BYTEND OY – DATA PROCESSING AGREEMENT

Last updated: 18 August 2026

This Data Processing Agreement ("DPA") forms part of the agreement governing Customer's use of Match ("Principal Agreement").

1. Parties

1.1 Customer / Controller

Customer: [CUSTOMER LEGAL NAME]
Business ID: [BUSINESS ID]
Registered address: [ADDRESS]
Contact: [EMAIL]

("Customer" or "Controller")

1.2 Processor

Bytend Oy
Business ID: **3640672-3**
Traktoritie 2
Helsinki, Finland
Email: **mohamed@bytend.com**

("Bytend" or "Processor")

Customer and Bytend are together the "Parties".

---

2. Purpose and Scope

This DPA governs Bytend's Processing of Customer Personal Data on behalf of Customer in connection with Match.

This DPA is intended to satisfy the requirements applicable to controller-processor arrangements under Regulation (EU) 2016/679 ("GDPR"), the Finnish Data Protection Act (1050/2018) and other applicable European Union or Finnish data-protection legislation.

Where Bytend processes personal data for its own independent purposes, including account administration, billing, security, support and its own legal obligations, such processing is outside the scope of this DPA and is described in Bytend's Privacy Policy.

---

3. Definitions

Unless otherwise stated:

"Customer Data" means data submitted to or processed through Match by or on behalf of Customer.

"Customer Personal Data" means Personal Data contained in Customer Data that Bytend Processes on Customer's behalf under the Principal Agreement.

"Data Protection Law" means GDPR, the Finnish Data Protection Act and other binding EU or Finnish legislation governing the relevant Processing.

"Personal Data Breach" has the meaning given in GDPR.

"Subprocessor" means another processor engaged by Bytend to Process Customer Personal Data on Customer's behalf.

Terms such as "Controller", "Processor", "Data Subject", "Personal Data", "Processing" and "Supervisory Authority" have the meanings given in GDPR.

---

4. Roles of the Parties

4.1 Customer

Customer acts as Controller of Customer Personal Data and determines the purposes and essential means of the Processing.

Customer is responsible for:

a. ensuring that Customer Personal Data is collected and Processed lawfully;

b. providing necessary information to Data Subjects;

c. establishing an appropriate lawful basis;

d. ensuring that its instructions to Bytend comply with Data Protection Law;

e. applying data-minimisation principles; and

f. determining whether any Processing requires a data protection impact assessment.

4.2 Bytend

Bytend acts as Processor of Customer Personal Data and will Process Customer Personal Data only on documented instructions from Customer, except where Processing is required by applicable Union or Finnish law.

Where legally permitted, Bytend will inform Customer before Processing Customer Personal Data pursuant to such a legal requirement.

---

5. Customer Instructions

5.1 Documented Instructions

The Principal Agreement, this DPA, Customer's configuration of Match and lawful instructions submitted through agreed support or administrative channels constitute Customer's documented instructions.

Customer instructs Bytend to Process Customer Personal Data as reasonably necessary to:

a. provide Match;

b. host and store Customer Data;

c. perform data cleaning, validation and enrichment;

d. provide AI-assisted functions;

e. maintain security and service integrity;

f. provide support;

g. maintain backups;

h. return or delete Customer Data;

i. use authorised Subprocessors; and

j. make international transfers permitted by this DPA.

5.2 Unlawful Instructions

If Bytend reasonably believes an instruction infringes Data Protection Law, Bytend will notify Customer unless prohibited from doing so.

Bytend may suspend the affected Processing until the Parties resolve the issue.

---

6. Purpose Limitation and No Training

6.1 Purpose Limitation

Bytend will not Process Customer Personal Data for purposes incompatible with Customer's documented instructions.

6.2 No AI Training

Bytend will not use Customer Personal Data to train or fine-tune general-purpose or foundational AI models operated by Bytend or any third party.

Bytend will not voluntarily opt Customer Personal Data into a third-party AI provider's general model-training or model-improvement programme.

6.3 AI Inference

Customer authorises Bytend to send limited Customer Data to authorised AI API providers where necessary to provide an AI-enabled Match function requested or enabled by Customer.

Bytend will apply data-minimisation practices and commercial/API privacy controls appropriate to the relevant integration.

---

7. Confidentiality and Personnel

Bytend will ensure that persons authorised to Process Customer Personal Data:

a. are bound by confidentiality obligations or an appropriate statutory duty of confidentiality;

b. are granted access only where reasonably necessary for their duties; and

c. receive access appropriate to their role.

Bytend remains responsible for ensuring that its personnel Process Customer Personal Data consistently with this DPA.

---

8. Technical and Organisational Measures

8.1 General Standard

Taking into account:

a. the state of the art;

b. implementation costs;

c. the nature, scope, context and purposes of Processing; and

d. risks to the rights and freedoms of natural persons,

Bytend will implement and maintain appropriate technical and organisational measures designed to provide a level of security appropriate to the risk.

Current categories of measures are described in **Schedule 3**.

8.2 Changes

Bytend may update its security measures as technology and threats evolve, provided that the overall level of protection is not materially reduced.

---

9. Subprocessors

9.1 General Authorisation

Customer grants Bytend general written authorisation to engage Subprocessors in connection with the Service.

The Subprocessors currently relevant to Customer Personal Data are described in Schedule 2.

9.2 Subprocessor Obligations

Before a Subprocessor Processes Customer Personal Data, Bytend will impose data-protection obligations appropriate to the relevant Processing and consistent with the requirements applicable to Bytend under this DPA.

Bytend remains responsible to Customer for the performance of its Subprocessors' relevant data-protection obligations as required by GDPR.

9.3 Changes

Bytend will give Customer reasonable advance notice, normally at least fifteen (15) days, before a new Subprocessor begins materially Processing Customer Personal Data, where practicable.

Notice may be provided by email, through Match or through an up-to-date subprocessor notice maintained by Bytend with an appropriate notification mechanism.

9.4 Objections

Customer may object to a new Subprocessor within ten (10) days after receiving notice where Customer has reasonable and documented grounds relating specifically to the protection of Customer Personal Data.

The Parties will attempt in good faith to identify a commercially reasonable solution.

If no reasonable solution is available and the objection is objectively justified by data-protection concerns, Customer may terminate the materially affected Service without a termination penalty before the relevant new Subprocessor begins Processing Customer Personal Data.

An objection may not be based solely on general commercial preference unrelated to data protection.

---

10. International Transfers

10.1 EEA Processing

Bytend intends to maintain its primary production database and relevant cloud hosting within the EU/EEA as described in Schedule 2.

10.2 Third-Country Access

Customer acknowledges that international service providers or their personnel and subprocessors may in some circumstances Process or access Customer Personal Data outside the EEA.

Customer authorises such Processing where carried out in accordance with this Section.

10.3 Transfer Mechanisms

Where a transfer subject to Chapter V GDPR occurs, Bytend will ensure that an appropriate transfer mechanism applies, including where relevant:

a. a European Commission adequacy decision;

b. the EU-US Data Privacy Framework for an eligible and participating recipient;

c. the European Commission's Standard Contractual Clauses adopted under Implementing Decision (EU) 2021/914; or

d. another lawful transfer mechanism.

10.4 Supplementary Measures

Where required by applicable law, Bytend will assess relevant international-transfer risks and implement reasonable supplementary contractual, organisational or technical measures.

---

11. Data Subject Requests

Taking into account the nature of the Processing, Bytend will provide reasonable assistance to Customer through appropriate technical and organisational measures, insofar as possible, to enable Customer to respond to requests concerning Data Subject rights.

If Bytend receives a Data Subject request relating to Customer Personal Data, Bytend will:

a. notify Customer without undue delay where reasonably identifiable; and

b. not substantively respond on Customer's behalf except on Customer's documented instructions or where legally required.

---

12. Personal Data Breaches

12.1 Notification

Bytend will notify Customer without undue delay after becoming aware of a Personal Data Breach affecting Customer Personal Data and, where reasonably feasible, aims to provide an initial notification within twenty-four (24) hours after awareness.

12.2 Information

As information becomes available, the notification will include available details reasonably necessary for Customer to assess its obligations, including where applicable:

a. the nature of the breach;

b. categories of affected data;

c. categories and approximate number of affected Data Subjects;

d. approximate number of affected records;

e. likely consequences;

f. mitigation or remediation measures taken or proposed; and

g. an appropriate contact point.

Information may be supplied in phases where it is not available at the same time.

12.3 No Admission

A breach notification does not constitute an admission of fault or liability.

12.4 Assistance

Bytend will reasonably cooperate with Customer in investigating, mitigating and remediating the breach.

---

13. Security, DPIAs and Prior Consultation

Taking into account the nature of Processing and information available to Bytend, Bytend will provide reasonable assistance to Customer in fulfilling obligations relating to:

a. security of Processing;

b. Personal Data Breach assessment and notification;

c. data protection impact assessments; and

d. prior consultation with a Supervisory Authority,

where such obligations relate specifically to Processing performed by Bytend under this DPA.

Bytend may charge reasonable fees for exceptional assistance requiring substantial resources beyond normal service obligations, provided that any fee is communicated in advance unless the assistance is required because of Bytend's breach of this DPA.

---

14. Special Categories and Unintended Personal Data

14.1 Intended Scope

Match is not designed for intentional Processing of special-category data, criminal-offence data or other highly sensitive Personal Data.

14.2 Customer Obligation

Customer must not intentionally upload such information unless the Parties have expressly agreed in writing to the additional Processing requirements.

14.3 Incidental Data

If Customer inadvertently includes incidental Personal Data in a project file, Bytend will Process that information under this DPA while it remains within Customer Data.

The accidental inclusion of such data does not authorise Bytend to use it for an independent purpose.

---

15. Return and Deletion

15.1 During the Term

Customer may retrieve or export Customer Data through available Match functionality, subject to the Principal Agreement.

15.2 Recovery Period

Following termination, Customer will normally have thirty (30) days to retrieve available Customer Data unless:

a. the Parties agree otherwise;

b. earlier deletion is requested by Customer and technically feasible; or

c. retention is required by law.

15.3 Active Systems

Customer Personal Data will be deleted from active production systems no later than thirty (30) days after termination of the affected Service.

15.4 Backups

Residual Customer Personal Data contained solely in ordinary backups will be deleted or overwritten through the normal backup lifecycle within ninety (90) days after termination.

During that period, backup data will remain protected and will not be restored to ordinary active Processing except where reasonably necessary for disaster recovery, security or legal purposes.

15.5 Legal Retention

Where applicable law requires continued retention, Bytend may retain the minimum data required for the legally required period and will restrict further Processing to the relevant legal purpose.

15.6 Certification

Upon reasonable written request after the applicable deletion periods, Bytend will provide written confirmation that deletion has been completed in accordance with this Section.

---

16. Audit and Compliance Information

16.1 Compliance Information

Bytend will make available to Customer information reasonably necessary to demonstrate compliance with Article 28 GDPR and this DPA.

Bytend may satisfy reasonable audit requests initially through:

a. security documentation;

b. compliance documentation;

c. vendor or subprocessor information;

d. policies;

e. audit reports or certifications where available; and

f. written responses.

16.2 Customer Audit

Where the information supplied under Section 16.1 is insufficient to demonstrate compliance, Customer may conduct or appoint an independent professional auditor to conduct a reasonable audit.

Except where a Supervisory Authority requires otherwise or a serious incident reasonably requires urgent investigation:

a. audits must be conducted during normal business hours;

b. Customer must normally provide at least thirty (30) days' notice;

c. audits may normally occur no more than once in any twelve-month period;

d. the auditor must be bound by confidentiality obligations;

e. an audit must not compromise the security or confidentiality of another customer; and

f. the audit must not unreasonably disrupt Bytend's operations.

16.3 Costs

Customer bears its reasonable audit costs and Bytend may charge reasonable costs for substantial audit assistance, unless the audit identifies a material breach of this DPA by Bytend, in which case Bytend will bear its own reasonable internal costs relating to remediation.

---

17. Regulatory Cooperation

Bytend will cooperate with competent supervisory authorities to the extent required by Data Protection Law in relation to Processing performed under this DPA.

Nothing in this DPA restricts the lawful investigative or enforcement powers of a Supervisory Authority.

---

18. Liability

18.1 Contractual Allocation

The liability limitations and exclusions in the Principal Agreement apply to contractual claims arising from this DPA to the maximum extent permitted by law.

Accordingly, unless mandatory law prohibits the limitation, the aggregate inter-party contractual liability relating to this DPA forms part of, and does not increase, the aggregate twelve-month liability cap stated in the Principal Agreement.

18.2 Statutory Rights

Nothing in this DPA:

a. limits a Data Subject's statutory rights;

b. prevents a Supervisory Authority from exercising its legal powers;

c. prevents the imposition of an administrative measure or fine where legally permitted; or

d. modifies any liability that cannot legally be excluded, limited or allocated by contract.

18.3 Responsibility Between the Parties

To the extent permitted by law, each Party is responsible for losses caused by its own breach of its obligations under Data Protection Law or this DPA.

---

19. Term and Termination

This DPA takes effect when the Principal Agreement becomes effective and remains in force for as long as Bytend Processes Customer Personal Data on Customer's behalf.

Termination of the Principal Agreement does not terminate obligations under this DPA that by their nature continue until Customer Personal Data has been returned, deleted or lawfully retained.

---

20. Order of Precedence

If this DPA conflicts with the Principal Agreement concerning Processing of Customer Personal Data, this DPA prevails to the extent of that conflict.

For commercial matters unrelated to Processing of Customer Personal Data, the Principal Agreement prevails.

---

21. Governing Law and Jurisdiction

This DPA is governed by the laws of Finland.

The Parties will first seek to resolve disputes through good-faith negotiations.

Any dispute arising from or relating to this DPA that cannot be resolved amicably will be subject to the exclusive jurisdiction of the **Helsinki District Court (Helsingin käräjäoikeus)**, without limiting mandatory rights of Data Subjects or Supervisory Authorities under GDPR.

SCHEDULE 1 – DETAILS OF PROCESSING

1. Subject Matter

Provision of the Match cloud-based B2B SaaS platform, including storage, management, validation, classification, cleaning, enrichment and AI-assisted analysis of Customer Data.

2. Duration

Processing continues for the term of the Principal Agreement and applicable return, deletion and backup periods described in this DPA.

3. Nature of Processing

Processing may include:

a. collection from Customer;

b. uploading;

c. hosting and storage;

d. organisation;

e. structuring;

f. formatting;

g. validation;

h. retrieval;

i. classification;

j. enrichment;

k. comparison and matching;

l. AI-assisted inference;

m. duplicate identification;

n. transmission to authorised Subprocessors;

o. logging;

p. backup;

q. customer support;

r. export; and

s. deletion.

4. Purposes

The purposes are:

a. providing Match;

b. managing construction-material and project information;

c. producing suggested matches and data enrichments;

d. enabling Customer users to review and validate information;

e. maintaining service security and reliability;

f. providing technical support; and

g. performing Customer's documented instructions.

5. Categories of Data Subjects

The intended categories are principally:

a. Customer employees;

b. Customer Authorised Users; and

c. Customer administrators.

Project datasets are not intended to contain personal data concerning other categories of individuals.

Where Customer inadvertently includes information relating to another individual, that person may become an incidental Data Subject for purposes of this DPA.

6. Types of Personal Data

Depending on Customer's use, Customer Personal Data may include:

a. name;

b. work email address;

c. business telephone number;

d. job title;

e. employer or organisation;

f. user role;

g. account identifiers;

h. IP address;

i. technical and usage logs;

j. user audit events; and

k. incidental personal information unintentionally contained in Customer-uploaded files or free-text fields.

7. Sensitive Data

Special categories of Personal Data, criminal-offence information and other highly sensitive Personal Data are not intended categories of Processing and should not intentionally be uploaded.

8. Processing Frequency

Processing may occur continuously or on demand throughout Customer's use of Match.

SCHEDULE 2 – SUBPROCESSORS AND RELEVANT SERVICE PROVIDERS

A. Subprocessors for Customer Personal Data

1. Supabase

Purpose: Database infrastructure, authentication and storage.

Primary relevant region: EU North / Stockholm for Bytend's configured production environment.

Customer Data may be processed as required to provide database, authentication and storage functions.

2. Amazon Web Services (AWS)

Purpose: Cloud infrastructure, hosting and related technical services.

Primary relevant region: EU regions as configured by Bytend.

3. Vercel

Purpose: Frontend deployment, application hosting/delivery and related application infrastructure.

Depending on deployment architecture, Vercel may process technical request metadata or transient application information.

Bytend will apply appropriate Chapter V GDPR safeguards if relevant Personal Data is processed outside the EEA.

4. OpenAI

Purpose: LLM inference used for AI-assisted enrichment, classification, cleaning and related Match functionality.

Only information reasonably necessary for the requested AI function should be transmitted.

Bytend does not opt API data into general model training.

Eligible zero-data-retention or European data-residency functionality may be used where enabled for Bytend's relevant OpenAI API project and endpoint.

If such configuration is not enabled, applicable OpenAI API retention arrangements may apply.

B. Billing Provider

Stripe

Purpose: Payment processing, invoicing and subscription administration.

Stripe principally processes billing and customer-administration information in connection with activities for which Bytend acts as an independent controller.

Customer project datasets are not intended to be transmitted to Stripe.

To the extent Stripe becomes a Subprocessor for particular Customer Personal Data in a specific configuration, the requirements of Section 9 will apply accordingly.

SCHEDULE 3 – TECHNICAL AND ORGANISATIONAL MEASURES

Bytend maintains measures appropriate to the nature and risks of the Processing. Measures include, as applicable:

1. Access Control

a. access to production systems restricted to authorised persons;

b. access based on operational need;

c. least-privilege principles;

d. secure authentication and session management; and

e. removal or modification of access when no longer required.

2. Tenant and Workspace Separation

Technical controls are designed to logically segregate Customer Workspaces and restrict users to data they are authorised to access.

3. Encryption

Bytend uses:

a. industry-standard encrypted network connections for transmission of relevant data; and

b. infrastructure-provider encryption for stored information where supported and applicable.

4. Logging and Monitoring

Systems may maintain:

a. authentication logs;

b. security events;

c. application errors;

d. relevant audit events; and

e. user-confirmed Review-First actions.

Logs are subject to access restrictions and defined retention periods.

5. Backup and Recovery

Relevant production systems use backup or recovery mechanisms appropriate to the system.

Backup copies are protected from ordinary unauthorised access and are subject to defined expiration cycles.

6. Software and Infrastructure Security

Bytend applies commercially reasonable practices concerning:

a. software updates;

b. security patches;

c. dependency management;

d. infrastructure configuration;

e. vulnerability remediation; and

f. development access controls.

7. Incident Management

Bytend maintains procedures for:

a. identifying security incidents;

b. containment;

c. investigation;

d. remediation;

e. recovery; and

f. Personal Data Breach notification where required.

8. Subprocessor Management

Bytend evaluates relevant service providers and enters into appropriate contractual data-protection arrangements before allowing them to Process Customer Personal Data.

9. Data Minimisation

Bytend designs Match so that only information reasonably necessary for Service functionality should be processed.

Where feasible, AI integrations are designed to limit the content transmitted to information needed for the relevant inference operation.

10. AI Data Governance

Customer Personal Data is not intentionally used to train or fine-tune general-purpose or foundational AI models.

Bytend does not voluntarily enable general model-training use of Customer API data.

11. Retention and Deletion

Bytend maintains processes designed to implement the active-system, backup and logging retention periods established in the Principal Agreement, Privacy Policy and this DPA.

12. Human Review

AI-assisted data-processing workflows use the Match Review-First architecture under which material AI suggestions are intended to be presented for user review before confirmed changes are made to core Customer project data.