DATA PROCESSING AGREEMENT (DPA)

Version: 1 October 2026

Introduction

This DPA with its annexes is an attachment to the agreement (the "Agreement") between Epassi Nederland B.V. ("Epassi Nederland") and Epassi NL Platform Transactions B.V. ("Epassi Platform Transactions") respectively as service providers and the client (the "Client") as specified in the Agreement.

The DPA is used by both Epassi Nederland and Epassi Platform Transactions, meaning that the DPA applies separately to the Agreement between Client and Epassi Nederland, and to the Agreement between Client and Epassi Platform Transactions. Both Epassi Nederland and Epassi Platform Transactions are independent contracting parties which are not liable for the actions of the other.

When performing the services specified in the Agreement, Epassi Nederland and Epassi Platform Transactions may process personal data on the Client's behalf. In such cases, Epassi Nederland and Epassi Platform Transactions act as Processor, and the Client as Controller. References in this DPA to "Processor" shall be references to Epassi Nederland or Epassi Platform Transactions as the case may be (depending on the Agreement that is applied in a particular case), and references to "Controller" shall be references to the Client.

Article 1. Definitions

In this DPA, capitalized terms shall have the following meaning:

- **Autoriteit Persoonsgegevens:** the Dutch data protection supervisory authority, tasked with enforcing the compliance with applicable privacy laws and regulations.
- **GDPR:** the General Data Protection Regulation (Regulation (EU) 2016/679 of the 27th of April 2016).
- **Data Subject(s):** the natural person or persons to whom the Personal Data relates.
- **Annex(es):** each annex to this DPA. The annexes are inextricably linked to this DPA.
- **Third Party/Third Parties:** any natural person, legal entity, government agency, department or other body, not being the Processor
- **EEA:** the European Economic Area.
- **Incident:** any event whereby or as a result of which Personal Data is destroyed, altered, lost and/or unjustifiably disclosed to a Third Party or enables said Third Party to gain unauthorized access to the Personal Data.
- **Log:** the (computer)file(s) in which the processing activities are automatically recorded.
- **Personal Data:** any information relating to an identified or identifiable natural person (i.e. Data Subject) that is processed by the Processor on behalf of the Controller.
- **Sub-processor:** a party that is engaged by the Processor in order to perform its obligations under the Agreement. The Sub-processor is (mainly) tasked with the processing of Personal Data.
- **Applicable Data Protection Law:** the GDPR, the Dutch GDPR Implementation Act (Uitvoeringswet AVG) and any other applicable national and European laws and regulations on the protection of personal data.
- **DPA:** the present Data Processing Agreement and its Annexes.

Article 2. General Provisions

2.1 Controller determines the purpose and the means of the processing activities. Controller therefore falls within the scope of article 4 (7) GDPR. Processor is exclusively engaged to process Personal Data on behalf and on written instruction of the Controller. Processor therefore falls within the scope of article 4 (8) GDPR.

2.2 Processor will provide Controller with all necessary information in order to comply with the applicable privacy laws and regulations.

Article 3. Processing of Personal Data

3.1 Processor shall process the Personal Data for Controller in accordance with the applicable privacy laws and regulations. Annex 1 contains an overview of the type(s) of Personal Data that is/are processed, the categories of the Data Subjects to which the Personal Data relates and the purpose and means by which/for which the Personal Data is processed.

3.2 The Processor shall only process Personal Data in accordance with the Controller's instructions. The Processor will only deviate from these instructions if it is legally obliged to do so, or if compliance with an instruction would result in a breach of laws or regulations.

3.3 When processing Personal Data, the Processor shall not deviate from the purpose for which the Personal Data was originally provided by the Controller, unless it is obliged to do so on the grounds of a statutory provision.

3.4 The Processor shall not provide the Personal Data to a Third Party, unless this exchange takes place on the written instruction and/or with the written consent of the Controller. The Processor is also allowed to provide the Personal Data to a Third Party, if the exchange is necessary to comply with a legal obligation.

3.5 Processor shall ensure that the Personal Data will not be processed outside of the EEA, unless Controller has given its written consent.

3.6 If Processor has received permission from the Controller to process the Personal Data outside of the EEA, the Processor shall implement appropriate safeguards to protect the Personal Data, including the use of the standard contractual clauses provided by the European Commission (Implementing Decision (EU) 2021/914) and/or only processing or transferring Personal Data on the basis of an adequacy decision (article 45 GDPR) and/or approved certification mechanisms (article 42 GDPR).

Article 4. Technical and organizational measures

4.1 In accordance with article 32 GDPR, the Parties shall take and maintain appropriate technical and organizational measures to ensure an appropriate security level relative to the associated risk(s). Annex 2 gives an overview of the technical and organizational measures taken by the Processor. These measures will be periodically evaluated and, if necessary, amended.

4.2 When implementing security measures, the Processor will take 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 for the rights and freedoms of the Data Subject.

4.3 The Processor shall maintain an audit trail of relevant processing activities (e.g. system logs) sufficient to demonstrate compliance with this DPA. Upon the Controller's request, the Processor will provide access to such logs without undue delay.

Article 5. Assistance

5.1 Processor shall, to the extent required by article 28, section 3 (f) of the GDPR, provide all reasonable assistance to Controller to enable Controller to comply with its obligations under the GDPR, such as with respect to security, data breaches and data protection impact assessments, considering the information available to and the role of Processor, and to the extent that the Controller does not have access to the relevant information itself. Processor shall be entitled to charge its reasonable internal costs and expenses incurred because of its compliance with this article.

5.2 As soon as the Processor receives a request from a Data Subject, such as a request for information, access, rectification, erasure, restriction of processing and/or data portability (articles 13 – 20 GDPR), or any other right that the Data Subject might invoke, this request shall be forwarded to the Controller without undue delay.

5.3 The Processor shall provide all reasonable assistance to the Controller after the latter receives a request from the Data Subject, so that the Controller might be able to fulfil its statutory obligations under the applicable privacy laws and regulations.

Article 6. Audits

6.1 The Controller shall have the right, at its own expense, to conduct audits of the Processor's systems, processes, and records directly involved in processing the Controller's Personal Data under this DPA. Audits shall be conducted no more than once per calendar year per Controller, except in cases of a suspected Incident, legal requirement, or as otherwise agreed in writing. The Controller shall provide reasonable prior written notice of at least thirty (30) days before any audit. The Processor shall provide reasonable assistance to facilitate such audits, including, after consultation with the Controller, access to relevant personnel, systems, and records directly relating to the processing activities covered by this DPA.

6.2 The costs of the audit shall be borne by the Controller. If the audit demonstrates material non-compliance by the Processor with this DPA, the reasonable costs of the audit shall be borne by the Processor.

6.3 The Processor shall provide all reasonable assistance to any investigation conducted by the Autoriteit Persoonsgegevens or any other relevant supervisory authority into the Processor's processing activities. The Processor shall notify the Controller without undue delay upon becoming aware of such an investigation, unless prohibited by law from doing so.

Article 7. Incidents

7.1 Upon becoming aware of a security incident which has led, or is reasonably likely to have led, to a personal data breach (as defined by the GDPR), the Processor shall notify the Controller without undue delay and, in any case, no later than the end of the next business day.

7.2 The Processor shall take all reasonable measures to limit the consequences of the Incident and/or prevent a new Incident. Processor shall also provide all reasonable cooperation to Controller in assessing the Incident, so that the latter can comply with its statutory obligations consisting of notifying the competent supervisory authorities and/or informing the Data Subjects.

Article 8. Sub-processors

8.1 The Controller hereby grants permission to the Processor to engage Sub-processors for the performance of the Agreement. The current list of Sub-processors engaged by the Processor is

available at www.epassi.nl/static/subverwerkers. The use of specific Sub-processors may vary depending on the Services and features selected by the Controller, and not all listed Sub-processors will apply to every Controller.

8.2 If the Processor wishes to engage or replace a Sub-processor, it must inform the Controller thereof. The Controller is then entitled to object to this proposal within a term of fourteen (14) days after receipt of the notification. If the Controller does not object within fourteen (14) days after receipt of the information regarding the intended change, it shall be deemed to have authorized the intended change.

8.3 The Processor shall enter into an agreement with the Sub-processors that it has engaged. This agreement must be in accordance with the applicable privacy laws and regulations. The Processor will impose terms and conditions that are substantially equivalent to those set out in this DPA on the Sub-processor.

Article 9. Confidentiality

9.1 The Processor shall keep all Personal Data that it processes on behalf of the Controller confidential. The provisions on confidentiality in the general terms and conditions applicable to the Agreement apply.

9.2 The Controller shall treat all information regarding the Processor's security measures, IT systems, Sub-processors and internal processes that it obtains under this DPA, including information provided in the context of an audit, as confidential and shall not disclose it to third parties, except to the extent required by a legal obligation.

Article 10. Term and Termination

10.1 This DPA shall enter into force at the time of conclusion of the Agreement and shall continue to be in force for as long as the Agreement is in force. The DPA shall end by operation of law upon termination of the Agreement. Obligations of a permanent nature shall remain in force between the Parties after the DPA has been terminated and/or ended (by operation of law).

10.2 The Processor's obligations regarding the return and deletion of Personal Data upon termination are set out in Annex 1 (Processing Details).

10.3 In the event of bankruptcy, this DPA shall remain in full force and effect between the Parties, in order to enable the continuity of the processing within the context in which the Personal Data were initially provided.

Article 11. Final Provisions

11.1 The provisions on applicable law and competent court in the Agreement apply to this DPA.

11.2 In the event of a conflict between this DPA and the Agreement, this DPA shall prevail insofar as the processing of Personal Data is concerned.

Annex 1: Processing Details

1. Categories of Data Subjects

The individuals to which the Personal Data relates are:

- Employees of Controller.

2. Types of Personal Data

The types of Personal Data processed by the Processor are:

In case Epassi Nederland B.V. is the Processor:

The following Personal Data is always processed by Epassi Nederland B.V.:

- First name;
- Last name;
- Date of birth;
- Hire date;
- Contract end-date;
- IP address;
- Coarse location based on IP address;
- Business email address;
- Private email address upon Controller request;
- Benefit transactions made;
- Employee ID;
- In case sports subscriptions (corporate fitness) are provided:
  - Gender
  - Full address
  - Phone number
  - IBAN information

In case Epassi NL Platform Transactions B.V. is the Processor:

The following Personal Data is always processed by Epassi NL Platform Transactions B.V.:

- First name;
- Last name;
- Business email address;
- Private email address (if requested by Controller);
- Benefit transactions made;
- In case sports subscriptions (corporate fitness) are provided:
  - Gender
  - Full address
  - Phone number
  - IBAN information

3. Nature and purpose of processing

Processor processes the Personal Data for the following purposes:

In case Epassi Nederland is the Processor:

- Providing the services as agreed in the Agreement, including in particular offering the Epassi Platform to Controller for managing their employee benefits, creating and managing employee accounts in the Epassi Platform, creating and acquiring third-party benefits (including transferring Personal Data to third party partners that offer such benefits);
- Storage of the Personal Data in the back-end of the Epassi Platform;
- Accessing the Personal Data in the back-end through the Epassi Platform for the purpose of presenting the Personal Data to users in the front-end;
- To provide support to employees of Controller in regards to their usage of the Epassi Platform;
- To communicate with employees of Controller around the functionalities and updates in regards to the Epassi Platform;
- To analyze usage patterns and improve the Epassi Platform's performance, user experience, and service offerings;
- To monitor and ensure the security and integrity of the platform, including preventing unauthorized access and addressing security incidents;
- To provide the Controller with a web portal for analyzing usage by the employees of Controller and managing the Epassi Platform.

In case Epassi Platform Transactions is the Processor:

- To access and process all data relating to benefits purchased on behalf of Controller in order to invoice/set-off the value of the benefits in accordance with the Agreement.

The Personal Data is **not processed** for the following purposes:

- To perform analysis and/or create reports on the usage of benefits in a non-anonymised way;

Retention period for the Personal Data

- Following the termination of the business relationship, the Controller shall have a period of thirty (30) days (the "Retention Period") to request the export or deletion of Personal Data. During the Retention Period, the Controller may instruct the Processor to either: a. export the Personal Data in a commonly used, machine-readable format, or b. delete the Personal Data.
- Upon either receiving a request from the Controller to delete Personal Data or the expiration of the Retention Period, whichever occurs first, the Processor shall, within a maximum period of thirty (30) days: a. permanently delete or destroy all Personal Data, or b. anonymize all Personal Data to ensure that the data subjects are no longer identifiable, unless longer storage is required by law. In addition, the Processor shall ensure that any Personal Data present at its Sub-processors shall be deleted, destroyed, or anonymized as well.
- The Processor shall confirm in writing to the Controller that all Personal Data has been deleted, destroyed, or anonymized in accordance with this clause within ten (10) days following the completion of such actions.

4. Processing outside of the EEA

The Personal Data is primarily processed within the European Economic Area (EEA). While the Processor uses Sub-processors that may have their headquarters outside the EEA, any transfer of Personal Data

outside the EEA shall only occur in compliance with GDPR Chapter V, including the use of appropriate safeguards such as Standard Contractual Clauses or other lawful transfer mechanisms.

Contact details

For questions or comments regarding this DPA and the Annexes thereof, please contact the representative of the Processor:

S. Cune, DPO, privacy@epassi.nl

Annex 2: Technical and Organisational Measures

This Annex contains the technical and organizational measures implemented by the Processor to protect Personal Data. The measures included in this Annex may be amended and/or expanded upon if and when necessary. Controller considers the measures listed below to be appropriate to mitigate the level of risk that is involved when outsourcing certain processing activities to the Processor.

1. Technical measures

- The Processor holds an ISO/IEC 27001:2022 certification. The Processor shall provide a copy of the certificate and the statement of applicability upon request.
- Processor uses Amazon Web Services as a cloud provider. Amazon Web Services is among others: ISO/IEC 27001:2022, 27017:2015, 27018:2019, 27701:2019, 22301:2019, 9001:2015, and CSA STAR CCM v4.0 certified.
- Processor uses encryption at rest and in transit for its storage system, namely AWS RDS and AWS S3 that is secured with AES-256.
- Human error risk mitigation
  - The passwords and credentials for the internal systems are stored in a password manager application that is subject to audit.
  - Any data request, even from internal team members, will first be scrutinized and assessed in order to preserve confidential data and to have an audit trail of the action.
- Access to cloud services
  - The services are not exposed to the internet but are behind a Virtual Private Cloud that can only be accessed with the appropriate credentials.
- Hardening policies
  - Processor uses a CVE (Common Vulnerabilities and Exposures) scanner for all software packages and images and only promotes safe builds to its production environment.
- Auditing and monitoring
  - In order to automatically keep an acceptable level of security the Processor continuously monitors its platform for the following: SSL certificates for the API; AWS audit trail for resource access; server level resource access; database connection access.
- The data can only be accessed by the system engineers and staff who have been granted explicit access and training to view the data.
- The communication between the mobile application and the Epassi Platform API is accomplished via HTTPS connection and the authentication and authorization process is secured using JWT (JSON Web Token).
- Employee hardware is enrolled into JAMF MDM and is encrypted, remotely accessible and can be locked and wiped in case of loss or damage. The Processor uses a continuous vulnerability scanner for its customer facing services using intruder.io instead of scheduled pen tests. This offers real time protection against new and developing CVEs.

2. Organizational measures

- An Incident Response Plan is in place to offer guidance for employees or incident responders who believe they have discovered or are responding to a security incident.

- The Processor offers guidance and training to employees in order to help them identify phishing and social engineering.
- Employees of the Processor only have access to personal data if and as soon as permission has been granted.
- There is an exit procedure. This describes the steps to be taken to technically deny access to the various systems and offices, so that a former employee cannot gain unwanted access to these systems.
- Internal Information Security Policy. The following security guidelines are in place and apply to all employees:
  - Google Workspace 2FA / MFA is mandatory and must be set up within 24 hours of creation of the employee account;
  - Always use Google SSO to log in to other accounts and enable 2FA / MFA;
  - Secure your work laptop and phone with a password and do not leave it unlocked/open and unattended;
  - Do not leave passwords or important notes on paper around the office;
  - Do not allow unauthorized access to the office;
  - Store all passwords and sensitive data in 1password;
  - Be wary of phishing and scamming attempts. Do not click on suspicious links;
  - Do not share passwords in clear text via email, SMS or Slack. Instead use 1password;
  - Do not store sensitive customer data (emails, names, other PII) on your personal devices.