

Schedule A to Subscription and End User License Agreement

PRIVACY POLICY AS OF 1 June 2026

1. GENERAL

This is the Privacy Policy of T.R. Björkbom-Trading Oy ("Company" or "We") applicable to Helm1 website and services operated by Company. Some websites, web pages or services of Company may be subject to specific terms of use. In this case the Privacy Policy constitutes an integral part of such terms; however, should any contradictions occur, such terms shall prevail over this Privacy Policy. In the following by user (the "User" or "You") is meant any individual user of the website and/or thereto related services of Company, and any legal entity represented by such individual user.

Company website may contain links to other websites. Company Privacy Policy applies only to Company website, so if User click on a link to another website, User must read their privacy policy and terms of service.

We operate a software-as-a-service platform (Helm1) which we provide to our business clients and their authorized users. This Privacy Policy explains how we process personal data in our capacity as a data controller — that is, when we determine the purposes and means of processing — in connection with that service provider–client relationship.

When the User has become the User of Helm1 and thereto related services, where applicable, the Google Privacy Policy and Terms of Service and AWS privacy policy and terms of service are applied together with the agreement/s governing the use of Helm1 Technology.

The User agrees to be bound by this Privacy Policy, as amended from time to time, by visiting and/or using the website of Company or by registering and disclosing personal information to Company in connection with its web pages or services as well as by using the services of Company. Any use or disclosure may take place only if the User agrees to this Privacy Policy in its entirety.

Company respects the privacy of the User and commits itself to observe the applicable laws and statutes of Finland and the European Union relating to privacy as well as principles expressed in this Privacy Policy. When Company is the controller of the personal data for the purposes of the Finnish Data Protection Act, with exception where the User is under third-party privacy policy and terms of service according to this Privacy Policy.

This Privacy Policy does not cover personal data that we process on behalf of and under the instructions of our client as a data processor (e.g. data that clients upload or generate within Helm1). The processing of that data is governed by the Data Processing Agreement between us and the relevant client, which Company and client execute separately or which comes into effect by client entering into Helm1 Subscription and End User License Agreement (hereinafter also "SaaS Agreement"). If you have questions about data processed on behalf of a client, please contact that client directly.

If Company and/or Company's service providers processing personal data on Company's behalf transfer personal data to countries outside the EU or the EEA, the transfer is subject to standard data protection clauses adopted by the EU Commission or other appropriate safeguards, unless the EU Commission has found that the level of data protection is adequate in the country in question.

2. CONTROLLER INFORMATION

This Privacy Policy concerns personal data that Company processes about User as a controller. Please find below Company's contact information.

Name: T.R. Björkbom-Trading Oy

Address: Veneentekijäntie 8, Helsinki, Finland

Web address: www.helm1.com

Contact person in data protection issues: John Björkbom

E-mail: [john.bjorkbom\(a\)bjorkbomtrading.fi](mailto:john.bjorkbom@bjorkbomtrading.fi)

3. USE OF DATA

3.1 Personal data

In general the websites of Company can be browsed without providing any personal data about the User. When the User opts to use or purchase the services provided by Company or to otherwise register at the website of Company providing certain contact and identity information, billing information and other personal data will be required.

Company will hold and process any personal data which the User provides via the websites or by submitting emails and/or online forms for its own internal business purposes.

This Privacy Notice applies to the following categories of individuals whose personal data we process as a data controller:

- Representatives, employees, and authorized contacts of our current, prospective, and former clients (including individuals who enquire about or purchase the Helm1 service on behalf of a client organization);
- Individuals who contact our customer support, sales, or account management teams; and
- Other business contacts, partners, suppliers, and professional advisors with whom we interact in connection with the provision of the Helm1 service.

3.2 Data you provide directly to us

We collect personal data that you or your employer provides to us when you:

- Enquire about, purchase, or subscribe to the Helm1 service (e.g. name, job title, work email address, telephone number, employer name and address);
- Contact our sales, customer support, or account management teams (e.g. name, contact details, content of communications);

- Subscribe to our newsletter or marketing communications (e.g. email address, communication preferences); or
- Submit a job application or otherwise correspond with us.

3.3 Data we collect automatically

When you visit our website, we may automatically collect certain technical information, including:

- Device and browser information (e.g. device type, operating system, browser type and version);
- IP address and approximate geographic location derived from it;
- Login timestamps, session duration, and access logs;
- Feature usage data and interaction logs (which pages or features you use, how often, and for how long); and
- Cookies and similar tracking technologies (see Section 3.10 below for further details).

3.4 Data we receive from third parties

We may receive personal data about you from third parties, including:

- Our clients, who may provide us with the contact details of their authorized users when setting up accounts;
- Business directories, professional networks (e.g. LinkedIn), or publicly available sources, where we have a legitimate business reason to do so; and
- Referral partners or resellers who introduce us to prospective clients.

3.5 How we use your personal data

Company shall not pass on or sell online personal data to third parties. Company may, however, share data within its organization. This may include Company's employees, agents, contractors and sub-contractors and the use of third-party systems to process such data. Company may use email address or other contact information for queries and other contacts in relation to development and improvement of its services as well as for marketing of its own services to the User.

Company may also send proposals and offers based on the usage statistic of the User in a responsible manner.

By sending personal data to Company the User is explicitly consenting to the processing and transfer of such data in ways described above. Company cannot be responsible for personal data which the User uploads and shares between other users of the services of Company. The User and the users of the shared information are responsible to maintain applicable statutory privacy.

The table below sets out the purposes for which we process your personal data as a data controller, the legal basis we rely on under Article 6 GDPR, and how long we retain the data.

Processing Activity	Personal Data Processed	Legal Basis	Retention Period	Recipients / Disclosures
Account and contract management	Name, job title, work email, telephone, employer name and address, account credentials, communication history, contract and order details	Performance of a contract (Art. 6(1)(b)); Legal obligation (Art. 6(1)(c)) — accounting and record-keeping requirements	Duration of the SaaS Agreement + 5 years	Internal account management teams; finance and legal teams; group companies (if any); professional advisors (confidential)
Billing and invoicing	Name, work email, billing address, payment method details (tokenised / card-not-present), VAT/tax number, transaction history, invoice records	Performance of a contract (Art. 6(1)(b)); Legal obligation (Art. 6(1)(c)) — tax and accounting law	Duration of the SaaS Agreement + 5 years (statutory minimum for accounting records under applicable law)	Finance team; payment processor(s) — see Section 6; tax authorities where required by law
Customer support and service delivery	Name, work email, telephone, job title, support ticket content (may include technical details and information you choose to share), device and browser information	Performance of a contract (Art. 6(1)(b)); Legitimate interests (Art. 6(1)(f)) — providing effective support and improving service quality	Duration of SaaS Agreement + 12 months	Customer support team; technical operations team; Sub-Processors providing support tooling
Sending operational and service communications	Name, work email, telephone (where provided)	Performance of a contract (Art. 6(1)(b)) — for essential service communications	Duration of SaaS Agreement	Communications platform provider(s) — see Section 6

		(e.g. security alerts, maintenance, legal notices, changes to terms)		
Sending marketing and product update communications	Name, work email, employer, communication preferences	Consent (Art. 6(1)(a)) — where required; or Legitimate interests (Art. 6(1)(f)) — for business-to-business marketing to existing clients and prospects, subject to opt-out	Until you withdraw consent or opt out, or 3 years from last interaction, whichever is earlier	Marketing platform provider(s)
Service analytics and improvement	Pseudonymised usage data, log data, feature interaction data, performance and stability metrics, error reports	Legitimate interests (Art. 6(1)(f)) — improving the SaaS Service, ensuring platform security and stability, and developing new features	12 months (pseudonymised data); raw logs retained for 30 days	Internal analytics and engineering teams; analytics platform provider(s)
Security monitoring and fraud prevention	IP address, login data, access logs, device information, anomalous activity indicators	Legitimate interests (Art. 6(1)(f)) — protecting our systems, clients, and users from security threats and fraudulent activity	3 years (security logs)	Internal security team; security tooling providers
Legal and regulatory compliance	As required by applicable law (e.g. name, address, transaction data for tax, anti-money	Legal obligation (Art. 6(1)(c))	As required by the applicable legal obligation	Relevant regulatory or law enforcement authorities where required by law; legal advisors

	laundering, or export control purposes)			
Establishing, exercising, or defending legal claims	Personal data relevant to the claim, as determined by the circumstances	Legitimate interests (Art. 6(1)(f)) — access to justice and protection of our legal rights	Duration of relevant legal proceedings + 5 years	Legal advisors; courts and tribunals; counterparties to proceedings
Recruitment and job applications	Name, contact details, CV/resume, employment history, qualifications, references, interview notes	Steps taken at your request prior to entering into a contract (Art. 6(1)(b)); Legitimate interests (Art. 6(1)(f)) — managing recruitment	6 months from conclusion of recruitment process (unsuccessful applicants); duration of employment + 10 years (successful applicants)	HR team; hiring managers; recruitment platform provider(s) — see Section 6

Special categories of personal data: We do not intentionally collect or process special categories of personal data (such as health data, data revealing racial or ethnic origin, or data concerning criminal convictions) in our own-controller capacity. If you provide such data to us incidentally, we will process it only to the extent necessary to respond to your request and will delete it once the matter is resolved.

3.6 Automated decision making and profiling

We do not make any decisions about you that are based solely on automated processing, including profiling, that produce legal effects concerning you or similarly significantly affect you within the meaning of Article 22 GDPR.

3.7 Who we share your personal data with

Within our organization. Access to your personal data within our organization is restricted to employees and contractors who need it to perform their job functions, including our account management, finance, legal, customer support, security, and engineering teams. All staff are subject to binding confidentiality and data protection obligations.

Third-party service providers. We engage carefully selected third-party service providers to support our operations. These providers process personal data on our behalf (as our processors) or as independent controllers, as:

- Payment processors

- Cloud infrastructure / hosting providers
- Customer support platform
- CRM and marketing automation
- Analytics providers
- Security and monitoring tools
- Email and communications providers
- Recruitment platforms
- Professional advisors

Authorities and legal disclosures. We may disclose personal data to public authorities, law enforcement, regulators, or courts where required to do so by applicable law, by court order, or to protect our legal rights, the safety of our users, or the integrity of our services. We will, where legally permitted, notify you before making such a disclosure.

Business transfers. In the event of a merger, acquisition, reorganization, sale of assets, or insolvency proceedings involving our business, personal data may be transferred to the acquirer or successor entity as part of that transaction, subject to equivalent data protection protections.

3.8 International Data Transfers

We are based in the European Economic Area (EEA) and may transfer personal data to countries outside the EEA. Where we do so, we ensure that appropriate safeguards are in place to protect your data in accordance with applicable data protection law, including the EU General Data Protection Regulation (GDPR).

Such safeguards may include:

- Standard Contractual Clauses approved by the European Commission;
- Transfers to countries recognized by the European Commission as providing an adequate level of data protection; or
- Other legally recognized transfer mechanisms where applicable.

3.9 How long we keep your personal data

We retain personal data only for as long as necessary to fulfil the purposes for which it was collected, including for the purposes of satisfying any applicable legal, accounting, or regulatory requirements. The retention periods applicable to each processing activity are set out in the table in Section 3.5.

In determining the appropriate retention period, we consider the nature and sensitivity of the personal data, the potential risk of harm from unauthorized use or disclosure, the purposes for which we process the data and whether we can achieve those purposes through other means, and applicable legal requirements.

At the end of the applicable retention period, personal data is securely deleted or anonymized. Where anonymization is not possible (for example, because the data is stored

in backup archives), we will securely store the data and isolate it from any further processing until deletion is possible.

3.10 Cookies

We may place in your computer information in the form of a text file known commonly as a “cookie”. A cookie may enable collection of certain information about the computer of the User, including the internet protocol (IP) address, the computer’s operating system, the browser type and the address of any referring sites. The use of cookies is intended to provide benefits to the User, such as eliminating the need to enter password frequently during a session. Cookies are also used for website traffic analysis and anonymous demographic profiling in order to improve services of Company.

3.11 Security

We take the security of your personal data seriously and implement appropriate technical and organizational measures to protect it against unauthorized access, accidental loss, alteration, or disclosure.

These measures include:

- Encryption of personal data in transit and at rest;
- Access controls ensuring that only authorized personnel can access your data;
- Regular security assessments and testing of our systems; and
- Staff training on data protection and information security.

While we do our best to protect your personal data, please be aware that no method of transmission over the internet is completely secure. In the event of a data breach that is likely to affect your rights and freedoms, we will notify you and the relevant supervisory authority as required by law.

4. AMENDMENTS

Company may change or modify this Privacy Policy in its sole discretion. Changes become effective immediately upon posting them at Company website. The continued use of the websites or services of Company after any changes or modifications constitutes the User's acceptance to such. The User should review the most current version of the Privacy Policy at the above-mentioned web address regularly.

5. APPLICABLE LAW

This Privacy Policy shall be construed, governed and enforced in accordance with the laws of Finland without giving effect to any principle of law which would result in the application of laws of any other jurisdiction, and irrespective whether the websites of Company have been accessed from Finland or abroad. Helsinki District Court, Finland (Helsingin käräjäoikeus) shall have exclusive jurisdiction over any dispute arising out of use or non-use of the websites of Company.

6. USER RIGHTS

We would like to make sure you are fully aware of all of your data protection rights. Every user is entitled to the following:

The right to access - You have the right to request Company for copies of your personal data. Company may charge you a small fee for this service.

The right to rectification - You have the right to request that Company corrects any information you believe is inaccurate. You also have the right to request Company to complete information you believe is incomplete.

The right to erasure - You have the right to request that Company erases your personal data, under certain conditions.

The right to restrict processing - You have the right to request that Company restricts the processing of your personal data, under certain conditions.

The right to object to processing - You have the right to object to Company's processing of your personal data, under certain conditions.

The right to data portability - You have the right to request that Company transfers the data that we have collected to another organization, or directly to you, under certain conditions. If you make a request, Company has one month to respond to you. If you would like to exercise any of these rights, please contact Company at email: [john.bjorkbom\(a\)bjorkbomtrading.fi](mailto:john.bjorkbom(a)bjorkbomtrading.fi)

In case personal data of a User is removed Company may not be able to continue to provide services to that User.