PTTRNS Intelligence B.V.
Marconilaan 16
5621 AA Eindhoven
The Netherlands

VAT: NL856261282B01
KVK: 65791703
IBAN: NL12 INGB 0007 4349 51

+31 (0)40 747 0655
info@pttrns.ai
www.pttrns.ai

Data Processing Agreement

Data of publication: February 14th, 2022

This Data Processing Agreement (the “DPA”) supplements the commercial agreement (“Agreement”) between PTTRNS Intelligence BV (“PTTRNS”) and the customer that has executed or agreed to the Agreement (“Customer”). Capitalized terms used, but not defined, in this DPA are defined in the Agreement.

Nature of the Data and Role of the Parties.

The rights and obligations in this DPA apply solely to the Processing of Personal Data by the Services by PTTRNS on behalf of Customer, but does not apply to Beta Services. For the purposes of this DPA, references to Customer Data refer to any Personal Data incorporated in the Customer Data.

Data Processing.

Instructions

The Agreement and this DPA constitute Customer’s instructions to PTTRNS to Process Customer Data. PTTRNS will use and Process Customer Data as Customer instructs in order to deliver the Services and to fulfil PTTRNS’s obligations under the Agreement and this DPA. PTTRNS will inform Customer of any legal requirement which prevents it from complying with Customer’s instructions, unless prohibited from doing so by applicable law.

Processing Activities

PTTRNS, its staff, and Sub-processors will only Process Customer Data to provide the Services and to fulfil PTTRNS's obligations in this Agreement. The categories of Personal Data to be Processed by PTTRNS and the Processing activities to be performed under this Agreement are set out in Exhibit A.

Personnel
Any PTTRNS personnel who have access to Customer Data will be bound by appropriate confidentiality obligations.

Security

Security Measures.
PTTRNS will implement the technical and organizational measures set forth in the Agreement for the applicable Services, the current version of which are listed in Exhibit B.

Security Incidents.
PTTRNS will promptly, and without undue delay, notify Customer in writing at the email address associated with the account if a Security Incident occurs, so long as applicable law allows this notice. Without limiting the foregoing, PTTRNS will use commercially reasonable efforts to provide this notice within 72 hours of confirming the existence of a Security Incident. PTTRNS may limit the scope of, or refrain from delivering, any disclosures to the extent reasonably necessary to avoid compromising the integrity of our security, an ongoing investigation, or any PTTRNS customer's or end user's data. "Security Incident" in this context means any actual unauthorized disclosure of or access to Customer Data, or compromise of PTTRNS's systems that we determine is reasonably likely to result in such disclosure or access, caused by failure of PTTRNSs Security Measures and excluding any unauthorized disclosure or access that is caused by Customer or its End Users, including Customer or its End Users' failure to adequately secure equipment or accounts.

Notification

PTTRNS will assist the Customer in ensuring compliance with its obligations pursuant to EU Data Protection Laws by providing relevant information which may include:

- The nature of the Security Incident, including, where possible, the categories and approximate number of personal data records concerned
- The estimated consequences of the Security Incident
- The measures taken or to be taken to address the Security Incident, including, where appropriate, the measures to mitigate its possible adverse effect
- The name and contact details of the Data Protection Officer or other contact from whom more information may be obtained;

Should it not be feasible for PTTRNS to provide all of the relevant information in its initial notification to the Customer, we will provide further relevant details without undue delay.

Sub-processors.

Use of Sub-Processors
Customer consents to PTTRNS's appointment of Subcontractors, including Sub-processors, to perform the Services. Where a Sub-processor will process Personal Data, PTTRNS will

ensure that the Sub-processor is subject to substantially similar data protection obligations as those set forth in this DPA regarding Personal Data and which satisfy the requirements of EU Data Protection Laws. PTTRNS will list its current Sub-processors on their website. PTTRNS will remain liable for all acts or omissions of its Subcontractors or Sub-processors, and for any subcontracted obligations.

Customer Objections

PTTRNS may add or remove Sub-processors from time to time. PTTRNS will inform Customer in advance of new Sub-processors for the applicable Services as described in the list of Sub-processors. If Customer objects to a change, it will provide PTTRNS with notice of its objection to privacy@pttrns.ai including reasonable detail supporting Customer's concerns within sixty days of receiving notice of a change from PTTRNS. PTTRNS will then use commercially reasonable efforts to review and respond to Customer's objection within thirty days of receipt of Customer's objection. PTTRNS's response to Customer's objection will include reasonable accommodations that Customer or PTTRNS can take to limit or prevent a new unwanted Sub-processor from acting as a processor of Customer Data when Customer makes use of the Services. If PTTRNS does not respond to a Customer objection as described above, or cannot reasonably accommodate Customer's objection, Customer may terminate the Agreement by providing written notice to PTTRNS.

Data Subject Rights

Customer is responsible for responding to any request by a data subject to exercise their rights under applicable privacy laws. If PTTRNS receives any such request in relation to the Customer Data, PTTRNS will direct the applicable data subject to Customer to exercise his or her rights without undue delay after verifying the request pertains to Customer Data.

Compliance Assistance

To assist Customer with its compliance obligations under applicable privacy laws related to security, data protection impact assessments, and prior consultation with supervisory authorities, PTTRNS will make the following available during the Term

- The information contained in Exhibit A
- Applicable Security Measures and Security Resources set forth in Exhibit B.

If, after reviewing the aforementioned materials, Customer reasonably believes it needs further information in order to meet its compliance obligations, PTTRNS will use commercially reasonable efforts to respond to written questions by Customer regarding the materials. Without limiting the foregoing, PTTRNS will comply with valid requests from relevant supervisory authorities to the extent required by applicable EU Data Protection Law.

Deletion

Upon Termination of the Agreement and this DPA, PTTRNS will delete Stored Data in Customer's account in a commercially reasonable period of time following receipt of an Administrator's request to do so prior to such termination. Notwithstanding the foregoing, Customer acknowledges and agrees that PTTRNS may be a controller with respect to certain Account Data, and may retain this data in accordance with applicable privacy laws, provided that PTTRNS is solely responsible for its compliance with these laws in connection with its own Processing.

Inspections and assurances

Customer Review

If Customer reasonably believes it needs information in order to confirm PTTRNS's compliance with the provisions of the Agreement relating to Personal Data, PTTRNS will use commercially reasonable efforts to respond to written questions by Customer.

Customer Inspection.

If Customer is not satisfied with PTTRNS's responses to questions provided pursuant to, PTTRNS will permit an agreed upon Customer representative, subject to appropriate confidentiality obligations, to visit PTTRNS's premises and discuss PTTRNS's responses with PTTRNS personnel.

Process for Inspections

PTTRNS reserves the right to:

- Charge a separate fee for its reasonable costs associated with performing any of its obligations with regards to such inspections or review inquiries. PTTRNS will provide an estimate of these fees to Customer prior to incurring the costs.
- Object to any Customer representative participating in an inspection on the basis that they are not qualified, are not bound by an adequate requirement to protect confidential PTTRNS information, or are a competitor of PTTRNS.

Customer inspections can take place only after Parties mutually agree on the scope, timing, and duration of the inspection. PTTRNS reserves the right to limit the scope and duration of an inspection to the extent reasonably necessary to avoid compromising the integrity of PTTRNS's security or any PTTRNS customer's or end user's data.

European Data

Customer agrees that PTTRNS and its Sub-processors may transfer, store, and Process Customer Data in locations other than Customer's country. Personal Data that is subject to EU Data Protection Laws will only be Processed inside the EEA, United Kingdom, or Switzerland.

Insurance

PTTRNS maintains a liability insurance, which may include coverage for privacy and network security liability, losses or damages due to the unauthorized use/access of a computer system or database, and defense of any regulatory action involving a breach of privacy, as well as other coverage areas. Upon Customer's reasonable written request, and no more than once per year, PTTRNS will provide a certificate of insurance evidencing its coverages.

Effect of DPA

If a provision in this DPA conflicts with a provision in the Agreement, then this DPA will prevail with respect to the processing of Personal Data. The Agreement will remain in full force and effect and will be unchanged except as modified by this DPA. This DPA will terminate automatically upon expiration or termination of the Agreement.

Exhibit A: Details of processing

Subject Matter of the Personal Data Processing

The provision of the Services by PTTRNS to Customer.

Duration of the Personal Data Processing

The Term, and any period after the Term prior to PTTRNS's deletion of Customer Personal Data.

Nature and Purpose of the Personal Data Processing

To enable Customer to receive and PTTRNS to provide the Services.

Categories of Personal Data

The Personal Data that will be included in Customer Data will depend upon Customer's use of the Services. To the extent the Customer Data contains Personal Data, it may consist of identifying information of end users (such as name, photo's, email address, physical address, IP address, or other unique identifier), identifying information of third parties with whom data is shared, organization data. and any other Personal Data contained in documents, images and other content or data in electronic form stored or transmitted by End Users via the Services.

Data Subjects

The categories of data subjects will depend upon Customer's use of the Services. To the extent the Customer Data contains Personal Data, it may concern Customer's End Users including employees, contractors, collaborators and customers of the Customer, any individuals collaborating, sharing, or transacting with these End Users, or any other individual whose information is stored by Customer in the Stored Data as identified in records maintained by Customer acting as controller pursuant to Article 30 of the GDPR.

Exhibit B: Technical and Organizational Measures

Data Privacy Contact

The data privacy officer of the Data Importer can be reached at privacy@pttrns.ai

Security Measures

The Data Importer has implemented and will maintain appropriate administrative, technical and physical safeguards to protect personal data as further described below. Data Importer may update these security measures from time to time, provided that Data Importer will notify Data Exporter if Data Importer updates the security measures in a manner that materially diminishes the administrative, technical or physical security features.

1. Service Security

1.1 *Architecture*. Data Importer's Services are designed with multiple layers of protection, covering data transfer, encryption, network configuration and application-level controls that are distributed across a scalable, secure infrastructure. The service can be utilized and accessed through a number of interfaces. Each has security settings and features that process and protect Customer Data while ensuring ease of access.

1.2 *Reliability*. Data Importer's Services are developed with multiple layers of redundancy to guard against data loss and ensure availability.

1.3 *Encryption*. To protect Customer Data in transit between the Customer and Data Importer, Data Importer uses Secure Sockets Layer (SSL)/Transport Layer Security (TLS) for data transfer. Stored Data at rest is encrypted. Data Importer's encryption key management infrastructure is designed with operational, technical and procedural security controls with limited direct access to keys.

1.4 *User Management Features*. Data Importer's service allows for the use of an authentication procedure which adds an extra layer of protection.

1.5 *External Data Centers*. Data Importer's corporate and production systems are housed at third-party subservice organization data centers hosted by reputed Cloud Providers, which at present include AWS, Azure, Hertzner and Google.

2. Information Security

2.1 *Policies*. Data Importer has established a thorough set of security policies covering areas of information security, physical security, incident response, logical access, physical production access, change management and support. These policies are reviewed and approved at least annually. Data Importer personnel are notified of updates to these policies and are provided security training.

2.2 *Personnel Policy and Access*. Data Importer's internal policies require onboarding procedures that include security policy acknowledgement, communicating updates to security policy, and non-disclosure agreements. All personnel access is removed when an employee or contractor leaves the company. Data Importer employs technical access controls and internal policies to prohibit employees or contractors from arbitrarily

accessing file data and to restrict access to metadata and other information about end users' accounts. In order to protect end user privacy and security, only a small number of employers or contractors have access to the environment where end user files are stored.

2.3 *Network Security*. Data Importer maintains network security and monitoring techniques that are designed to provide multiple layers of protection and defence. Data Importer employs industry-standard protection techniques such as firewalls and network monitoring.

2.4 *Change Management.* Data Importer ensures that security-related changes have been authorized prior to implementation into the production environments. Source code changes are initiated by developers that would like to make an enhancement to a Data Importer application or service. Changes to Data Importer's infrastructure are restricted to authorized personnel only.

3. Physical Security

3.1 *Infrastructure*. Physical access to subservice organization facilities where production systems reside are restricted to personnel authorized by Data Importer, as required to perform their job function. Any individuals requiring additional access to production environment facilities are granted that access through approval by appropriate management.

3.2 *Office*. Data Importer maintains a physical security service that is responsible for enforcing physical security.