ProcessMind Data Processing Addendum

Effective starting: June 23, 2024

Introduction

This Data Processing Addendum ("DPA") supplements the ProcessMind Customer Agreement, or other agreement in place between Customer and ProcessMind covering Customer's use of ProcessMind's Services and related Support and Advisory Services (the "Agreement"). Unless otherwise defined in this DPA or in the Agreement, all capitalized terms used in this DPA will have the meanings given to them in Section 9 of this DPA.

1. Scope and Term.

1.1 Roles of the Parties.

(a) Customer Personal Data. ProcessMind will Process Customer Personal Data as Customer's Processor in accordance with Customer's instructions as outlined in Section 2.1 (Customer Instructions).

(b) ProcessMind Account Data. ProcessMind will Process ProcessMind Account Data as a Controller for the following purposes: (i) to provide and improve the Services; (ii) to manage the Customer relationship (communicating with Customer and Users in accordance with their account preferences, responding to Customer inquiries and providing technical support, etc.), (iii) to facilitate security, fraud prevention, performance monitoring, business continuity and disaster recovery; and (iv) to carry out core business functions such as accounting, billing, and filing taxes.

(c) ProcessMind Usage Data. ProcessMind will Process ProcessMind Usage Data as a Controller for the following purposes: (i) to provide, optimize, secure, and maintain ProcessMind's Services; (ii) to optimize user experience; and (iii) to inform ProcessMind's business strategy.

(d) Description of the Processing. Details regarding the Processing of Personal Data by ProcessMind are stated in Schedule 1 (Description of Processing).

1.2 Term of the DPA. The term of this DPA coincides with the term of the Agreement and terminates upon expiration or earlier termination of the Agreement (or, if later, the date on which ProcessMind ceases all Processing of Customer Personal Data).

1.3 Order of Precedence. If there is any conflict or inconsistency among the following documents, the order of precedence is: (1) the applicable terms stated in Schedule 2 (Region-Specific Terms including any transfer provisions); (2) the main body of this DPA; and (3) the Agreement.

2. Processing of Personal Data.

2.1 Customer Instructions. ProcessMind must Process Customer Personal Data in accordance with the documented lawful instructions of Customer as stated in the Agreement (including this DPA) and respective Orders, as necessary to (i) enable the use of various features and functionalities in accordance with the Documentation (including as directed by Users through the Services), (ii) provide Support or Advisory Services or (iii) comply with its legal obligations. ProcessMind will notify Customer if it becomes aware, or reasonably believes, that Customer's instructions violate Applicable Data Protection Law.

2.2 Confidentiality. ProcessMind must treat Customer Personal Data as Customer's Confidential Information under the Agreement. ProcessMind must ensure personnel authorized to Process Personal Data are bound by written or statutory obligations of confidentiality.

3. Security.

3.1 Security Measures. ProcessMind has implemented and will maintain appropriate technical and organizational measures designed to protect the security, confidentiality, integrity and availability of Customer Data and protect against Security Incidents. Customer is responsible for configuring the Services and using features and functionalities made available by ProcessMind to maintain appropriate security in light of the nature of Customer Data. ProcessMind's current technical and organizational measures are described [here](link Security Measures). Customer acknowledges that the Security Measures are subject to technical progress and development and that ProcessMind may update or modify the Security Measures from time to time, provided that such updates and modifications do not materially decrease the overall security of the Services during a Subscription Term.

3.2 Security Incidents. ProcessMind must notify Customer without undue delay and, where feasible, no later than seventy-two (72) hours after becoming aware of a Security Incident. ProcessMind must make reasonable efforts to identify the cause of the Security Incident, mitigate the effects and remediate the cause to the extent within ProcessMind's reasonable control. Upon Customer's request and taking into account the nature of the Processing and the information available to ProcessMind, ProcessMind must assist Customer by providing information reasonably necessary for Customer to meet its Security Incident notification obligations under Applicable Data Protection Law. ProcessMind's notification of a Security Incident is not an acknowledgment by ProcessMind of its fault or liability.

4. Sub-processing

4.1 General Authorization. By entering into this DPA, Customer provides general authorization for ProcessMind to engage Sub-processors to Process Customer Personal Data. ProcessMind must: (i) enter into a written agreement with each Sub-processor imposing data protection terms that require the Sub-processor to protect Customer Personal Data to the standard required by Applicable Data Protection Law and to the same standard provided by this DPA; and (ii) remain liable to Customer if such Sub-processor fails to fulfill its data protection obligations with regard to the relevant Processing activities under the Agreement.

4.2 Notice of New Sub-processors. ProcessMind maintains an up-to-date list of its Sub-processors [here](link list subprocessors), which contains a mechanism for Customer to subscribe to notifications of new Sub-processors. ProcessMind will provide such notice, to those emails subscribed, at least thirty (30) days before allowing any new Sub-processor to Process Customer Personal Data (the "Sub-processor Notice Period").

4.3 Objection to New Sub-processors. Customer may object to ProcessMind's appointment of a new Sub-processor during the Sub-processor Notice Period. If Customer objects, Customer, as its sole and exclusive remedy, may terminate the applicable Order for the affected Service and related Support and Advisory Services in accordance with Section 11.2 (Termination for Convenience) of the Agreement.

5. Assistance and Cooperation Obligations.

5.1 Data Subject Rights. Taking into account the nature of the Processing, ProcessMind must provide reasonable and timely assistance to Customer to enable Customer to respond to requests for exercising a data subject's rights (including rights of access, rectification, erasure, restriction, objection, and data portability) in respect to Customer Personal Data.

5.2 Cooperation Obligations. Upon Customer's reasonable request, and taking into account the nature of the applicable Processing, ProcessMind will provide reasonable assistance to Customer in fulfilling Customer's obligations under Applicable Data Protection Law (including data protection impact assessments and consultations with regulatory authorities), provided that Customer cannot reasonably fulfill such obligations independently with help of available Documentation.

5.3 Third Party Requests. Unless prohibited by Law, ProcessMind will promptly notify Customer of any valid, enforceable subpoena, warrant, or court order from law enforcement or public authorities compelling ProcessMind to disclose Customer Personal Data. ProcessMind will follow its law enforcement guidelines in responding to such requests. In the event that ProcessMind receives an inquiry or a request for information from any other third party (such as a regulator or data subject) concerning the Processing of Customer Personal Data, ProcessMind will redirect such inquiries to Customer, and will not provide any information unless required to do so under applicable Law.

6. Deletion and Return of Customer Personal Data.

6.1 During Subscription Term. During the Subscription Term, Customer and its Users may, through the features of the Services, access, retrieve or delete Customer Personal Data.

6.2 Post Termination. Following expiration or termination of the Agreement, ProcessMind must, in accordance with the Documentation, delete all Customer Personal Data. Notwithstanding the foregoing, ProcessMind may retain Customer Personal Data (i) as required by Applicable Data Protection Law or (ii) in accordance with its standard backup or record retention policies, provided that, in either case, ProcessMind will maintain the confidentiality of, and otherwise comply with the applicable provisions of this DPA with respect to retained Customer Personal Data and not further Process it except as required by Applicable Data Protection Law.

7. Audit.

7.1 Audit Reports. ProcessMind is regularly audited by independent third-party auditors and/or internal auditors, including as described here. Upon request, and on the condition that Customer has entered into an applicable non-disclosure agreement with ProcessMind, ProcessMind will supply a summary copy of relevant audit report(s) ("Report") to Customer, so Customer can verify ProcessMind's compliance with the audit standards against which it has been assessed, and this DPA. If Customer cannot reasonably verify ProcessMind's compliance with the terms of this DPA, ProcessMind will provide written responses (on a confidential basis) to all reasonable requests for information made by Customer related to its Processing of Customer Personal Data, provided that such right may only be exercised no more than once every twelve (12) months.

7.2 On-site Audits. Only to the extent Customer cannot reasonably satisfy ProcessMind's compliance with this DPA through the exercise of its rights under Section 7.1 above, or where required by Applicable Data Protection Law or a regulatory authority, Customer, or its authorized representatives, may, at Customer's expense, conduct audits (including inspections) during the term of the Agreement to assess ProcessMind's compliance with the terms of this DPA. Any audit must (i) be conducted during ProcessMind's regular business hours, with reasonable advance written notice of at least sixty (60) calendar days (unless Applicable Data Protection Law or a regulatory authority requires a shorter notice period); (ii) be subject to reasonable confidentiality controls obligating Customer (and its authorized representatives) to keep confidential any information disclosed that, by its nature, should be confidential; (iii) occur no more than once every twelve (12) months; and (iv) restrict its findings to only information relevant to Customer.

8. International Provisions.

To the extent ProcessMind Processes Personal Data protected by Applicable Data Protection Laws in one of the regions listed in Schedule 2 (Region-Specific Terms), the terms specified for the applicable regions will also apply, including the provisions relevant for international transfers of Personal Data (directly or via onward transfer).

9. Definitions.

"Applicable Data Protection Law" means all Laws applicable to the Processing of Personal Data under the Agreement.

"ProcessMind Account Data" means Personal Data relating to Customer's relationship with ProcessMind, including: (i) Users' account information (e.g. name, email address); (ii) billing and contact information of individual(s) associated with Customer's ProcessMind account (e.g. billing address, email address, or name); (iii) Users' device and connection information (e.g. IP address); and (iv) content/description of technical support requests (excluding attachments) alongside with the Support Entitlement Number (SEN).

"ProcessMind Usage Data" means Personal Data relating to or obtained in connection with the use, performance, operation, support or use of the Services. ProcessMind Usage Data may include event name (i.e. what action Users performed), event timestamps, browser information, and diagnostic data. For clarity, ProcessMind Usage Data does not include Customer Personal Data.

"Controller" means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

"Customer Personal Data" means Personal Data contained in Customer Data and/or Customer Materials that ProcessMind Processes under the Agreement solely on behalf of Customer. For clarity, Customer Personal Data includes any Personal Data included in the attachments provided by Customer or its Users in any technical support requests.

"Personal Data" means information about an identified or identifiable natural person, or which otherwise constitutes "personal data", "personal information", "personally identifiable information" or similar terms as defined in Applicable Data Protection Law.

"Processing" (and **"Process"**) means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

"Processor" means the entity which Processes Personal Data on behalf of the Controller.

"Security Incident" means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data Processed by ProcessMind and/or its Sub-processors.

"Sub-processor" means any third party (inc. ProcessMind Affiliates) engaged by ProcessMind to Process Customer Personal Data.

Schedule 1 Description of Processing

1. Categories of data subjects whose Personal Data is Processed: Customer and its Users.

2. Categories of Personal Data Processed: ProcessMind Account Data, ProcessMind Usage Data, and Customer Personal Data.

3. Sensitive data transferred: ProcessMind Account Data and Customer Usage Data do not contain data (i) revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, (ii) genetic data, biometric data Processed for the purposes of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation, or (iii) relating to criminal convictions and offences (altogether "Sensitive Data"). Subject to Sections 5.3 and 5.4 of the Agreement (Sensitive Health Information and HIPAA, GDPR Compliance), Customer or its Users may not upload content to the Services which may include Sensitive Data, the extent of which is determined and controlled solely by Customer.

4. The frequency of the transfer: Continuous.

5. Nature of the Processing: ProcessMind will Process Personal Data in order to provide the Services and related Support and Advisory Services in accordance with the Agreement, including this DPA. Additional information regarding the nature of the Processing (including transfer) is described in respective Orders for relevant Services and Documentation referring to technical capabilities and features, including but not limited to collection, structuring, storage, transmission, or otherwise making available of Personal Data by automated means.

6. Purpose(s) of the Processing:

6.1. Customer Personal Data: ProcessMind will Process Customer Personal Data as Processor in accordance with Customer's instructions as set out in Section 2.1 (Customer Instructions).

6.2. ProcessMind Account Data and ProcessMind Usage Data: ProcessMind will Process ProcessMind Account Data and ProcessMind Usage Data for the limited and specified purposes outlined in Section 1.1 (Roles of the Parties).

7. Duration of Processing:

7.1. Customer Personal Data: ProcessMind will Process Customer Personal Data for the term of the Agreement as outlined in Section 6 (Deletion and Return of Customer Personal Data).

7.2. ProcessMind Account Data and ProcessMind Usage Data: ProcessMind will Process ProcessMind Account Data and ProcessMind Usage Data only as long as required (a) to provide Services and related Support and Advisory Services to Customer in accordance with the Agreement; (b) for ProcessMind's legitimate business purposes outlined in Section 1.1 (Roles of the Parties); or (c) by applicable Law(s).

8. Transfers to (Sub-)processors: ProcessMind will transfer Customer Personal Data to Sub-processors as permitted in Section 4 (Sub-processing).

Schedule 2 Region-Specific Terms

Unless otherwise defined in this DPA or in the Agreement, all capitalized terms used in this Schedule will have the meanings given to them in Section 4 of this Schedule.

1. Europe, United Kingdom and Switzerland.

1.1 Customer Instructions. In addition to Section 2.1 (Customer Instructions) of the DPA above, ProcessMind will Process Customer Personal Data only on documented instructions from Customer, including with regard to transfers of such Customer Personal Data to a third country or an international organisation, unless required to do so by Applicable Data Protection Law to which ProcessMind is subject; in such a case, ProcessMind shall inform Customer of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest. ProcessMind will promptly inform Customer if it becomes aware that Customer's Processing instructions infringe Applicable Data Protection Law.

1.2 European Transfers. Where Personal Data protected by the EU Data Protection Law is transferred, either directly or via onward transfer, to a country outside of Europe that is not subject to an adequacy decision, the following applies:

(a) The EU SCCs are hereby incorporated into this DPA by reference as follows:

(i) Customer is the "data exporter" and ProcessMind is the "data importer". (ii) Module One (Controller to Controller) applies where ProcessMind is Processing ProcessMind Account Data or ProcessMind Usage Data. (iii) Module Two (Controller to Processor) applies where Customer is a Controller of Customer Personal Data and ProcessMind is Processing Customer Personal data as a Processor. (iv) Module Three (Processor to Processor) applies where Customer is a Processor of Customer Personal Data and ProcessMind is Processing Customer Personal Data as another

Processor. (v) By entering into this DPA, each party is deemed to have signed the EU SCCs as of the commencement date of the Agreement.

(b) For each Module, where applicable:

(i) In Clause 7, the optional docking clause does not apply. (ii) In Clause 9, Option 2 applies, and the time period for prior notice of Sub-processor changes is stated in Section 4 (Sub-processing) of this DPA. (iii) In Clause 11, the optional language does not apply. (iv) In Clause 17, Option 1 applies, and the EU SCCs are governed by Irish law. (v) In Clause 18(b), disputes will be resolved before the courts of Ireland. (vi) The Appendix of EU SCCs is populated as follows:

The information required for Annex I(A) is located in the Agreement and/or relevant Orders. The information required for Annex I(B) is located in Schedule 1 (Description of Processing) of this DPA. The competent supervisory authority in Annex I(C) will be determined in accordance with the Applicable Data Protection Law; and The information required for Annex II is located here.

1.3 Swiss Transfers. Where Personal Data protected by the Swiss FADP is transferred, either directly or via onward transfer, to any other country that is not subject to an adequacy decision, the EU SCCs apply as stated in in Section 1.2 (European Transfers) above with the following modifications:

(a) All references in the EU SCCs to "Regulation (EU) 2016/679" will be interpreted as references to the Swiss FADP, and references to specific Articles of "Regulation (EU) 2016/679" will be replaced with the equivalent article or section of the Swiss FADP; all references to the EU Data Protection Law in this DPA will be interpreted as references to the FADP.

(b) In Clause 13, the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner.

(c) In Clause 17, the EU SCCs are governed by the laws of Switzerland.

(d) In Clause 18(b), disputes will be resolved before the courts of Switzerland.

(e) All references to Member State will be interpreted to include Switzerland and Data Subjects in Switzerland are not excluded from enforcing their rights in their place of habitual residence in accordance with Clause 18(c).

1.4 United Kingdom Transfers. Where Personal Data protected by the UK Data Protection Law is transferred, either directly or via onward transfer, to a country outside of the United Kingdom that is not subject to an adequacy decision, the following applies:

(a) The EU SCCs apply as set forth in Section 1.2 (European Transfers) above with the following modifications:

(i) Each party shall be deemed to have signed the UK Addendum. (ii) For Table 1 of the UK Addendum, the parties' key contact information is located in the Agreement and/or relevant Orders. (iii) For Table 2 of the UK Addendum, the relevant information about the version of the EU SCCs, modules, and selected clauses which this UK Addendum is appended to is located above in Section 1.2 (European Transfers) of this Schedule. (iv) For Table 3 of the UK Addendum:

The information required for Annex 1A is located in the Agreement and/or relevant Orders. The Information required for Annex 1B is located in Schedule 1 (Description of Processing) of this DPA. The information required for Annex II is located here. The information required for Annex III is located in Section 4 (Sub-processing) of this DPA.

(b) In Table 4 of the UK Addendum, both the data importer and data exporter may end the UK Addendum.

1.5 Data Privacy Framework. ProcessMind participates in and certifies compliance with the Data Privacy Framework. As required by the Data Privacy Framework, ProcessMind (i) provides at least the same level of privacy protection as is required by the Data Privacy Framework Principles; (ii) will notify Customer if ProcessMind makes a determination it can no longer meet its obligation to provide the same level of protection as is required by the Data Privacy Framework Principles, and (iii) will, upon written notice, take reasonable and appropriate steps to remediate any unauthorized Processing of Personal Data.

2. United States of America. The following terms apply where ProcessMind Processes Personal Data subject to the US State Privacy Laws:

2.1. To the extent Customer Personal Data includes personal information protected under US State Privacy Laws that ProcessMind Processes as a Service Provider or Processor, on behalf of Customer, ProcessMind will Process such Customer Personal Data in accordance with the US State Privacy Laws, including by complying with applicable sections of the US State Privacy Laws and providing the same level of privacy protection as required by US State Privacy Laws, and in accordance with Customer's written instructions, as necessary for the limited and specified purposes identified in Section 1.1(a) (Customer Personal Data) and Schedule 1 (Description of Processing) of this DPA. ProcessMind will not:

(a) retain, use, disclose or otherwise Process such Customer Personal Data for a commercial purpose other than for the limited and specified purposes identified in this DPA, the Agreement, and/or any related Order, or as otherwise permitted under US State Privacy Laws;

(b) "sell" or "share" such Customer Personal Data within the meaning of the US State Privacy Laws; and

(c) retain, use, disclose or otherwise Process such Customer Personal Data outside the direct business relationship with Customer and not combine such Customer Personal Data with personal information that it receives from other sources, except as permitted under US State Privacy Laws.

2.2. ProcessMind must inform Customer if it determines that it can no longer meet its obligations under US State Privacy Laws within the timeframe specified by such laws, in which case Customer may take reasonable and appropriate steps to prevent, stop, or remediate any unauthorized Processing of such Customer Personal Data.

2.3. To the extent Customer discloses or otherwise makes available Deidentified Data to ProcessMind or to the extent ProcessMind creates Deidentified Data from Customer Personal Data, in each case in its capacity as a Service Provider, ProcessMind will:

(a) adopt reasonable measures to prevent such Deidentified Data from being used to infer information about, or otherwise being linked to, a particular natural person or household;

(b) publicly commit to maintain and use such Deidentified Data in a de-identified form and to not attempt to re-identify the Deidentified Data, except that ProcessMind may attempt to re-identify such data solely for the purpose of determining whether its de-identification processes are compliant with the US State Privacy Laws; and

(c) before sharing Deidentified Data with any other party, including Sub-processors, contractors, or any other persons ("Recipients"), contractually obligate any such Recipients to comply with all requirements of this Section 2.3 (including imposing this requirement on any further Recipients).

3. South Korea

3.1. Customer agrees that it has provided notice and obtained all consents and rights necessary under Applicable Data Protection Law for ProcessMind to Process ProcessMind Account Data and ProcessMind Usage Data pursuant to the Agreement (including this DPA).

3.2. To the extent Customer discloses or otherwise makes available Deidentified Data to ProcessMind, ProcessMind will:

(a) maintain and use such Deidentified Data in a de-identified form and not attempt to re-identify the Deidentified Data; and

(b) before sharing Deidentified Data with any other party, including Sub-processors, contractors, or any other persons ("Recipients"), contractually obligate any such Recipients to comply with all requirements of this Section 3.2 (including imposing this requirement on any further Recipients).

4. Definitions.

4.1 Where Personal Data is subject to the laws of one the following regions, the definition of "Applicable Data Protection Law" includes:

(a) Australia: the Australian Privacy Act;

(b) Brazil: the Brazilian Lei Geral de Proteção de Dados (General Personal Data Protection Act);

(c) Canada: the Canadian Personal Information Protection and Electronic Documents Act;

(d) Europe: (i) the Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation, or GDPR) and (ii) the EU e-Privacy Directive (Directive 2002/58/EC) as amended, superseded or replaced from time to time ("EU Data Protection Law");

(e) Japan: the Japanese Act on the Protection of Personal Information;

(f) Singapore: the Singapore Personal Data Protection Act;

(g) South Korea: the South Korean Personal Information Protection Act ("PIPA") and the Enforcement Decrees of PIPA;

(h) Switzerland: the Swiss Federal Act on Data Protection and its implementing regulations as amended, superseded, or replaced from time to time ("Swiss FADP");

(i) The United Kingdom: the Data Protection Act 2018 and the GDPR as saved into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 as amended, superseded or replaced from time to time ("UK Data Protection Law"); and

(j) The United States: all state laws relating to the protection and Processing of Personal Data in effect in the United States of America, which may include, without limitation, the California Consumer Privacy Act, as amended by the California Privacy Rights Act, and its implementing regulations ("CCPA"), the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Connecticut Data Privacy Act, and the Utah Consumer Privacy Act ("US State Privacy Laws").

4.2. “Deidentified Data” means data that cannot reasonably be used to infer information about, or otherwise be linked to, a data subject.

4.3. “Data Privacy Framework” means the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S. Data Privacy Framework self-certification program operated by the US Department of Commerce.

4.4. “Europe” includes, for the purposes of this DPA, the Member States of the European Union and European Economic Area.

4.5. “EU SCCs” means the contractual clauses annexed to the European Commission’s Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as amended, superseded, or replaced from time to time.

4.6. “Service Provider” has the same meaning as given in the CCPA.

4.7. “UK Addendum” means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force 21 March 2022, as amended, superseded or replaced from time to time.