Polski | English

This is a courtesy translation for convenience only. In case of any discrepancy, the Polish original (prywatnosc.html / prywatnosc.pdf) is the legally binding version.

PRIVACY POLICY — TIMEGUARDIAN.PL

Last updated: September 14, 2026

§1. DATA CONTROLLER

1. The controller of personal data of Users of the timeguardian.pl website is an individual: Bartosz Wania, residing in Poland, conducting sales under Poland's unregistered-activity regime (hereinafter the "Controller"). The Controller's full address details are provided to the buyer in the email confirming the purchase.

2. Contact with the Controller is via email: kontakt@timeguardian.pl.

§2. PURPOSES AND LEGAL BASIS FOR PROCESSING

1. Performance of the transaction and provision of services (Art. 6(1)(b) GDPR): We process the email address, name, and purchase data in order to generate and send the License Key.

2. Maintaining the Parent Panel account (Art. 6(1)(b) GDPR): We process the email address, a securely hashed password (bcrypt), the name of the child's computer, and the ntfy service token, to enable remote management of the program.

3. License verification and security (Art. 6(1)(f) GDPR — legitimate interest): We process the device hardware identifier (HWID), operating system version, and IP addresses (in server logs for a maximum of 30 days), for the purpose of protecting the software against piracy and IT attacks.

§3. DATA RELATED TO THE CHILD'S ACTIVITY

1. The Software allows a parent to remotely view a child's activity (including on-demand screenshots, active-app reports, and text messages) via a notification system running on the Controller's server (ntfy.timeguardian.pl).

2. Text messages (commands, chat, activity reports) are stored on the Controller's server for a maximum of 7 days, after which they are automatically and permanently deleted. Screenshots pass through the server only transiently, solely to be delivered to the parent, and are automatically and permanently deleted after at most 1 hour. This data is not used by the Controller for any purpose other than the technical relay of its delivery to the parent.

3. The legal basis for processing is the performance of the remote-management service for the parent/legal guardian (Art. 6(1)(b) GDPR). The sole recipient and decision-maker regarding the use of this content is the parent/legal guardian using the Parent Panel — the Controller does not analyze or use this data for any other purpose.

4. A parent/legal guardian who configures the Software on their child's computer acts as the person exercising parental authority and is responsible for ensuring that their use of the Software complies with applicable law, including the scope of monitoring of their own minor child.

5. The program additionally collects aggregated daily usage statistics (total screen time in minutes, number of blocked attempts to launch an application or visit a website) — without any content of the activity itself (no site names, app names, or message content). This data is used solely to generate a weekly summary email for the parent/legal guardian. The parent may unsubscribe from this email at any time via a link in its footer — no login or additional data is required to do so.

§4. DATA RETENTION PERIOD

- Purchase data: for 6 years (in accordance with the general limitation period for civil claims under Polish law).
- Parent Panel account data: until an account-deletion request is submitted, or after 3 years of inactivity.

• Text messages (commands, chat, activity reports): maximum 7 days, after which automatic and permanent deletion.

• Screenshots: maximum 1 hour (transient data, solely for delivery to the parent).

• Aggregated daily statistics (total time, number of blocks): 7 days — used solely to generate the weekly summary email, then automatically and permanently deleted.

• Server logs: up to 30 days.

§5. RECIPIENTS OF DATA

1. Data may be disclosed only to entities necessary for the operation of the service:

a) Paddle.com Market Ltd. — handling payments as Merchant of Record (Paddle processes the data necessary to complete and settle transactions under its own terms, described in Paddle's privacy policy);

b) secure hosting providers within the EU, and the ntfy infrastructure running on the Controller's server (message routing as described in §3);

c) Cloudflare, Inc. — ONLY when the parent enables the “Safe DNS” feature in the program: DNS queries from the child's computer are then routed to the public Cloudflare for Families service (addresses 1.1.1.3/1.0.0.3), under its own, independently audited privacy policy (the provider states it does not log DNS query history). The feature is enabled by default, but the parent can turn it off at any time in the Parent Panel;

d) browser push notification providers (e.g. Google Firebase Cloud Messaging, Mozilla Autopush, Apple Push Notification service) — ONLY when the parent actively enables push notifications in the Parent Panel, strictly to the extent technically necessary to deliver the notification to the parent's browser or device.

Data is not sold for marketing purposes.

§6. RIGHTS OF DATA SUBJECTS

1. Users have the right to access their data, rectify it, erase it (“the right to be forgotten”), restrict its processing, port it, and object to its processing. To exercise these rights, write to: kontakt@timeguardian.pl.

2. Users have the right to lodge a complaint with the President of the Polish Data Protection Authority (Urząd Ochrony Danych Osobowych, uodo.gov.pl).

§7. COOKIES AND SECURITY

1. The website uses only technical, strictly necessary cookies to maintain the login session. The connection is fully encrypted with an SSL certificate (HTTPS).

© 2026 Bartosz Wania · timeguardian.pl · kontakt@timeguardian.pl