**Archived version draft-2026-10-30**

This is the Tarumo data processing agreement as it was when archived on 30 October 2026. An archived version is never changed. An order records the identifier of the version accepted.

Download PDF · Current version · All versions · Suomeksi · Tarumo

DRAFT, PENDING APPROVAL

# Data processing agreement

Draft of 30 October 2026, not yet in force

Previous versions

**This is a draft pending approval by Enarra Oy.** The agreement takes effect only once the approved version is published on this page and the services, sub-processor agreements and security measures it describes are in use in production. Online ordering of the Small (Pieni) and Handover (Siirto) packages opens only after that.

The service provider is Enarra Oy (Business ID 3664892-5, Artturintie 4, 43500 Karstula, Finland), “Enarra”. Enarra provides a software service called Tarumo (the “Service”). Tarumo is the commercial name of the Service and not a registered secondary business name. The contracting party is Enarra Oy.

This agreement meets the requirements of Article 28 of the EU General Data Protection Regulation (2016/679, GDPR). It forms part of the contract between the Customer and Enarra, to which Tarumo's terms of service apply. The agreement is written in Finnish and English. The Finnish version is authoritative, and the English version is a faithful translation of it.

## Contents


- 1. Parties, roles and scope
- 2. Subject matter, nature and purpose of the processing
- 3. Duration of the processing
- 4. Data subjects

- 5. Personal data and retention
- 6. The Customer's instructions
- 6 a. The Customer's responsibilities as controller
- 7. Principles of the processing
- 8. AI and the Customer's data
- 9. Confidentiality and access by Enarra's staff
- 10. Security
- 11. Sub-processors
- 12. Location of data and transfers
- 13. Data subjects' rights
- 14. Personal data breaches and security incidents
- 15. Impact assessment and prior consultation
- 16. Audits
- 17. Return and deletion at the end of the contract
- 18. Liability
- 19. Term and changes
- 20. Contact details


## 1. Parties, roles and scope

- **The controller** is the company or other organisation that has ordered the Service, hereinafter the Customer.
- **The processor** is Enarra Oy (Enarra).
- The Customer acts as controller for the processing of the personal data whose purposes and essential means it determines in order to deploy and use the Service. Enarra processes this personal data as processor in accordance with the Customer's documented instructions. Enarra acts as an independent controller only for the processing operations whose purposes and essential means Enarra determines itself, such as its own invoicing, statutory bookkeeping and the security of the Service, to the extent that these purposes belong to Enarra. The parties define the roles per purpose as set out in the table below; this clause does not change the roles where the actual processing is otherwise.

| Processing and purpose | Customer | Enarra |
|---|---|---|
| The Customer's content: key people, knowledge areas, interviews, knowledge cards, knowledge packs, Mapping, incentives and the organisation's log | Controller | Processor |
| A user's or an accountant's membership of the Customer's organisation, their role and rights, and the log entries of what they do in the organisation | Controller | Processor |
| Card view rows as part of the organisation's log on the Customer's instruction (sections 5 and 10) | Controller | Processor |
| The user account shared across organisations, sign-in and authentication, the Service's security logs and abuse prevention, including when Enarra uses card view rows to investigate the security of its own Service | – | Independent controller to the extent that Enarra determines purposes and means |
| Enarra's invoices, invoice copies, payment data, statutory bookkeeping and the new-invoice notices to the accountant | – | Independent controller |
| Card payments through Stripe (online ordering, not yet live): Stripe is an independent controller for its own processing | – | Independent controller for its own part |

- This agreement covers the processing in which Enarra is the processor. The processing in which Enarra is the controller, such as the details of the Customer's contact person, invoicing, and the feedback and bug reports that users send to Enarra, is described in the privacy notice.
- **Enarra's own security processing.** To secure the Service, Enarra processes as an independent controller only this data: the user account and its sign-in methods, sign-in events and sessions, Enarra's administration log (the actions of Enarra's staff and the exceptional access sessions of section 9), the server's technical logs, the suppression list of bounced email addresses, and card view rows when Enarra uses them to investigate a security incident in its own Service. The purpose is to protect the Service, to prevent abuse and to investigate security incidents. The legal basis is Enarra's legitimate interest (Article 6(1)(f) GDPR). The retention periods are in sections 5 and 17 and in purpose 5 of the privacy notice. The content of interviews, knowledge cards, knowledge packs and Mapping, and the Customer's other content, are never Enarra's own controller data: Enarra processes them only as a processor under this agreement, also when it investigates a security incident.

- For online orders, the agreement is accepted when ordering. For other packages, it is accepted separately in the signed order and its annexes. In matters of personal data processing, this agreement takes precedence over the terms of service. A signed order may depart from this agreement only if the order names the item it changes. If the parties have signed a separate data processing agreement, that agreement applies instead of this one.
- The terms personal data, processing, controller, processor, data subject and personal data breach have the same meaning as in the GDPR.

## 2. Subject matter, nature and purpose of the processing

- **Subject matter:** the personal data that the Customer and its users store in the Service or that arises from using the Service.
- **Nature:** storage, organisation, retrieval, conversion of speech to text, processing by AI (follow-up questions in interviews, polished suggestions of the interviewee's answers, card drafts, content filtering, search vectors, answers in Ask, drafts of knowledge packs and pack proposals from mapping interviews), calculating risk and coverage, calculating incentive points and achievements, compiling the mapping report, sending emails, export, keeping a log, backup and deletion.
- **Purpose:** providing the Service to the Customer: identifying the risk of knowledge being lost by knowledge area, knowledge packs and Mapping, interviewing experts, knowledge cards, search and AI answers from published cards, incentives, the accountant's access to billing, reminders and notifications, data export, the log, and the maintenance, support and security of the Service. The Service is not used to evaluate or monitor employees (section 6 a).

## 3. Duration of the processing

The processing lasts for the term of the contract and, after it, for the transition period under section 12 a of the terms of service and the export period and deletion under section 17. Enarra's obligations apply as long as it processes the Customer's personal data.

## 4. Data subjects

- The Customer's users: administrators, managers, experts and readers, usually the Customer's employees or others working on its behalf.

- The accountant the Customer invites, including a person from an accounting firm outside the Customer.
- Key people, including those without a user account.
- People mentioned in interviews or knowledge cards, such as colleagues and suppliers' contact people.
- People whose data the Customer brings into the Service from its own systems, for example through the HR integration.

## 5. Personal data and retention

| Data | Retention |
|---|---|
| User data: name, email address, role, language, sign-in method and the Microsoft or Google account identifier, if used | As long as the person is a user or until the organisation's data is deleted |
| Accountant data: name, email address, invitation, start and end of access and the choice of new-invoice notices. The accountant's actions are recorded in the organisation's log. | As long as the person is the accountant or until the organisation's data is deleted. Log entries for the log's retention period. |
| Sign-in events and sessions (Enarra's own processing under section 1) | Sign-in events 90 days, sessions at most 30 days |
| Key person data: name, job title, starting year, departure date and whether the departure is confirmed or an estimate, knowledge areas, criticality and whether they are the only expert | For the term of the contract; an archived key person remains as the source of cards |
| Interview questions and answers (in the user interface visible only to the interviewee) | Deleted when the card made from the interview is approved or rejected, at the latest 30 days after the interview ends |

| Data | Retention |
| --- | --- |
| Dictation audio recordings (available only to the interviewee) | By default 30 days from transcription. The Customer can choose 0–30 days; 0 means that no audio is stored. Deleted at once when the card is approved or rejected or the answer is filtered. |
| Knowledge cards: content in the expert's words, source (expert and date), versions, archived versions and reports of outdated information | For the term of the contract. As a rule, cards are not deleted but replaced, and the version history is kept (exceptions in section 7). The content of a rejected draft is deleted. A draft that is neither approved nor rejected within 30 days is rejected and its content deleted. |
| Withdrawn knowledge cards (section 7) | A card withdrawn because of another person's personal data has its content blanked as soon as the administrator confirms the withdrawal. A card withdrawn because of confidential information or a trade secret has its content blanked at once or after 30 days, as the Customer chooses. A card withdrawn because of offensive text keeps its content, hidden, so that it can be corrected. A blanked card leaves only a stub with the reason and the date in the version history. |
| Search vectors from the text of published cards | As long as the card is published |
| Mapping: invitations (who was invited), the expert's choice to take part and drafts of pack proposals (visible only to the expert), and pack proposals sent in the expert's name | The content of drafts is deleted after 30 days. Invitations, choices and sent proposals are kept for the term of the contract. When a person's data is deleted, their choice and drafts are deleted. |
| Incentives: the person's points, level and achievements (visible only to them), their reward choices, rewards reported to the reward granter, and teams and team challenges | For the term of the contract. The reward granter's list shows given and closed rewards for 90 days. |
| Usage data: card read counts with no information about the reader, and the user's own "useful" marks | For the term of the contract |

| Data | Retention |
| --- | --- |
| Card view rows (who opened which card and when) and who reported a card. They are not shown to the Customer (section 10). | View rows 12 months from recording; report rows for the term of the contract |
| The organisation's log: what was viewed, changed, approved and exported, by whom and when. The Customer's administrators see the log except card views and card reports. | For the term of the contract |
| Notifications and reminders (email or Teams) | Enarra does not keep the content of messages separately. The email service (Scaleway) deletes the content after delivery, but keeps the sending metadata (recipient, subject, time and delivery status) under its terms for as long as Enarra's sending account is in use. The subject of interview and mapping reminders is neutral. The subject of other messages may contain the organisation's name. |
| The server's technical logs (without the content of interviews, cards or questions) | At most 30 days |

- Searches and questions in Ask are not stored or logged. A search counts only as an anonymous read of a card.
- Filtered content is not stored. Only a count per day and reason for each organisation is recorded, with no person or content. If the AI is unavailable, an interview answer or a card edit that passed the word lists is stored awaiting review (section 7).
- **Special categories and colleagues:** the Customer instructs that special categories of personal data (Article 9 of the GDPR), such as health data, and data on criminal offences (Article 10) are not stored in the Service, unless the Customer has shown a lawful special basis for the processing. Enarra uses automatic and, where needed, manual safeguards to seek to identify and block special categories of personal data, criminal offence data and content that evaluates individual employees. The safeguards do not catch every case. The Customer and the expert approving a card must check the content before publication; a card must not contain unnecessary personal data or data processed unlawfully. Enarra may block or remove content

that it reasonably suspects breaches these restrictions. The card approval view highlights names and other identifiers detected in the text, and the expert must tick "I have checked the card" before the card is published, in Teams too. A named colleague is replaced in a card by a job title or role when the name is not necessary to understand the instruction. If the name is needed, the Customer assesses the legal basis and the duty to inform before publication (section 6 a).

- **Backups:** Enarra backs up the database every night. The backups are encrypted with Enarra's keys before storage and kept in Helsinki (UpCloud). A backup is gone at the latest 36 days after it was made, so deleted data is gone from the backups within 36 days. An encrypted, locked copy in Paris (Scaleway), which cannot be changed or deleted before its retention ends and which is gone within the same time, is also planned for production; it is not yet in use. The database service (UpCloud) also keeps its own backups; their location and retention will be confirmed in writing by UpCloud before the Customer's data is processed in production. Dictated audio is not included in the backups.

## 6. The Customer's instructions

- Enarra processes personal data, including transfers outside the EU and the EEA, only on the Customer's documented instructions, unless Enarra has a statutory obligation to act otherwise. The instructions are this agreement, the terms of service, the order and the Customer's choices and actions in the Service, such as inviting users and the accountant, the retention period of audio recordings, sign-in methods, turning on incentives, Mapping, turning on the Teams app and HR integrations. The instructions also include the principles of section 7, such as interviews being visible in the user interface only to the interviewee and the deletion of interview texts under section 5.
- The Customer gives further instructions in writing through its administrators, and Enarra keeps them.
- By accepting this agreement, the Customer also instructs Enarra to
  - record card views and card reports in the organisation's log, used only to investigate security incidents, and to deliver a person's own rows to them under section 13 (section 10);
  - provide, in the export, read counts and "useful" counts per card as monthly totals of at least three reader-days, with no information about the readers (section 17);
  - count the use of the Service per organisation, such as key people, cards, interviews and AI calls, for billing, capacity and support. The counts contain no data on individual people;
  - transfer data under section 12.

- If EU or Finnish law requires Enarra to process the data otherwise, Enarra informs the Customer before the processing, unless the law prohibits this.
- If Enarra considers that an instruction infringes data protection law, it informs the Customer without delay and may refrain from following the instruction until the Customer confirms or changes it.

## 6 a. The Customer's responsibilities as controller

As controller, the Customer is responsible for the lawfulness of the processing. Enarra is responsible for its own obligations as processor, and this section does not release it from them. In particular, the Customer:

determines the legal basis. Processing employees' data is usually based on the Customer's legitimate interest in transferring knowledge, not on the employee's consent. The necessity requirement of section 3 of the Finnish Act on the Protection of Privacy in Working Life cannot be set aside by consent;

stores only data necessary for transferring knowledge. The departure date recorded is primarily an agreed departure or one the employee has announced, and an estimate is marked as an estimate. Risk is not based on the employee's age, health, presumed retirement or intentions, and a departure estimate is not used for personnel decisions;

informs employees and key people of the use of the Service before deployment (Articles 13 and 14 of the GDPR): the purpose, the data collected, who sees what, the retention periods and that the Service is not used to evaluate performance. Enarra provides the information about the Service needed for this and, on request, a template for a staff notice. The template is starting material that the Customer adapts to its own purpose, legal basis, staff, retention periods and procedures;

handles the deployment with its staff as the law requires: in a company with at least 50 employees under the Finnish Co-operation Act, including change negotiations if the deployment materially changes the organisation of work or the position of staff; in a company with 20–49 employees in the dialogue under section 7 a of the Co-operation Act and, where applicable, under section 16 a; and assesses whether section 21 of the Act on the Protection of Privacy in Working Life applies to how it uses the Service. In Enarra's view, the Service is not technical monitoring of employees when used for its intended purpose, but the assessment may change if the Customer uses it to follow employees' activity;

assesses before production use whether a data protection impact assessment is needed, and carries it out before the processing if the processing is likely to result in a high risk. In Enarra's

assessment it is usually needed, because the Service processes employees' data with AI. Enarra provides starting material for it (section 15), which is not a ready impact assessment;

does not use the Service or its data for monitoring employees, scoring individual performance, comparing employees, allocating tasks based on employees' behaviour or personal traits, or for decisions on employment (section 3 a of the terms of service). The Service's own incentives are permitted as they work in the Service (section 3 b of the terms of service);

instructs experts to describe practices rather than individual people, to refer to colleagues by job title or role and not to store data on health, trade union membership or other special categories of personal data, and checks the content of cards under section 5;

decides on data subjects' requests with Enarra's assistance (section 13);

takes into account that a copy of conversations in the Teams app remains in the Customer's Microsoft 365 environment (section 11);

decides who its accountant is, manages the accountant's access rights and removes the accountant when their task ends (section 7 a of the terms of service).

## 7. Principles of the processing

Enarra has built the Service on these principles and keeps them in force:

- **No evaluation of employees.** The Service has no features that evaluate or compare employees or score them for the employer. The risk radar is a fixed, rule-based calculation that assesses the continuity risk of a knowledge area, not how people perform.
- **The interview belongs to the interviewee.** In the user interface, interview text is visible only to the interviewee. Administrators and managers do not see the answers, the dates or the counts. Interview texts are deleted under section 5, at the latest 30 days after the interview ends. This visibility and this deletion are the Customer's documented instruction as controller, which the Customer gives by accepting this agreement. The only exception is a disclosure under a statutory obligation under section 13. Section 9 describes the technical access of Enarra's staff.
- **Published only with human approval.** A knowledge card is published only after the expert has checked and approved it. An unapproved card does not appear in search or in the AI's answers.
- **Answers with sources.** The AI answers only from published cards and states the source (expert and date).
- **Filtering is not reported.** Swear words are removed, and an offensive, inappropriate or unclear answer is left out. Filtered content is not stored and is not reported to the employer. When the

Service filters an answer, it tells the person why the answer was not saved (it appeared to contain swear words, personal data, confidential information or content against the terms of service) and advises them to rephrase it or to ask for a review at support@tarumo.fi. The notice does not reveal the filtered content to the employer. If the AI is unavailable at the time of the check, an interview answer or a card edit checked by the word lists is stored awaiting the AI's review. An answer awaiting review is visible only to the interviewee and is not used in cards, in mapping pack proposals or in prompts to the AI until it has been reviewed. A card awaiting review cannot be published until it has been reviewed. If the review filters an answer, its text and audio are deleted. The note of a card report is not stored at all if the AI cannot check it.

- **Mapping is voluntary.** The expert decides whether to take part in the mapping interview. An administrator or manager sees only that the expert has been invited. The choice is not consent under the GDPR; the processing rests on the Customer's legal basis (section 6 a). The mapping report contains only figures for the organisation and for packs, and figures below three people are shown as "fewer than 3". In a small organisation, something about individual people may still be inferred from the figures, so the Customer treats the report as personal data. A downloaded or printed report is the Customer's responsibility.
- **Incentives are not evaluation.** Incentives are off by default in an organisation, and everyone can switch them off for themselves. Personal points, levels and achievements are visible only to the person. A reward granter learns of an achievement and a reward only if the person agrees. Others see only team-level information. Points and achievements are not exported to HR or appraisal systems.
- **Knowledge is not silently deleted.** The operating principle is that knowledge is not deleted but replaced: an outdated or incorrect card is archived when a corrected version is approved, and the version history is kept. The principle gives way where the law, security or data subjects' rights require it. Withdrawn cards are handled as follows:
  The Customer's administrator can withdraw a card that contains offensive text, another person's personal data or confidential information. Enarra may also place a risky card in quarantine at once when this is needed to protect the security of the Service, the law or another person's rights, and asks the Customer for a decision.

  The card leaves search, AI answers and exports at once. Only the card's expert and the administrators can see it.

  The expert is told by email. The notice states the reason, and the expert can publish a corrected version.

When the reason is another person's personal data, the card's title and content are blanked as soon as the administrator confirms the withdrawal. When the reason is confidential information or a trade secret, the Customer chooses whether the content is blanked at once or after 30 days. A data subject's valid erasure request is handled without undue delay (section 13). A card withdrawn because of offensive text keeps its content, hidden.

A blanked card leaves no old content in the version history, only a stub with the reason and the date. The blanking also covers the card's earlier versions, the notes of reports about it and the search index, and open correction drafts of the card are rejected. The withdrawal and the blanking are logged without the card's content.
The other exceptions are the end of the contract and the exercise of data subjects' rights (sections 13 and 17).

## 8. AI and the Customer's data

- Enarra uses the Customer's data only to provide the Service. **Enarra never uses the Customer's data to develop or train AI models**, and this includes the diagnostic data mentioned below.
- Enarra is the provider of the Service's AI system and the Customer its deployer (section 3 a of the terms of service). The intended purpose and prohibited uses are set out in section 3 a of the terms of service. The Service tells users when they are interacting with AI. Answers in Ask, follow-up questions and card drafts are marked visibly and in a machine-readable way. Published knowledge cards carry a machine-readable marking under Article 50(2) of the AI Act and a visible note "Drafted with the help of AI, approved by the expert". The Service makes no decisions about people based solely on automated processing (Article 22 of the GDPR). The risk radar is a fixed, rule-based calculation of the risk of knowledge being lost, not an assessment of a person, and it does not use age.
- The AI models and speech recognition are Scaleway SAS's Generative APIs service in Paris. Under Scaleway's privacy terms, Scaleway does not collect, read, reuse or analyse the content of prompts or answers, does not use them to train or improve models, and the makers of the models have no access to them. Exceptions: if a request causes an error or appears abusive, Scaleway may store the full content of the request and access it for up to two weeks to investigate the fault or the abuse. In addition, Scaleway keeps anonymous usage data about the Service for six months. Enarra has asked Scaleway for binding information on what is kept in error and abuse cases, who can access it and whether it can be deleted; until it has been received, this section describes the terms Scaleway has published.
- The AI receives only the data needed at the time:

- in an interview and a mapping interview, the questions and answers, the names of the knowledge area and the part, and the content of the knowledge pack;
- for a polished suggestion, the interviewee's own answer (the interviewee can turn suggestions off);
- for a card draft, the interview's questions and reviewed answers and the content of the knowledge pack;
- for content filtering, an interview answer, a card draft and the expert's edits, the note of a card report, and the texts of knowledge packs written by administrators and managers;
- for a knowledge pack draft, the field, the role, the administrator's notes and the pack used as a base;
- for a mapping pack proposal, the part, the expert's reviewed answers and the names of the candidate packs;
- in Ask, the question and the titles, instructions, sources and dates of the best-matching published cards. The notes of card reports are not sent to the AI; the warning of a card reported as outdated or incorrect is shown next to the answer;
- for search vectors, the text of published cards and the question asked in Ask.

Interview texts never reach search or the answers in Ask.

## 9. Confidentiality and access by Enarra's staff

- Enarra ensures that personal data is processed only by those of Enarra's people who need it to provide, maintain or support the Service, and that they have committed in writing to confidentiality or are under a statutory duty of confidentiality.
- Access by Enarra's staff to the Customer's data is limited to the minimum their tasks require. Enarra's administration panel shows only counts and statuses of organisations, not the Customer's content or users' names.
- Interview texts are not visible in the ordinary administration tools: they are technically restricted so that the administration panel, the administration command line and scheduled jobs cannot reach them. Technical superuser rights (the database owner account, root access to the servers and the backup keys, which only the two founders hold) may nevertheless make it possible to reach data kept on the servers or in backups, including interview texts and audio recordings.
- Exceptional access is allowed only for a documented reason: security, the operation of the Service, a statutory obligation or an action the Customer has requested (for example a data

subject's request, section 13). It is made for a limited time and by a named person. Every exceptional access is logged as a session that records the reason, the Customer, who made it, when it started and ended, and what was done, and the other founder reviews every session afterwards. The log is a procedure, not a technical barrier: the database owner account and root access to the servers can technically bypass it. Interview texts are read only in a disclosure under section 13, for which the restriction is lifted separately and the disclosure is logged. Interview texts are deleted at the latest when the stated retention period ends; copies in backups are gone at the latest after 36 days.

- When Enarra's support invites a new first administrator for the Customer because the Customer has no working administrator, the Customer's contact person is told by email. If the contact person's address has changed within the last 30 days, the message also goes to the previous address. The invitation and the sending of the message are recorded in Enarra's log. This lets the Customer notice an unauthorised access attempt made through support and ask for the invitation to be cancelled.

## 10. Security

Enarra implements technical and organisational measures under Article 32 of the GDPR. They are described in more detail in Annex 1 (Technical and organisational measures), which is given as an annex to the signed agreement. The annex separates the measures in use from those that are put in place before the Customer's data is processed in production. The key measures:

- **Separation of customers:** every row of data belongs to one organisation, and row-level security (RLS) in the PostgreSQL database prevents seeing or changing other organisations' data. The separation is checked by automated tests on every change. The accountant has separate access of their own that sees only billing.
- **Encryption in transit:** connections to the Service and to the database are encrypted (TLS).
- **Encryption at rest:** Enarra's own backups are encrypted with Enarra's keys before storage. Encryption at rest of the database and of the servers' disks will be confirmed in writing by UpCloud and put in place before the Customer's data is processed in production.
- **Access control:** roles (administrator, manager, expert, reader) and the principle of least privilege, also in the database roles. Sign-in with an email link or code or with a Microsoft or Google account. Enarra's administration panel requires two-factor authentication, and the servers can be reached only with personal SSH keys. Administration command-line commands

that change data also require a fresh two-factor authentication code. Exceptional access by Enarra's staff is described in section 9.

- **Log:** the Service records what is viewed, changed, approved and exported. The Customer's administrators see the log and can export it, except card views and card reports. No role in the application, not even an administrator, sees those rows, so that the log does not tell who read or reported what. They are used only to investigate security incidents on the Customer's instruction (section 6) or to investigate the security of Enarra's own Service (section 1), and a person's own rows are delivered only to that person (section 13). The log cannot be changed afterwards.
- **Backups and restore:** the test environment's database is backed up every night, encrypted, to Helsinki, and the restore is tested automatically every month. The same nightly backup and monthly restore test, and an encrypted, locked copy in Paris, are planned for production. They are put in place when production is set up, before the Customer's data is processed.
- **Environments:** the Customer's data is not processed in the test environment.
- **Incidents:** Enarra records security incidents, investigates their scope and informs the Customer under section 14.
- **Data minimisation:** short retention periods (section 5), discarding filtered content and not storing searches.
- **Integration credentials** are stored encrypted, and the database does not see the encryption key.
- **Vulnerabilities:** Enarra receives vulnerability reports at security@tarumo.fi. The procedure is described at tarumo.fi/en/security and in the file `tarumo.fi/.well-known/security.txt`.

Enarra may update the measures as long as the level of protection does not decrease.

## 11. Sub-processors

The Customer gives Enarra general authorisation to use the sub-processors listed below. Enarra binds them in writing to the same data protection obligations as in this agreement and is liable for them as for itself. Enarra makes the sub-processor agreements in Enarra Oy's name and archives them before the personal data of the first customer is processed. The Service is in its pilot phase, and the production environment has not yet been set up.

| Sub-processor | Task | Location and transfers |
|---|---|---|
| UpCloud Oy | Servers, the PostgreSQL database and its own backups, Enarra's encrypted backups and storage of audio recordings | Helsinki, Finland. No transfers outside the EU. The location of the database service's own backups will be confirmed in writing before production. |
| Scaleway SAS | AI models and speech recognition (Generative APIs), sending emails and delivery notifications (Transactional Email, Topics and Events), and the encrypted, locked copy of the backups planned for production (Object Storage) | Paris, France. No transfers outside the EU. In error or abuse cases, the content of a request may be kept for up to two weeks (section 8). |
| Zoho (contracting party to be confirmed) | Enarra's mailboxes, such as support, which may receive the Customer's personal data in support requests | Zoho's EU data centre. Zoho's Indian group company may access the data for technical support. This is a transfer outside the EU, and it is based on the EU standard contractual clauses (section 12). |
| Microsoft Ireland Operations Ltd | Only if the Customer turns on the Teams app: Azure Bot Service, which relays messages between the Service and the Customer's Teams | Bot in the EU region. Some of Microsoft's Bot Framework services are global, so data may be transferred outside the EU under Microsoft's terms (the EU–US Data Privacy Framework and standard contractual clauses). The role, location and sub-processors are checked against Microsoft's service-specific terms before the app is turned on for a customer. |

- **Services the Customer chooses itself** are not Enarra's sub-processors: Microsoft Entra ID and Google sign-in and user provisioning (SCIM), where authentication takes place in the Customer's or user's own account under the provider's terms, HR systems from which the Customer brings data, and the Customer's own Microsoft 365 environment. Enarra processes the data it receives from them under this agreement.
- Stripe would process only Enarra's own customer and billing data, so it is not a sub-processor under this agreement. Stripe has not yet been switched on. It is described in the privacy notice.

- **Changes:** Enarra notifies the Customer's administrators of a new or replacement sub-processor by email and on this page at least 30 days in advance. The notice states the sub-processor's name, task, the data processed, location and the basis for transfers. The Customer may object to the change on reasonable data protection grounds during this time. If the matter cannot be resolved, the Customer may terminate the contract to end before the change, and the unused part of a prepaid period is refunded.
- On request, Enarra provides information on the sub-processors' own subcontractors to the extent available to it and a copy of the sub-processor's data protection terms. Trade secrets may be redacted. Enarra informs the Customer if a sub-processor fails to meet its data protection obligations.
- **Teams:** the Teams app is not on by default; the Customer's administrator decides whether to turn it on. When the Service is connected to the Customer's Teams, Microsoft processes the messages under the contract between the Customer and Microsoft. A copy of the conversation remains in the Customer's Microsoft 365 environment, where the Customer's administrators may be able to access it, for example with an eDiscovery search. The copy also contains text that the Service filters out. Enarra is not responsible for this data and cannot delete it there on a data subject's erasure request. The Customer should take this into account in its own data protection practices. The Service tells users about the copy before their first interview answer in Teams.

## 12. Location of data and transfers

- The Service's data is stored in the EU: the servers, the database, backups and audio recordings in Finland, and AI, speech recognition and sending emails in France. The locked copy of the backups planned for production is in France. The same information is at tarumo.fi/en/data-location.
- An EU data centre alone does not settle the question of transfers. The following are transfers outside the EU and the EEA, and the Customer instructs Enarra to make them by this agreement:
  - Zoho's technical support may access the data in Enarra's mailboxes from India. The transfer is based on the EU standard contractual clauses. Enarra has drafted a transfer impact assessment for it, and Zoho's contracting party and the terms of support access will be confirmed before the first customer. The Customer is asked not to send unnecessary personal data in support messages.
  - Microsoft's Teams services, only if the Customer turns on the app (section 11).

- Otherwise Enarra does not transfer the Customer's personal data outside the EU and the EEA. A new transfer is a change under section 19 and is made only on the basis of a Commission adequacy decision or standard contractual clauses with any necessary supplementary measures. The Customer receives a copy of the standard contractual clauses used on request.
- If the Customer turns on Microsoft or Google sign-in, these providers are the Customer's own providers and process sign-in data under their own terms.

## 13. Data subjects' rights

- The Customer decides on data subjects' requests. Enarra helps the Customer respond to them (access, rectification, erasure, restriction of processing, portability and objection). The Service has tools for this, such as export, correcting cards and removing a user from the organisation. Enarra provides the help within five working days of the Customer's request at the latest, so that the Customer can respond to the data subject within the statutory time.
- **A person's own card view and report rows:** when a data subject asks for access to their data, the Customer refers the request to Enarra in writing at tietosuoja@tarumo.fi. Enarra checks the requester's identity and the scope of the request, delivers the person's own rows directly to them in a secure way and records the disclosure. Enarra tells the Customer only that the request has been completed, without the content of the rows. Enarra does not decide on the Customer's behalf which rights apply or whether the data contains other people's protected information.
- At the Customer's request, Enarra deletes an individual person's data: the texts, audio recordings and unapproved drafts of their interviews are deleted, and the name and email address of their user account are deleted when they are not a user in other organisations. The data is gone from backups under section 5. The Customer decides at the same time whether the cards the person published keep their name or show "Former expert" as the source.
- A valid erasure request is handled without undue delay. Article 17 of the GDPR has exceptions, and the Customer assesses whether they apply. Blanking a card's content is described in section 7.
- In the user interface, interview texts and audio recordings are visible only to the interviewee (section 7). The person can see them in the Service for their retention period and can download their own interview texts. Enarra does not disclose them to the Customer except under the next item.
- **Disclosure under a statutory obligation.** Enarra may disclose interview texts or audio recordings still held to the Customer only at the Customer's written and reasoned request and

only if the Customer's statutory or employment-law obligations strictly require it, for example in an investigation by an authority. Enarra discloses them to an authority when the law or an order of an authority requires it. In both cases:

  - only what is strictly necessary is disclosed;
  - Enarra tells the interviewee of the disclosure, unless the law prohibits it;
  - every disclosure is logged;
  - data already deleted cannot be disclosed: interview texts are deleted at the latest 30 days after the interview ends and audio recordings under section 5;
  - content removed by content filtering is never stored, so it cannot be disclosed.
- If a data subject contacts Enarra directly, Enarra refers the request to the Customer without delay and does not answer it without the Customer's instruction.
- The help is free of charge, unless the requests are exceptionally numerous.

## 14. Personal data breaches and security incidents

- Enarra notifies the Customer of every personal data breach affecting the Customer's personal data without undue delay and at the latest within 24 hours of becoming aware of the breach or of a reasonable suspicion that one has occurred. The notice is given whether or not Enarra assesses the breach to pose a risk. Within the same time, Enarra notifies a security incident that materially affects the Customer's data or the availability of the Service.
- The first notice may be preliminary. Enarra supplements it as soon as the facts are confirmed. The notice is sent to the contact person the Customer has named and to the administrators. It states at least what happened, which categories of data and which people are affected and how many, Enarra's contact person, the likely consequences and what Enarra has done or will do.
- Enarra has a written procedure for handling personal data breaches that sets out the responsibilities, detection, assessment, notification and recording. Security reports to Enarra go to the security contact point security@tarumo.fi (section 20).
- The Customer is responsible for notifying the Data Protection Ombudsman and the data subjects. Enarra does not notify them on the Customer's behalf without the Customer's instruction, unless the law requires it. Enarra helps the Customer with the information needed, records breaches and gives the record to the Customer.

## 15. Impact assessment and prior consultation

On request and free of charge, Enarra gives the Customer starting material for an impact assessment: a description of the processing, data flows, retention periods, sub-processors, transfers, security measures and identified risks with their mitigations. The material is not a ready impact assessment: the Customer adapts it to its own purpose, legal basis, staff, retention periods and procedures and is responsible for the assessment. Enarra updates the material when the Service changes materially and also provides information for any prior consultation (Articles 35 and 36 of the GDPR).

## 16. Audits

- Enarra gives the Customer the information that demonstrates compliance with this agreement and the obligations of Article 28. Primarily this is done in writing, for example by answering the Customer's security questionnaire. On request, Enarra also provides its sub-processors' security certificates and reports to the extent available to it. No external security testing has been done in the pilot phase; on request, Enarra describes the internal reviews it has carried out.
- The Customer may also audit the processing once a year with 30 days' notice, or at once if there is a particular reason, such as a personal data breach. The audit is carried out by the Customer or by an independent auditor of its choice bound by confidentiality. The Customer bears its own costs.
- Written answers and answering a reasonable, ordinary security questionnaire are free of charge. If an audit requires substantial work from Enarra, Enarra may charge for its assistance at its usual hourly rates, unless the audit reveals material shortcomings in Enarra's processing.
- An audit must not endanger other customers' data or the security of the Service. The supervisory authority's right of inspection always applies.

## 17. Return and deletion at the end of the contract

- When the processing of personal data ends, Enarra, at the Customer's choice, returns the personal data or deletes it and deletes existing copies, unless Union or Member State law requires storage (Article 28(3)(g) of the GDPR). Return is made by export. The exportable data and the data not exported are the same as in section 9 of the terms of service, and they are listed below.
- When the contract ends or the Customer requests switching, Enarra makes available to the Customer the exportable data listed in the contract and in the current export specification in a

structured, commonly used and machine-readable format. The export specification identifies the categories of data, formats, structures, technical limitations and the retrieval procedure.

- After the contract ends, the Customer has an export period of at least 30 days. If the Customer has requested switching to another service or porting of data, the Service first continues for a 30-day transition period, and the export period begins only after that (section 12 a of the terms of service).
- Erasure under the GDPR, export under the Data Act and an employee's right of access to their own data are separate matters. They are reconciled per category of data in the table below and in section 13.

### Exportable data

The Customer's administrators can export themselves in the service:

- the published knowledge cards and their archived versions with their sources (the expert or "Former expert" and the dates), and the cards' warnings of outdated or incorrect information without who reported them, in Markdown and JSON;
- the organisation's log as CSV (at most the 10,000 newest events), except card views and card reports;
- the mapping report in Markdown, if the Customer has had Mapping;
- invoices as PDF files for as long as they are in the service: Customers paying on invoice from the service's invoice list, and Customers paying by card from Stripe's payment portal. The accountant can also download them.

In addition, administrators can download themselves, from the service's Organisation page, the published knowledge cards and the following data as one ZIP file in JSON. If an administrator cannot download them, for example because the organisation no longer has an administrator who can access the service, Enarra delivers them on request in JSON within 14 days at the latest:

- key people and their knowledge areas: departure date and its confirmation, criticality, whether they are the only expert, successor and link to a knowledge pack;
- the Customer's own knowledge packs and the Customer's changes to Enarra's packs with their versions, and the mapping pack proposals experts have sent;
- coverage by knowledge area and by part;
- users and their roles, the accountant, teams, team challenges, reward settings and the organisation's other settings;

- the organisation's whole log, except card views and card reports;
- read counts and "useful" marks per card as monthly totals, with no information about the readers or the card's author. Only completed calendar months in which the card has at least three reader-days are included; other months are not released and their figures are not carried over to other months. Reads are counted per day, and the Service aims to count the same reader once per card and day. The reads of a released month do not change, but the number of "useful" marks can go down if a mark is withdrawn or a user's data is erased, and a card leaves the file when it is corrected or withdrawn.

The structure and formats of the exported files are described at tarumo.fi/en/export. The contract is governed by the version of the export page archived under the same version identifier as the terms the Customer accepted. If a request is made within the export or retrieval period, Enarra delivers the data even if the delivery falls after that period ends, and does not delete the data before delivering it.

### Data not exported, and why

The following categories of data are not part of the Customer's export. This does not prevent switching: the content meant for the organisation's use moves as the published knowledge cards and the data listed above.

| Category | How it is handled | Why it is not exported to the Customer |
|---|---|---|
| Interview texts and audio recordings, undecided card drafts and draft mapping proposals | Short-lived working material of the interview, visible in the service only to the interviewee. The interviewee can download their own interview texts. An interview text is deleted when the card made from it is approved or rejected, and at the latest 30 days after the interview ended. An audio recording is deleted by default 30 days after transcription. | The Customer, as controller, has defined the material as the interviewee's working tool, not as the organisation's material (sections 5 and 6 of the data processing agreement). The knowledge meant for the organisation moves as approved knowledge cards. Free-form answers may contain information that it is not necessary to disclose to the employer under section 3 of the Finnish Act on the Protection of Privacy in Working Life. This does not limit the interviewee's own rights. |

| Category | How it is handled | Why it is not exported to the Customer |
|---|---|---|
| Personal points, levels, achievements and reward choices | Visible only to the person themselves. Incentives are off by default. The settings of team challenges and rewards are exported. | The data is collected for the person's own use. Disclosing it to the employer would make it material suited to evaluating employees, which section 3 a of the terms prohibits, and would breach purpose limitation (Article 5(1)(b) of the GDPR) and section 3 of the Act on the Protection of Privacy in Working Life. |
| Individual card view rows (who opened which card and when) | Exported only as monthly totals per card (at least three reader-days in the month) with no information about the readers (above). The rows are kept for 12 months to investigate security (section 5 of the data processing agreement). A person receives their own rows under section 13 of the data processing agreement. | Reading data per person would tell the employer who read what and would be suited to monitoring employees (section 3 a of the terms, section 3 of the Act on the Protection of Privacy in Working Life). The organisation's need to know how the cards are used is met by the totals. |
| Who reported a card | Reports are exported without the reporter. | The reporter's identity is not needed to correct the card, and keeping it confidential protects the reporter. |
| Filtered content | Not stored. | There is nothing to export. |
| Search index vectors | Computed from the published cards and deleted with them. | The vectors depend on the model and settings Enarra has chosen and are of no use in another service. They can be recomputed from the exported cards. Exporting them would reveal Enarra's technical implementation. |
| The AI's prompts and the intermediate results of the risk calculation | The service's internal workings. The result is shown in the coverage data. | Enarra's trade secrets and intellectual property, which are not exportable data (Article 2(38) of the Data Act). |
| The service's technical log and | Enarra's own processing for the service's security (privacy notice). | The log concerns the service's infrastructure and may contain other customers' data. |

| Category | How it is handled | Why it is not exported to the Customer |
|---|---|---|
| Enarra's administration log | What the Customer's users do is in the organisation's log, which is exported. | Disclosing it would weaken the service's security. |
| Enarra's general knowledge packs | The Customer's changes to them are exported. | Enarra's intellectual property. |

### Deletion

- After the export period, Enarra permanently deletes the Customer's personal data within 30 days at the latest and confirms the deletion in writing on request, unless keeping it is necessary under mandatory law or to establish legal claims. It is gone from the encrypted backups at the latest 36 days after deletion.
- Interview texts, audio recordings and unapproved drafts are deleted without being returned to the Customer, because they are meant only for the interviewee and are in any case deleted after a short time. The interviewee can download their own texts before the deletion.
- When the contract ends, Enarra asks Scaleway to delete the metadata of emails sent to the Customer's users. Whether Scaleway can delete them on request has not yet been confirmed.
- Enarra keeps only what the law requires or what is Enarra's own processing as controller:
  - invoices, vouchers and billing data that belong to Enarra's own bookkeeping, for the retention periods of the Finnish Accounting Act and VAT Act, in practice at least six years from the end of the year in which the financial year ends (the financial statements and the list of accounts ten years). The bookkeeping is kept in Enarra's own accounting system, whose server is at UpCloud in Finland. The invoices contain the billing contact's name and contact details;
  - the organisation's name and identifier and a record of the deletion;
  - Enarra's own administration log: entries on billing, payments, invoice documents and the hand-over of bookkeeping data for 6 years, technical failure events for 180 days, and other entries, such as administrators' views and sign-ins, for 24 months. Records of exceptional access sessions and their reviews, and of the deliveries and disclosures made under them (sections 9 and 13), are kept for 6 years, because they show how the Customer's data was accessed. The log is described in the privacy notice;
  - the deletion ledger (identifiers without names or addresses) for at most 40 days, so that the deletion can be repeated if the database is restored from a backup;

    - the blocklist of bounced email addresses, which holds only a keyed hash of the address and a masked hint.
- The PDF copies in the Service's invoice list are deleted with the organisation. The Customer keeps its purchase invoices in its own bookkeeping.

## 18. Liability

- Each party is liable to data subjects under Article 82 of the GDPR. The limitations of liability in this agreement do not limit the rights of third parties, including data subjects, under mandatory law. The parties' liability towards each other and any right of recourse are determined by this agreement and the applicable law. Each party bears the administrative fines imposed on it.
- Between the parties, the limitations of liability in section 14 of the terms of service apply, as follows. They are the same for both parties and apply to contractual claims for damages. Fees means the fees excluding VAT that the Customer has paid or that have fallen due for the Service in the 12 months before the event giving rise to liability.
- **General cap:** each party's total liability per contract year is at most the amount of the fees described above, but at least €5,000. For a one-off package (Handover and Mapping), the cap is the one-off fee, but at least €5,000.
- **Data protection and confidentiality:** liability arising from a breach of the obligations on processing personal data (data protection law and this agreement) or of the confidentiality obligation is subject to a separate cap instead of the general cap. It is, per contract year, three times the fees on which the general cap is based or €15,000, whichever is greater.
- The separate cap also covers, as direct damage, compensation that a party has paid to data subjects under Article 82 for a breach for which the other party is responsible and claims back under Article 82(5), and reasonable costs of investigating and notifying a personal data breach and of restoring data. The exclusion of indirect damage does not apply to these amounts.
- The limitations, including the separate cap, do not apply to the Customer's payment obligation, to damage caused intentionally or through gross negligence, to intentional misuse of the other party's trade secrets, to intentional infringement of intellectual property rights, to intentional circumvention of the Service's security, or to liability that cannot be limited under mandatory law. Other breaches of the terms of service and this agreement fall within the caps.
- A claim must be made in writing at the latest 12 months after the party discovered the damage or should have discovered it.

## 19. Term and changes

- The agreement is in force as long as Enarra processes the Customer's personal data.
- Enarra may change the agreement on the same terms as the terms of service (section 16 of the terms of service). Changes required by law, an order of an authority or security may take effect sooner. Section 11 applies to changes of sub-processors.
- A change that weakens the protection of personal data or extends the processing, such as a new transfer outside the EU or a longer retention period, is notified at least 90 days in advance. The Customer may object to it during the notice period. If the matter cannot be resolved, the Customer may terminate the contract to end before the change, and the unused part of a prepaid period is refunded.
- A signed agreement is governed by the version accepted as its annex. A later online version does not replace it automatically; the agreement is changed by the procedure in this section.
- If Enarra ceases its business or is declared bankrupt, the Customer has the right to receive its data by export and to require its deletion. Enarra also arranges this with its sub-processors.
- The order records which version the person ordering accepted and when. Every version has a permanent archived copy and a PDF file that can be saved. The order page links the PDF files before acceptance, and the order confirmation links the same files.

## 20. Contact details

Enarra Oy (Business ID 3664892-5)
Artturintie 4, 43500 Karstula, Finland
Contract matters: sales@tarumo.fi

Privacy contact point (data subjects' requests and data protection questions): tietosuoja@tarumo.fi. Security contact point (personal data breaches and vulnerabilities): security@tarumo.fi. Support: support@tarumo.fi. Enarra has not appointed a data protection officer. Enarra sends its notices to the Customer's administrators by email. The Customer names in the order, or tells Enarra, a contact person for data protection or security matters, to whom the notices under section 14 are sent in addition to the administrators.