

Privacy Policy

Umain Campaign Contracting Portal

Last Updated: May 25, 2026 Effective Date: March 28, 2026

1. Introduction

Umain AB ("Umain", "we", "us", or "our") is committed to protecting your privacy and complying with applicable data protection laws, including the General Data Protection Regulation (GDPR) EU 2016/679.

This Privacy Policy explains how we collect, use, share, and protect personal data of business contacts ("you") who use the Umain Campaign Contracting Portal ("Portal").

Important: This Portal is a business-to-business (B2B) service. The personal data we process relates to individual contact persons representing business organizations, not end consumers. Umain AB built and operates this Portal as its own product.

2. Data Controller

Umain AB Grev Turegatan 1, 114 46 Stockholm, Sweden Org.nr: 556885-8384

Privacy Contact: Email: campaign.privacy@umain.com

Supervisory Authority: Integritetsskyddsmyndigheten (IMY), Sweden Website: <https://www.imy.se>

3. What Personal Data We Collect

3.1 Information Received From Your Employer/Principal

When your organization invites you to the Portal, they provide us with:

Data Type	Purpose	Source
Full name	Identify the market contact	Your employer/principal (controller-to-controller transfer)
Email address	Portal invitation and login	Your employer/principal (controller-to-controller transfer)

This is a controller-to-controller data transfer under GDPR. Your employer/principal is the controller of their employee data and shares your name and email with Umain AB for the purpose of inviting you to the Portal.

Umain AB becomes an independent controller for that data for portal and campaign purposes.

3.2 Information You Provide Directly

When you use the Portal, we collect:

Data Type	Purpose	Mandatory/Optional
Country/Market	Campaign assignment (e.g., SE, NO, DK)	Mandatory
Organization name	Contract identification	Mandatory
Phone number	Optional contact method	Optional
Company legal entity name	Contract identification	Mandatory
Company registered address	Contract identification	Mandatory
Company org number	Contract identification	Mandatory
Invoicing email	Invoice delivery	Mandatory

Data Type	Purpose	Mandatory/Optional
Consent	Proof of terms acceptance	Mandatory
Contract signature	Legal agreement	Mandatory
Payment details	Payment processing	Mandatory

3.3 Information Automatically Collected

- Authentication logs: Login timestamps, OTP requests
- Payment information: Payment status, chosen payment plan
- Contract actions: Contract viewing, signing timestamps
- Feature toggles: Campaign activation/deactivation actions

4. Legal Basis for Processing (GDPR Art. 6)

We process your personal data based on the following legal grounds:

4.1 Contractual Necessity (Art. 6(1)(b))

Processing is necessary to:

- Execute campaign contracts
- Provide Portal access and functionality
- Process payments
- Deliver contract documents

4.2 Legal Obligation (Art. 6(1)(c))

We must retain certain data to comply with:

- Financial record-keeping laws
- Tax regulations
- Contract law

4.3 Legitimate Interests (Art. 6(1)(f))

We have legitimate interests in:

- Fraud prevention and security monitoring
- Internal audit and compliance
- System performance monitoring

Your rights: You can object to processing based on legitimate interests (see Section 9).

5. How We Use Your Personal Data

5.1 Primary Purposes

- Account Management: Create and maintain your Portal access
- Authentication: Send one-time passwords (OTP) via email
- Contract Execution: Generate, send, and store signed contracts via DocuSign
- Payment Processing: Enable payment via Stripe Checkout
- Communication: Send transactional emails (contract ready, payment confirmations, etc.)

5.2 We Do NOT Use Your Data For

- Marketing or promotional communications (unless separately consented)
- Selling or renting to third parties
- Automated decision-making with legal effects
- Profiling beyond operational needs

6. Who We Share Your Data With

6.1 Third-Party Service Providers (Processors)

All processors are contracted by Umain AB. Data Processing Agreements (DPAs) are required with each processor.

Provider	Purpose	Data Shared	Location	Transfer Mechanism
DocuSign	Contract signing & storage	Name, email, organization, contract details	EU	SCCs
Stripe	Payment processing	Email, payment amounts, customer ID	EU / US	EU-US DPF + SCCs
Resend	Email delivery (OTP codes)	Email, OTP code	US	EU-US DPF
DigitalOcean	Database & file storage	All Portal data	EU	SCCs
Vercel	Web hosting & serverless functions	Request logs, IP addresses	EU	SCCs
Eidra AB	Parent company - manages processor agreements	Administrative only. No direct data access	EU	DPA

6.2 Internal Systems

Your campaign status may be shared with internal systems to enable/disable campaign features. This is not considered a third-party transfer.

6.3 Legal Disclosures

We may disclose your data if required by:

- Court order or legal process
- Law enforcement or regulatory authorities
- Protection of Umain rights or property
- Prevention of fraud or illegal activity

7. International Data Transfers

All third-party processors are bound by Data Processing Agreements (DPAs) including Standard Contractual Clauses (SCCs). Where processors are based in the United States, we additionally require EU-US Data Privacy Framework (DPF) certification.

8. Data Retention

8.1 Retention Periods

We only store your data for as long as necessary to deliver the service and fulfill our legal and contractual obligations.

Data type	Retention Period
Contracts	7 years (Bokföringslag / Swedish Accounting Act)
Payment data	7 years (Swedish tax law)
Portal account data	Deleted on specific date (2026-12-30)

9. Your Rights Under GDPR

9.1 Right of Access (Art. 15)

You have the right to obtain:

- Confirmation that we process your personal data
- A copy of your personal data
- Information about how we use it

How to exercise: Contact campaign.privacy@umain.com.

9.2 Right to Rectification (Art. 16)

You can request correction of inaccurate or incomplete personal data.

How to exercise: Contact us or update your profile in the Portal settings.

9.3 Right to Erasure / "Right to be Forgotten" (Art. 17)

You can request deletion of your personal data if:

- It is no longer necessary for the purposes collected
- You withdraw consent (where applicable)
- You object to processing and there are no overriding legitimate grounds
- Data was unlawfully processed

Limitations: We may retain data if required for:

- Legal obligations
- Establishment, exercise, or defense of legal claims
- Active contract obligations

How to exercise: Contact campaign.privacy@umain.com. We will review your request and respond within 30 days.

9.4 Right to Restriction of Processing (Art. 18)

You can request that we limit how we use your data while:

- Verifying accuracy of contested data
- Assessing your objection to processing
- Retaining data you need for legal claims

How to exercise: Contact campaign.privacy@umain.com.

9.5 Right to Data Portability (Art. 20)

You can request your personal data in a structured, machine-readable format (JSON) to:

- Keep for your own records
- Transfer to another service provider

How to exercise: Contact campaign.privacy@umain.com. We will review your request and respond within 30 days.

9.6 Right to Object (Art. 21)

You can object to processing based on legitimate interests or for direct marketing.

Effect: We will stop processing unless we demonstrate compelling legitimate grounds.

How to exercise: Contact campaign.privacy@umain.com.

9.7 Right to Withdraw Consent

Where processing is based on consent, you may withdraw it at any time. This does not affect the lawfulness of processing before withdrawal.

9.8 Right to Lodge a Complaint (Art. 77)

You have the right to file a complaint with your national Data Protection Authority (DPA) if you believe we have violated your rights.

10. Data Security

10.1 Technical Measures

We implement industry-standard security measures:

- Encryption in transit: HTTPS/TLS for all communications
- Encryption at rest: Database and file storage encrypted
- Secure authentication: bcrypt-hashed passwords (OTP codes)
- Access control: Role-based access, JWT token-based authentication
- Webhook signatures: HMAC-SHA256 validation for incoming webhooks

10.2 Organizational Measures

- Admin access limited to authorized Umain personnel
- Regular security audits and vulnerability assessments
- Employee training on data protection
- Data Processing Agreements with all processors

10.3 Data Breach Response

In the event of a data breach affecting your personal data:

- We will notify the relevant supervisory authority (IMY) within 72 hours (GDPR Art. 33)
 - We will notify you directly if the breach poses a high risk to your rights (GDPR Art. 34)
 - We have an incident response plan in place
-

11. Cookies and Tracking

11.1 Essential Cookies Only

The Portal uses only essential cookies required for functionality:

- Session cookies (JWT authentication)
- Security cookies (CSRF protection)

11.2 No Tracking or Analytics

We do not use:

- Google Analytics or similar tracking tools
 - Advertising cookies
 - Social media pixels
 - Third-party tracking scripts
-

12. Changes to This Privacy Policy

12.1 Notification of Changes

We may update this Privacy Policy from time to time. Material changes will be communicated via email to your registered address

12.2 Version History

- March 27, 2026: Controller-to-controller data flow, Bokföringslag references, anonymization details, IMY as supervisory authority. Added Eidra as sub-processor.
 - March 10, 2026: Initial draft version
-

13. Contact Us

13.1 Privacy Questions

For questions about this Privacy Policy or your personal data:

Email: campaign.privacy@umain.com
Address: Grev Turegatan 1, 114 46 Stockholm, Sweden

13.2 Exercising Your Rights

To exercise any GDPR rights (access, rectification, erasure, etc.):

1. Email: campaign.privacy@umain.com with subject "GDPR Request" 2. Include: Your name, email, organization, and specific request 3. Response Time: We will respond within 30 days (may be extended to 60 days for complex requests)

14. Specific Information for EU/EEA Data Subjects

14.1 GDPR Compliance Statement

Umain AB is committed to full compliance with the EU General Data Protection Regulation (GDPR) for all data subjects in the European Economic Area (EEA).

14.2 Data Controller Details

For EU data subjects, the data controller is:

Umain AB Grev Turegatan 1, 114 46 Stockholm, Sweden Organization number: 556885-8384

14.3 EU Establishment

Umain AB is established in Sweden (EU). No separate EU representative is required under GDPR Art. 27.
