

DATA PROCESSING AGREEMENT

Version 05/2024

DATA PROCESSING AGREEMENT

between

DB2 VALUE CREATION BV

and

CUSTOMER

regarding processing of personal data through the DB2 Services

This **DATA PROCESSING AGREEMENT** (the “**DPA**”) is entered into by and between:

1. **DB2 Value Creation**, also known as **Contractify**, a company established and existing under the laws of Belgium, having its registered office at Polenstraat 163 – B-9940 Sleidinge, Belgium, VAT nr. BE0644714953 –. Kmo-, legally represented by Steven Debrauwere, CEO, hereinafter referred to as: “**Processor**”
2. The entity accepting the Principal Agreement and this DPA, hereinafter referred to as: “**Customer**” also referred to as “**Controller**”;

Take into account that:

- (A) Controller and Processor have entered into one or more contractual agreements (the “**Principal Agreement**”) pursuant to which Processor will provide certain Services related to contract management to Controller.
- (B) To the extent that the provision of such Services involves the processing of personal data, the parties have agreed to enter into this Data Processing Agreement (“**DPA**”) for the purposes of ensuring compliance with the applicable Data Protection Laws.

And have agreed as follows:

1. DEFINITIONS

- 1.1. Terms such as “**process/processing**”, “**data subject**”, “**data processor**”, “**data controller**”, “**data breach**”, “**data protection impact assessment**”, etc., shall have the same meaning ascribed to them in the Data Protection Laws, unless otherwise agreed upon in this DPA;
- 1.2. “**Authorised Subprocessors**” means (a) those Subprocessors set out in Annex 2 (*Authorised Subprocessors*); and (b) any additional Subprocessors consented to in writing by the Controller in accordance with section 5.1;
- 1.3. “**Data Protection Laws**” means in relation to any Personal Data which is Processed in the performance of the Principle Agreement the General Data Protection Regulation (EU)

2016/679 ("GDPR") and all local implementing or supplementing laws thereto and any other applicable data protection or privacy laws;

- 1.4. "EEA" means the European Economic Area;
- 1.5. "Personal Data" means the data described in Annex 1 (*Details of Processing of Personal Data*) and any other personal data uploaded in or processed via the Software by Controller;
- 1.6. "Services" means the services described in the Principal Agreement;
- 1.7. "Standard Contractual Clauses" means the standard contractual clauses for the transfer of personal data to processors established in third countries, as approved by the European Commission in Decision 2021/914/EU, or any set of clauses approved by the European Commission which amends, replaces or supersedes these;
- 1.8. "Subprocessor" means any data processor (including any third party and any Processor Affiliate) appointed by Processor to process personal data on behalf of the Controller;
- 1.9. "Supervisory Authority" means (a) an independent public authority which is established by a Member State pursuant to Article 51 GDPR; and (b) any similar regulatory authority responsible for the enforcement of Data Protection Laws;

2. PROCESSING OF THE PERSONAL DATA

- 2.1. Processor shall process the types of Personal Data relating to the categories of data subjects for the purposes of the Principal Agreement and for purposes as set out in Annex 1 (*Details of Processing of Personal Data*).
- 2.2. For the purposes set out in section 2.1. above, the Controller hereby instructs Processor to transfer Personal Data to the recipients in the countries listed in Annex 3 (*Authorised Transfers of Personal Data*) always provided that Processor shall comply with section 5 (*Subprocessing*) and 11 (*International Transfers of Personal Data*).
- 2.3. Parties agree that this DPA amends and replaces: (i) the provisions in the Principal Agreement that relate expressly to the parties' use of Personal Data, including any specific data protection clauses and data protection schedules in engagement letters; and (ii) any other provisions in the Agreement that conflict with the terms of this DPA.

3. PROCESSOR PERSONNEL

- 3.1. Without prejudice to any existing contractual arrangements between the parties, Processor guarantees that it shall treat all Personal Data as confidential and that it shall inform all its employees, agents, contractors and/or Authorized Subprocessors engaged in processing the Personal Data of the confidential nature of such Personal Data. Processor shall take reasonable steps to ensure the reliability of any employee, agent, contractor and/or Authorized Subprocessor who may have access to the Personal Data, ensuring in each case that access is limited to those persons or parties who need to access the relevant Personal Data, as reasonably necessary.
- 3.2. Processor shall use its best efforts to make sure that all such persons or parties involved in the processing of Personal Data:
 - have undertaken appropriate training in relation to the Data Protection Laws;

- are subject to confidentiality undertakings; and
- are subject to user authentication and log on processes when accessing the Personal Data.

4. SECURITY

4.1. Without prejudice to any other security standards agreed upon by the parties, Processor shall implement appropriate technical and organisational measures to ensure a level of security of the Personal Data appropriate to the risks. In assessing the appropriate level of security, Processor shall take into account the nature of its services and the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed. The technical and organisational measures shall include in any case reasonable measures:

- to ensure that the Personal Data can be accessed only by authorised parties as set forth in Annex 2 (*Authorised Subprocessors*) for purposes or in connection with Annex 1 (*Details of Processing of Personal Data*) to this DPA.
- to protect the Personal Data against accidental or unlawful destruction, accidental loss or alteration, unauthorized or unlawful storage, processing, access or disclosure;
- to identify vulnerabilities with regard to the processing of Personal Data in systems used to provide Services to the Controller.

4.2. The parties acknowledge that security requirements are constantly changing and that effective security requires frequent evaluation and regular improvements of outdated security measures. Processor will therefore evaluate the technical and organisational measures as implemented in accordance with this section on an on-going basis and will tighten, supplement and improve these measures in order to maintain an appropriate level of security.

4.3. Controller may provide written notice to Processor if in the reasonable opinion of Controller the technical and organisational measures set out in this section need to be changed to take account of a change of Data Protection Laws. Such written notice shall include a description of the change of law and details of the requested changes. In such case the Processor shall seriously review and consider the request of Controller and discuss in good faith with the Controller the reasonable possibilities of the discussed changes.

5. SUBPROCESSING

5.1. Subject to section 5.3, Processor shall notify the Controller if Processor engages any new Subprocessors to process Personal Data. Controller may not unreasonably refuse the use of Subprocessor.

5.2. With respect to each Subprocessor, Processor shall:

- provide the Controller with details of the processing to be undertaken by each Subprocessor;

- carry out adequate due diligence on each Subprocessor to ensure that it is capable of providing the level of protection for the Personal Data as is required by this DPA including without limitation sufficient guarantees to implement appropriate technical and organisational measures in such a manner that Processing will meet the requirements of this DPA;
- include terms in the contract between Processor and each Subprocessor which are as strict as those set out in this DPA, and shall supervise compliance thereof; and
- insofar as that contract involves the transfer of Personal Data outside of the EEA, incorporate the Standard Contractual Clauses or such other mechanism as directed by the Controller into the contract between Processor and each Subprocessor to ensure the adequate protection of the transferred Personal Data, or such other arrangement as the Controller may approve as providing an adequate protection in respect of the processing of Personal Data in such third country(ies).

5.3. The Controller hereby authorises Processor to engage those Subprocessors set out in Annex 2 (*Authorised Subprocessors*).

6. DATA SUBJECT RIGHTS

6.1. Processor shall promptly, and in any case within five (5) working days, notify the Controller if it receives a request from a data subject under any Data Protection Laws in respect of Personal Data, including requests by a data subject to exercise rights in chapter III of GDPR, and shall provide full details of that request.

6.2. Processor shall co-operate as requested by the Controller to enable the Controller to comply with any exercise of rights by a data subject under any Data Protection Laws in respect of Personal Data and comply with any assessment, enquiry, notice or investigation under any Data Protection Laws in respect of Personal Data or this DPA, which shall include:

- the provision of reasonable necessary information requested by the Controller within any reasonable timescale specified by the Controller in each case, including full details and copies of the complaint, communication or request and any Personal Data it holds in relation to a data subject;
- where applicable, providing such assistance as is reasonably requested by the Controller to enable the Controller to comply with the relevant request within the timescales prescribed by the Data Protection Laws; and
- implementing any additional technical and organisational measures as may be reasonably required by the Controller to allow the Controller to respond effectively to relevant complaints, communications or requests.

7. INCIDENT MANAGEMENT

7.1. Processor shall notify the Controller immediately, and in any case within forty-eight (48) hours upon becoming aware of or reasonably suspecting a data breach, providing the Controller with sufficient information which allows the Controller to meet any obligations to report a data breach under the Data Protection Laws. Such notification shall as a minimum:

- describe the nature of the data breach, the categories and numbers of data subjects concerned, and the categories and numbers of Personal Data records concerned;
- communicate the name and contact details of Processor's data protection officer or other relevant contact from whom more information may be obtained;
- describe the likely consequences of the data breach; and
- describe the measures taken or proposed to be taken to address the data breach.

7.2. Processor shall fully co-operate with the Controller and take such reasonable steps as are directed by the Controller to assist in the investigation, mitigation and remediation of each data breach, in order to enable the Controller to *(i)* perform a thorough investigation into the data breach, *(ii)* formulate a correct response and to take suitable further steps in respect of the data breach in order to meet any requirement under the Data Protection Laws.

7.3. The parties agree to coordinate and cooperate in good faith on developing the content of any related public statements or any required notices for the affected persons. Processor shall not inform any third party without first obtaining the Controller's prior written consent, unless notification is required by EU or Member State law to which Processor is subject, in which case Processor shall to the extent permitted by such law inform the Controller of that legal requirement, provide a copy of the proposed notification and consider any comments made by the Controller before notifying the data breach.

8. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

8.1. Processor shall provide reasonable assistance to the Controller with any data protection impact assessments which are required under Article 35 GDPR and with any prior consultations to any Supervisory Authority of the Controller or any of its affiliates which are required under Article 36 GDPR, in each case in relation to processing of Personal Data by Processor on behalf of the Controller and taking into account the nature of the processing and information available to Processor.

9. DELETION OR RETURN OF CONTROLLER PERSONAL DATA

9.1. Processor shall promptly and in any event within 90 (ninety) calendar days of the earlier of: *(i)* cessation of processing of Personal Data by Processor; or *(ii)* termination of the Principal Agreement, at the choice of the Controller either:

- return a complete copy of all Personal Data to the Controller by secure file transfer in such format as notified by the Controller to the Processor and securely wipe all other copies of Personal Data processed by Processor or any Authorised Subprocessor; or
- securely wipe all copies of Personal Data processed by Processor or any Authorised Subprocessor,
- and in each case provide written certification to the Controller that it has complied fully with this section 9.

10. AUDIT RIGHTS

10.1. Processor shall make available to the Controller on request all information necessary to demonstrate compliance with this DPA and allow for and contribute to audits, including inspections by the Controller or another auditor mandated by the Controller of any premises where the processing of Personal Data takes place. Processor shall permit the Controller or another auditor mandated by the Controller to inspect, audit and copy any relevant records, processes and systems in order that the Controller may satisfy itself that the provisions of Data Protection Laws and this DPA are being complied with. In case of an audit at the premises of Processor, the Controller must announce such audit at least two weeks prior to the audit and agree with Processor on the scope of the audit. Processor shall provide full co-operation to the Controller in respect of any such audit and shall at the request of the Controller, provide the Controller with evidence of compliance with its obligations under this DPA. Processor shall immediately inform the Controller if, in its opinion, an instruction pursuant to this section infringes the GDPR or other EU or Member State data protection provisions.

11. INTERNATIONAL TRANSFERS OF CONTROLLER PERSONAL DATA

11.1. Processor shall not (permanently or temporarily) process the Personal Data nor permit any Authorised Subprocessor to (permanently or temporarily) process the Personal Data in a country outside of the European Economic Area without an adequate level of protection, other than in respect of those recipients in such countries listed in Annex 3 (*Authorised Transfers of Personal Data*), unless authorised in writing by the Controller in advance.

11.2. When requested by the Controller, Processor shall promptly enter into (or procure that any relevant Subprocessor of Processor enters into) an agreement with the Controller including or on such clauses as adopted by the European Commission and/or such variation as Data Protection Laws might require, in respect of any processing of Personal Data in a country outside of the European Economic Area without an adequate level of protection.

12. INDEMNITY

12.1. Notwithstanding any contrary provisions in the Principal Agreement, Processor and Controller indemnify each other against all claims, actions, third party or Supervisory Authority claims, losses, damages and expenses incurred and arising directly or indirectly out of or in connection with a breach of this DPA.

12.2. The liability of the Processor towards the Controller, including the indemnification mentioned in section 12.1., is limited to the amount that Processor's insurer pays out. In case Processor's insurer does not pay out, then the liability of the Processor towards the Controller, including the indemnification mentioned in section 12.1., is limited to the fees paid by the Controller to the Processor for the services provided under the Principal Agreement during the 12 months prior to the inception of the claim.

13. INTELLECTUAL PROPERTY

13.1. The provision of Personal Data by the Controller to the Processor shall not constitute a grant of license or a transfer of rights on this Personal Data further than is necessary for the completion of the Services.

14. MISCELLANEOUS

- 14.1. Subject to section 14.2, the parties agree that this DPA and the Standard Contractual Clauses shall terminate automatically upon termination of the Principal Agreement or expiry or termination of all service contracts entered into by Processor with the Controller pursuant to the Principal Agreement, whichever is later.
- 14.2. Any obligation imposed on Processor or Controller under this DPA in relation to the processing of Personal Data shall survive any termination or expiration of this DPA.
- 14.3. With regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA and any other agreements between the parties, including but not limited to the Principal Agreement, the provisions of this DPA shall prevail with regard to the parties' data protection obligations for Personal Data.
- 14.4. Insofar reasonable, the compliance by Processor or Controller with the provisions of this DPA will be at no additional cost to the other Party. Should Controller have specific requests for Processor, then the Parties will reasonably discuss an appropriate fee for such specific requests.
- 14.5. Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either *(i)* amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, *(ii)* construed in a manner as if the invalid or unenforceable part had never been contained therein.
- 14.6. This DPA is governed by the laws of Belgium. Any disputes arising out or in connection with this DPA shall be brought exclusively before the competent court of Ghent.

ANNEX 1: DETAILS OF PROCESSING OF PERSONAL DATA

This Annex 1 includes certain details of the processing of Personal Data as required by Article 28(3) GDPR.

Subject matter and duration of the processing of Personal Data

- Implementation and/or use of the Software for the duration of the Principal Agreement, which includes specifically the general registration and management of Contracts of the Controller within the Software;
- Enabling the Processor to provide, operate, maintain, optimise and further improve the Software and the functionalities therein, including the development of new functionalities and other activities reasonably related to proper contractorship and the proper performance of the Principal Agreement.

The nature and purpose of the processing of Personal Data

- As with every organisation, Controller concludes contracts and therefore has a need to properly register and manage those contracts. To do this efficiently, Controller uses the Software of Processor. Because contracts often contain Personal Data, and because user credentials are needed to use the Software, this process of contract management via the Software results in the processing of Personal Data by Controller and Processor.
- Personal Data is also processed to provide, operate, maintain, optimise, update and further develop the Software, and any reasonable processing purposes in connection hereto, such as the provision of support in relation to the Software.
- Personal Data may also be processed if so required by EU or Member State law to which Processor is subject (Processor shall to the extent permitted by such law inform the Controller of the legal requirement before processing that Personal Data).

The types of Personal Data to be processed

Processor only processes Personal Data uploaded to the Software by Controller. For example the Personal Data in contracts and/or other documents which Controller wants to manage or wants to be managed in the Software. The Personal Data in the contracts and/or documents may differ per contract and branche. This Personal Data may include, but is not limited to:

- Name, phone- or cell phone number, job-title, professional email address, private email address, demographics (gender), signature, address, bank account number.

The categories of data subject to whom the Personal Data relates

The categories of data subjects are dependent on the parties with whom the Controller contracts. The categories of data subjects may include, but is not limited to:

- Employees of Customer;
- Business-contacts / clients of Customer;
- Suppliers of Customer.

ANNEX 2: AUTHORISED SUBPROCESSORS

Controller and Processor agree that Processor may use of the services of following parties for the processing of Personal Data relating to the Principal Agreement and the purposes stated in Annex 1 (*Details of Processing Personal Data*):

Name	Location of Hosting	DPA	Nature & Purpose of Processing
Digital Ocean	EU(Germany/NL)	DPA online	Infrastructure & Hosting: Cloud infrastructure: hosting and storage
AWS	EU (Dublin, Ireland)	DPA online	Infrastructure & Hosting: Cloud infrastructure: hosting and storage
Google Cloud	EU (Belgium)	DPA online	Cloud Service Provider
Mailchimp	USA	DPA online	Email service provider
Hotjar	EU	DPA online	User behaviour
Slaask	USA	DPA online	Customer support chat
Totango	EU	DPA online	Customer success platform
Meilisearch	EU	DPA online	Vector search
Nitro sign	EU (France)	DPA signed	E-signing
DocuSign	EU (Ireland)	DPA online	E-signing
Hubspot	EU (Germany)	DPA signed	CRM & Marketing
Functional Software, Inc. d/b/a Sentry	USA	DPA signed	Infrastructure & Hosting: Error monitoring
OpenAI	USA	DPA online	Generative AI services provider for intelligence product features
Pusher	UK	DPA online	real-time communication and collaboration

ANNEX 3: AUTHORISED TRANSFERS OF CONTROLLER PERSONAL DATA

Include details of (i) locations of the Processor and Subprocessor, including those within the EEA and outside of the EEA; (ii) full legal name of each recipient entity to whom data will be transferred:

- Contractify, Polenstraat 163, 9940 Evergem, België (Location of processing: EU);
- Digital Ocean, LLC,, 101 6th Ave New York, NY 10013 (Location of processing: EU);
- Meilisearch, 52 Boulevard de Sébastopol, 75003 Paris, France (Location of processing: EU)
- Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland. (Location of processing: EU);
- Amazon Web Services EMEA SARL (AWS), 38 Avenue John F. Kennedy, L-1855, Luxembourg. (Location of processing: EU).
- Nitro Sign, 447 Sutter St, STE 405 #1015 | San Francisco, CA 94108, USA (Location of processing: EU) → integratie voor digitale ondertekening
- Docusign International (Emea) Limited, 5 Hanover Quay, Ground Floor, Dublin 2, Republic of Ireland (Location of processing: EU) → integratie voor digitale ondertekening
- Mailchimp (The Rocket Science Group, LLC), 675 Ponce de Leon Ave NE Suite 5000, Atlanta, GA 30308 USA (Location of processing: US)
- Hotjar Ltd, Dragonara Business Centre 5th Floor, Dragonara Road, Paceville St Julian's STJ 3141 Malta (Location of processing:EU)
- Slaask, Inc., 2443 Fillmore St #380-7996, San Francisco, CA 94115, USA (Location of processing: US)
- Hubspot, 1 Sir John Rogerson's Quay, Dublin 2, Ireland (Location of processing: US)
- Totango, 1 Twin Dolphin Dr., Redwood City, CA 94065, United States (Location of processing: EU)
- Functional Software, Inc. d/b/a Sentry, 1 Baker Street, Suite 5B, San Francisco, CA 94117, USA (Location of processing: US)
- OpenAI, 3180 18th Street, 94110 San Francisco, California, USA (Location of processing: US)

- Pusher, 6 New Street Street Square New Fetter, 8th Floor, EC4A 3 AQ London, UK
(Location of processing: EU)