PRIVACY POLICY FOR TEHTRIS MTD

The privacy protection in the personal data processing is a major concern to which TEHTRIS pays particular attention. That is why we want to be completely transparent about the data we collect to protect your Device.

This Privacy Policy describes the data processing terms by the **TEHTRIS Mobile Threat Defense ("MTD")** application.

By downloading and activating **TEHTRIS MTD**, you indicate that you consent to the data collection, use, disclosure and storage practices described in this Policy.

TEHTRIS reserves the right to modify this Privacy Policy at any time as legislation, our data collection and use practices, and the **TEHTRIS MTD**' functionalities evolve. Please check this page periodically for the latest changes. Your continued use of **TEHTRIS MTD** application following the posting of changes to this Privacy Policy indicates your acceptance of those changes.

You may have been directed to download and activate the **TEHTRIS MTD** application. If you have any questions or requests regarding the data collection, use, disclosure and security practices under the present terms and conditions, please direct them directly to TEHTRIS.

TEHTRIS respects your privacy and your personal data.

1. *What is TEHTRIS MTD?*

TEHTRIS MTD is a mobile threat defense application performing security audits on Android and iOS devices. **TEHTRIS MTD** application detects network, application, and system anomalies while meeting compliance requirements.

TEHTRIS MTD is managed from a centralized console to which technical information collected from your Device is transmitted.

2. *What data is collected on my Device?*

As soon as you have been enrolled into the **TEHTRIS MTD** application from your side and/or by your Employer's operational team, it begins collecting data from your Device. **TEHTRIS MTD** collects certain categories of data on your Device:

- Enrollment data: email address;
- Device data: manufacturer, model, CPU model, built-in biometric features, kernel, uptime, operating system version, protection settings, compromission indicators, configuration parameters, IP address;
- Application data: metadata for all applications installed on your Device (package names, display names, versions). For any unknown applications from our knowledge base, we may upload their payloads.
- Geolocation data: geolocation or last known locations of the Device, when the feature is activated from your side and/or by your Employer's operational team;
- Web content data: consulted domain names, when the feature is activated from your side and/or by your Employer's operational team;

3. *How is my data used?*

We use the data we collect for a variety of business purposes depending on the following:

- Enrollment data: used to authenticate your Device during the enrollment process;
- Device data: used to analyze your Device to determine if it has been compromised or insecurely configured, for example to detect if it has been infected, rooted or jailbroken, or if no password has been configured;
- Application data: used to perform analysis of application files to determine whether certain applications exhibit malicious behavior.
- Geolocation data: used to provide location context to detections;
- Web content data: used to block access to malicious websites and conduct in-depth investigations.

Your Employer's operational team will be notified if you encounter a threat.

If we disclose the results of our analysis to the public, we do so in aggregate and anonymized form to protect your privacy and that of your Employer's operational team.

The legal basis for the use of your information, as set out in this Privacy Policy, depends on your relationship with your Employer's operational team and the use case in which your Employer's operational team is involved. It may include the following purposes:

a) the use of your personal information is necessary to fulfill our obligations under any contract we enter with you (for example, for your Employer's operational team to perform the employment contract or for TEHTRIS to comply with the Terms of Use that you have agreed to by downloading and/or using our applications); or

b) if the use of your information is not necessary for the performance of a contract, it is nevertheless necessary for our legitimate interests or those of your Employer's operational team or third parties (for example, to ensure the security of the services, to operate the services, to ensure secure environments for our staff, your Employer's operational team to make and receive payments, to prevent fraud), as well as to comply with legal requirements, such as data security.

4. *Is my data shared with third parties?*

For security and technical organizational reasons, TEHTRIS stores your personal data at its OVH Cloud data hosting provider located in France. By default, when we process your personal data, everything is protected and encrypted, which means that OVH Cloud cannot read your data, thanks to a robust internal security model (security and privacy by design). This data retention is only used for secure storage purposes.

We may be required by law, court decisions and/or requests from public and governmental authorities to disclose your personal data. We may also disclose your personal data if we believe in good faith that such action is necessary to comply with legal requirements or legal process; prevent crime or protect national security; protect users or the public. We may also disclose personal information if we determine in good faith that disclosure is reasonably necessary to protect our rights and exercise available remedies, enforce this Privacy Policy, your Terms of Use.

We do not use the data collected on your Device to sell you products. Nor do we share it with third parties for marketing purposes.

The central management console in **TEHTRIS MTD** allows your Employer's operational team or persons authorized by your Employer's operational team to access certain information related to the security of your Device.

TEHTRIS MTD shares with your Employer's operational team only the information necessary to enable your Employer's operational team to ensure that your Device does not pose a threat and complies with your entity's security policies. **TEHTRIS MTD** may inform your Employer's operational team about applications on your Device.

Your Employer's operational team can view your Device attributes such as model and the applications installed. To learn the possible consequences of violating your Entity's policies, please contact your Employer's operational team.

TEHTRIS MTD does not allow your Employer's operational team to view the content of your personal email and SMS messages, contacts or calendar.

5. *How is my data protected?*

To protect your personal data, TEHTRIS uses all technical and organizational security measures within its power to minimize the risk of accidental or intentional manipulation, loss, destruction and access by unauthorized persons. TEHTRIS' security measures and procedures are continually improved as new technologies become available.

All TEHTRIS employees as well as potential subcontractors are subject to an obligation of confidentiality.

We retain personal data only for as long as reasonably necessary to provide our products and services to comply with legal requirements. In general, the data collected by **TEHTRIS MTD** is kept on a best-efforts basis up to the storage capacity of our disks and for a period that complies with the recommendations of the CNIL ('Commission Nationale de l'Informatique et des Libertés').

If your Employer's operational team has authorized the capture of geolocation data, this data will be kept for the same period as described above.

6. *Where is my data stored?*

For reasons of security and technical organization, TEHTRIS stores your personal data at its OVH Cloud data host, located in European Economic Area. By default, when we process your personal data, everything is protected and encrypted, which means that OVH Cloud cannot read your data, thanks to a robust internal security model (security and privacy by design). This data retention is only used for secure storage purposes.

7. *What are my rights and choices regarding my data?*

Where the processing of Data is subject to your consent, you may withdraw such consent at any time, without affecting the lawfulness of the processing carried out prior to such withdrawal. To withdraw your consent, please contact your Employer's operational team.

You have the right to (1) request access to, and correction or deletion of, the information collected about them; (2) request to limit the processing of their information; (3) object to the processing of their information; or (4) in certain very limited cases, request the portability of certain information. To exercise these or other rights, please contact your Employer's operational team.

You also have the right to file a complaint regarding the way your personal data is processed on behalf of your Employer's operational team with the supervisory authority: **Commission Nationale de l'Informatique et des Libertés** (French Data Protection Authority).

8. *Data Protection Officer's contact details*

For all your requests concerning your personal data processing, we invite you to contact TEHTRIS DPO - privacy@tehtris.com.

Last policy updated: 24 April 2025