ENGLISH

Privacy Policy for the itmatch.dev Platform

Information about personal data processing and the use of cookies

Effective date: 13 September 2026 | Version: 1.0

Platform Operator and data controller within the scope described below: YASTIK SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ, a Polish limited liability company with its registered office in Wrocław, address: 49 Księcia Witolda Street, unit 15, 50-202 Wrocław, Poland, KRS 0001074378, NIP 8971930898, REGON 527157682, share capital PLN 5,000. Privacy contact: privacy@itmatch.dev.

1. Scope and key information

This Policy explains processing connected with the itmatch.dev B2B website and Platform for visitors, Company Administrators, Managers, contacts and Specialists described by Vendors. It covers the website, user panel, communications, support and security.

The Platform is solely for Companies and people acting professionally for them. Specialists in Profiles have no own accounts. The Operator does not sell personal data and does not disclose a Specialist's surname or contact details to Clients.

The application runs on AWS EC2; application data is held in encrypted PostgreSQL RDS; private files and backups are in S3 with SSE-KMS; transactional e-mail uses AWS SES. The primary Region is Frankfurt, Germany (eu-central-1). Redis runs on EC2. Cloudflare provides DNS, reverse proxy/tunnel and traffic protection. Only cookies necessary for sessions and CSRF protection are used.

2. Data controller and contact

The controller for account data, technical and security data, Company verification, support, complaints, legal communications and claims is YASTIK SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ, 49 Księcia Witolda Street, unit 15, 50-202 Wrocław, Poland, KRS 0001074378, NIP 8971930898, REGON 527157682.

Privacy requests: privacy@itmatch.dev or the Operator's postal address. Technical support: support@itmatch.dev. Legal and illegal-content notices: legal@itmatch.dev. Identity or authority may be verified before disclosure or action.

No data protection officer has been appointed. privacy@itmatch.dev is the privacy and rights contact.

3. Roles of the Vendor, Client and Operator

The Vendor as controller decides whom to add, the data scope, recipients and when a first name is disclosed. It is responsible for lawful basis, accuracy, transparency and individual rights.

The Operator as processor stores and technically processes Profiles on the Vendor's documented instructions, including rules-based matching and controlled disclosure. Details: https://itmatch.dev/en/legal/dpa/.

The Operator as separate controller determines purposes and means for account data, security logs, support, complaints, legal compliance, legal acceptances and claims.

A selected Client may become a separate controller for Profile data received for its own lawful assessment and negotiations. Vendor and Client remain responsible for their own later use and contracts.

4. Data subjects and data sources

Processing may concern website visitors, Company Administrators and Managers, Company representatives, support contacts, communication participants, and employees, contractors or other Specialists described by a Vendor.

Data comes from the User or Company; from the Vendor entering a Profile manually, through API or by uploading a CV; from Platform use and technical logs; from inter-Company communication; and from public business registers. The Platform collects no telephone numbers or bank/payment-provider data.

Before upload, the Vendor must have a lawful basis, provide required information, make this Policy available and satisfy the conditions for first-name disclosure.

5. Categories of data

Account data: name, business e-mail, password hash, role, permissions, optional image, e-mail-verification status and settings/change history. No telephone numbers are collected.

Company data: name, address, NIP, KRS, REGON, website, logo, description, verification status and identifying representative/contact data.

Specialist Profile data: full name stored in the system; location, position, projects and dates, skills, domains, experience, education, languages, availability, rate or commercial expectations, CV text and fields proposed from it. Before Vendor approval the Profile is anonymous; afterwards only the first name, without surname or contact data, is shown to the selected Client.

Requirement data: project or role, budget, work model, requirements, technology, locations, education, dates and other Client input.

Communications and activity: messages, PDF/DOCX files, arbitrary links, offers, replies, invitations, interviews, statuses, events and matches. A recognised signing-service link may only be visually highlighted.

Technical/security data: IP, session identifiers, browser/device, login time, requests, errors, failed logins, IP blocks, change logs and legal-acceptance records.

Do not upload identity documents, Polish PESEL numbers, health, biometric, conviction or other special-category data without a dedicated function and lawful basis.

6. Purposes and lawful bases

Account creation and Services — contract performance for a sole trader or legitimate interests of the Operator and Company in serving Company representatives — Article 6(1)(b) or (f) GDPR.

Company/authority verification — contract performance, fraud prevention and legitimate interests in trustworthy access — Article 6(1)(b) and (f).

Matching, communications and negotiations — service performance and Companies' legitimate interests in finding and offering Specialist services — Article 6(1)(b) and (f); the Vendor determines the Profile basis.

Optional CV-text extraction and form proposals through OpenAI — execution of the Vendor's DPA instruction and legitimate interest in efficient data entry; data is saved only after the User's decision. The feature makes no decision about a person.

Security, abuse prevention, support, complaints, compliance and claims — as applicable contract, legal obligation and legitimate interests — Article 6(1)(b), (c) and (f).

Platform improvement — legitimate interests, using aggregated or anonymised data first — Article 6(1)(f). The Operator does not train its own AI models on Company data or CVs.

Consent — Article 6(1)(a) — applies only where a Vendor chooses it as the proper basis for first-name disclosure or law requires separate voluntary consent. The Operator sends no marketing and uses no optional cookies.

7. Employee Profiles and controlled disclosure

Only Company Administrators and Managers have Platform accounts. An Employee Profile is created and managed by the Vendor; the individual described in it does not log into the Platform.

At the matching stage, the profile is presented anonymously to selected recipients. It is not public and is not available to every registered Company. The Vendor selects potential recipients and separately confirms when identifying information may be disclosed.

After Vendor confirmation, a selected Client may see the individual's first name, without the surname, and position. Contact details are not disclosed; contact takes place through the Vendor. The Vendor may restrict access or instruct the Operator to delete the profile at any time, subject to data lawfully retained in communication history or for other permitted purposes.

The Vendor is responsible for keeping the profile current, handling objections and withdrawal of consent, and promptly instructing the Operator to amend or delete data. The Operator assists the Vendor with rights requests under the DPA.

8. Matching and automated processing

Profiles are matched to Requirements algorithmically under rules that may consider location, experience, skills, education, languages, availability, technologies and project terms. Matching itself does not use AI.

The optional OpenAI feature receives CV text, not the file, and proposes form data. Before saving, the User sees every field, may edit or delete it and decides whether to save. OpenAI does not select, reject or assess a Specialist and makes no legal or similarly significant decision.

The Platform makes no automatic employment, counterparty, contract or terms decision. Vendor and Client decide. A temporary automatic IP block after suspicious login attempts is a security measure reviewable by support.

9. Messages, support and administrative access

Messages are visible to conversation participants according to Platform roles and permissions. The Operator does not continuously monitor correspondence.

Production data may be accessed only by the Operator's authorised system administrator/CTO acting from Poland with mandatory MFA, and only for support, security, notices, complaints or legal duties. Changes are logged; mere viewing is not separately logged. Production data is not used in staging.

Companies should not include excessive or special-category data or unnecessary Specialist contact details. Participants remain responsible for later use of communications, files and links.

10. Free Platform and no payment data

The Platform is currently free. The Operator charges no subscription, fee or commission, handles no Platform payments and collects no card, bank-account, invoice or payment-identifier data through the Platform.

If a paid service is offered later, the documents will first be updated and the data scope, recipients and retention disclosed before the Company's separate explicit acceptance. No change will apply retroactively.

11. Strictly necessary cookies only

The Platform uses only two first-party, strictly necessary cookies: csrftoken protects forms and requests against CSRF; sessionid maintains the authenticated session. Login or safe use may fail without them.

csrftoken may be stored for up to 12 months under the current configuration. sessionid lasts for the authenticated session and is invalidated on logout or expires under server configuration. Browser deletion or blocking may prevent account use.

No functional, analytics or marketing cookies are used; there is no cookie tracking or consent-choice record. No consent banner is shown because only technologies necessary for the requested service are used. Details: https://itmatch.dev/en/legal/cookies/.

Cloudflare provides DNS, reverse proxy/tunnel and traffic protection, but no additional Platform cookie is used in the current configuration. Documents will be updated before that setup is expanded.

12. Recipients and service providers

Data may be received only as necessary by selected Vendors and Clients; the authorised Operator administrator; Amazon Web Services EMEA SARL (EC2, RDS, S3, KMS and SES in eu-central-1); Cloudflare for DNS, reverse proxy/tunnel and traffic protection; the relevant OpenAI group entity providing optional CV-text API processing; confidential advisers; authorities/courts where legally required; and a legal successor subject to individual rights.

Only CV text needed to propose fields, not the original file, is sent to OpenAI. OpenAI does not use API data for model training by default, but standard abuse-monitoring logs may include content and metadata and be retained by OpenAI for up to 30 days unless an approved shorter retention control or Zero Data Retention applies to the Operator's account. The Operator does not currently claim ZDR.

Providers are bound by appropriate terms and purpose limitation. Current list: https://itmatch.dev/en/legal/subprocessors/. The Operator does not sell data.

13. Transfers outside the EEA

Primary application data is stored in AWS Frankfurt, Germany. Cloudflare's global infrastructure may process DNS and HTTP-request technical data, while OpenAI's global infrastructure may process CV text sent to its API; this may involve limited access or transfer outside the EEA. A Company may also choose a counterparty in any country.

For transfers outside the EEA the Operator uses a Chapter V GDPR mechanism, such as an adequacy decision, EU–US Data Privacy Framework for an eligible recipient or Standard Contractual Clauses with assessment and supplementary measures where needed.

Where a Vendor discloses a Profile to a Client outside the EEA, the Vendor as controller is responsible for lawfulness, transfer mechanism and Specialist information. The Operator may require confirmation or restrict access where law requires.

14. Retention periods

The following reflects current mechanisms and criteria. An erasure right, legal duty, security need or claim may require earlier erasure or justify longer restricted retention.

- Account, Profile and Requirement: 7-day reversible grace period after deletion request, then anonymisation or soft deletion. Records marked is_removed currently remain in the database without an automated physical-deletion deadline, until individual erasure/anonymisation or a necessity review.
- Chats, offers, stages, contracts and Transaction Documents: soft-deleted when a Company closes; no automated purge deadline. They may remain until manual erasure/anonymisation, purpose expiry, a justified request or the end of evidence/claim needs.
- Application security/audit data, IP, django-axes, auditlog and legal-acceptance IP: no automatic 12-month purge; retained for security/evidence until manual deletion or periodic review. CloudWatch server logs are generally configured for 14–30 days.

- Support and complaints: soft-deleted with no fixed automated purge; until manual deletion, purpose expiry or claim closure.
- Terms/DPA/NDA acceptances and Policy acknowledgement: retained after User anonymisation as version/time/IP evidence, with no automated purge, until evidential purpose ends, manual deletion or legally required restriction.
- Automated RDS backups: production up to 14 days; staging up to 7 days. Production data is not used in staging.
- S3 database dumps: no lifecycle is currently configured, so they remain until manual deletion. Deleted data may remain in RDS until backup expiry and in an S3 dump until that dump is manually deleted.

The Operator should regularly assess necessity and erase or irreversibly anonymise data once no purpose or basis remains. Permanently anonymous statistics may be retained longer.

15. Account and profile deletion and business history

A deletion instruction starts a 7-day grace period during which it can be reversed. The account and relevant profile data are then anonymised or soft-deleted and access is removed. A neutral deleted-user label may remain in history.

Soft deletion is not automatic physical deletion. Messages, offers, contracts, events and acceptance records also concern other Companies or support evidence and currently have no automated purge. Access remains restricted and an individual may request erasure or restriction; the Operator balances the request against others' rights, law and claims.

Deleting a Specialist Profile removes it from active matching and disclosure. Data already in lawfully retained communication may remain minimally. Production RDS copies expire within 14 days; S3 dumps require manual deletion.

16. Individual rights

Depending on the lawful basis and circumstances, an individual has the right to information; access and a copy; rectification; erasure; restriction; data portability; objection to processing based on legitimate interests; withdrawal of consent at any time without affecting prior processing; and complaint to a supervisory authority.

Rights are not absolute. The Operator or competent Vendor may refuse to the extent permitted by law, including where data is required by a legal obligation, the rights of others or the establishment, exercise or defence of legal claims. Any refusal will be appropriately explained.

An individual described in an Employee Profile should generally address a request to the Vendor that created the profile and acts as controller. A request may also be sent to privacy@itmatch.dev; the Operator will forward it to the appropriate Vendor and assist under the DPA, and will respond directly for processing under its own control.

17. Exercising rights and copies of data

The Operator responds to a valid request without undue delay, generally within one month. Where necessary due to complexity or the number of requests, this may be extended by two further months; the individual will be informed of the extension and reasons.

Rights requests are generally free. For manifestly unfounded or excessive requests, the Operator may charge a reasonable fee or refuse to act as permitted by the GDPR.

The Platform does not currently provide a self-service bulk export of all Company data. This does not restrict an individual's statutory right to a copy or data portability where the relevant conditions are met.

18. Security

Measures include HTTPS/TLS, cryptographic password hashing, role-based least privilege, mandatory MFA for administrative access, failed-login blocking, encrypted RDS, private S3 with SSE-KMS and temporary authenticated links, encrypted backups and incident procedures. Redis runs on EC2.

Production access is currently limited to one authorised system administrator/CTO in Poland. Changes are logged, but each view is not separately logged. Production data is not used in staging. Companies remain responsible for their credentials and permissions.

PDF/DOCX files and external links may come from other Users. Visual highlighting of a signing link does not guarantee authenticity or security; verify sender, domain and document before opening or signing. No system is absolutely secure.

19. Minors, marketing and notifications

Only adults acting for Companies may hold accounts. The Platform is not directed to children.

The Operator sends no newsletter or marketing messages, performs no advertising profiling and makes no SMS/telephone contact. The Platform collects no telephone numbers.

AWS SES may send only transactional messages from no-reply@itmatch.dev: registration, e-mail confirmation, password reset, invitations, new messages, matches, interviews, offers, document changes and security alerts. no-reply is not a contact address; use support@itmatch.dev, privacy@itmatch.dev or legal@itmatch.dev.

20. Complaints, Policy changes and language versions

An individual may lodge a complaint with the President of the Personal Data Protection Office, ul. Stanisława Moniuszki 1A, 00-014 Warsaw, using the channels listed at uodo.gov.pl. Before lodging a complaint, we encourage contact at privacy@itmatch.dev so that the matter can be investigated.

The Operator may update this Policy when functions, providers, law or processing change. Material changes will be notified in advance through the Platform or work e-mail where feasible and appropriate. The date and version at the top identify the current text.

This Policy is prepared in Polish, English and Russian. If there is any inconsistency, the Polish version prevails. Translations are provided for convenience.