Rapport Employee Privacy Notice

Template for Rapport customers

GUIDANCE FOR CUSTOMERS – DELETE BEFORE ISSUING

This template helps Rapport customers meet their transparency obligations to employees and contractors whose devices are enrolled in Rapport. Your organisation is the controller and is responsible for the final notice. Before issuing it: (1) replace all text in yellow brackets; (2) delete sections for features you have not enabled; (3) confirm your lawful basis and any consent requirements; (4) complete any works-council, employee-representative or similar consultation required where you operate; (5) check local electronic-monitoring notice rules, some of which require written or electronic acknowledgement by employees (for example in New York); and (6) have it reviewed by your legal adviser. (7) EEA/UK: complete a DPIA; do not rely on consent as your lawful basis for employees. India: until 13 May 2027 the SPDI Rules apply, so obtain written consent if passwords, financial or health information may be collected; from that date DPDP s.7(i) permits processing for employment purposes, but give this notice anyway and offer it in English or a language in the Eighth Schedule.

[[Organisation name]] – Privacy notice: Rapport device monitoring and support

Effective: **[date]**

Notice version: [version/date]

1. Who is responsible

[Organisation legal name and address] ("we") is the controller of the personal information described in this notice. We use Rapport, a service provided by Actionable Science, Inc. (Rezolve.ai), which processes the information on our behalf and only on our instructions. **[If applicable: Our Data Protection Officer can be contacted at …]**

2. Why we use Rapport

- To keep work devices secure, updated and performing well.
- To detect and diagnose technical problems, and to fix them remotely.
- To deploy software and security updates.
- **[If Workforce Activity is enabled: To understand, at group level, how technology is used so we can plan improvements.]**

3. What information is collected

Category	Information	When
Device and software inventory	Device name, operating system and build, hardware, network interfaces, firmware, battery health, installed software and versions, installed and pending updates[, and the employee the device is assigned to]	Continuously
Performance and reliability	Processor, memory, disk, network and power measurements; names and resource use of the busiest programs (without arguments or file paths); start-up, sign-in and resume times; application crash and hang summaries; system restarts	Continuously
Network quality	Connection type, VPN state, Wi-Fi signal strength and response time, without network names	Continuously
Presence	Whether someone is at the device (yes/no), without any input content	Continuously
Workforce activity [delete if not enabled]	Daily active, idle, after-hours and weekend minutes; time by broad category (such as browser, email, office). Application names stay on the device	Continuously
Support activity	Files, command output and system information accessed by IT staff or the AI assistant while resolving an issue; records of each action	Only when IT staff act on a device

4. What routine monitoring never collects

Rapport's routine monitoring never collects your keystrokes, screen content, clipboard contents, browsing history, the content of your documents or messages, or the names of Wi-Fi networks you connect to. Section 5 explains when IT staff or the AI assistant may access content on your device

5. When IT staff work on your device

Our authorised IT staff can use support tools on your device to resolve problems: scripts, file transfer and **[if AI Features are enabled: an AI assistant]**. These tools can access content on the device where needed. Scripts and file transfers require approval through our authorised IT process before they run, subject to our configured settings. This approval may be given by an authorized Administrator and does not necessarily require your individual approval. **[Describe your internal rules, for example: "IT staff will contact you before opening files in your personal folders, except in a security emergency."]** Once enabled, the AI assistant may read accessible text files and run read-only diagnostic commands without separate approval for each action, subject to the configured controls. Retrieved file contents and diagnostic results may be sent to Anthropic.

[Delete if AI Features are not enabled:] The AI assistant sends the information it uses to Anthropic, Rezolve.ai's AI provider, to generate answers. If IT staff approve it, this can include clipboard contents or a screenshot. Anthropic does not retain that information or use it to train its models. The AI assistant is blocked from reading browser, email and messaging data on devices with the current Rapport agent. It cannot make changes to your device without approval.

6. Lawful basis [[confirm for your jurisdiction]]

[For the EEA and UK deployments, identify the legal basis for each purpose in Section 2. Where relying on legitimate interests, describe those interests. Where relying on a legal obligation, identify the relevant obligation.] our legitimate interests in securing and maintaining our IT systems and supporting our staff; compliance with our legal obligations to keep personal data secure; and, for Workforce Activity, our legitimate interests in planning technology at group level, which we have balanced against your interests.

7. How we use and do not use it

We use the information only for the purposes in section 2. We do not use Rapport to score individual productivity or to make decisions about you based solely on automated processing, except where it reveals a security incident or a serious breach of our policies. **[If Workforce Activity is enabled: Workforce activity is shown only for groups of five or more devices.]**

8. Who can see it

Authorised members of **[our IT team and other named teams]**. Rezolve.ai and its sub-processors (listed at https://www.rezolve.ai/legal/subprocessors) process it to provide the service, under contracts that protect it.

9. International transfers

Rapport stores information in the United States. **[For the EEA/UK: You may request information about, or a copy of, the applicable transfer safeguards by contacting [contact details]. Transfers are protected by the European Commission's Standard Contractual Clauses and the UK International Data Transfer Addendum.]** Rezolve.ai's support team in India may access information when needed to resolve a support case.

10. How long it is kept

Information	Kept for
Detailed performance measurements and support command records	[90 days]
Experience events, activity categories and AI assistant sessions	[180 days]
Device history, alerts, issues and the IT activity log	[365 days]
Daily and hourly summaries and inventory history	[400 days]

[Adjust if you change the default retention settings.] When a device is retired, its Device Data is deleted in accordance with the applicable deletion arrangements. Related Audit Log entries remain for the stated retention period.

11. Your rights

Depending on where you work, you may have the right to access, correct or delete your information, to restrict or object to its use, and to complain to a data protection authority. To exercise your rights, contact **[privacy or HR contact]**. We will not treat you unfavourably for exercising your rights.

Where processing is based on consent, you may withdraw that consent by [method], without affecting the lawfulness of processing before withdrawal. Where applicable, you may also request a portable copy of your information. You may complain to [relevant supervisory authority and contact/link]. Further, we will tell you about material changes to this notice before they take effect.

12. Questions

Contact **[contact details]**. Rezolve.ai's Privacy Policy is available at https://www.rezolve.ai/legal/privacy-policy.

Our employee privacy notice is available at [*insert link*].

13. Acknowledgement of receipt — [use where required]

I acknowledge that I have received the Rapport Employee Privacy Notice, version [●], dated [●]. This acknowledgement records receipt and does not waive my rights or constitute consent to processing where separate consent is required.

Employee name: [●]

Signature/electronic acknowledgement: [●]

Date: [●]