ENGLISH — CONVENIENCE TRANSLATION

itmatch.dev Master DPA

Data Processing Agreement — Vendor Module and Client Module

OPERATOR / PROCESSOR	COMPANY / CONTROLLER
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, share capital PLN 5,000 (the "Operator")	The Company identified in the Company Account and electronic acceptance record, acting as a Vendor, Client or both (the "Company")

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

1. Parties, formation and scope

The Operator is the entity identified in the masthead above. The Company is the business or other professional entity whose legal name, address and registration identifiers are recorded in the Company Account. If the same Company uses the Platform as both Vendor and Client, both Modules apply concurrently to the relevant processing operations.

The person accepting this DPA represents that they are an adult and have authority to bind the Company. The Operator records at least the DPA version, acceptance date and time, User and Company identifier and the IP address used for acceptance. The electronic record is evidence of conclusion; the Company may request a copy of the applicable version.

This DPA governs only the Operator's processing of Company Personal Data as a Processor to supply the Services. Processing for which the Operator acts as a separate Controller — including user accounts, authentication and security, Company verification, support, complaints, legal compliance and claims — is outside this DPA and is governed by the Privacy Policy at https://itmatch.dev/en/legal/privacy/.

2. Definitions

GDPR — Regulation (EU) 2016/679; the terms "controller", "processor", "personal data", "processing", "personal data breach" and "supervisory authority" have the meanings given in the GDPR.

Data Protection Laws — the GDPR, the Polish Personal Data Protection Act of 10 May 2018 and any other mandatory law applicable to processing under this DPA.

Platform — the B2B service available at https://itmatch.dev, including its dashboard, API, matching, messaging, offer and interview features.

Vendor — a Company legally entitled to offer the services of its employees, contractors, sole traders or other specialists and to create their Profiles.

Client — a Company that posts Requirements and evaluates services of individuals presented by Vendors.

Company Personal Data — personal data submitted to the Operator by or for the Company and processed by the Operator as Processor, including Profiles, Requirements, messages, attachments, offers, interviews and activity history.

Documented Instruction — an instruction recorded in this DPA, the Terms, Platform settings or actions, access controls, an API request or a written support request.

Subprocessor — another processor engaged by the Operator to process Company Personal Data.

Transaction Document — a PDF or DOCX file containing an ordinary B2B agreement or a document related to negotiating, concluding or performing a transaction between Vendor and Client.

3. Roles and allocation of responsibility

The Company is the Controller of Company Personal Data and determines the purposes and essential means of processing. The Operator is the Processor for technical storage, organisation, retrieval, filtering, matching, disclosure to selected recipients, transmission, restriction and deletion in accordance with Documented Instructions.

After a Vendor-confirmed disclosure of a Profile to a selected Client, that Client may become a separate Controller of received data for its own assessment, negotiations, due diligence and contract conclusion. Vendor and Client are responsible for their own subsequent processing and the appropriate sharing mechanism. They are not joint controllers merely because they use the Platform unless they jointly determine purposes and means within Article 26 GDPR.

This DPA does not replace a data-sharing agreement, privacy notice, NDA or other arrangement required directly between Vendor and Client. The Operator does not become an employer, employment agency, transaction party or representative of the individual described in a Profile.

If the Operator determines the purposes and means of processing Company Personal Data outside Documented Instructions, it assumes Controller obligations to the extent required by Data Protection Laws, without prejudice to the Company's other remedies.

4. Subject matter, nature, purpose and duration

Processing supports Profiles and Requirements, rules-based matching, communication, offers, interviews, stages, PDF/DOCX files, links, support and security.

Operations include collection, recording, organisation, storage, viewing, filtering, rules-based matching, controlled disclosure, transmission, restriction, anonymisation and erasure. At the User's optional instruction, CV text without the original file is sent to the OpenAI API to propose form fields. The User reviews, edits, deletes and decides whether to save. OpenAI performs no matching or person-related decision.

The DPA applies from acceptance throughout the Services and afterwards while the Operator processes Company Personal Data, including soft-deleted data and backups under clause 16 and Annex 7.

5. Documented Instructions

The Operator processes Company Personal Data only on the Company's Documented Instructions, including for a transfer to a third country, unless Union or Member State law requires processing. In that event the Operator informs the Company of the legal requirement before processing unless the law prohibits the information on important grounds of public interest.

Actions by a Company Administrator or authorised Manager, recipient configuration, disclosure confirmation, file upload, API request and deletion request constitute Documented Instructions. A support instruction must originate from an authorised work e-mail address or be verified through another secure method.

If the Operator considers an instruction to infringe Data Protection Laws, it promptly informs the Company and may suspend performance until clarified. The Operator need not perform an instruction outside the Services; the Parties may agree its scope, timing and reasonable cost.

6. Company's obligations as Controller

The Company ensures and remains responsible for the lawfulness of Documented Instructions and Company Personal Data. In particular, it identifies a lawful basis, provides required notices, respects rights and objections, minimises data, sets retention, maintains accuracy and discloses data only to authorised recipients.

Before creating a Profile, a Vendor ensures that it genuinely employs, engages or is otherwise validly authorised to offer that person's services; has a lawful basis for processing and disclosure; has provided the required information; has obtained consent where required or selected as the basis; and can demonstrate its authority to the Operator and Client. It must not publish an individual without their knowledge or whose services it is not entitled to offer.

A Client posts only genuine, current and non-discriminatory Requirements and does not upload candidate data obtained outside a Vendor. The Company grants access only to authorised persons, reviews roles regularly and promptly revokes access when authority ends.

The Company must not submit Article 9 special-category data, Article 10 criminal-conviction data, identity documents, PESEL numbers, health or biometric data or other high-risk data, except the strictly limited ordinary Transaction Document data permitted under Clause 17.

7. Operator's obligations as Processor

The Operator processes only under the DPA and Documented Instructions; ensures confidentiality; maintains Annex 4 measures; follows Subprocessor rules; assists with rights and Articles 32–36 GDPR; performs return/erasure as accurately described in clause 16 and Annex 7; and supplies information and audits under clause 15.

The Operator does not sell Company Personal Data, use it for marketing or an independent candidate database, or train its own AI models on it. OpenAI does not use API data for model training by default, but standard abuse-monitoring logs may include content and metadata and be retained for up to 30 days unless approved shorter retention or ZDR applies. The Operator does not currently claim ZDR.

The Operator may create irreversibly anonymous statistics and informs the Company if it cannot meet a material DPA duty.

8. Personnel, confidentiality and administrative access

Production access is currently limited to the Operator's authorised system administrator/CTO acting from Poland, bound by confidentiality and least privilege. MFA is mandatory.

Messages, files or accounts may be accessed only for support, security, a complaint, outage or legal duty. Changes are logged; mere viewing is not separately logged. Dialogues are not routinely monitored. Production data is not used in staging.

The Company is responsible for credential confidentiality and its Administrators' and Managers' permissions.

9. Security of processing

Risk-appropriate measures include HTTPS/TLS, password hashing, roles and least privilege, mandatory administrative MFA, encrypted RDS, private S3 with SSE-KMS and temporary authenticated links, encrypted backups, failed-login blocking and incident procedures. Annex 4 gives details.

Measures may change without materially reducing overall protection and are reviewed after a material change or incident.

The Company uses secure devices and unique passwords, promptly removes access and verifies recipients, files and links. The Operator does not guarantee automated malware scanning or external-link authenticity.

10. Data-subject rights

The Company is responsible for responding to data-subject requests. If the Operator receives a request concerning Company Personal Data, it does not respond substantively without the Company's instruction unless legally required. It forwards the request to the appropriate Company without undue delay and no later than 3 Business Days after identifying the relevant Controller.

Taking account of the nature of processing, the Operator assists through appropriate technical and organisational measures with access, rectification, erasure, restriction, portability, objection and other rights. The Company sends instructions in time to meet statutory deadlines and supplies information needed to identify the data securely.

The Operator need not disclose another Company's data, trade secrets, security information or material whose disclosure would infringe third-party rights. The Parties cooperate on redaction, a limited extract or another proportionate solution.

11. Personal Data Breaches

After becoming aware of a Personal Data Breach affecting Company Personal Data, the Operator notifies the Company without undue delay; the first notice is sent no later than 48 hours after awareness. If complete information is not yet available, the Operator provides it in phases without further undue delay.

To the extent known, notice contains the nature of the Breach; categories and approximate number of individuals and records; a contact point; likely consequences; measures taken or proposed; detection date; and information required for the Company's assessment under Articles 33 and 34 GDPR.

The Operator preserves evidence, investigates the cause, contains the impact, documents the Breach and cooperates with the Company. The Company decides on notification to the authority and individuals unless the Operator has an independent legal duty. A notice is not an admission of liability.

12. DPIAs, prior consultation and authorities

Taking account of the processing and information available, the Operator provides reasonable assistance with security compliance, data protection impact assessments, prior consultation and demonstrating compliance. Assistance may include descriptions of architecture, measures, flows, Subprocessors and retention, subject to confidentiality and security.

If a supervisory authority contacts the Operator directly about Company Personal Data, the Operator promptly informs the Company where legally permitted and coordinates the response. It does not disclose more data than a valid binding demand requires.

Standard reasonable assistance required by this DPA is included in the Services. Additional bespoke and labour-intensive work may be subject to a pre-agreed charge unless needed because of the Operator's breach of this DPA or law.

13. Subprocessors

The Company gives general written authorisation for Annex 5 and the current list at https://itmatch.dev/en/legal/subprocessors/. The initial list includes AWS, Cloudflare and the OpenAI API provider for CV text.

The Operator gives at least 30 days' notice before adding or replacing a Subprocessor. The Company may object on a specific data-protection risk; the parties seek mitigation.

If unresolved, the new Subprocessor will not be used for that Company or the Company may terminate the affected part without penalty. Urgent security or law may require shorter notice.

Each Subprocessor is bound by written data-protection duties. The Operator remains responsible to the extent required by Article 28 GDPR.

14. Transfers outside the EEA

The primary application, RDS, files and backups operate in AWS Frankfurt (eu-central-1). 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 transfers outside the EEA.

The Operator uses a Chapter V GDPR mechanism: adequacy, EU–US DPF for an eligible recipient, or appropriate SCCs with assessment and supplementary safeguards.

A Vendor may select a Client in any country. The Vendor as Controller is responsible for disclosure/transfer basis, information and safeguards. The Operator may refuse without a suitable mechanism.

15. Information, audits and inspections

The Operator makes available information reasonably necessary to demonstrate compliance with Article 28 GDPR. An audit begins with documents, a questionnaire and a remote meeting. An on-site audit is permitted where those steps do not provide sufficient assurance or where required by an authority, a material Breach or credible evidence of non-compliance.

An ordinary audit may occur once per year on 30 days' written notice, during business hours and without unreasonable disruption. The auditor must be independent, competent, confidentiality-bound and not a direct Operator competitor. An audit does not permit access to other Companies' data, source code or information whose disclosure would reduce security.

Frequency and notice limits do not apply to an authority-mandated audit or one reasonably required after a Breach or serious suspected non-compliance. The Company bears its own and the Operator's reasonable costs if no material Operator non-compliance is found; otherwise the Operator bears its remediation and reasonable verification costs.

16. Return, deletion and end of Services

Before termination the Company may submit a verified request for a manual return in a reasonable common format, excluding other Controllers' data, security data and separate-Controller data.

Deleting an Account, Profile or Requirement starts a reversible 7-day period, then anonymisation or soft deletion. is_removed records remain without automated hard deletion. Closing a Company soft-deletes chats, offers, stages and Transaction Documents; automated purge is not implemented.

Records may remain until manual erasure/anonymisation, purpose expiry, a justified request or the end of legal, evidential or other-Controller needs. Access is restricted and soft-deleted data is not used for new purposes.

RDS backups expire within 14 days in production and 7 days in staging. Production data is not used in staging. S3 database dumps have no lifecycle and remain until manual deletion.

17. Attachments, Transaction Documents and prohibited data

Only skill-assessment materials to which the Vendor has rights may be added to a Profile. A closed dialogue permits PDF, DOCX and arbitrary links connected with negotiation or B2B. A recognised signing-service link may be highlighted, but that does not authenticate it.

Files are private and available to authenticated authorised participants through temporary addresses. A document may contain ordinary B2B contract, representative, Company, signature and business-contact data. The Platform processes no payments, though a Company contract may contain the Companies' own settlement data.

Identity-document scans, Polish PESEL numbers, private Specialist contacts, health, biometric, conviction and other Article 9/10 data are prohibited without an express feature and lawful basis.

The Operator does not claim automated malware scanning and does not guarantee link safety. Companies verify sender, domain, file and document before opening or signing.

18. Liability, precedence and amendments

The Parties' liability under this DPA is subject to the limitations and exclusions in the Terms to the maximum extent permitted by law. Nothing limits data-subject rights, supervisory authority powers or liability that cannot be limited under the GDPR or Polish law.

This DPA prevails over the Terms for processing and protection of Company Personal Data. An individual agreement prevails only where it expressly modifies an identified DPA clause and preserves Article 28 GDPR requirements.

The Operator may amend the DPA for changes in law, Services, Subprocessors or measures. It gives at least 30 days' prior notice of a material change unless law or urgent security requires less. A change may not retroactively reduce protection. The Company may terminate the affected Service before a material unacceptable change takes effect.

19. Governing law, notices and language

This DPA is governed by Polish law. Disputes are submitted to the common court competent for the Operator's registered office unless mandatory law requires otherwise. The supervisory authority in Poland is the President of the Personal Data Protection Office.

DPA notices are sent through the Platform, to the Company Administrator's work e-mail or to privacy@itmatch.dev. A Subprocessor or amendment notice sent to the current Company Account e-mail is deemed delivered under the Terms. The Company keeps its contact details current.

This DPA is in Polish, English and Russian. Polish prevails; translations are for convenience. Severability and survival apply as required.

Annex 1. General processing description

Element	Description
Subject matter	Supply and maintenance of itmatch.dev B2B Platform functions under the Terms, this DPA and Company actions.
Duration	For the Services and processing for the Company. Deletion: 7-day grace, then anonymisation/soft deletion without general automated hard deletion. RDS: production 14 days, staging 7 days; S3 dumps until manual deletion.
Operations	Collection, storage, viewing, filtering, rules-based matching, optional CV-text transfer to OpenAI for form proposals, disclosure, transmission, restriction, anonymisation and erasure.
Purposes	Profiles and Requirements, matching, communications, offers, interviews, B2B documents, support, integrity and Service security.
Frequency	Continuous during the active Account and as Users act; incidental after termination only for return, erasure, backup or legal requirements.
Primary location	AWS Frankfurt (eu-central-1): EC2, encrypted RDS, private SSE-KMS S3 and SES; Cloudflare's global infrastructure and optional OpenAI API under Annex 6.

Controllers are the Companies registered on the Platform. The Processor is the Operator. Party contact details are established by the masthead, Company Account and acceptance record.

Annex 2. Vendor Module

Scope	Vendor as Controller
Data subjects	Employees, contractors, consultants, sole traders and other specialists whose services the Vendor may lawfully offer; representatives and contacts in documents.
Profile data	Full name in system; location, role, projects/dates, skills, domains, experience, education, languages, availability, rate, CV text and proposed fields.
Disclosure	Initially available only to selected recipients in non-identifying form. After separate Vendor confirmation, a selected Client may see the first name without surname and position; the individual's contact details are not disclosed.

Scope	Vendor as Controller
Source	Vendor enters manually/by API or uploads a CV; reviews, edits, deletes and decides whether to save proposals.
Purpose	Present available services, technically match genuine Requirements, negotiate and communicate through the Vendor.
Specific duties	Lawful basis, notice, consent where required, entitlement to offer services, accuracy, minimisation, rights handling and immediate withdrawal when authority ends.

A Vendor must not create a Profile for an individual whom it does not employ or lawfully represent, or without that individual's required awareness, information and lawful basis.

Annex 3. Client Module

Scope	Client as Controller
Data subjects	Client representatives and contacts; conversation participants; individuals in Profiles disclosed by a Vendor.
Requirement data	Project or role description, budget, remote option, requirements, client-project information, technology stack, permitted locations, education, languages and duration; Client representative's first and last name and work e-mail.
Received data	Anonymous matching data and — only after Vendor confirmation — the individual's first name without surname and position; messages, offers, interview times and permitted Transaction Documents.
Purpose	Publish a genuine need, find an appropriate service, assess, negotiate, interview and prepare an agreement with the Vendor.
Specific duties	Truthfulness and non-discrimination, lawful further use of disclosed data, recipient limitation, no attempt to obtain private contact and no upload of candidate data sourced outside the Vendor.
Further use	After disclosure the Client may act as separate Controller. The DPA does not govern its substantive decision or replace agreements with the Vendor and notices to the individual.

Annex 4. Technical and organisational measures

Area	Current minimum measure
Transmission	HTTPS/TLS for Platform and API connections.

Area	Current minimum measure
Identity	Cryptographic password hashing; individual accounts; mandatory MFA for system administrators.
Authorisation	Company Administrator and Manager roles; function permissions; logical Company separation and application-level authorisation checks; least privilege.
Privileged access	Only the system administrator/CTO in Poland; MFA and confidentiality. Changes are logged; reads are not. No production data in staging.
Infrastructure	Application and Redis on EC2; encrypted PostgreSQL RDS; S3, KMS and SES; eu-central-1; separated environments.
S3 storage	Private buckets, authorisation, temporary signed URLs and SSE-KMS; all User files private.
Network	Cloudflare for DNS, reverse proxy/tunnel and traffic protection; it may process HTTP-request technical data. The application and AWS handle login blocking and event logs.
Continuity	RDS: production up to 14 days, staging up to 7 days. S3 dumps have no lifecycle and require manual deletion.
Files	PDF/DOCX and links in private dialogues; temporary URLs; signing links may be highlighted. Automated malware scanning is not claimed.
Incidents	Identification, containment, evidence preservation, escalation and Company-notification procedure; security event records.
Review	Adequacy review at reasonable intervals and after a material change or incident; risk-based remediation of identified gaps.

No representation is made that AWS EBS encryption, a dedicated KMS key, ISO 27001/SOC 2 certification or penetration testing is in place until actually implemented and verified.

Annex 5. Initial Subprocessor list

Subprocessor	Services	Location / data	Safeguard
Amazon Web Services EMEA SARL	EC2, RDS, S3, KMS, SES	Frankfurt, Germany (eu-central-1); limited support	AWS DPA; SCC/other Chapter V mechanism

Subprocessor	Services	Location / data	Safeguard
Cloudflare, Inc. and applicable group entities	DNS, reverse proxy/tunnel and traffic protection	Global; DNS and HTTP-request technical data	Cloudflare DPA; Chapter V mechanism where required
Applicable OpenAI group entity supplying API	Optional CV-text processing	Global, possible USA; logs up to 30 days; no ZDR claim	OpenAI DPA; DPF or SCC

Annex 6. International transfers

Scenario	Mechanism and responsibility
AWS eu-central-1	Primary storage in Germany. Access or onward processing outside the EEA only under the AWS DPA, relevant SCCs, transfer assessment and supplementary measures where required.
Cloudflare	DNS, reverse proxy/tunnel and traffic protection; Cloudflare may process HTTP-request technical data. If a personal-data transfer becomes material, the Operator will apply an appropriate Chapter V GDPR mechanism.
Vendor-selected Client outside EEA	Vendor as Controller ensures the basis, transparency and Chapter V mechanism. The Operator performs technical disclosure only on documented instruction and may request confirmation of safeguards.
OpenAI API	CV text only; OpenAI DPA mechanism; standard logs up to 30 days unless shorter retention/ZDR is approved.

On reasonable request, the Operator provides information about the mechanism and a copy of relevant safeguards to the extent permitted, with redaction of trade secrets, other-customer data and security information.

Annex 7. Return and deletion procedure

A. Return choice

- Before Account deletion or the termination date, the Company sends a verified request to privacy@itmatch.dev identifying the scope and secure recipient.
- The Operator confirms scope and prepares a manual return in a reasonable, commonly used format suitable for the data; this may include structured data files and PDF copies of attachments.

- Return excludes another Controller's data, trade secrets, security information and Operator separate-controller data. After return, erasure follows unless the Company documents another lawful instruction.

B. Erasure choice

- "Delete Company without a copy" is the documented erasure choice; no prior return request at termination has the same effect.
- Active Profiles and Requirements: 7-day grace after instruction, then anonymisation or soft deletion; no automated hard deletion of is_removed records.
- RDS backups expire within 14 days in production and 7 days in staging. S3 dumps remain until manual deletion because no lifecycle is configured.
- Shared data retained by another Controller is minimised; legally required data is isolated. On reasonable request after completion, the Operator confirms erasure.

C. Operational retention before termination

Category	DPA rule
Active Profiles and Requirements	7-day grace, then hidden and anonymised/soft-deleted; no automated hard deletion of is_removed records.
Messages, offers, interviews and transaction history	Soft-deleted on Company closure; no automated purge. Until manual erasure/anonymisation, purpose expiry, request or end of evidential need.
Files and Transaction Documents	Private; soft-deleted with dialogue; no automated purge, subject to the other Company's rights.
Backups	RDS: production 14 days, staging 7 days. S3 dumps until manual deletion.