AGREEMENT FOR THE PROCESSING OF PERSONAL DATA

This data processing agreement (hereinafter "DPA") forms an integral part of the Contractual Relationship between the parties.

BETWEEN: **PARTENA SECRETARIAT SOCIAL D'EMPLOYEURS ASBL**

having its registered office at 1000 Brussels, rue Ravenstein 36

and registered with the Crossroads Bank for Enterprises under number 0409.536.968

duly represented by Günther Van Weyenberg

in the capacity of Chief Operating Officer

hereinafter referred to as the "Processor";

AND:

having its registered office at

and registered with the Crossroads Bank for Enterprises under number

duly represented by

in the capacity of

hereinafter referred to as the "Controller";
Jointly "the Parties" or separately "the Party";

IT IS HEREBY AGREED AS FOLLOWS:

Article 1: Definitions

The following terms, used in this DPA with a capital letter, shall have the meaning given to them in this article, unless clearly indicated otherwise by the context:

"**Contractual Relationship**"	means the main agreement between the Parties defining the delivery of the services and/or products or the collaboration between the Parties, including all its amendments and annexes and anything that is subsequently agreed between the Parties with respect to this DPA;
"Applicable Regulations on Data Protection"	means all data protection regulations applicable to the Processing and use of Personal Data in the context of the activities carried out under the Contractual Relationship, including the General Data Protection Regulation (as defined hereunder) and the transposition of this Regulation in Belgian law;
"DPA"	means this data processing agreement, including its annexes;

Version: July 2026

"GDPR"	means the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 applicable as of 25 May 2018;
"Personal Data"	means any information relating to an identified or identifiable natural person (hereinafter referred to as the "data subject"); an "identifiable natural person" is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
"Process" or "Processing"	means any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, modification or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, deletion or destruction;
"Personal Data Breach"	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to, Personal Data transmitted, stored or otherwise Processed;
"Technical and Organisational Measures"	means the technical and organisational measures as defined in the GDPR;
"Supervisory Authority"	means an independent public authority established by a Member State of the European Union pursuant to Article 51 of the GDPR.

Article 2: Purpose of the DPA

The purpose of this DPA is to define the conditions under which the Processor undertakes to perform Processing of Personal Data on behalf of the Controller as defined in the Contractual Relationship or described in Annex 1 of this DPA.

Within the context of their Contractual Relationship the Parties agree to comply with the Applicable Regulations on Data Protection and, in particular, the GDPR.

Article 3: Term of the agreement

This DPA shall come into force on the effective date of the Contractual Relationship.

The Processor may Process the Personal Data transmitted by the Controller for as long as necessary for the performance of the assignment as specified in the Contractual Relationship or Annex 1 of this DPA.

Article 4: Obligations of the Processor

The Processor agrees to comply with the following obligations:

Article 4.1: Data Processing:

The Processor agrees to Process the Data in accordance with the written instructions of the Controller set out in the Contractual Relationship or in Annex 1 of this DPA.

Should the Processor reasonably consider that an instruction constitutes a violation of the GDPR or another provision of EU or Member State law on Data Protection ("**Challenged Instruction**"), it shall immediately inform the Controller of such situation.

Upon providing such notification, the Processor shall be entitled to suspend performance of the Challenged Instruction and to continue to Process the Personal Data in accordance with previously provided instructions. The Controller shall not be entitled to any indemnity or damages for such stay in performance.

If the Processor is required under European Union law or the law of the Member State under which it operates to transfer Personal Data to a third country or an international organisation, it shall inform the Controller of this legal obligation prior to Processing, unless the relevant law prohibits such information for substantial reasons of public interest.

Article 4.2: Confidentiality:

The Processor undertakes to guarantee the confidentiality of the Personal Data Processed within the context of the Contractual Relationship between the Parties.

To this end, access to Personal Data shall be strictly limited to persons who must have access to or have knowledge of the Personal Data within the framework of the execution of the Contractual Relationship between the Parties.

The confidentiality obligation shall remain in effect after the termination of the Contractual Relationship between the Parties.

Article 4.3: Authorised persons:

The Processor undertakes to ensure that persons authorised to Process Personal Data shall:

- undertake to respect the confidentiality of the Personal Data and be subject to an appropriate legal obligation of confidentiality;
- be made aware / receive training regarding the protection of Personal Data.

Article 4.4: Technical and Organisational Measures:

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the Processing as well as the risks of varying likelihood and severity to the rights and freedoms of natural persons, the Processor shall implement appropriate Technical and Organisational Measures to ensure a level of security appropriate to the risk.

These Technical and Organisational Measures shall include, *inter alia* and as appropriate, the list of applicable minimum security measures, as foreseen in appendix 2 of this DPA.

In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by Processing, in particular resulting from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

Article 4.5: Sub-Processing

The Processor may use another Processor (hereinafter the Sub-Processor).

The Processor may continue to work with Sub-Processors that had already been appointed on the effective date of the DPA and as listed in Appendix 3 of this DPA, provided the following conditions are met without undue delay:

a) the Processor must ensure in advance that the Sub-Processor can provide sufficient guarantees regarding the implementation of Appropriate Technical and Organisational Measures such that the Processing meets GDPR requirements.
b) the Processor shall contractually impose on the Sub-Processor the same Data Protection obligations as those set out in Article 4 of this DPA.

By signing this DPA, the Controller grants the Processor the general authorisation to recruit Sub-Processors.

Within the context of this general authorisation, the Processor undertakes to inform the Controller, subject to at least two (2) weeks advance notice, of the changes envisaged regarding the addition or replacement of Sub-Processors, allowing the Controller to object to these changes on reasonable grounds. Unreasonable and invalid objections shall include but are not limited to undocumented objections; reasonable and valid objections include but are not limited to situations where the Controller has documented reasons to question the ability of the Sub-Processor to protect the Personal Data and guarantee the confidentiality of these Pesonal Data. To be valid, objections must be raised before half of the advance notice has expired.

The Processor shall provide a reasoned reply to the (reasonable and valid) objections raised.

Should the Sub-Processor fail to fulfil its Data Protection obligations, the Processor shall remain fully liable towards the Controller for the performance of the Sub-Processor's obligations.

Article 4.6: Rights of data subjects

It is the responsibility of the Controller to provide the data subjects with the information pursuant to their rights (Chapter III of the GDPR). Processor does not contact data subjects unless after explicit instruction by the Controller.

To the extent possible, taking into account the nature of the Processing, and by means of appropriate Technical and Organisational Measures, the Processor shall provide all reasonable assistance to allow the Controller to fulfil its obligation to comply with requests made by data subjects to the Controller for exercising their rights.

Article 4.7: Assistance to the Controller with respect to the impact assessment and prior consultation:

The Processor shall assist the Controller in ensuring compliance with its obligations with respect to impact assessment and prior consultation (as described in the articles 35 and 36 of the GDPR), taking into account the nature of Processing and the information available to the Processor (except to the extent such information is already available to the Controller).

Article 4.8: Personal Data Breach

The Processor shall notify the Controller of any Personal Data Breach as soon as possible after having become aware of such Personal Data Breach, without undue delay.

This notification shall be accompanied, when possible, with the following information enabling the Controller, if necessary, to notify the competent Supervisory Authority of such Personal Data Breach:

a) time, date and location of the awareness of the Personal Data Breach;
b) a detailed description of the incident including a description of the (likely) impacted Personal Data;
c) the likely consequences of the Personal Data Breach including the consequences for the impacted data subjects;
d) the likely timeframe necessary to recover the Personal Data, where appropriate;
e) the measures taken or to be taken to mitigate the effects of a Personal Data Breach; and
f) any additional information at the Controller's request to report the Personal Data Breach in accordance to the Applicable Regulations on Data Protection.

Article 4.9: Deletion or return of Personal Data

The Processor shall delete or have Sub-Processors delete all copies of the Personal Data transmitted by the Controller without undue delay, in all cases within 12 months from the date on which the service provision relating to the Processing of Personal Data expired (End Date).

At its discretion, the Controller may request, in a written notice to that effect to the Processor within 15 days of the End Date, that the Processor return a complete copy of all Personal Data.

The Processor shall respond to any such written request without undue delay and at the latest within 3 months of the End Date.

If, under European Union law or the law of a Member State, the Processor is required to retain the Personal Data transmitted by the Controller for an imposed period, the time limits indicated above shall only begin at the end of the imposed period. In such case the Processor shall ensure the confidentiality of such Personal Data and shall ensure that such Personal Data of the Controller is Processed exclusively for the purposes specified under the laws that require them to be retained.

Article 4.10: Documentation and audit rights

At the request of the Controller, the Processor shall make available all the necessary information to demonstrate compliance with this DPA and to allow audits or inspections to be carried out by the Controller itself or by an auditor appointed by the Controller for such purpose.

Standard documentation is made available by the Processor free of charge to the Processor via the Partena Professional trust platform https://tprm.partena-professional.be/SSE. For additional information and documentation, the Processor shall be entitled to a reasonable fee from the Controller, who will be informed thereof in advance

All audit requests shall be submitted in writing by the Controller at least 15 working days in advance.

The audit shall only take place during working hours, without substantially disrupting the Processor's business operations. The audits will be charged at a daily rate of 1.500,00 € (VAT not included). Standard documentation for the purpose of these audits shall be made available by the Processor to the Controller free of charge through the Partena Professional trust platform at https://tprm.partena-professional.be/SSE. For additional information and documentation, the Processor may charge a reasonable fee to the Controller, who will be informed thereof in advance

Article 5: Final provisions

Article 5.1: Jurisdiction and governing law

The Parties declare that the court given (sole or exclusive) jurisdiction in the Contractual Relationship between the Parties shall also have (sole or exclusive) jurisdiction over any dispute and any claims that may arise as a result of this DPA, including any disputes relating to its existence, its legal validity or its termination or the consequences of its nullity.

The Parties declare that this DPA, as well as all non-contractual or other obligations attached to this DPA, shall be governed by the laws of the country determined in the Contractual Relationship between the Parties.

Article 5.2: Conflict of terms

Unless stipulated by law, the provisions of the Contractual Relationship shall prevail should there be a conflict between this DPA and the Contractual Relationship between the Parties.

Article 5.3: Validity and enforceability

The invalidity or non-enforceability of any provision of the DPA, whatever it may be, shall not affect the validity or enforceability of any other provision of the DPA.

The corresponding provision shall be either (1) replaced by a valid and enforceable provision that is closest to the original intention of the Parties or, if this is not possible, (2) shall be interpreted as if the invalid or unenforceable provision had never been part of this DPA.

PROCESSOR	**CONTROLLER**
Duly represented by:	Duly represented by:
Name: Günther Van Weyenberg	Name:
Capacity: Chief Operating Officer	Capacity:
Date:	Date:
Signature:	Signature:
Contact information data protection officer: privacy@partena.be	Contact information data protection officer (if applicable):

ANNEX 1: DETAILS RELATING TO THE PROCESSING OF THE CONTRACTING PARTY'S PERSONAL DATA

This Annex 1 contains certain details regarding the Processing of the Personal Data transmitted by the Controller, as stipulated in Article 28(3) of the GDPR.

Purpose and duration of the Processing of the Personal Data transmitted by the Controller

The purpose and duration of the Processing of the Personal Data transmitted by the Controller are described in the Contractual Relationship and this Annex

Nature and purpose (aim) of the Processing of the Personal Data transmitted by the Controller

Calculation of gross and net remuneration, social security contributions, withholding tax and other authorized deductions, in accordance with the legal and regulatory provisions and the instructions of the Client, as well as the preparation of social documents and the processing of social declarations and tax.

Seen the legal obligations of the Processor as a recognized payroll office, the retention by the Processor of all Personal Data processed is 7 years after the year following the processing of this Personal Data.

Types of Personal Data transmitted by the Controller

Personal identification data, financial identification data, studies, personal characteristics, wages, profession & employment, presence, work organization.

In no case shall the Processor Process Personal Data as referred to in Articles 9 and 10 GDPR.

Categories of Interested Parties to which the Personal Data transmitted by the Controller relates

The personnel and former personnel employed by the Controller.

ANNEX 2: APPLICABLE MINIMUM SECURITY MEASURES

1. Security policy

- The Processor has a security policy and security procedures in place.
  These are reviewed periodically, updated and communicated to staff and authorized third parties.

2. Organization of security

- Security responsibilities are defined and assigned at the Processor.

3. Human Resources

- The Processor's internal and external employees are made aware of the security of information and personal data in particular.

4. Asset management

- The Processor has an inventory of assets that is regularly updated.
  The rules for the use of these assets are defined and clearly communicated.

5. Physical and environmental security

- The Processor's premises where the information, data and their processing devices are located, have a secure access.
- The server rooms have specific physical protection measures. Only authorized staff has access to these server rooms.

6. Operational security

- The Processor implements antivirus and anti-malware measures to prevent any alteration or theft of data using malicious software.
  These protections are regularly updated.
- The Processor has a process for managing access requests. The employees' access is limited to the information necessary for the performance of their duties.
- Administrator rights on the systems are strictly limited to essential persons.
- The Processor has a password policy (incl. special characters and/or minimum length, regular change, multi-factor authentication).
- The use of storage media (USB, external hard disk, ..) is regulated. No data can be saved on media not belonging to the Processor.

7. Security of communications

- The Processor uses security measures to protect information transfers by using secure protocols.

8. Application or system development and maintenance

- The Processor ensures that security requirements are guaranteed during the development and maintenance of software and systems.
- Change management procedures are documented (control point and validation).
- The Processor separates the development and test environments from the production environment.
- The Processor ensures the security of the systems and performs tests before use.

9. Incident management

- The Processor has a documented incident management procedure that is communicated to staff and authorized third parties.

10. Continuity

- The Processor limits the risk of system failure through good maintenance and redundancy.
- Backup copies of the data are systematically made and kept in separate secure premises.
- A systems restoration plan is established by the Processor.
- Tests are carried out regularly and staff are made aware.

ANNEX 3: SUB-PROCESSORS

As of the date of signing this DPA, the Processor uses the following sub-processors for the services indicated in this list:

Sub-Processor	Services	Location
KEYES (formerly NRB – Network Research Belgium NV/SA) CBE 0430.502.430	Infrastructure Hosting	Belgium
Doccle PLC CBE 0846.382.408	• Provisioning of digital pay slips • Printing provider	Belgium