Description: Agentoverse takes a robust approach to security to protect user data, workflows, and our infrastructure. This Security section details our security practices, controls, and commitments. It covers areas such as data encryption, access management, secure development practices, and how we handle authentication information and credentials. Our goal is to provide a secure environment for our users, while also clarifying the shared responsibility (what we do and what users should do to keep accounts and data safe). (Czech version follows English.)

Infrastructure Security

- **Hosting:** Our Platform is hosted on secure cloud infrastructure. We choose reputable providers that offer strong physical and network security. Data centers have 24/7 monitoring, access control, and other safeguards to prevent unauthorized physical access.

- **Network Security:** We employ firewalls and network segmentation to limit access to our systems. Only necessary network ports are open, and internal systems are protected behind virtual private networks (VPNs) or other access controls. We regularly update and patch servers, operating systems, and software to protect against known vulnerabilities.

- **Encryption in Transit:** All communication between your browser and our Platform is encrypted using HTTPS (TLS encryption). This ensures that data transmitted (such as login credentials, API calls, and any content you send to the Platform) cannot be easily intercepted or read by attackers.

- **Encryption at Rest:** Our databases and storage volumes are encrypted at rest. This means that even if the storage media were accessed without authorization, the data would not be readable without the proper decryption keys. Sensitive data, such as passwords and authentication tokens, are further protected (passwords are salted and hashed using strong algorithms, and API keys or secrets are encrypted).

Access Control and Authentication

- **Limited Personnel Access:** Only a small, authorized team of Agentoverse personnel has access to production systems or user data, and then only on a need-to-know basis (for example, to provide support or maintain the system). Access is protected with strong authentication (such as multi-factor authentication) and is logged and audited. Our team members are bound by confidentiality obligations.

- **Authentication Security:** User passwords are never stored in plaintext. We hash and salt passwords with industry-standard hashing algorithms (e.g., bcrypt or Argon2), so that even if our database were compromised, the original passwords would not be easily retrievable. We also encourage users to choose strong, unique passwords for our Platform. (In future, we may implement optional two-factor

authentication (2FA) for user accounts to further enhance security.)

- **User Credentials and Tokens:** If our Platform needs to store credentials or API tokens to connect to external services on behalf of a user (for example, if an Agent requires an API key to function), we treat those as highly sensitive. Such credentials are stored in an encrypted form in our database or a secure vault. They are decrypted only when needed for execution of workflows and are never exposed in plaintext to unauthorized parties. We also ensure that these secrets are not logged or exposed in Platform interfaces.

- **Session Management:** Sessions are securely managed. The session cookies we issue are flagged as HttpOnly and Secure, which means they are not accessible via JavaScript and only transmitted over HTTPS. We also implement session timeout and inactivity logout mechanisms to reduce risk from abandoned sessions.

Secure Development and Testing

- **Secure Coding Practices:** Our development team follows secure coding guidelines. We review code for security issues and use static analysis tools to catch common vulnerabilities (like SQL injection, XSS, etc.). We also maintain dependencies and update them regularly to incorporate security fixes.

- **Environment Separation:** We separate development, testing, and production environments. Test data is anonymized or synthetic to avoid using real personal data in non-production environments.

- **Penetration Testing and Vulnerability Scans:** We periodically conduct vulnerability scanning of our Platform and underlying infrastructure. We also plan regular penetration tests by independent security experts. Any findings are triaged and fixed with high priority.

- **Bug Bounty and Responsible Disclosure:** We value input from the security community. If you discover a vulnerability or security issue in our Platform, we encourage responsible disclosure. Please contact us at **orbitcare@agentoverse.com** with the relevant details. We will investigate all legitimate reports and fix confirmed issues as soon as possible. (We may consider a bug bounty reward program to incentivize ethical hacking and reporting.)

Data Isolation and Privacy

- **Tenant Isolation:** If applicable, each user's data and workflows are logically separated from others'. For example, your workflows and any runtime data are not accessible to other users unless you explicitly share them. We enforce authorization checks at every layer to ensure users can only access resources (agents, workflows, data) that they are permitted to.

- **Workflow Execution:** Workflows running in the Agentoverse cloud are executed in a sandboxed environment. This environment is designed to prevent one workflow from interfering with or accessing data of another. Agents execute with only the permissions they need to perform their function, following the principle of least privilege.

- **Monitoring and Logging:** We monitor our systems for unusual activities, intrusions, or misuse. Security logs are maintained and reviewed. Access to sensitive logs is restricted and logs are retained according to our retention policy for audits and forensic purposes if needed.

Handling of Security Incidents

- **Incident Response Plan:** We have an incident response plan in place. If a security incident is detected (such as a data breach or successful attack), we will immediately activate our incident response procedures. This involves:

    - Assembling a response team.

    - Containing and mitigating the issue (for instance, isolating affected systems, rotating keys, etc.).

    - Investigating the incident to determine scope, root cause, and affected data.

    - Fixing the vulnerability or issue that led to the incident.

    - Restoring secure operations.

    - Communicating with affected users and authorities as required by law (e.g., under GDPR, notifying the supervisory authority within 72 hours and users if there is a high risk to their rights).

- **User Notifications:** If your data is involved in a breach that poses a risk to you, we will notify you in a timely manner via the email associated with your account, providing an explanation of what happened and what steps we are taking. We may also post prominent notices on our website if broader notification is needed.

- **Continuous Improvement:** After an incident is resolved, we conduct a post-mortem analysis to learn from it and improve our processes and security measures to prevent future incidents.

User Responsibilities and Best Practices

Security is a shared responsibility. While we do our best to secure the Platform, users also have a role in maintaining security:

- **Protecting Credentials:** You should keep your account credentials confidential. Do not reuse passwords from other services, and ideally use a password manager to generate and store a strong password unique to Agentoverse. If you suspect your login information has been compromised, change your password immediately and inform us.

- **Account Usage:** Remember to log out of the Platform when using a shared or public computer. Use caution when sharing workflows or Agents, as any data you include might be visible to others if you make them public.

- **Personal Data in Workflows:** Avoid unnecessarily including sensitive personal data in your workflows, especially if you intend to share an Agent or workflow. While we secure data in transit and at rest, the best protection for sensitive data is not to input it unless needed. If an Agent processes personal data of others, ensure you have the right to do so and consider data minimization.

- **Updates and Awareness:** Keep your devices and browsers updated with the latest security patches. Use antivirus software and be vigilant against phishing attempts. Agentoverse will never ask you for your password via email or any channel outside the secure login form.

By following these best practices and our provided security features, you can help protect your own data and contribute to the overall security of the Platform.

Compliance and Standards

Our security program is designed in line with industry best practices and frameworks. While Agentoverse is not yet formally certified under standards like ISO 27001 or SOC 2, we aim to align our policies and procedures with the spirit of those standards. As we grow, we may pursue relevant certifications to provide external validation of our security posture.

We also comply with all applicable legal requirements regarding security and data protection, such as GDPR's Article 32 (Security of Processing), and relevant Czech laws on cybersecurity and data protection.