

Terms Of Use - Product-Specific Addendum – CyberHQ.ai

Effective 18th September 2026 v1

General

1. This **addendum** supplements and forms part of the Avertro Terms of Use (**terms**). It applies specifically to the CyberHQ.ai **services**. In the event of any conflict between this addendum and the terms, this addendum shall prevail with respect to the services, except that the Data Processing Addendum (DPA) governs the processing of personal data and notification of a personal data breach uniformly across all CyberHQ® products.
2. We may update this addendum with notice as permitted under the terms.

Definitions

3. Words defined in the terms will have the same meaning in this addendum.
4. Any words in bold text in this addendum will have the same meaning every time they are used.
5. **Cloud model** means the hosted SaaS version of the services, including any deployment via AWS Marketplace or similar marketplaces.
6. **CyberHQ.ai** is one of Avertro's CyberHQ® products, as defined in the Terms of Use. The Terms of Use, Acceptable Use Policy, Support Policy, and Technical SLA apply to CyberHQ.ai as they do to Avertro's other CyberHQ® products, except where this addendum states otherwise.
7. **Deployment package** means the software package provided by us containing the services (or components thereof), including updates.
8. **Monitored data** means any data collected by the service's sensors, extensions, agents, or other components, including (without limitation) web browsing activity, URLs, file upload/download metadata (names, types, sizes, content indicators where configured), destinations, behavioral patterns, device information, timestamps and related personal data.
9. **Self-hosted model** means the version of the services delivered via a deployment package that customer deploys, configures and runs in its own infrastructure or cloud environment.

Deployment models

10. The services are offered in two deployment models, as specified in the applicable quotation or order:
 - a. **Cloud model:** we host and operate the services as a SaaS solution. The services are available from Avertro or via marketplace listing, e.g., AWS Marketplace. You access the services via sensors/extensions or other provided mechanisms. Monitored data collected by the services is transmitted to and processed in our (or the marketplace provider's) infrastructure in accordance with applicable data protection and AI regulations. You consent to such

processing and transmission and are responsible for any required cross-border data transfer mechanisms.

- b. **Self-hosted model:** we make the deployment package available for download (via secure registry, portal or marketplace). You are solely responsible for downloading, deploying, configuring, managing, securing and maintaining the services and all your underlying infrastructure (compute, storage, orchestration, networking, etc.) in its own environment. All monitored data remains under your exclusive control and is processed locally except during optional support sessions.

License grants

- 11. The license granted under the terms is supplemented as follows for the services:
 - a. **Cloud model:** you may access and use the hosted services, including the right to deploy sensors or extensions, as described in the documentation.
 - b. **Self-hosted model (deployment package):** In addition to the general license, we grant you the right to download, install, deploy, and run the deployment package (and any updates we provide) in your own environment solely for your internal business purposes.
 - c. You must not (nor permit others to) modify, adapt, reverse engineer, decompile, disassemble, create derivative works of or otherwise attempt to derive the source code of any component of the deployment package, nor copy, distribute, sublicense, sell, or redistribute it or any portion thereof.
 - d. You acknowledge that the deployment package may contain third-party software, open-source components, or other materials (**third-party components**) that are subject to their own license terms. A list of third-party components and their applicable licenses is provided in the THIRD-PARTY-NOTICES.txt file (or equivalent) included in the deployment package or available in the documentation. You are solely responsible for complying with all such third-party license terms when using the services. Any failure to comply with these licenses constitutes a breach of the terms.
- 12. All use of the services (in either model) remains subject to the license scope, limitations and restrictions set out in the terms, the order and the documentation.

Updates

- 13. We will make updated deployment packages (for self-hosted model) or updates to the hosted service (cloud model) available periodically. For the self-hosted model, you are responsible for promptly deploying updates, particularly critical security updates (recommended within 30 days). Failure to apply updates may result in degraded performance, security risks, or loss of support eligibility.

Customer responsibilities and regulatory compliance

- 14. The services involve monitoring of employee and user activity, including potential interactions with third-party generative AI tools, for data loss prevention, risk detection and security purposes. The services may be classified as a high-risk AI system under applicable laws.
- 15. You acknowledge you are solely responsible for:
 - a. ensuring your deployment and use of the services complies with all applicable laws, including employment laws, data protection laws (e.g., GDPR, CCPA/CPRA), workplace monitoring and

- surveillance requirements and AI-specific regulations (such as the EU AI Act and US state AI laws);
 - b. providing all necessary notices to, and obtaining all required consents (or establishing another valid lawful basis) from your employees, contractors, and other data subjects before deployment and ongoing use;
 - c. conducting any required Data Protection Impact Assessments (DPIAs), AI impact assessments, risk evaluations or equivalent assessments for your specific use case;
 - d. ensuring the monitoring is proportionate, necessary and limited to legitimate business purposes;
 - e. complying with any human oversight, transparency, explainability or appeal requirements under applicable AI or privacy laws;
 - f. maintaining the security and proper configuration of any deployed deployment packages and infrastructure (self-hosted model); and
 - g. all data storage, backups, disaster recovery, and infrastructure costs in your environment.
16. You represent and warrant that you have (or will obtain) all necessary rights and permissions for the collection and processing of monitored data. We have no responsibility for your compliance with these obligations.

Data processing

- 17. To the extent the services involve processing of personal data, you are the data controller (or business) and we are the data processor (or service provider). Processing occurs only in accordance with your documented instructions and the terms (including any separate Data Processing Addendum).
- 18. In the cloud model, we process monitored data in its environment.
- 19. In the self-hosted model, we do not process monitored data on an ongoing basis. Our role is limited to supplying the deployment package and support.
- 20. Details of processing (categories of data, purposes, etc.) are set out in the applicable Data Processing Addendum or order.
- 21. Further detail on the specific categories of data collected via the CyberHQ.ai browser extension, sensors, extensions or agents (including monitored data) is set out in the CyberHQ.ai Browser Extension — Privacy & Data Disclosure, available on our website.

Security and breach notification

- 22. We will implement reasonable technical and organizational measures to protect monitored data consistent with industry standards.
- 23. In the event of a personal data breach affecting monitored data under our control, we will notify you without undue delay (and no later than 48 hours where required) and provide you with reasonable assistance.
- 24. For the self-hosted model, you are solely responsible for security of the deployed instance and any resulting breaches.

No legal or compliance advice; disclaimers

- 25. We do not provide legal, employment, regulatory or compliance advice. The services provide a tool to assist with your risk detection and security monitoring. You remain solely responsible for all decisions,

actions, investigations or employment consequences arising from use of the services or monitored data.

26. To the fullest extent permitted by law:

- a. we disclaim all liability for claims by your employees, contractors or third parties related to monitoring activities or your compliance failures; and
- b. we have no control over your deployment environment and disclaim liability for issues arising from your infrastructure, configuration, or failure to apply updates.

Termination and post-termination

27. Upon termination or expiration of your license:

- a. Cloud access ends immediately; and
- b. For self-hosted, you must cease use of all components of the deployment package and delete all copies (except as required by law for archival purposes). We may require certification of deletion.