DATA PROCESSING AGREEMENT

This Data Processing Agreement ("DPA"), including its Annexes, describes the Parties' obligations under applicable data protection laws with respect to the Processing of Personal Data.

This DPA is between Customer, as identified on the signed Order Form, and Krane Labs bv, a limited liability company having its registered seat in Gent, at Sint-Baafsplein 10, 9000 Gent, Belgium and registered in the Belgian Crossroads Bank for Enterprises under number BE1004567533 ("Service Company" or "Krane Labs").

Krane Labs and Customer together will be referred to as the "Parties".

DEFINITIONS

In this DPA, the following terms have the meanings set forth below. Capitalised terms used but not defined herein shall have the meaning set forth in the Master Services Agreement ("MSA") or Professional Services Agreement ("PSA").

TERM	MEANING
Main Agreement	The agreement between Customer and Service Company for the provision of Services, including the applicable MSA or PSA and Order Form ("Main Agreement").
Data Protection Laws	All applicable legislation relating to data protection and privacy, including, without limitation, the EU General Data Protection Regulation, all local laws and regulations which amend or replace any of them, together with any national implementing laws in any Member State of the European Economic Area (EEA), to the extent applicable, and in any other country, as amended, repealed, consolidated or replaced from time to time.
Employee	Employee, part-time or full-time, on payroll, agent, director, or long-term contractor of Customer or its affiliates.
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data.
Partner Companies	Companies not related to Customer, but essential for the project for which Krane Labs provides Services, such as software development companies, key suppliers, other processors and their Employees.
Services	The services provided by Krane Labs to Customer under the Main Agreement, including the applicable Order Form or statement of work.
Standard Contractual Clauses	The standard contractual clauses for international transfers adopted by the European Commission, including Commission Implementing Decision (EU) 2021/914 of 4 June 2021, or any successor clauses replacing them.
Sub-processor	Any third person, entity or company engaged by Processor to Process Personal Data in the provision of the Services under the Main Agreement.

The terms "Commission", "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", "Processor", "Processing" and "Supervisory Authority" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

1. PURPOSE

1.1. Scope

Krane Labs has agreed to provide Services to Customer in accordance with the terms of the Main Agreement.

Krane Labs as Data Processor: The Parties agree that, with regard to the Processing of Personal Data, Customer may act either as Controller or Processor and Krane Labs is Processor or Sub-Processor for all Personal Data Processed on behalf of Customer, except for Customer Relationship Data as set forth below.

Krane Labs as Data Controller: The Parties agree that, with regard to the Processing of Customer Relationship Data, Krane Labs is an independent Controller and not a joint Controller with Customer. Krane Labs may Process Customer Relationship Data as Controller:

- to manage the relationship with Customer;
- to carry out Krane Labs' core business operations, such as accounting and filing taxes;
- to detect, prevent, or investigate Data Breaches, fraud, and other abuse or misuse of the Services;
- to comply with applicable law; and
- as otherwise permitted under Data Protection Laws and in accordance with this DPA, the Main Agreement, and Krane Labs' Privacy Policy.

The scope of this DPA is limited to situations where Krane Labs is a Data Processor and Customer is either the Controller, or where Krane Labs is a Sub-processor and Customer is the Processor. Processing for which Krane Labs acts as an independent Controller is governed by Krane Labs' Privacy Policy and applicable Data Protection Laws, unless expressly agreed otherwise.

In this DPA, "Controller" means Customer and "Processor" means Krane Labs, unless expressly stated otherwise.

The Processing activities, Personal Data and categories of Data Subjects for which Krane Labs Processes Personal Data on behalf of Customer are identified in Annex A.

2. OBLIGATIONS

2.1. Controller Obligations

Controller is responsible for the Personal Data which Processor will Process and shall ensure compliance with all Data Protection Laws, including requirements pertaining to the transfer of Personal Data under this DPA and the Main Agreement. Controller warrants that it has the right to Process the Personal Data and the right to appoint Processor to Process Personal Data on behalf of Controller.

Controller agrees that, without limitation of Processor's obligations under this DPA, Controller is solely responsible for its use of the Services, including:

(a) making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Personal Data;

(b) securing the account authentication credentials, systems and devices Controller uses to access the Services;

(c) securing Controller's systems and devices that it uses with the Services; and

(d) ensuring that any Personal Data made available to Processor is limited to what is necessary for the Services and is lawfully made available to Processor.

2.2. Processor Obligations

Processor undertakes to:

(a) Process the Personal Data only in accordance with documented instructions from Controller and take necessary steps to ensure that any natural person acting under its authority who has access to Personal Data does not Process the Personal Data except upon instructions from Controller;

For the purposes of this DPA, the Main Agreement, this DPA, the applicable Order Form, and Customer's use of the Services constitute Controller's documented instructions to Processor. Processing outside the scope of those instructions requires prior written agreement between the Parties, unless required by applicable law.

(b) promptly inform Controller if, in Processor's opinion, an instruction regarding the Processing of Personal Data provided to Processor by Controller infringes applicable Data Protection Laws;

(c) implement appropriate technical and organisational measures to protect Personal Data, considering the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons; and

(d) without undue delay inform Controller if it receives a complaint or request relating to either Party's obligations under Data Protection Laws relevant to this DPA, including any compensation claim from a Data Subject or any notice, investigation or other action from a Supervisory Authority, and provide Controller with relevant details of such investigation, complaint or request unless not permitted by law or by request of the Supervisory Authority.

3. TRANSFERS AND SUB-PROCESSORS

3.1. Transfer of Personal Data

Where Personal Data relating to an EU Data Subject is transferred outside of the EEA, it shall be Processed by an entity:

(i) located in a country, territory or sector recognised by the European Commission as ensuring an adequate level of protection;

(ii) certified under an adequacy mechanism recognised under Data Protection Laws, such as the EU-US Data Privacy Framework where applicable; or

(iii) subject to appropriate safeguards under Data Protection Laws, including the Standard Contractual Clauses and supplementary measures where required.

3.2. Sub-processors

Controller consents to Processor's use of Sub-processors specified in Annex B. This list may be updated by Processor from time to time in accordance with this Section 3.2.

Processor will provide Controller the possibility to object to each new Sub-processor that will be involved solely for the scope of the Processing activities identified in Annex A.

Prior to engaging a new Sub-processor, Processor shall notify Controller thereof and provide Controller at least 14 days to object, except where Processor reasonably believes engaging a new Sub-processor on an expedited basis is necessary to protect the confidentiality, integrity or availability of the Personal Data or avoid material disruption to the Services. In that case, Processor will give such notice as soon as reasonably practicable.

If, within five days after such expedited notice or within the general objection period described above, Controller notifies Processor in writing that Controller objects to Processor's appointment of a new Sub-processor based on reasonable data protection concerns, the Parties will discuss such concerns in good faith and whether they can be resolved. Objections to new Sub-processors shall be submitted to support@krane-labs.com.

Controller acknowledges that Sub-processors may be essential to provide the Services and that objecting to the use of a Sub-processor may prevent Processor from offering the relevant Services to Controller. If the Parties are not able to mutually agree to a resolution of such concerns, Controller, as its sole and exclusive remedy, may terminate the affected Services for convenience.

All Sub-processors who Process Personal Data in the provision of Services to Controller shall comply with obligations equivalent to those set out in this DPA. Processor shall, prior to disclosure of Personal Data to any Sub-processor, carry out appropriate due diligence to assess whether the Sub-processor is capable of providing the level of protection for Controller Personal Data required by this DPA and enter into an agreement with that Sub-processor under which the Sub-processor agrees to comply with obligations equivalent to those set out in this DPA.

The latest version of the DPA and Annex B will be made available online at https://www.krane-labs.com/legal/dpa. The version applicable to Customer remains the version incorporated into or attached to the Main Agreement. Processor may update Annex B in accordance with this Section 3.2. Any other change to this DPA applies to Customer only if agreed in accordance with Section 9.2 or the Main Agreement.

3.3. AI and Customer Personal Data

Processor does not use Personal Data Processed on behalf of Customer under this DPA for training third-party AI models.

Processor does not submit Personal Data Processed on behalf of Customer under this DPA to third-party AI providers unless this is separately agreed with Customer, instructed by Customer, or necessary for a specifically agreed Service. Where such Personal Data is present and such use is agreed, the relevant provider shall be included as a Sub-processor or otherwise covered by appropriate data processing terms.

4. SECURITY

4.1. Security Measures

Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including as appropriate:

(i) the pseudonymisation and encryption of Personal Data;

(ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and Services;

(iii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and

(iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.

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

Processor may update or modify its technical and organisational measures from time to time, including to reflect changes in technology, risk, Services, or applicable law, provided that such updates do not materially reduce the overall level of protection for Personal Data.

4.2. Data Breach Notification

Processor shall notify Controller without undue delay of any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data after discovery, insofar as the Personal Data Breach is related to Processing of Personal Data by Processor in its capacity as Processor.

If the Personal Data Breach concerns Personal Data for which Processor is Controller, as described in Processor's Privacy Statement or this DPA, Processor reserves the right to treat the Personal Data Breach as Controller.

A delay in giving a Personal Data Breach notice requested by law enforcement or required in light of Processor's legitimate need to investigate or remediate the matter before providing notice shall not constitute an undue delay.

Such notices will describe, to the extent possible, details of the Personal Data Breach, including steps taken to mitigate the potential risks. Without prejudice to Processor's obligations under this Section 4.2, Controller is solely responsible for complying with Personal Data Breach notification laws applicable to Controller and fulfilling any third-party notification obligations related to Personal Data Breaches.

Processor's notification of or response to a Personal Data Breach under this Section 4.2 will not be construed as an acknowledgement by Processor of any fault or liability with respect to the Personal Data Breach.

5. AUDIT

5.1. Audit Scope

Processor will maintain records of its Processing activities carried out on behalf of Controller and will make available to Controller the information reasonably necessary to demonstrate its compliance with the obligations set out in this DPA.

Processor may limit the scope of information made available to Controller if Controller is a competitor of Processor, provided that such limitation does not violate Data Protection Laws.

Controller's inspection rights under this DPA do not extend to Processor's employee payroll, personnel records, internal security-sensitive information, trade secrets, information relating to other customers, or any portions of its sites, books, documents, records, or other information that do not relate to the Services or the Processing of Controller Personal Data.

5.2. Audit Process

Subject to thirty days prior written notice from Controller and at Controller's additional expense, including all reasonable costs and fees for any and all time Processor expends on such audit in addition to the rates for Services performed by Processor, Processor and Controller shall mutually agree to appoint a third-party auditor to verify that Processor is in compliance with the obligations under this DPA.

In no event shall the Parties agree to a third-party auditor that is a competitor of Processor. Audits and inspections will be carried out at mutually agreed times during regular business hours. Controller shall be entitled to exercise this audit right no more than once every twelve months.

5.3. Confidentiality

All information obtained during any request for information or audit will be considered Processor's Confidential Information under the Main Agreement and this DPA. The results of the inspection and all information reviewed during such inspection will be deemed Processor's Confidential Information.

The third-party auditor may only disclose to Controller specific violations of this DPA, if any, and the basis for such findings, and shall not disclose any of the records or information reviewed during the inspection.

6. DATA PROTECTION IMPACT ASSESSMENTS AND PRIOR CONSULTATIONS

6.1. Assistance

Processor shall assist Controller with undertaking an assessment of the impact of Processing Personal Data under Article 35 GDPR and with any consultations with a Supervisory Authority under Article 36 GDPR, if and to the extent such assessment or consultation is required under Data Protection Laws and where Processor is allowed and/or required to cooperate.

Such assistance shall be provided at Controller's expense unless otherwise agreed in the Main Agreement or Order Form.

7. DATA SUBJECT RIGHTS

7.1. Assistance

If Processor receives a request from a Data Subject in relation to Controller Personal Data, Processor will advise the Data Subject to submit their request to Controller and/or forward the request to Controller, and Controller will be responsible for responding to any such request.

Upon Controller's request and at Controller's expense, Processor will provide Controller with such assistance as it may reasonably require to comply with obligations under Data Protection Laws to respond to requests from Data Subjects to exercise their rights under Data Protection Laws, such as rights of access, rectification, erasure, restriction, portability and objection, in cases where Controller cannot reasonably fulfil such requests independently via its access to Processor's products and Services.

8. MISCELLANEOUS

8.1. Confidentiality

Processor shall keep confidential all Personal Data and shall ensure that all employees, agents, officers and contractors having access to or being involved with the Processing of Personal Data are aware of the confidential nature of the Personal Data, are contractually bound to keep the Personal Data confidential, and are informed of and comply with the obligations of this DPA.

8.2. Liability

Any and all liability arising out of this DPA will be governed by the relevant provisions of the Main Agreement, including limitations of liability.

Notwithstanding the provisions of the Main Agreement, each Party shall only be liable to the other Party for damages it causes the other Party by a breach of this DPA. These damages shall be clearly demonstrated.

Processor will only be liable for damage caused by Processing where it has not complied with obligations of Data Protection Laws specifically directed to processors or where it has acted outside of or contrary to Controller's lawful instructions as described in this DPA. In that context, Processor will only be liable if Controller proves that Processor is responsible for the event giving rise to the damage.

Nothing in this DPA shall limit any rights a Data Subject may have directly under applicable Data Protection Laws. As between the Parties, Controller shall remain responsible for the lawfulness of the Processing, the content and accuracy of the Personal Data, the instructions given to Processor, and communications with Data Subjects and

Supervisory Authorities, except to the extent Processor is directly responsible under Data Protection Laws.

8.3. Term and Termination

The term of this DPA shall coincide with the commencement of the Main Agreement and/or use of the specific product or Service as included in Annex A.

This DPA shall terminate automatically together with termination of the Main Agreement and/or use of the specific product or Service as included in Annex A, whichever is terminated first.

Upon termination of this DPA, Processor shall, upon Controller's request, return the Personal Data to Controller or to a Processor nominated by Controller, or delete the Personal Data, unless Processor is required to retain a copy in accordance with applicable law.

Where the Services concern Customer-owned cloud accounts, projects, clusters, repositories, or systems, Customer remains responsible for revoking Processor's access to those environments at termination or offboarding. Once such access is revoked, Processor no longer has access to Personal Data in those environments. If Processor separately holds electronic Controller Personal Data outside Customer-owned environments that is no longer necessary for the Services or for legal, accounting, compliance, or administrative obligations, Processor shall delete or destroy such Personal Data upon request or at the end of the applicable retention period.

9. FINAL PROVISIONS

9.1. Entire Agreement

This DPA constitutes a part of the Main Agreement. All rights and obligations stemming from the Main Agreement are also applicable to this DPA. Annex A and Annex B constitute an integral part of this DPA.

9.2. Amendment by Agreement Only

No variation of this DPA shall be valid unless it is in writing and signed by authorised representatives of each Party, except for updates to Annex B made in accordance with Section 3.2.

9.3. Severability

Each of the provisions in this DPA is distinct and severable, and if any provision, or part of a provision, is held unenforceable, illegal or void in whole or in part by any court, regulatory authority or other competent authority, it shall to that extent be deemed not to be part of this DPA and the enforceability, legality and validity of the remainder of this DPA will not be affected.

The Parties agree to attempt to substitute for any invalid or unenforceable provision a valid or enforceable provision which achieves to the greatest extent possible the same effect as would have been achieved by the invalid or unenforceable provision.

Except for amendments implemented by this DPA, the Main Agreement remains unchanged and in full force and effect.

9.4. Governing Law

This DPA shall be governed by and interpreted in accordance with the laws of Belgium. Each Party consents to the exclusive jurisdiction of the courts of Gent to settle any disputes arising from this DPA.

Should any court or administrative body of competent jurisdiction find any provision of this DPA to be invalid, unenforceable or illegal, the other provisions of this DPA shall remain in full force and effect.

A. ANNEX A: SPECIFICATION OF PROCESSING PERSONAL DATA

A.1. PURPOSE OF THE PROCESSING

Processing of Personal Data, if any, is directly related to the provision of the Services provided under the Main Agreement. The purposes of the Processing are:

- Processing of Personal Data under the direction of Controller by Processor where necessary for supporting the hosting, maintenance, and management of applications within a public cloud environment as part of the provision of Controller's services.
- Processing, under the instructions of Controller, involving the collection, storage, retrieval, protection, monitoring, support, or administration of data, potentially including Personal Data, within systems managed or supported by Processor under the Main Agreement.
- Supporting a reliable and secure public cloud hosting environment for applications that may require the Processing of end-user data, in line with the service provision and business objectives of Controller.

Where the relevant Order Form or scope of work does not require Processor to Process Personal Data on behalf of Controller, this Annex A applies only to the extent Personal Data is actually present in systems, accounts, logs, tools, tickets, documentation, or environments managed or supported by Processor under the Main Agreement.

A.2. CATEGORIES OF DATA SUBJECTS

Processor may Process Personal Data of the following categories of Data Subjects for Controller, to the extent such data is present in systems managed or supported by Processor under the Main Agreement:

- end-users of Controller's services, where those services are hosted on or interact with platforms managed or supported by Processor;
- employees, contractors, or representatives of Controller;
- employees, contractors, or representatives of Controller's clients, suppliers, or business partners;
- individuals whose Personal Data may be processed as part of service provision by Controller and managed or supported by Processor, such as website visitors, application users, or support contacts.

A.3. TYPES OF PERSONAL DATA

Processor may Process the following types of Personal Data for Controller, to the extent such data is present in systems managed or supported by Processor under the Main Agreement:

- contact information, such as names, email addresses, addresses, telephone numbers, and business contact details;
- digital and technical information, such as IP addresses, cookie data, identifiers, access logs, authentication logs, and system usage data;
- personal user content, such as files, messages, records, form submissions, and data uploaded or provided by end-users;
- application, infrastructure, support, or operational data that may contain Personal Data depending on Controller's application and data model.

Controller remains responsible for determining which Personal Data is present in its applications, cloud environments, systems, logs, exports, repositories, and other Customer-controlled environments.

A.4. CUSTOMER-OWNED CLOUD ENVIRONMENTS

Krane Labs supports Customer's hosting needs in public cloud environments. Customer typically has a direct contract with the relevant public cloud provider performing the infrastructure hosting.

While Krane Labs may require access to a separate account, project, subscription, cluster, or environment within Customer's cloud account, those accounts, projects, subscriptions, clusters, and environments are owned by Customer unless expressly agreed otherwise in an Order Form.

As such, the majority of the Processing performed under the Main Agreement happens on infrastructure which is not owned by Krane Labs. Besides Processing directly related to supporting the hosting infrastructure, Krane Labs may use additional cloud infrastructure and supporting services needed to deliver the Services to Customer.

Krane Labs has limited own equipment used to Process Personal Data. Therefore, many controls around physical hosting facilities are primarily provided by the relevant public cloud provider or Customer-owned infrastructure provider, not directly by Krane Labs.

A.5. SECURITY MEASURES

All applications, systems and procedures relating to them are subject to Krane Labs ISMS policies. Policies and controls relevant for the scope of provided Services may include:

- employee screening;
- security awareness program;
- segregation of duties;
- change management;
- vulnerability management;
- incident management;
- resilience and backup management;
- strong access control enforcement, including IAM and MFA;
- user authorisation reviews;
- data classification standards and data policy;
- network environment segregation;
- secure encryption standards;
- encryption key management;
- encryption in transit and, where applicable, at rest;
- third-party risk management;
- availability and error monitoring;
- secure development life cycle;
- dependency management and known vulnerability scanning;
- static code security analysis;
- staff endpoint security.

B. ANNEX B: SUB-PROCESSORS

The following Sub-processors may Process Personal Data in connection with Krane Labs' provision of the Services. The specific use of each Sub-processor depends on the Services provided under the Main Agreement and the Processing activities described in Annex A.

For Sub-processors that offer regional hosting, the Location of Processing column describes the primary configured hosting or storage location used by Krane Labs where reasonably available. Support, administration, security, or onward Sub-processor access may occur from other locations subject to the applicable transfer mechanism.

SUB-PROCESSOR	LOCATION OF PROCESSING	TRANSFER MECHANISM	PURPOSE	PERSONAL DATA PROCESSED
Dabble CommV, Belgium	Belgium	n/a	Customer Training	Employee contact details
Google Workspace / Google LLC, USA	EU	EU-US Data Privacy Framework and/or SCC 2021/914 as applicable for onward transfers	Email, file storage, and collaboration	Business relationship data, employee and partner contact details, access details, IP addresses, documentation, meeting notes, sample data
Google Cloud / Google LLC, USA	EU	EU-US Data Privacy Framework and/or SCC 2021/914 as applicable for onward transfers	Hosting Krane Labs internal systems and supporting services	Business relationship data, employee and partner contact details, access details, IP addresses
Amazon Web Services / Amazon Web Services Inc., USA	EU	EU-US Data Privacy Framework and/or SCC 2021/914 as applicable for onward transfers	Hosting Krane Labs internal systems and supporting services	Business relationship data, employee and partner contact details, access details, IP addresses
STACKIT / Schwarz Digits Cloud GmbH, Germany	EU	n/a	Cloud hosting, cloud infrastructure services, and supporting services	Business relationship data, employee and partner contact details, access details, IP addresses, hosted data where applicable to the Services
Notion Labs Inc., USA	USA	EU-US Data Privacy Framework and/or SCC 2021/914 as applicable	Documentation, knowledge management, meeting notes, and internal systems	Business relationship data, employee and partner contact details, access details, IP addresses, documentation, meeting notes
AgileBits Inc. / 1Password, Canada	EU	Adequacy mechanism and/or SCC 2021/914 as applicable for onward transfers	Secret management	Employee and partner contact details, access details, secrets and credentials where applicable

GitHub Inc., USA	Worldwide, mostly USA	EU-US Data Privacy Framework and/or SCC 2021/914 as applicable	Code hosting and repository collaboration	Employee and partner contact details, access details, access keys, IP addresses, repository data where applicable
Aikido Security bv, Belgium	EU	n/a; SCC 2021/914 as applicable for onward transfers	Security services	Employee and partner contact details, access details, IP addresses, vulnerability and security metadata
NG Communications bv, Belgium	EU	n/a	Telephony services	Employee contact details
Slack Technologies LLC, USA	USA	EU-US Data Privacy Framework and/or SCC 2021/914 as applicable	Communication and collaboration	Business relationship data, employee and partner contact details, access details, IP addresses, documentation, meeting notes
Asana Inc., USA	USA	EU-US Data Privacy Framework and/or SCC 2021/914 as applicable	Project management	Business relationship data, employee and partner contact details, access details, IP addresses, documentation, meeting notes
MailerLite Limited, Ireland	EU	SCC 2021/914 as applicable for onward transfers	Email marketing, lead intake, forms, and subscriber management	Business contact details, email addresses, form submission metadata, subscription status, IP addresses, interaction data
HubSpot Ireland Limited, Ireland	EU	SCC 2021/914 and/or EU-US Data Privacy Framework as applicable for onward transfers	CRM, sales pipeline, marketing, and contact management	Business contact details, company details, email and communication metadata, notes, deal records, form submissions, interaction history, IP addresses where applicable
Tally BV, Belgium	EU	n/a; SCC 2021/914 as applicable for onward transfers	Forms, lead intake, surveys, and contact form submissions	Business contact details, form submission content, email addresses, metadata, IP addresses where applicable

This list may be updated from time to time in accordance with Section 3.2 of this DPA.