

Privacy Notice

HAVU-trailgame / HAVU-polkupeli / HAVU-stigspelet

1. Data Controller

- **Name:** University of Vaasa
- **Business ID:** 0209599-8
- **Address:** Wolffintie 34
- **Postal code:** 65200
- **City:** Vaasa, Finland
- **Phone:** 0503449726
- **Email:** support@havupeli.jansoftware.fi

2. Contact Person for Registry Matters

- **Organization / unit:** University of Vaasa / School of Technology and Innovation Management / Computer Science
- **Name:** Jyri Nieminen
- **Address:** Wolffintie 34
- **Postal code:** 65200
- **City:** Vaasa, Finland
- **Phone:** +358 29 449 8263
- **Email:** jyri.nieminen@uwasa.fi

3. Data Protection Officer

- **Organization:** University of Vaasa
- **Name:** Sami Kinnunen
- **Email:** tietosuojavastaava@uwasa.fi
- **Phone:** 0443248761

4. Purpose of the Registry

Personal data is processed in the HAVU service for the following purposes:

- creating and authenticating user accounts
- managing login sessions and access rights
- recording route progress for registered users
- handling feedback, contact requests, bug reports, and feature suggestions
- ensuring the security of the service, preventing misuse, and maintaining operations
- managing administrative rights related to route creation

5. Legal Basis for Data Collection and Processing

The processing of personal data is primarily based on:

- performance of a contract or provision of the service when a user creates an account, logs into the service, and uses features intended for registered users
- the legitimate interest of the data controller in ensuring the security, administration, and functionality of the service
- consent insofar as the user provides personal data in connection with feedback or a contact request

6. Data Content of the Registry

The following data may be processed in the service:

User Account Data

- name
- email address
- password hash (password is not stored in plain text)
- user role
- user's public identifier
- most recent login time

Login and Session Data

- session data
- timestamp of login
- IP address at the time of login
- selected language preference

Progress Data from Registered Users

- data on visited checkpoints
- data on completed routes
- timestamps of completions

Feedback Form Data

- feedback type (contact request, bug report, feature suggestion)
- name
- email address
- message
- page URL from which the feedback was submitted
- possible association with a logged-in user

Route Maintenance Data

- route and checkpoint content
- media files associated with the route creator's user identifier

Location Data

- the browser requests the user's device location for playing routes
- the service uses location to verify proximity to checkpoints during gameplay
- the user's continuous GPS location is not stored in the server database

7. Data Retention Period

Personal data is retained only for as long as necessary for the purposes described in this notice, unless legislation requires a longer retention period.

Estimates for this service:

- user account data is retained as long as the account is active; after account deletion, data is deleted or anonymized without undue delay, unless retention is necessary for establishing, exercising, or defending legal claims or fulfilling a legal obligation
- gameplay progress data is retained as long as the user account exists or as needed for providing service functionality; upon account deletion, data is deleted or anonymized unless retention is necessary for the reasons mentioned above
- feedback form data is retained as long as required for processing the feedback and any follow-up communication, after which the data is deleted or anonymized without undue delay
- technical session and cookie data in the service persists in the browser according to cookie settings and session duration

8. Regular Data Sources

Data is primarily obtained from:

- the data subject themselves during account creation, login, and use of the feedback form
- user activity within the service, such as completing routes and checking in at checkpoints
- the user's browser and device in connection with the technical operation of the service, such as session and language settings

9. Regular Data Disclosures and Data Transfers Outside the EU/EEA

Data is not regularly disclosed to third parties except in situations that are necessary for the technical implementation of the service.

The service uses Google reCAPTCHA v3 to prevent misuse of the feedback form. In this context, data may be transmitted to Google in accordance with its own terms and privacy policies. Google may also process data outside the European Union or the European Economic Area.

For any transfers outside the EU/EEA, appropriate safeguards under applicable data protection legislation are applied, such as Standard Contractual Clauses (SCCs) approved by the European Commission, or another transfer mechanism accepted under applicable law.

Feedback form messages are also sent via the server's email system to the service support address. Messages can only be read by University of Vaasa employees approved by the contact person for registry matters.

10. Use of Cookies

The service uses functionally necessary cookies and similar session mechanisms, such as:

- a PHP session cookie for maintaining the user's login and session
- a language preference cookie for remembering the user's chosen interface language

The service does not use analytics or marketing cookies.

Additionally, Google reCAPTCHA may use its own technical mechanisms for preventing misuse.

11. Protection of the Registry

Data containing personal information is protected with appropriate technical and organizational measures. These include:

- processing user data stored in the database only in parts necessary for the operation of the service
- storing passwords as hashes
- restricting access rights based on login and user roles
- protecting the feedback form with reCAPTCHA verification
- storing uploaded files in a separate directory structure
- restricting administrative access rights to only those persons who need them

12. Automated Decision-Making

The service does not carry out automated individual decision-making or profiling under Article 22 of the EU General Data Protection Regulation that would have legal effects concerning the data subject.

13. Rights of the Data Subject

Under applicable data protection legislation, the data subject has the right to:

- access their personal data
- request the rectification of inaccurate data
- request the erasure of their data when there is no longer a basis for processing
- request the restriction of processing
- object to the processing of their personal data in applicable situations
- receive their data in a transferable format where this right applies to the processing in question
- withdraw consent when processing is based on consent
- lodge a complaint with a supervisory authority (in Finland, the Office of the Data Protection Ombudsman, tietosuoja.fi)

Data access requests and other requests concerning the processing of personal data should be directed to the contacts listed in sections 1-3 of this notice.