor will notify the Controller accordingly within 14 days, if and as far as permitted by law. The Processor will take account of all instructions from the Controller when dealing with the request or order and the Processor will also cooperate as fully as is reasonably required with the Controller.

7.3
If the Processor is prohibited by law from meeting his obligations under Clause 7.2, the Processor will nonetheless protect the reasonable interests of the Controller. This includes, in any event, the following:

a) the Processor will assess (i) how far the Processor is legally obliged to comply with the request or order, and (ii) how far the Processor is actually prohibited from complying with his obligations towards the Controller under Clause 7.2;
b) the Processor will only cooperate with the request or order if he is legally obliged to do so;
c) the Processor will not pass on any more personal data than is strictly necessary to comply with the request or order.

Article 8 - Liability

8.1
The provisions on liability of the Agreement also apply to the rights and obligations under this Processing Agreement, unless mandatory provisions of the law dictate otherwise.

Article 9 - Term and termination

9.1
This Processing Agreement will enter into force on the date of the last signing of the Agreement by the Parties. The term of the Processing Agreement is equal to the term of the Agreement.

9.2
This Processing Agreement will end by operation of law at the end of the Agreement. The Processing Agreement cannot be terminated separately from the Agreement. The provisions of this Processing Agreement that are intended to remain in force after termination, will remain in full force after termination of the Processing Agreement.

9.3
At the end of this Processing Agreement, the Processor will return all personal data in its possession and received from the Controller to the Controller or destroy them. Any costs related to the return and/or transfer of the personal data shall be borne by the Controller, provided that such costs are reasonable, transparent, cost-based, and specified in advance by the Processor.

9.4
The provisions of paragraph 3 of this article do not apply if a statutory provisions prevents the full or partial return or destruction of personal data by the Processor. The Processor will in that event continue to process the personal data only in so far as necessary to comply with its statutory obligations.

9.5
If the Processor is unable to return or delete the personal data for technical reasons, the Processor will notify the Controller immediately. In that event, the Processor shall take all necessary measures to come as close as possible to a full and permanent return or destruction of the personal data and make the personal data unsuitable for further processing.

Article 10 – Transfer to third countries

10.1
Processor is entitled to process personal data within the European Economic Area (EEA). Transfer of personal data to countries outside the EEA or an international organization is permitted only if the country ensures an adequate level of protection or it has put in place appropriate safeguards for this purpose, as referred to in Article 45 and 46 GDPR.

10.2
If the Processor must provide personal data to any third party on the basis of a legal obligation applicable in national or European regulations, the Processor will verify the basis of the request and the identity of the requester, and the Processor will immediately notify the Controller in this regard prior to provision, unless the law prohibits this for important reasons of general interest.

Article 11 – Costs

11.1
The costs of the processing of data that are inherent to the normal performance of the Agreement are deemed included by the fees already payable under the Agreement.

11.2
Any support or any other additional service provision that the Processor shall provide under this Processing Agreement, or that is requested by the Controller, including all requests for additional information, will be charged to the Controller at the usual rates.

11.3
The previous provision does not apply if the work relates to a substantial failure of the Processor under this Processing Agreement. The work will in that event be carried out free of charge (without prejudice to the Controller's right to recover the actual damage from the Processor).

Article 12 - Miscellaneous

12.1
This Processing Agreement forms an integral part of the Agreement. All rights and obligations under the Agreement, including the provisions on liability, therefore also apply to this Processing Agreement. In the event of contrariety between the provisions of this Processing Agreement and the Agreement regarding the protection of personal data, the provisions of this Processing Agreement will prevail.

12.2
In the event of future changes in the national or European laws and regulations on the protection of Personal Data, the Parties will change this Processing Agreement in so far as this is necessary to comply with such new laws and regulations.

12.3
Changes in this Processing Agreement are only valid if agreed in writing and accepted by both Parties.

Thus drawn up, agreed and signed in duplicate:

<NAME CLIENT>	FELLOW DIGITALS GMBH
_____	_____
Signature	*Signature*
Name:_____	Name: M.C.P. de Graaf
Position:_____	Position: CEO
Date:_____	Date: February 3, 2026

Annex 1

Subject Processing / Type of Personal Data

The processing of personal data relates to the use of the “Intranet” application (a social intranet), and the “LMS” application (an online training platform). Personal data of the user is stored in this application. Ultimately, the users decide for themselves which personal data they make available for processing in the application.
The platform’s functionality only requires users to provide an email address, first name, and last name. Input of other fields in the user profile can be made mandatory by the Controller. Administrators can also invite users anonymously in the application.
The processing of personal data depends on what the Controller includes in the application, but will, in most cases, consist of the processing of:

- Name (first and last name)
- Email address
- Organization
- Personal photo
- Personal documents
- Customer files
- Knowledge and skills (expert function)
- Date and time of activity

Duration

The Processor shall not retain personal data made available to it under this Processing Agreement for longer than necessary for the performance of the services, unless because of a legal obligation imposed on the Processor, the Processor must retain certain personal data for longer.
The Controller further has its own responsibility about the duration of the storage of (personal) data. The information posted by a user will remain available for the duration of the Agreement, as long as the user leaves this information in the application(s).

Nature and purpose

Processor performs the following processing of personal data for the Controller: Storage, collection and presentation of personal data within the application(s) and related additional services, such as for example providing (remote) support at the request of the Controller.
The purposes for which the personal data will be processed: For the purposes of providing services, cooperation and knowledge sharing between the users of the application(s).

Categories of data subjects

Application users: Employees and external cooperation parties of the Controller.

Sub-processors

Processor has engaged the following sub-processors for the provision and maintenance of its applications:

Sub-processors when standard functionality is used				
Sub-processors that are engaged by Processor to process personal data	(Category of) Personal data that sub-processor processes	Type of processing	Country of processing	Country of residence of sub-processor
Exonet B.V.	See part "Subject Processing / Type of Personal Data" in Annex 1	Hosting	The Netherlands (EU)	The Netherlands (Zevenaar)
Rapidmail GmbH	E-mail addresses	Transmission / delivery of e-mails from applications *(Emails will be deleted within 10 days)*	Germany (EU)	Germany (Freiburg im Breisgau)
Transloadit-II GmbH	Video files	Transcoding of video files *(All files will be deleted within 24 hours)*	Ireland (EU)	Germany (Berlin)
Sub-processors when artificial intelligence functionality is used				
Sub-processors that are engaged by Processor to process personal data	(Category of) Personal data that sub-processor processes	Type of processing	Country of processing	Country of residence of sub-processor
Mistral AI	User input	Content generation using Large Language Model (AI)	Sweden (EU)	France (Paris)
DeepL GmbH	User input	Translation	Among others, Sweden and Iceland (always within the EU)	Germany (Cologne)
HeyGen Technology, Inc.	User input	Text-to-video generation *(Videos will be deleted within 24 hours)*	United States of America	United States of America (Los Angeles, CA)

Processor engages Exonet B.V. as hosting party. Exonet B.V. has ISO 9001, ISO 27001 and NEN 7510 certification on full services at the time of entering into this Processing Agreement.
Exonet B.V. uses the following data centers: BIT B.V., Galileïlaan 19, 6716 BP Ede (NL) and Smartdc B.V., Van Nelleweg 1, 3044 BC Rotterdam (NL). At the time of entering into this Processing Agreement, the data centers have the following certifications: ISO 27001 and NEN 7510.

The Processor warrants that it has agreed with the sub-processors it engages for AI-related functionalities that any personal data shall be used solely for the performance of this agreement and shall not be used for the training of artificial intelligence models, in accordance with Article 28 of the General Data Protection Regulation (GDPR).

Location of processing

The Processor shall in principle process personal data only within the European Economic Area (EEA). Processing outside the EEA is only permitted if the respective third country ensures an adequate level of data protection pursuant to an adequacy decision by the European Commission, or if appropriate safeguards exist in accordance with Chapter V of the General Data Protection Regulation (GDPR), such as the use of Standard Contractual Clauses (SCCs). The Processor shall ensure that its sub-processors also comply with these requirements.

Annex 2

Technical and organizational measures

The Controller will take the following technical and organizational security measures to protect the personal data against breaches:

- the appointment of a coordinator at the Controller;
- no passing of user names and passwords by one user to another user;
- no granting of access to unauthorized persons;
- independent log out after use.

The Processor will take the following technical and organizational security measures to protect the personal data against breaches:

At Fellow Digitals:
Processor is ISO 27001, ISO 27701 and NEN 7510 certified. This means that information security is an integral part of its business processes and that these processes and procedures meet the requirements in these standards.
The security measures that the Processor will take include as a minimum:

- (password) security;
- encryption (HTTPS);
- annual preventive security assessments performed by external security specialists;
- internal agreements/procedures regarding access.

At Hosting parties (Exonet B.V., Exa 55, 6902 KH Zevenaar):
At the time of entering into this Processing Agreement, Exonet B.V. has taken the following measures.

Data centre

- Burglary prevention by 24x7x365 monitoring by means of security guards and camera monitoring; burglary detection and alarm; strict access control by means of digital registration, access cards, biometric access and server racks with certificate locks.
- Power supply by high-capacity and minimum n+1 redundant power supply; emergency power from independent generators and on-site fuel storage and 24x7x365 supply; entirely separate power distribution via A and B feed to rack infrastructure.
- Fire prevention by means of fully analogue addressable fire detection system in all spaces; smoke detection system; gas extinguishing system in technical spaces.
- Cooling by means of high-capacity cooling facility and cooling units, as a minimum N+1; control of temperature and air humidity by means of CRAC units.
- Certifications Data centre: ISO 27001 and NEN 7510.

Network & infrastructure

- Cabling in server rooms is separated; separate bundles for power cable and for fibreglass cables or UTP network cabling.
- Network equipment spread over multiple data centres, redundancy is present in the field of routers, core switches, internal and external connections (multiple connections to transit suppliers and Internet Exchanges), geographically separate routes between multiple data centres. The whole network is based on dynamic routing so that traffic is rerouted in the event of outage of components.

Platform infrastructure

- Redundant server and storage hardware through virtualization.
- Encryption of storage at disk level.
- Backup with snapshot technology, located in separate data center; frequency and retention defined in SLA.
- Fully separated cold standby disaster recovery facility in separate data center.
- Backup and disaster recovery facility run on separate hardware from production.
- Secure connections using HTTPS / TLS.
- Anti-DDoS infrastructure protects critical parts of the network and other infrastructure.
- Logical access based on password policy and/or VPN keys, access lists for access of IP addresses on information systems, firewalls, possibility of central logging of information systems and detection systems for certain unauthorized changes.
- Network segmentation through the use of VLANs.
- Standard firewall and antivirus on all servers.

Organization

- Exonet B.V.: ISO 9001, ISO 27001 and NEN 7510 certification for full service provision.
- Duty of confidentiality of all employees, Code of Conduct obligation for all employees, no temporary staff.
- Security officer within the organization, security awareness training for all employees.

Additional services

- Daily operating system security updates; additional updates in the event of serious security risks and leaks.

Annex 3

Notification of breach

The Processor will comply with the following agreements when giving notifications to the Controller: The Processor Security reports incidents and data leaks by sending an e-mail to the Coordinator of the Controller. In the event of absence of the Coordinator of the Controller, the Controller will ensure that the notification is forwarded to the Replacement Coordinator of the Controller. The Coordinator or Replacement Coordinator of the Controller confirms receipt of the notification by e-mail to the Processor.

The contact details of the Coordinator of the Controller are:

Last name: _____ First name: _____

Job title: _____

E-mail: _____ Phone: _____

Postal address: _____

Place: _____

Are personal health data being processed on the platform? Yes / No

The Processor will as a minimum include the following information in a notification of a Data Leak:

a) the (suspected) cause of the Data Leak;
b) the consequences of the Data Leak, as then known and/or expected;
c) location data of the Data Leak;
d) any unauthorized recipients of the Personal Data and information available about them;
e) proposed measures to mitigate the damage;
f) other data that a notification of a Data Leak to a supervisory authority and to a data subject must include according to relevant laws and regulations.

The contact details of the Coordinator of the Processor are:

Name: Martyna Sagel
E-mail: privacy@fellowdigitals.com
Telephone: +49 (0)221 828 293 64
Address: Brüsseler Straße 25, 50674 Amsterdam (NL)