

ENGLISH — CONVENIENCE TRANSLATION

itmatch.dev Master Platform NDA

Mutual non-disclosure agreement — Operator ↔ Company and Vendor ↔ Client

OPERATOR	COMPANY
YASTIK SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ, 49 Księcia Witolda Street, unit 15, 50-202 Wrocław, Poland, NIP 8971930898, KRS 0001074378, REGON 527157682, share capital PLN 5,000	The Company identified in the Company Account and electronic acceptance record

This Master Platform NDA ("NDA") forms part of the Terms: <https://itmatch.dev/en/legal/terms/>. It is concluded through the single acceptance checkbox selected by an authorised Company Administrator. It applies to free access and future Services separately accepted by the Company. Effective date: 13 September 2026. Version: 1.0.

1. Parties, contractual layers and acceptance

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. Company means the business in the Account acting as Vendor, Client or both.

The single checkbox accepts the binding Terms, DPA and this NDA and acknowledges the Privacy and Cookie Policies. The Operator records versions, date/time, User, Company and IP.

The NDA creates mutual Operator–Company protection and a direct mutual Vendor–Client layer for each Interaction. The latter arises automatically at the first Protected View of the other Company's information.

The Operator only presents the NDA and records evidence. It is not an agent, Company-contract party, Specialist employer or guarantor.

2. Definitions

Confidential Information — any non-public information described in Clause 4, irrespective of form, medium, language or marking and whether disclosed directly, through the Platform, in a call, interview or presentation, or inferred from a combination of data.

Disclosing Party — the Operator or Company to which Confidential Information relates or which is entitled to disclose it.

Receiving Party — the Operator or Company that obtains access to Confidential Information.

Authorised Person — a Company Administrator or Company Manager with the required Company Account permission; for the Operator, an authorised employee or provider under Clause 9.

Outsider — any person other than the parties to the relevant relationship and their Authorised Persons. A participating Vendor, Client and their Authorised Persons are not Outsiders for that Interaction.

Vendor — a Company offering a Specialist's or team's services through the Platform.

Client — a Company publishing a Requirement or evaluating a Vendor's services.

Profile — information about a Specialist or team, including skills, experience, availability, commercial expectations, certificates and portfolio.

Requirement — a vacancy, project request or other description of a service sought, including budget, requirements, location, technology and project information.

Protected View — a Company's first opening of another Company's Profile, Requirement or other non-public material, including material initially shown in non-identifying form.

Platform Interaction — a Protected View and the related match, messages, offer, interview, negotiation, documents and subsequent transaction.

Trade Secret — information meeting the applicable statutory conditions for a trade secret at the relevant time, including Article 11 of the Polish Act on Combating Unfair Competition.

3. Scope, mutuality and start of protection

Duties are mutual. Protection does not depend on a Transaction, full identity, marking or future paid plan; the Platform is currently free.

The Vendor–Client layer starts at the first Protected View and covers the Companies and information in that Interaction.

Negotiations, the Interaction, rates, prices and terms may be known to participants but remain confidential from third parties.

Contractual confidentiality applies, and qualifying Trade Secrets retain statutory protection.

4. What constitutes Confidential Information

Confidential Information is any non-public information that a reasonable business would regard as confidential in the circumstances, including:

- Profiles, Specialist identities and attributes, skills, experience, availability, salary or commercial expectations, certificates and portfolios;
- Requirements, budgets, rates, working conditions, permitted locations, criteria, technology, architecture and information about the project and end client;
- matches, messages, notes, calls, interviews, offers, negotiations, transaction history and reasons for decisions;
- contracts, drafts, signatures, invoices, settlement information, PDF/DOCX documents, links and other attachments;

- strategies, margins, prices, forecasts, sales plans, customer and supplier lists, procedures and Company know-how;
- the Operator's source or object code, APIs, technical documentation, data models, architecture, matching mechanisms, safeguards, vulnerabilities, logs, roadmaps and non-public statistics;
- copies, extracts, analyses, compilations and inferences from which any of the above can be reconstructed or derived.

Information disclosed orally in an interview, call, meeting or presentation is protected without later written confirmation where its nature or the circumstances indicate confidentiality. The absence of a "Confidential" label does not remove protection.

A Company's public registry details, public website, logo and public description are not Confidential Information by themselves. A non-public arrangement of that data, verification material, analysis or connection with an Interaction may remain confidential.

5. Exclusions and disclosures protected by law

The confidentiality duty does not apply to information the Receiving Party demonstrates by reliable records: (a) became public without breach of this NDA; (b) was lawfully known without confidentiality duty before disclosure; (c) was lawfully obtained from a third party without breach; (d) was independently developed without use of Confidential Information; or (e) was expressly released in documentary form by the Disclosing Party.

Public availability of individual elements does not make a non-public compilation, structure, relationship or inference public. The Receiving Party bears the burden of establishing an exclusion.

The NDA does not prohibit a disclosure protected by mandatory law, including public-interest reporting of wrongdoing, legally protected expression, protection of a legitimate interest or necessary disclosure to worker representatives. Clause 14 governs disclosure compelled by an authority.

Personal data remains additionally subject to the GDPR, the applicable Privacy Policy and DPA. This NDA is not a legal basis for processing personal data and does not restrict data-subject rights.

6. Permitted Purpose and use limitation

The Receiving Party may use Confidential Information solely to use the Platform, assess a match, prepare and conduct an interview, negotiate, conclude and perform a lawful B2B agreement between Vendor and Client, and settle and protect rights arising from that relationship (the "Permitted Purpose").

Information must not be used for unrelated recruitment, development of a competing product, an independent candidate or customer database, market profiling, unagreed benchmarking, marketing, data sale or an advantage unrelated to the Permitted Purpose.

A necessary copy may be transferred to secure corporate e-mail, CRM or document systems only for the Permitted Purpose and with access at least as restrictive as on the Platform. This does not permit bulk export.

The Receiving Party limits use and disclosure to the minimum necessary and promptly ceases use when the Permitted Purpose ends.

7. Access and Authorised Persons

Direct access to a Company's Confidential Information on the Platform is limited to its Company Administrators and Company Managers who hold the necessary permissions. The Company regularly reviews roles, does not share credentials and promptly revokes access when the need or authority ends.

A Company must not disclose Confidential Information to other employees, affiliates, advisers or contractors unless the Disclosing Party consents or disclosure is required by law under Clause 14. An Administrator or Manager remains responsible for secure use of approved corporate systems.

As a narrow exception, a Vendor may disclose to a Specialist the minimum Client Confidential Information needed to assess a project or prepare an interview if the Specialist is first bound by materially equivalent confidentiality duties. The Vendor is responsible for that disclosure and the Specialist's acts as for its own.

Each Company is responsible to the Disclosing Party for breaches by its Administrators, Managers and persons to whom it disclosed information within a permitted exception.

8. Standard of protection, copying and channels

The Receiving Party protects Confidential Information with at least the care used for its own information of similar sensitivity and no less than reasonable professional care. It applies access controls, secure devices and corporate accounts, updates, session protection and other risk-appropriate measures.

Screenshots, individual downloads, printing and copies are permitted only where needed for the specific Interaction. Copies retain their confidential status, are kept in controlled locations and follow the same deletion periods.

Confidential Information must not be sent through personal mailboxes, public links, open repositories, unsecured media or channels without clearly restricted recipients. The Receiving Party verifies the recipient and material before sending.

A Platform file type or function is not confirmation that its content is safe. Each Company is responsible for checking files before sending and opening them under the Terms.

9. Operator-side confidentiality

The Operator uses Company Confidential Information only to provide and secure the Services, perform rules-based matching, deliver communications, support complaints, prevent abuse, enforce agreements and comply with law. It does not use it to bill the Company because the Platform is free.

Production access is currently limited to the authorised system administrator/CTO in Poland, bound by confidentiality, least privilege and mandatory MFA. Changes are logged; mere viewing is not separately logged. Dialogues are not routinely monitored.

Infrastructure providers may use information only for the instructed service under written duties. The Operator may create only irreversibly anonymous or aggregated statistics that identify no Company, Specialist, Interaction or document.

10. Prohibited activities

Without prior consent from the relevant Disclosing Party, the following are prohibited:

- scraping, crawling, bulk reading, copying or indexing Profiles, Requirements, messages or other resources;
- building a separate database from Platform information, combining data to reconstruct a database, or reselling or sharing data;
- attempting to re-identify an anonymous or restricted Profile, searching for Specialist contacts or bypassing staged disclosure;
- reverse engineering, decompiling, protocol analysis, unauthorised security testing, bypassing access controls or exploiting Platform vulnerabilities;
- entering Confidential Information into a public or external AI system, language model, automated translator or analytics service, or using it for model training or evaluation;
- spam, social-media publication, public discussion of an Interaction or disclosure to a competitor or Outsider.

Reverse-engineering restrictions apply to the maximum extent permitted by law and do not exclude rights that cannot be contractually restricted. Authorised security testing requires the Operator's prior written scope.

11. Profiles, Specialist identity and third-party information

The Vendor warrants that it is entitled to offer the Specialist's services, has a basis to disclose the information and has given required information to the individual and, where necessary, obtained appropriate consent. A Vendor must not publish a person whom it does not employ, represent or otherwise have the right to present.

A Profile may first be disclosed to selected recipients in non-identifying form. After separate Vendor confirmation, the selected Client may see the first name without surname and position; Specialist contact data is not part of the standard Profile disclosure.

The Client must not attempt to determine the Specialist's full identity, surname, private contact details or employer outside the approved process. Accidentally learned contact details remain Confidential Information and must not be used for direct contact without Vendor consent.

A party disclosing another person's information, certificate, portfolio or document is responsible for the right to use it. The NDA transfers no third-party rights and does not replace personal-data, copyright or professional-secrecy duties.

12. Protection of the Vendor relationship and Interaction

For 12 months after the last permitted disclosure of a non-public Profile or a specific Specialist's identity, the Client must not use Platform information to contact, hire, contract with or obtain that Specialist while bypassing the Vendor.

This covers affiliates and persons acting for the Client. If the Specialist makes direct contact because of the Interaction, the Client informs the Vendor and does not exploit it to bypass the Vendor.

It does not apply to a proven prior active relationship, a general public recruitment response without Confidential Information, or express Vendor consent.

This protects a specific Interaction, not a general no-hire. It does not restrict the Specialist's freedom or lawful competition and creates no Operator commission or fee.

13. Security and confidentiality incident

Each Party maintains safeguards appropriate to the nature of the information, access method and likely impact of a breach. A Company secures Accounts, passwords, devices, sessions and roles and promptly revokes unauthorised access.

A Party that becomes aware of unlawful acquisition, use, loss or disclosure of Confidential Information notifies the relevant Disclosing Party without undue delay and no later than 48 hours after awareness. Notice to the Operator is sent to privacy@itmatch.dev.

As available, the notice describes the nature and timing, affected information and persons, likely impact, measures taken or planned, containment status and a secure contact. Lack of complete information does not delay the first notice; updates may be phased.

The responsible Party promptly contains the event, reasonably preserves necessary evidence, removes the cause, prevents recurrence and cooperates proportionately with the affected Party. Notice and cooperation do not by themselves admit liability.

14. Legally compelled disclosure and protected reports

Where a court, authority or mandatory law requires disclosure, the Receiving Party — unless prohibited — gives advance notice to the Disclosing Party, identifies the basis and scope and allows a reasonable opportunity to seek protection.

The Receiving Party discloses only the legally required minimum, seeks confidential treatment or a protective measure where available and continues to protect the remainder. If advance notice is prohibited, it notifies promptly after the prohibition ends where lawful.

The NDA does not restrict reports to authorities, whistleblowers, worker representatives or others where disclosure is protected by mandatory law. The reporting person should still limit disclosure to the necessary minimum where the law permits.

15. Return, deletion and restricted archival copy

Upon a verified Disclosing Party request or when the Permitted Purpose ends, the Receiving Party ceases ordinary use and, within a reasonable period normally not exceeding 30 days, returns or deletes active copies of the identified Confidential Information under its control.

The request must reasonably identify the information and Interaction. Deletion must not prejudice the other Company's rights to its own messages, offers, signed agreement, transaction history or material required to perform the contract and defend claims. Access and further use are then restricted to that permitted purpose.

Deletion of a Company Account and data held by the Operator follows the DPA, Privacy Policy and Terms. Shared messages and documents may remain in the other Company's view; that does not release it from this NDA.

The Receiving Party may retain one restricted archival copy only where required by law, accounting, insurance or defence of a claim. It is segregated from ordinary use, accessible only for the mandatory purpose and protected throughout retention. Rotating backups may expire in the ordinary cycle without restoration to use.

After completion, the Receiving Party confirms deletion on reasonable request, subject to lawfully retained copies. It need not delete public, independently developed or its own information.

16. Term and survival

The NDA applies from electronic acceptance while the Account or Services continue. Each Vendor–Client layer applies from the relevant Protected View through the Interaction and then for the periods below.

For ordinary Confidential Information, non-disclosure and use restrictions continue for three years after the later of the last disclosure of that information or the end of the relevant Interaction or Service. For a Trade Secret, they continue for as long as the information meets the statutory conditions for secrecy.

The 12-month period in Clause 12 runs independently. Personal-data duties continue under law, the DPA and Privacy Policy. Ownership, deletion, archive, incident, liability, remedy, governing-law and language provisions survive for as long as their purpose requires.

17. Enforcement, suspension and remedies

A remediable breach may be warned and given a cure period. Credible risk of disclosure, bulk extraction, control circumvention or serious harm permits immediate necessary access restriction.

Repeated or material breach may cause Account suspension/deletion. The Disclosing Party may seek cessation, deletion/delivery, interim relief, proven loss and statutory remedies.

The Operator enforces its own rights and Platform rules, including system protection and no scraping. It does not pursue a Vendor's or Client's claim or guarantee recovery.

18. Liability, no assurance and ownership rights

Liability is subject to the Terms to the maximum lawful extent. Limits do not apply where prohibited or to wilful breach, unlawful Trade Secret use or knowing disclosure.

The Operator is responsible for its own duties but not an independent breach by Vendor, Client or their people unless culpable Operator conduct caused or materially enabled it.

Information is for assessment and is not a warranty of completeness, availability or outcome absent an express assurance. The NDA transfers no ownership/licence and requires no Transaction.

19. Relationship with the Terms, DPA and separate NDA

The NDA is part of the Terms and prevails for confidentiality. The Terms prevail for access, moderation and liability unless express protection is reduced.

The DPA and Privacy Policy prevail for bases, roles, rights, retention and personal-data security.

Vendor and Client may conclude a separate NDA that prevails between them where expressly more detailed or strict, without restricting Operator/Platform rights or data rules.

The NDA creates no Operator commission or fee.

20. Notices, amendments, governing law and language

NDA notices are sent through the Platform, to the current Company Administrator work e-mail or to privacy@itmatch.dev. The Company keeps contacts current. An urgent incident notice should be labelled for rapid identification.

The Operator may amend the NDA for changes in law, Platform functions or risk. It gives at least 30 days' notice of a material change unless law or urgent security requires less. A change will not retroactively reduce protection for information already disclosed; a Company may end access before an unacceptable change takes effect.

The NDA is governed by Polish law. Disputes are submitted to the common court competent for the Operator's registered office unless mandatory law requires otherwise. Invalidity of one term does not affect the remainder; it should be replaced by a lawful term closest to its permitted purpose.

The NDA is prepared in Polish, English and Russian. If versions differ, the Polish version prevails. Translations are for convenience and do not alter the binding Polish text.

Annex 1. Information and permitted-access matrix

Category	Status and permitted access
Public Company data	Name, public address, NIP/KRS/REGON, website, logo and public description are not confidential by themselves. Verification material, analysis and the connection to an Interaction may be confidential.
Specialist Profile	Confidential. Initially shared with selected recipients in non-identifying form; after Vendor confirmation, first name without surname and position for the selected Client.
Requirement / project	Confidential unless the Client expressly publishes a public version. Access only for Authorised Persons and, to the minimum extent, a Specialist through the Vendor.
Messages and interviews	Confidential between participants. Oral information is protected without later marking.
Rates, prices and negotiations	May be known by participating Companies and Authorised Persons; confidential against Outsiders.
Contracts and PDFs	Confidential; copying only for the Interaction. Personal data and prohibited categories also follow the DPA, law and Terms.
Operator technology	Code, APIs, architecture, safeguards, vulnerabilities, logs and roadmap are confidential; no reverse engineering or testing without consent.
Anonymous statistics	Not Company Confidential Information if irreversibly anonymous, aggregated and does not reveal an Interaction or document.

Annex 2. Practical boundaries of use and circumvention

Permitted	Prohibited
An authorised Manager opens a Profile and assesses fit.	Bulk browsing or scraping Profiles to build a separate database.
One transaction copy in a secure corporate system.	A public link, personal e-mail, unrestricted folder or disclosure to a competitor.
The Vendor gives a bound Specialist the minimum project description.	The Vendor gives the Specialist the full database, other Profiles, competitor rates or unnecessary Client data.
Contacting the Vendor through the Platform and entering the agreed contract.	Finding Specialist contact details and contracting directly using Platform information to circumvent.
A general public recruitment campaign without Confidential Information.	Targeting a disclosed Specialist through ads, an affiliate or another intermediary to circumvent.
Ordinary corporate tools with access controls.	Pasting information into public AI, an external translator or a training system without consent.

If a Company is uncertain whether intended contact or disclosure is within the Permitted Purpose, it should obtain the Disclosing Party's consent before acting.

Annex 3. Minimum electronic acceptance record

Field	Value / source
Operator	YASTIK SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ, 49 Księcia Witolda Street, unit 15, 50-202 Wrocław, Poland, NIP 8971930898, KRS 0001074378, REGON 527157682
Company	Legal name, identifiers and address from the Company Account
Accepting user	User identifier, name, work e-mail and Company Administrator role
Acceptance	Date and time, version number, displayed language, confirmation of the mandatory checkbox and available technical data
Vendor–Client Interaction	Both Company identifiers, Profile or Requirement identifier and time of the first Protected View
Content	Immutable copy of the accepted NDA version and linked Terms

The Operator retains the record for as long as needed to evidence conclusion and performance and defend claims under the Privacy Policy and law. On a justified request it may provide the Company with the accepted version and confirmation of acceptance within a reasonable scope.