

Data processing agreement

The club is the controller of its members' data, and EIT is the processor. This agreement is entered into with each club before EIT is taken into use. Yellow fields are filled in before signing. This is a translation – the Norwegian version applies in case of conflict.

between **Club name**, org. no. **org. no.** (controller, hereinafter “the Club”)

and **Provider name**, org. no. **org. no.**, which provides the EIT service (processor, hereinafter “the Provider”)

The agreement is entered into under Article 28 of the General Data Protection Regulation (GDPR) and the Norwegian Personal Data Act. It applies together with the agreement on the use of EIT (the main agreement). In case of conflict, this agreement takes precedence as regards the processing of personal data.

1. Purpose and scope

1. The Provider processes personal data on behalf of the Club in order to deliver EIT: member register, check-in and training log, attests for firearms applications, payment, competitions, courses, calendar and duties, messages, club operations (club gun loans, keys, till, membership fees, volunteer hours, incidents, range checks, badge shooting) and related functions.
2. The Club is the controller and determines the purpose of the processing. The Club is responsible for having a legal basis for the processing, for informing the members (privacy notice), and for the data the Club's administrators enter.
3. The Provider shall only process the data as set out in this agreement and the Club's documented instructions. Use of the functions in EIT and the settings chosen by the Club's administrators are regarded as the Club's instructions. The Provider shall inform the Club if the Provider considers an instruction to be in breach of the regulations.
4. The Provider shall not use the data for its own purposes, sell it, use it for marketing or disclose it to others, except as follows from section 6 or from law.

2. What data and whom it concerns

Data subjects

- Members and applicants for membership
- Participants in courses and competitions, including people from other clubs
- People who are issued keys or borrow club guns, and guests at badge shooting
- People mentioned in incident reports and messages from the club

Categories of data

CATEGORY	EXAMPLES
Identity and contact	Name, email, mobile number, date of birth, shooter ID, profile photo, chosen language
Membership	Role, category, status, federation, membership fee and exemptions
Activity	Check-in (time and range), sessions, results, competitions, courses, qualifications, duties, volunteer hours
Payment	Amount, status and reference from Vipps. Card numbers and bank details are not processed by EIT
Firearms and attests	Attests for firearms applications, club gun loans (borrower and date of birth), the member's own firearms, serial numbers and images of weapon cards
Documents and photos	Documents uploaded by the member (course certificates, competition licences, membership cards), photos in the shooting diary, signatures when keys are issued
Communication	Messages from the club, incident reports and follow-up
Technical data	Login sessions, a change log for important actions, technical logs on the server

EIT is not designed for special categories of personal data (GDPR Article 9) or data relating to criminal offences. The Club shall limit such data. Incident reports about injuries may contain health data – the Club should describe the incident without stating more than necessary.

3. Confidentiality and access

1. Only people at the Provider who need it in order to operate, troubleshoot or provide support shall have access to the data. They are bound by confidentiality, also after they have left.
2. The Provider does not look at the Club's data unless it is needed for operation, troubleshooting or support the Club has asked for. Access to the server is logged.

4. Security

1. The Provider shall implement appropriate technical and organisational measures under GDPR Article 32. The measures are set out in Appendix A and may be improved without amending the agreement, but shall not be weakened.
2. The Provider shall regularly test that the measures work, including that backups can be restored.

5. Personal data breaches

1. The Provider shall notify the Club without undue delay, and no later than 36 hours after the breach was discovered, so that the Club can notify the Norwegian Data Protection Authority within 72 hours.
2. As far as is known, the notice shall describe what has happened, which data and how many data subjects are affected, the likely consequences and the measures taken. Information not yet known shall be provided later.
3. The Provider shall assist the Club in reporting the breach and, where relevant, informing the data subjects.

6. Sub-processors

1. The Club approves the sub-processors in Appendix B. The Provider shall have agreements with them that give at least the same protection as this agreement.
2. The Provider shall notify the Club at least 30 days before a new sub-processor is taken into use or a sub-processor is replaced. The Club may object on reasonable grounds, and may then terminate the agreement with effect from the change.
3. The Provider is liable to the Club for the sub-processors' processing.

7. Transfers outside the EU/EEA

The data is stored and processed in Norway and the EU/EEA. The Provider shall not transfer data to countries outside the EU/EEA without the Club's written consent and a valid transfer mechanism under Chapter V of the GDPR.

8. Assistance to the Club

1. EIT has functions for access, rectification, erasure and data portability: members see and correct their own data and download their own training log, the administrator can correct and delete members, and all the Club's data can be exported. If the Club needs more help fulfilling the data subjects' rights, the Provider shall assist.
2. The Provider shall assist the Club with data protection impact assessments and prior consultations with the Norwegian Data Protection Authority where relevant.
3. Requests from data subjects that reach the Provider are forwarded to the Club without being answered, unless the Club has asked otherwise.

9. Audit and documentation

1. The Provider shall give the Club the information needed to demonstrate that the agreement is complied with.
2. Once a year, or after a security breach, the Club may request a review of the security measures. The review is agreed with reasonable notice and carried out in writing as far as possible. Each party covers its own costs.

10. Duration, termination and deletion

1. The agreement applies as long as the Provider processes personal data for the Club.

2. The Club's administrator can download all the Club's data (CSV and JSON) at any time under Club settings → Export of all data.
3. When the main agreement ends, the Provider deletes the Club's data within 30 days, unless the Club requests another deadline in writing or the law requires storage. Backups are deleted when they rotate out, no later than 35 days after the deletion. The Provider confirms the deletion in writing on request.
4. User accounts that are also members of other clubs in EIT are kept, but all data linked to the Club is deleted.

11. Liability

The parties' liability follows GDPR Article 82. Otherwise, the limitations of liability in the main agreement apply, insofar as they do not conflict with the regulations.

12. Governing law and disputes

The agreement is governed by Norwegian law. Disputes shall first be sought resolved through negotiations. If this does not succeed, **venue, e.g. the Provider's home court** is the agreed venue.

13. Contact persons

	THE CLUB	THE PROVIDER
Name	name	name
Email	email	post@eit.no
Phone	phone	phone

Changes of contact persons are notified in writing.

Signatures

The agreement is made in two copies, one for each party, or signed electronically.

Place and date

For the Club: **name and role**

Place and date

For the Provider: **name and role**

Appendix A – Security measures

AREA	MEASURES
Location	Server with hosting provider in country in the EU/EEA . No storage outside the EU/EEA
Transfer	All traffic encrypted with HTTPS (TLS 1.2 or newer) and HSTS
Storage	Documents, weapon cards, photos, signatures and the clubs' Vipps and SMS keys are encrypted with AES-256-GCM. The key is stored separately from the database
Passwords	Stored as bcrypt hashes. Login with Vipps is possible. Repeated failed attempts are stopped
Access in the app	Roles (member, range officer, administrator). Clubs are separated from each other. Nobody can approve their own sessions or attests
Application security	Protection against CSRF, security headers (CSP), rate limiting, file type checks on uploads
Server access	Only named people at the Provider, with SSH keys and two-factor authentication. Access is logged
Backups	Every night. Stored on the server, at another location in Norway and in cloud storage in the EU/EEA. The last 30 are kept. Restoring is tested how often, e.g. every quarter
Updates	Security updates of the operating system, Docker and dependencies are applied continuously
Logging	A change log for important actions in the app. Technical logs on the server are deleted after number of days
Monitoring	The service is monitored, and the Provider is alerted in case of downtime

Appendix B – Sub-processors

SUB-PROCESSOR	WHAT	LOCATION
name	Operation of server, database and files	country in the EU/EEA
name	Cloud storage of backups	country in the EU/EEA
name or “the Provider itself”	Backups at another location in Norway	Norway
name	Sending email (passwords, notifications, messages)	country in the EU/EEA
name, e.g. Sveve AS	Sending SMS – only when the Club uses EIT’s shared SMS setup	country

Not sub-processors under this agreement:

- **Vipps MobilePay:** The Club has its own agreement with Vipps MobilePay for payment. For “Log in with Vipps”, Vipps MobilePay is an independent controller for the login.
- **The Club’s own SMS provider:** If the Club uses its own SMS agreement, that provider is the Club’s own processor.
- **Push notifications:** Notifications to phones are sent via the browser’s push service (e.g. Google, Apple, Mozilla). The content is end-to-end encrypted, so the service cannot read it.
- **MET Norway:** The weather forecast on the big screen is fetched without personal data.

Version 1.0 · October 2026 · English translation of «Databehandleravtale»