Description: In this section, we outline how Agentoverse complies with the General Data Protection Regulation (GDPR) and related data protection laws. We describe our roles as a controller and processor, the principles we follow in processing personal data, and the measures we take to uphold data subjects' rights and data security. This section complements our Privacy Policy by focusing specifically on GDPR requirements and how we meet them, both for users in the EU and our global user base. (Czech version follows the English text.)

Data Protection Principles

Agentoverse is committed to processing personal data in accordance with the core principles set out in Article 5 of the GDPR:

- **Lawfulness, Fairness, and Transparency:** We process personal data only if there is a valid legal basis (as described in our Privacy Policy), and we do so in a fair manner. We are transparent about our data practices, providing clear information through documents like the Privacy Policy and this GDPR section.

- **Purpose Limitation:** We collect personal data for specific, explicit, and legitimate purposes and do not process it further in a manner incompatible with those purposes. For example, if we collect your email to manage your account, we do not use it later for unrelated purposes without your consent.

- **Data Minimization:** We ensure that the personal data we process is adequate, relevant, and limited to what is necessary for the purposes for which it is processed. As described, we only collect basic account information and usage data needed to run the service effectively, and nothing excessive.

- **Accuracy:** We take reasonable steps to keep personal data accurate and up-to-date. We correct or delete data that is inaccurate.

- **Storage Limitation:** We retain personal data only as long as needed for the purposes or as required by law. After that, we delete or anonymize the data. Our retention practices are detailed in the Privacy Policy.

- **Integrity and Confidentiality:** We process personal data in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage. This includes technical and organizational security measures (see Security section for details).

By adhering to these principles, Agentoverse strives to maintain high standards of data protection and GDPR compliance in all our processes.

Roles: Controller vs Processor

Agentoverse may act both as a "data controller" and as a "data processor" under GDPR, depending on the context:

- **Agentoverse as Controller:** For personal data that you provide to us directly as part of using the Platform (e.g., your registration email, account information, etc.), Agentoverse is the data controller. We determine the purposes and means of processing that data (e.g., using your email to manage your account), as described in our Privacy Policy.

- **Agentoverse as Processor:** In some cases, you (the user) might be using the Platform to process personal data of others as part of your workflow. For instance, if you use an Agent through our Platform that processes data about third parties (such as customers or other individuals' information that you input), you may be the data controller for that data, and Agentoverse is acting as a data processor on your behalf, by carrying out technical processing operations per your instructions.

When Agentoverse acts as a processor for you (the user is the controller), the following terms apply (constituting a data processing addendum in accordance with GDPR Article 28):

- We will process personal data only on your documented instructions (the use of the Platform and configuration of workflows by you is considered your instruction to process data in certain ways), unless required otherwise by law.

- We ensure that persons authorized to process the data have committed to confidentiality or are under an appropriate statutory obligation of confidentiality.

- We take all measures required by Article 32 of GDPR for security of processing, including encryption and other measures described in our Security Policy, to protect personal data.

- We will not engage another sub-processor without general or specific authorization. (By agreeing to our Terms, you give us a general authorization to use certain sub-processors as needed for our operations, such as cloud hosting providers or email service providers. We maintain a list of key sub-processors in our Privacy Policy or can provide it upon request. Any sub-processors are bound by similar data protection obligations.)

- We will assist you, insofar as possible, in fulfilling your obligations to respond to data subject requests (for example, if an individual whose data you processed via our Platform requests access or deletion, we will help you by providing relevant data or deleting it, as applicable) and to ensure compliance with your obligations under Articles 32 to 36 of GDPR (security measures, breach notifications, data protection impact assessments, etc.), taking into account the nature of processing and information available to us.

- If we become aware of a personal data breach affecting data we process on your behalf, we will notify you without undue delay, providing you with sufficient

information to meet any regulatory reporting requirements.

- Upon termination of your account or upon your request, we will delete or return to you all personal data that we have processed on your behalf, unless we are required by law to retain it. (Typically, data in workflows is not stored by us long-term, but any residual data or backups will be securely deleted.)

- We submit to audits or inspections by you or an auditor mandated by you as needed to demonstrate compliance with these obligations, provided such requests are reasonable and with prior notice.

In practice, since our Platform primarily passes through the data you input to Agents and does not store it persistently, our role as a processor is limited and transient. Nonetheless, we are committed to ensuring that any processing on your behalf is done in accordance with GDPR requirements.

Data Subject Rights and Requests

Under GDPR, individuals have rights as described in the Privacy Policy's "Your Rights" section. Agentoverse, as a controller, has established processes to address any requests we receive from users or other data subjects exercising these rights. When we act as a processor for you (the user being the controller for data of third parties), we will forward any such requests to you or advise the requester to contact you, since you are the data controller in that context.

Notably:

- We have procedures to verify identity of requesters to prevent unauthorized access when someone exercises a right (like access to personal data).

- We honor rights requests within the statutory time frames (usually one month).

- If we cannot comply with a request (due to legal reasons or others), we will explain the reason to the requester.

- We do not charge any fee for handling requests in most cases, unless the request is manifestly unfounded or excessive, in which case we may charge a reasonable fee or refuse the request in line with GDPR.

International Data Transfers

Agentoverse is based in the EU (Czech Republic) and generally stores and processes personal data on servers located in the EU. If we were to transfer personal data outside the European Economic Area (for example, if we use a service provider in another country or if you access the service from outside the EU), we ensure that an adequate level of protection is maintained. This means:

- Transfers may go to countries that the European Commission has deemed as providing an adequate level of data protection.

- For transfers to countries without an adequacy decision (such as the United States, unless covered by an adequacy decision or successor framework), we use appropriate safeguards like Standard Contractual Clauses, in combination with additional security measures if necessary.

- We will comply with any updated requirements of EU law regarding data transfers (for example, assessments following the Schrems II decision, etc.).

By using Agentoverse, you understand that your personal data may be accessed by our team or sub-processors in other jurisdictions strictly for the purposes described (for example, support or maintenance), but always under the protection of the aforementioned safeguards.

As part of our Platform operations, we also use Google Analytics and Google Ads, which may involve transferring certain data to the United States. These services are provided by Google LLC, which acts as an independent data controller. The data transfer relies either on the EU-U.S. Data Privacy Framework or on the European Commission's Standard Contractual Clauses. For more details on how Google processes data, please refer to their Privacy Policy: https://policies.google.com/privacy

Data Protection Officer and Contact

At our current scale, Agentoverse is not legally required to appoint a Data Protection Officer (DPO), as we do not engage in large-scale processing of sensitive data or systematic monitoring of individuals beyond what is necessary for our service. However, we take privacy seriously. We have a dedicated team member responsible for overseeing GDPR compliance and data protection matters.

If you have questions, concerns, or requests relating to data protection or GDPR compliance, you can reach out to us at **orbitcare@agentoverse.com**. We will respond promptly and work to address any issues.

Our supervisory authority in the EU is the Czech Office for Personal Data Protection (ÚOOÚ). You have the right to contact this authority or your local data protection authority if you believe we are not meeting our obligations.

Accountability and Record-Keeping

We maintain records of processing activities where required (as per GDPR Article 30) and regularly review our data protection practices. We also perform data protection impact assessments (DPIAs) if we implement new processing that may pose high risks to individuals' rights, although our current operations likely do not require a DPIA due to the limited scope of data we handle.

Agentoverse’s management is committed to GDPR compliance and fostering a privacy-centric culture. We train our staff on data protection principles and ensure that

privacy by design and by default is considered in developing our Platform (for instance, we strive to minimize personal data usage and build secure systems from the ground up).