ENGLISH — CONVENIENCE TRANSLATION

itmatch.dev Cookie Policy

Rules for storing information on devices and using similar technologies

OPERATOR	DOCUMENT
YASTIK SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ, Polish limited liability company, 49 Księcia Witolda Street, unit 15, 50-202 Wrocław, Poland, KRS 0001074378, NIP 8971930898, REGON 527157682	Effective date: 13 September 2026 Version: 1.0 Cookie settings: not applicable — strictly necessary cookies only

This Policy explains how itmatch.dev uses cookies and similar technologies on https://itmatch.dev, Operator-controlled subdomains, the Platform dashboard, API documentation, and the demo page. Read it together with the Privacy Policy: https://itmatch.dev/en/legal/privacy/. If translations differ, the Polish version prevails.

1. Operator, scope and audience

The Operator is YASTIK SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ, 49 Księcia Witolda Street, unit 15, 50-202 Wrocław, Poland, KRS 0001074378, NIP 8971930898, REGON 527157682, share capital PLN 5,000. The Policy covers itmatch.dev, the user panel, API, documentation and user-accessible demo, and controlled subdomains.

The Platform is B2B, but this Policy applies to every visitor. External sites have their own policies. Contact: privacy@itmatch.dev. There is no cookie-settings panel because only strictly necessary cookies are used.

2. What cookies and similar technologies are

Cookie — a small text file or identifier stored by a browser on a device and returned with later requests to the relevant domain.

First-party cookie — a cookie set or read in the itmatch.dev domain or an Operator-controlled subdomain.

Third-party cookie — a cookie set or read by another provider’s domain when its tool has actually been activated.

Session cookie — a cookie generally removed when the browser session ends; a persistent cookie remains until its expiry or manual deletion.

Similar technology — browser local storage, a pixel, SDK, tag, or another mechanism that stores information on or reads it from a device. The currently verified Platform version does not use localStorage, sessionStorage, or IndexedDB.

An authentication cookie value is a random or opaque session identifier, not the user's password. Passwords are not stored in cookies.

3. Currently verified state

The Platform uses only first-party csrftoken and sessionid cookies. No other cookie or optional identifier is used.

There is no cookie tracking or consent-choice record. Cloudflare provides DNS, reverse proxy/tunnel and traffic protection, but no additional Platform cookie is used in the current configuration.

4. When and why a cookie may be set

csrftoken may be set on page opening to protect requests and forms against CSRF. sessionid is set on login or authenticated-session start and carries an opaque identifier, not a password.

Both are technically necessary for the secure service requested by the user. Blocking may prevent login or form submission.

5. Cookie categories

Category	Current status	Rule
Strictly necessary	Active: csrftoken and sessionid.	Necessary for the secure expressly requested service; no consent. Browser deletion may stop operation.
Functional	Not used.	Future use requires separate assessment and consent where required.
Analytics	Not used.	No cookie analytics.
Marketing	Not used.	No advertising or marketing profiling.

Strictly necessary is the only active category. Functional, analytics and marketing cookies are not used.

6. No consent banner and browser control

No consent banner or category switches are shown because no consent-requiring technology operates. Users may manage necessary cookies in the browser, but blocking them may prevent the service.

7. No cookie-consent record

The Operator collects no cookie consent and keeps no choice record because only strictly necessary cookies are used. The Account's legal-document acceptance is a separate record and is not cookie consent.

8. No active optional services

No optional analytics, advertising, marketing or payment tool is active for cookies or declared as a planned deployment.

Before any consent-requiring technology is enabled, the Operator will update documents, assess provider/transfers, block it pending choice and deploy a compliant consent mechanism.

9. Cloudflare and no additional cookies

Cloudflare handles DNS, reverse proxy/tunnel and traffic protection. No additional Cloudflare cookie has been observed or configured for the Platform in the current setup.

If Cloudflare or another feature begins setting additional cookies, the register and information will be updated before use and the legal basis reassessed.

10. Data and purposes

Cookies may involve a CSRF token and random session ID, while server-side processing may also involve IP, browser, time and security events. They do not store passwords or Profile, CV or message content.

Purposes are request/form protection, authentication, session continuity, abuse prevention and security.

11. Legal bases

Under Articles 399–400 of the Polish Electronic Communications Law, device storage/access consent is unnecessary where required for transmission or an electronic service expressly requested by the user. csrftoken and sessionid meet that criterion in the current setup.

Where associated information is personal data, processing relies as appropriate on contract performance or legitimate security interests — Article 6(1)(b) or (f) GDPR. With no optional technologies, consent is not a current basis.

12. Retention and deletion

csrftoken may last up to 12 months under the current setup. sessionid lasts for the authenticated session and is invalidated on logout or expires under server configuration.

Users may delete cookies earlier. Account closure invalidates sessions; a device copy should no longer authenticate. Server-log retention is in the Privacy Policy.

13. Recipients and transfers

Cookie-related technical data is processed by the Operator and AWS in Frankfurt (eu-central-1). Cloudflare provides DNS, reverse proxy/tunnel and traffic protection and may therefore process

HTTP-request technical data; the Platform does not use additional Cloudflare cookies in the current setup.

The Operator does not sell cookie data. Recipient and transfer details: https://itmatch.dev/en/legal/privacy/.

14. Browser controls, changes and contact

Browsers let users view, block and delete cookies. Blocking csrftoken or sessionid may prevent secure forms, login or session continuity.

The Policy will be updated before a new category, purpose or provider is introduced. Questions: privacy@itmatch.dev. Polish is binding; English and Russian are convenience translations.

Schedule 1. Current and conditional cookie register

A. Current first-party cookies

Name	Trigger and purpose	Category and consent	Maximum lifetime
csrftoken	May be set on opening; protects requests and forms against CSRF.	Strictly necessary; no consent.	Up to 12 months; earlier on browser deletion.
sessionid	Set on login/authenticated session; random identifier, not password.	Strictly necessary; no consent.	Authenticated session; until logout or configured expiry.

B. Additional Cloudflare cookies — not currently observed

Name	Condition and purpose	Status / typical lifetime
None	Cloudflare handles DNS, reverse proxy/tunnel and traffic protection; no additional Platform cookie is used in the current setup.	No active cookie; Policy update if this changes.

If a production audit identifies a different name, provider, purpose, or lifetime, the Operator updates this register and, where required, the banner before continued use.

Schedule 2. Minimum choice record and activation rule

Element	Scope	Period / protection
Not applicable	No consent or choice record; csrftoken and sessionid only.	Cookies activate technically when needed; browser controls remain available.