

BYTEND OY – PRIVACY POLICY

Last updated: 18 August 2026

1. Scope and Controller

This Privacy Policy explains how Bytend Oy processes personal data in connection with the Match B2B SaaS platform, related websites, account administration, customer relationships, support, security and billing.

For the processing described in this Privacy Policy, the controller is:

Bytend Oy

Business ID: **3640672-3**

Traktoritie 2

Helsinki, Finland

Privacy contact: **mohamed@bytend.com**

Match is intended exclusively for business customers. Users of Match are normally employees or other authorised representatives of Bytend's corporate customers.

2. Bytend's Controller and Processor Roles

2.1 Bytend as Controller

Bytend acts as an independent controller where it determines why and how personal data is processed for its own legitimate business purposes, including:

- a. creation and administration of user accounts;
- b. authentication and access management;
- c. administration of the customer relationship;
- d. billing and subscription administration;
- e. customer support;
- f. service security and fraud prevention;
- g. system and audit logging;
- h. legal compliance;
- i. contractual communications; and

j. Bytend's own business records.

2.2 Bytend as Processor

Customers may upload construction-project files and other Customer Data to Match.

Such project information is generally intended to consist of technical, commercial, material and construction data rather than personal information.

If Customer Data contains personal data, the customer generally determines the purpose of that processing and acts as controller. Bytend processes that Customer Personal Data on the customer's behalf as a processor.

Such processing is governed by Bytend's Data Processing Agreement and the customer's instructions rather than this Privacy Policy alone.

3. Personal Data We Process as Controller

3.1 Account and User Information

We may process:

- a. first and last name;
- b. business email address;
- c. telephone number, where provided;
- d. employer or organisation;
- e. job title or user role;
- f. Workspace name;
- g. account identifiers;
- h. authentication information and associated account metadata; and
- i. account status and permissions.

3.2 Customer and Contract Information

We may process:

- a. company name;
- b. Business ID and billing information;

- c. contact-person details;
- d. subscription plan;
- e. orders and contractual communications;
- f. invoice and payment status; and
- g. customer-service history.

3.3 Technical, Security and Usage Information

We may process:

- a. IP address;
- b. browser and device information;
- c. login timestamps;
- d. session information;
- e. security events;
- f. error and diagnostic information;
- g. API and application events;
- h. activity and audit-log information; and
- i. actions confirmed by users in the Review-First workflow.

3.4 Support Communications

If a user contacts Bytend for support, we may process the contact details, message content, attachments and technical information necessary to investigate and respond.

3.5 Payment Information

Stripe or another payment provider may process payment details in connection with subscriptions.

Bytend primarily processes information necessary to administer the subscription, such as billing identifiers, payment status, invoice information and related business contact information.

4. Purposes and Legal Bases

4.1 Provision and Administration of B2B Services

We process business-user account and customer-contact information to provide and administer Match for our corporate customers.

Because individual users are ordinarily employees or representatives of the corporate customer rather than parties personally purchasing the Service, this processing generally relies on Bytend's legitimate interests in:

- a. performing its B2B customer relationships;
- b. allowing authorised customer personnel to use Match;
- c. administering user access; and
- d. communicating with customer representatives.

4.2 Security and Service Integrity

We process technical logs, security events and account information on the basis of our legitimate interests in:

- a. protecting Match and Customer Data;
- b. detecting and investigating unauthorised access;
- c. preventing abuse;
- d. troubleshooting faults;
- e. maintaining service reliability; and
- f. establishing, exercising or defending legal claims where necessary.

4.3 Billing and Administration

We process customer and billing information for our legitimate interests in administering our commercial relationships and collecting amounts due.

Where retention or processing is required by accounting, tax or other applicable legislation, processing is also based on compliance with a legal obligation.

4.4 Support

Support information is processed on the basis of our legitimate interest in providing customer support and maintaining the Service.

4.5 Consent

Where applicable law requires consent for a particular processing activity, such as certain non-essential cookies or a separately agreed identifiable-person marketing testimonial, processing will be based on consent.

Consent can be withdrawn for future processing at any time.

5. AI Processing

5.1 AI-Assisted Service

Match uses artificial-intelligence functionality to assist with data cleaning, classification, enrichment, duplicate detection and preparation of suggested matches and other Outputs.

5.2 Review-First Design

AI-generated suggestions are designed to be reviewed by a human user.

Bytend does not use the described Match functionality to make solely automated decisions about an individual that produce legal effects or similarly significant effects on that individual.

5.3 Customer Project Data

Where an LLM processes personal data contained in Customer Data, Bytend processes that information as a processor on behalf of the relevant customer.

5.4 No Training

Bytend does not use Customer Data to train or fine-tune its own or third-party general-purpose or foundational AI models.

Bytend does not voluntarily opt Customer Data into a third-party LLM provider's general model-training programme.

For OpenAI API processing, Bytend uses business/API controls under which API content is not used for general model training by default.

Where eligible zero-data-retention or European data-residency configurations are available and enabled, Bytend may use those configurations. Where such configuration is not enabled, the provider's ordinary API retention rules may apply.

6. Sources of Personal Data

Personal data is primarily obtained:

- a. directly from the user;

- b. from the user's employer or another authorised representative of the customer;
- c. through use of Match;
- d. from technical systems and security logs;
- e. from customer-support communications; and
- f. from payment and subscription service providers.

Customer project data is obtained from the customer and processed under the customer's responsibility and instructions.

7. Service Providers and Recipients

Bytend uses third-party service providers where necessary to operate Match.

Relevant providers currently include:

7.1 Supabase

Used for database, authentication and related storage infrastructure.

Bytend's primary Supabase production region is configured in the EU North / Stockholm region.

7.2 Amazon Web Services (AWS)

Used for cloud infrastructure and related technical services.

Bytend uses EU regions for relevant production infrastructure.

7.3 Vercel

Used for frontend deployment, application delivery and related technical hosting functionality.

Depending on technical configuration, Vercel may process technical request information and transient application data.

7.4 Stripe

Used for payment processing, billing and subscription administration.

7.5 OpenAI

Used through the OpenAI API for AI-assisted data enrichment and related inference functionality.

OpenAI API data is not voluntarily enabled by Bytend for general model training.

7.6 Other Recipients

Personal data may also be disclosed where necessary:

- a. to professional advisers subject to confidentiality obligations;
- b. to public authorities where disclosure is legally required;
- c. in connection with a merger, acquisition, financing or corporate restructuring subject to appropriate confidentiality protections; or
- d. to enforce or defend legal rights.

Bytend does not sell personal data to advertisers.

8. International Data Transfers

Bytend's primary application and database infrastructure is intended to be located in the EU/EEA.

Some service providers are international organisations or may permit support personnel or subprocessors located outside the EEA to process or access limited personal data.

Where personal data is transferred outside the EEA, Bytend will ensure that the transfer is based on a mechanism permitted under Chapter V GDPR, such as:

- a. a European Commission adequacy decision;
- b. the EU-US Data Privacy Framework where the relevant US recipient validly participates in that framework;
- c. the European Commission Standard Contractual Clauses; or
- d. another legally valid transfer mechanism.

Where required, Bytend will assess the relevant transfer circumstances and implement supplementary safeguards appropriate to the risks.

A copy of applicable transfer safeguards may be requested by contacting Bytend, subject to reasonable redaction of confidential information.

9. Retention

Bytend applies different retention periods depending on the purpose and type of data.

9.1 Active Accounts

Account and operational customer information is normally retained while the customer relationship or relevant user account remains active.

9.2 Termination and Customer Data

Following termination of a Match subscription, customer project data will normally remain available for retrieval for up to thirty (30) days.

Customer Data is then deleted from active production systems no later than thirty (30) days after termination unless a shorter period has been agreed or retention is legally required.

Residual copies stored solely in ordinary backups are deleted or overwritten through the normal backup cycle within ninety (90) days after termination.

Backup copies are not returned to ordinary production use except where necessary for legitimate disaster recovery or security purposes.

9.3 Security and Audit Logs

Routine security, authentication and audit logs are normally retained for up to twelve (12) months from creation unless a longer period is necessary for investigation of a security incident, legal claim or other documented reason.

9.4 Support Information

Ordinary customer-support correspondence may be retained for up to twenty-four (24) months after resolution where reasonably necessary for service history, quality assurance or dispute management.

9.5 Accounting and Statutory Records

Invoices, accounting material and other records subject to mandatory statutory retention requirements are retained for the applicable period required by Finnish law.

9.6 Legal Claims

Information necessary to establish, exercise or defend a legal claim may be retained for as long as reasonably required for that purpose under applicable limitation periods.

9.7 Anonymised Data

Information that has been irreversibly anonymised and is no longer Personal Data may be retained for statistical or service-development purposes.

10. Data Minimisation and Sensitive Data

Match is designed primarily for construction material and project information.

Customers are instructed not to intentionally upload unnecessary special-category data, criminal-offence data, personal identity codes, health information, payment-card data or other sensitive personal data.

If personal information is incidentally included in a project file, Bytend applies the safeguards required by its DPA and processes the information on the customer's behalf.

11. Security

Bytend maintains technical and organisational measures designed to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure and unauthorised access.

Measures include, as appropriate to the relevant system:

- a. logical Workspace separation;
- b. access controls and least-privilege principles;
- c. secure authentication and session controls;
- d. encryption in transit;
- e. infrastructure-provider encryption at rest where applicable;
- f. security and audit logging;
- g. backups and recovery procedures;
- h. security incident procedures;
- i. vendor and subprocessor management; and
- j. data-retention and deletion controls.

No Internet-connected system can be guaranteed to be completely secure.

12. Cookies and Similar Technologies

Match may use cookies or similar technologies that are technically necessary for authentication, security, session management and provision of the Service.

If Bytend introduces non-essential analytics, advertising or similar technologies for which consent is required, the user will be provided with appropriate information and a consent mechanism before those technologies are activated.

13. Customer Names and Logos

Bytend's Terms of Service may permit Bytend to display the corporate name and company logo of a customer to identify that company as a Match or Bytend customer.

A corporate company name and logo will not ordinarily constitute personal data merely because they identify a legal entity.

If marketing material includes an identifiable individual's photograph, personal testimonial, endorsement or other Personal Data, Bytend will identify an appropriate legal basis and obtain separate permission where required.

Customers may request removal of their corporate name or logo in accordance with the Terms by contacting **mohamed@bytend.com**.

14. Data Subject Rights

Subject to the conditions and limitations of GDPR, a data subject may have the right to:

- a. obtain confirmation of whether Bytend processes their personal data;
- b. obtain access to their personal data;
- c. require inaccurate data to be corrected;
- d. require deletion of personal data in applicable circumstances;
- e. restrict processing in applicable circumstances;
- f. object to processing based on legitimate interests;
- g. receive applicable personal data in a portable format where the statutory requirements for portability are met; and
- h. withdraw consent where processing is based on consent.

Rights are not absolute and may be subject to statutory exceptions.

Where Bytend processes Customer Personal Data solely as a processor, a rights request concerning that data should normally be directed to the relevant customer, which is the controller. If such a request is received directly by Bytend, Bytend will handle it in accordance with the DPA and applicable law.

15. Right to Object

Where Bytend processes personal data on the basis of legitimate interests, the data subject has the right to object to the processing based on grounds relating to their particular situation.

Bytend will cease such processing where required by GDPR unless Bytend demonstrates compelling legitimate grounds for continuing the processing or the processing is necessary for the establishment, exercise or defence of legal claims.

16. Complaints

A data subject who considers that Bytend's processing of personal data infringes applicable data-protection law has the right to lodge a complaint with a competent supervisory authority.

In Finland, the competent national supervisory authority is the **Office of the Data Protection Ombudsman (Tietosuoja-valtuutetun toimisto)**.

We encourage data subjects to contact Bytend first where appropriate so that we have an opportunity to investigate the concern.

17. Identity Verification

Bytend may request information reasonably necessary to verify the identity of a person exercising data-protection rights.

Bytend will not request more verification information than reasonably necessary.

18. Changes to this Privacy Policy

Bytend may update this Privacy Policy where its processing activities, Service, legal obligations or service providers materially change.

The current version will be made available through Bytend's website or the Match Service.

Where required by law or appropriate due to the significance of a change, affected users will be notified separately.

19. Contact

Questions and requests concerning this Privacy Policy or Bytend's processing of Personal Data may be sent to:

Bytend Oy
Traktoritie 2
Helsinki, Finland
Email: mohamed@bytend.com