

Data Processing Agreement

Our E.U. Data Processing Agreement (DPA) describes how Amla Commerce processes and protects E.U. personal data, that is subject to the General Data Protection Regulation (GDPR) and other E.U. laws, uploaded to or used in our products and services by our customers.

Our privacy, security, compliance, and infrastructure teams have worked with our external advisors to create the E.U. DPA to make sure that it's current, comprehensive and represents our business practices.

Signing a DPA with Amla Commerce will enable Amla Commerce to transfer data outside of the E.U./E.A.A. as necessary for Amla Commerce to perform the services you have requested.

**Data Processing
Agreement for Cloud
Services**

This data processing agreement (the "Data Processing Agreement") is by and between on the one hand **Account Name** having a principal place of business **Street, City State Country** ("Customer") and

For Amla Commerce Cloud Services: **Amla Commerce**, having a principal place of business at 10400 W Innovation Dr #210, Milwaukee, WI 53226, USA ("Amla Commerce"); or

For Znode Services: whichever of **Znode**, a company incorporated in the State of Wisconsin, with its principal place of business at 10400 W Innovation Dr #210, Milwaukee, WI 53226, USA.

Amla Commerce and Znode provide certain hosted services. This Data Processing Agreement supplements any Cloud License Agreement for such services, as applicable and is meant to ensure the parties' compliance with the requirements imposed by the applicable data protection laws and regulations for Customer's use of Cloud Services.

This Data Processing Agreement is intended to provide consistent obligations for each of Amla Commerce and Znode, where possible, but highlights those areas where there may be service-specific differences.

If the parties previously entered into a data processing agreement for Cloud Services, this Data Processing Agreement shall now supersede the foregoing.

1. Definitions.

The capitalized terms will have the meanings set forth below:

- a. "Cloud Services" means the collective Amla Commerce Cloud Services or Znode Services that are subject to the provisions of this Data Processing Agreement.
- b. "Cloud License Agreement" means the Amla Commerce Agreement or Znode Agreement, as applicable for the respective Cloud Service.
- c. "Amla Commerce Cloud Services" means the On-demand Services or Managed Services provided by Amla Commerce, including Support Services where processing of Personal Data is expressly permitted.
- d. "European and UK Data Protection Laws" means the EU GDPR, Directive 2002/58/EC (as amended by Directive 2009/136/EC) concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), the UK GDPR and any national laws or regulations implementing the foregoing, and any amendments or replacements thereto.
- e. "EU GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council.
- f. "EU Personal Data" means Customer Personal Data and Customer Group Personal Data to which the EU GDPR is applicable.

- g. "EU Standard Contractual Clauses" means in respect of EU Personal Data, the standard contractual clauses for the transfer of personal data to third countries adopted by the European Commission under Commission Implementing Decision (EU) 2021/914 including the text from module three of such clauses and no other modules and not including any clauses marked as optional in the clauses except as specified in this Agreement.
- h. "Instruction" means any documented instruction - written or by data input - received by Processor from Customer, including licenses granted under the Cloud License Agreement.
- i. "Znode Agreement" means the agreement (commonly named an end user subscription agreement, end user services agreement, master subscription and services agreement, or licensing agreement) and all related orders for Znode Services, licensed by Znode or Amla Commerce.
- j. "Znode Services" means the software as a service and Support Services under the Znode Agreement.
- k. "Personal Data" shall have the same meaning as defined under European and UK Data Protection Laws.
- l. "Personal Data Breach" means a confirmed unauthorized access by a third party or confirmed accidental or unlawful destruction, loss or alteration of Personal Data.
- m. "Process" or "Processing" shall have the meaning as defined under applicable European and UK Data Protection Laws.
- n. "Processor" is either Amla Commerce or Znode, for the respective Cloud Services provided by that party to Customer.
- o. "Support Services" means the applicable customer support services provided by Processor under the Cloud License Agreement.
- p. "UK GDPR" means the GDPR as applicable as part of UK domestic law by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (as amended).
- q. "UK Personal Data" means Customer Personal Data and Customer Group Personal Data to which the UK GDPR is applicable.

All other capitalized terms not defined in this Data Processing Agreement shall have the meanings ascribed to them in the respective Cloud License Agreement, as applicable.

2. Applicability.

- a. The provisions of this Data Processing Agreement are applicable to the Processing of Personal Data by the respective Processor, to the extent the Processing and use of such Personal Data is permitted under the Cloud License Agreement.
 - i. In case of discrepancies between this Data Processing Agreement and the applicable Cloud License Agreement, the provisions of this Data Processing Agreement shall prevail.

3. Processing and Categories of Personal Data.

- a. Details of Processing of Personal Data. The subject matter, nature and purpose and details and duration of the data processing and the details of the type of Personal Data and categories of data subjects are as determined by the Customer and as permitted under the Cloud License Agreement.
- b. Locations of Processing.
 - i. Amla Commerce Processes Personal Data in the locations described in the Amla Commerce Privacy Center website: <https://www.AmlaCommerce.com/go/processing>.
 - ii. Znode Processes Personal Data in one of the available European hosting locations, selected by Customer.

4. Data Controller.

In accordance with all applicable data protection laws, Customers shall be the data controller.

5. Processor's Responsibility.

- a. Processor will only Process Personal Data within the scope of Customer's Instructions for the applicable Cloud Services including with regard to transfers of Personal Data to third countries. Processor shall notify Customer promptly if it considers that an Instruction from Customer is in breach of European Data Protection Law, and Processor shall be entitled, but not obliged, to suspend execution of the Instructions concerned, until Customer confirms such Instructions in writing. Notwithstanding the foregoing, Processor may process the Personal Data if it is required under law to which it is subject. In this situation, Processor shall inform Customer of such a requirement before Processor Processes the data unless the law prohibits this on important grounds of public interest.

6. Technical and Organizational Measures and Security of Processing.

- a. Taking into account 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, Processor has implemented and maintains technical and organizational measures to ensure a level of security of the processing of Personal Data appropriate to the risk of the respective Cloud Service.

- b. Processor has implemented further measures with respect to security of the Processing of Personal Data and law enforcement requests:
 - i. Amla Commerce Certifications and Security White Papers which apply to all the Cloud Services.
- c. Processor's Technical and Organizational Measures are subject to technical progress and further development. Accordingly, Processor reserves the right to modify the Technical and Organizational Measures provided that the functionality and security of the Cloud Services are not degraded.

7. Personal Data Breach

In the case of a Personal Data Breach, Processor will notify Customer without undue delay after Processor becomes aware of the Personal Data Breach via the email address specified by Customer in Clause 15 or as may be provided in the Cloud Services user interface and, as required by Article 33 of the General Data Protection Regulation, Processor shall supply Customer with information regarding the Personal Data Breach (to the extent that such information is available to Processor) to enable Customer to comply with its notification requirements to the supervisory authority (and, if necessary, the relevant data subjects) under European and UK Data Protection Laws. Processor will, promptly, commence a forensic investigation of a Personal Data Breach and take appropriate remedial steps to prevent and minimize any possible harm. For the avoidance of doubt, Personal Data Breaches will not include unsuccessful attempts to, or activities that do not, compromise the security of Personal Data including, without limitation, unsuccessful login attempts, denial of service attacks and other attacks on firewalls or networked systems.

8. Further Obligations

- a. Taking into account the nature of the Processing under this Data Processing Agreement, Processor shall take all reasonable steps to assist Customer in meeting Customer's obligations under Articles 30, and 32 to 36 of GDPR. Each party shall be responsible for maintaining its own record of processing activities.
- b. Processor will, at the choice of the Controller, delete or return to the Controller all Personal Data after the end of the applicable Cloud License Agreement, unless applicable law requires continued storage of Personal Data.

9. Responsibilities of the Data Controller.

- a. Customer shall comply with all applicable data protection laws.
- b. Instructions. Customer shall give Instructions to Processor as agreed by the Parties in the Cloud License Agreement.
- c. Information Duty. If Customer becomes aware of any breaches of, or other irregularities with, the requirements of all applicable data protection laws, if required by applicable law, Customer shall promptly notify and provide Processor with Instructions detailing the Processing activities Processor must take to ensure the protection of Personal Data, or avoid non-compliance with applicable data protection laws.

10. Costs.

In the event that Customer instructs Processor to provide assistance which goes beyond the standard functionality of the Service(s), then Processor may charge Customer for any costs beyond the agreed upon license fees to the extent it is not commercially reasonable for Processor to provide such assistance without charge (considering relevant factors such as volume of requests, complexity of Instructions and timescale requested). This shall include, without limitation, costs incurred by Processor in executing Customer's Instructions relating to the erasure, additional storage and/or retention of Customers Personal Data, and compliance with any subject access request received by Customer in accordance with Clause 11.

11. Access and Data Deletion.

Data Subject Requests. Processor will promptly inform Customer of any data subject requests it receives in connection with the Cloud Services licensed by Customer. Customer is responsible for ensuring such requests are handled in accordance with European and UK Data Protection Laws. Processor will implement appropriate technical and organizational measures to assist Customer with its obligations in connection with such data subject requests.

12. Audit

- a. Customer may audit Processor's compliance with the terms of this Data Processing Agreement up to once per year (either for itself or on behalf of a regulatory body to which it is subject and only pursuant to a formal request for information from such regulator) ("Audit").
- b. Customer agrees that its right to audit set out above means that it shall be entitled to exercise the following process:
 - i. Customer will be able to review the output of the formal annual independent review of Processor's Technical and Organizational Measures as described under Clause 6, to be conducted by a reputable qualified third party ("Compliance Report").
 - ii. Upon review of the Compliance Report if Customer identifies areas that have not been covered that it is lawfully permitted to audit under this Data Processing Agreement, then Customer will submit an additional list of reasonably specific and detailed questions to Processor in writing. ("Audit Questions").
 1. Within a reasonable timeframe, Processor will respond to the Audit Questions ("Responses") to Customer (or its regulator if so instructed by Customer).
 2. Customer agrees that upon receipt of the responses to the Audit Questions Customer will have completed its Audit, unless Customer can objectively demonstrate that the Responses do not adequately demonstrate Processor's compliance with its statutory obligations and this Data Processing Agreement. Under such an event, Customer may

then be entitled to invoke the process set out below.

- iii. Subject to compliance with i. and ii. above, Customer shall be entitled to request a formal audit of Processor's compliance with this Data Processing Agreement concerning the Audit Questions not already covered by the documentation provided by Processor ("Gap Audit"). To do so, Customer must submit a detailed audit plan to Processor at least two weeks in advance of the proposed audit date. The audit plan must describe the proposed scope, duration, and start date of the Gap Audit. Processor will review the audit plan and provide Customer with any concerns or questions (for example, any request for information that could compromise Processor security, privacy, employment or other relevant policies), and work with Customer to agree on a final audit plan.

1. The Gap Audit will at all times be subject to the following:

- a. It must be conducted during normal business hours at the applicable facility, subject to Processor policies with respect to on-site visitors and may not unreasonably interfere with Processor business activities.
- b. The parties agree to use the least intrusive means to verify Processor's compliance with obligations under this Data Processing Agreement.
- c. The Parties agree to respect the need for Processor to maintain the security of facilities and uninterrupted business operation, protect themselves and customers from risk and to prevent disclosure of information that would jeopardize the confidentiality of Processor or Processor's customers' information.
- d. If Customer appoints a third party to conduct the Gap Audit, the third party must be mutually agreed to by Customer and Processor and must execute a written confidentiality agreement acceptable to Processor before conducting the Gap Audit.
- e. Where Customer is conducting a Gap Audit as a result of a regulator's requests, and if Processor and/or Processor's sub-processor believe that it is not possible to meet a specific time frame set by the regulator, Processor and/or its sub-processor will assist Customer to explain this to the relevant regulator. Customer acknowledges that access to the sub- processor's facilities is subject to agreement from the relevant sub- processor, and that Processor cannot guarantee access to that sub- processor's facilities at any particular time.
- f. Customer will provide Processor any Gap Audit reports generated under this section, unless prohibited by law. Customer may use the Gap Audit report only for the purposes of meeting its regulatory audit requirements and/or confirming compliance with

the requirements of this Data Processing Agreement. The Gap Audit report is Confidential Information of the parties under the terms of the Cloud License Agreement.

- iv. With exception of the Compliance Reports, any Audits and any related costs incurred by Processor (e.g. damages caused by Customer or its auditors to facilities or data held therein) are at the Customer's expense.
- c. In the event that Customer's competent supervisory authority rules that the audit process agreed and exercised under clause b. above is insufficient, the Parties will jointly agree on an audit process and scope to address the concerns raised by Customer's competent supervisory authority.

13. Sub-processors and International Transfers

- a. Customer agrees that Processor shall be entitled to use sub-processors for the respective Cloud Service listed as follows:

Such sub-processors may be affiliates of the Processor or third-party service providers.

- b. Processor has entered into agreements with the third-party sub-processors which ensure that such sub-processors shall be obliged to meet equivalent obligations as those set out in this Data Processing Agreement.
- c. Transfers of EU and UK Personal Data to Third Country Sub-processors. For the transfers of EU Personal Data or UK Personal Data to sub-processor which is an Amla Commerce Affiliate located in a third country which does not provide adequate protection for Personal Data Amla Commerce and the applicable Amla Commerce Affiliate have entered into the EU Standard Contractual Clauses [implemented by the Processor] in order to provide appropriate safeguards for the transfer of such EU Personal Data and UK Personal Data in accordance with the European and UK Data Protection Laws.
- d. In any event, where Processor's sub-processor fails to fulfil its data protection obligations, whether under Clause 13 b, c above, Processor will remain responsible.
- e. Sub-processor Agreements. Where the EU Standard Contractual Clauses are applicable, the parties agree that the obligation at Clause 9(a) of the EU Standard Contractual Clauses to seek approval for sub-processors is met by the process outlined above. Contact Information and Notifications:
- f. For Processor: Data Protection Officer - Amla Commerce
10400 West Innovation
Milwaukee, WI 53226
Email: Anand.Garodia@amla.io
- g. For Customer:
Customer Data Protection Officer:
Anand Garodia
Anand.Garodia@amla.io

14. Miscellaneous.

No amendment, change or suspension of this Data Processing Agreement shall be valid unless agreed upon in writing between Customer and the relevant Processor and unless this Data Processing Agreement is expressly referred to.

15. Independent Parties.

Amla Commerce and Znode are independent parties and the processing activities with respect to each Processor under this Data Processing Agreement are solely the responsibility of that Processor for their respective Cloud Services.