Archived version draft-2026-10-28

This is the Tarumo data processing agreement as it was when archived on 28 October 2026. An archived version is never changed. An order records the identifier of the version accepted.

Current version · All versions · Suomeksi · Tarumo

DRAFT, PENDING APPROVAL

Data processing agreement

Draft of 28 October 2026, not yet in force

Previous versions

This is a draft pending approval by Tarumo Oy. The agreement takes effect only once the approved version is published on this page. Online ordering of the Small (Pieni) and Handover (Siirto) packages opens only after that.

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 Tarumo Oy, 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 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 Tarumo'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 and scope

- **The controller** is the company or other organisation that has ordered the Tarumo service, hereinafter the Customer.
- **The processor** is Tarumo Oy (business ID 3664892-5, Artturintie 4, 43500 Karstula, Finland), hereinafter Tarumo.
- The agreement covers the personal data that Tarumo processes on the Customer's behalf when providing the Tarumo service. This includes the user account of the accountant the Customer invites and the log data arising from the accountant's actions, because the Customer decides who sees its billing.
- The agreement does not cover data that Tarumo processes as a controller, such as the details of the Customer's contact person, Tarumo's own invoices, the PDF copies in the service's invoice list, the new-invoice notices sent to the accountant, and the feedback and bug reports that users of the service send to Tarumo. Those are described in the privacy notice.
- For online orders, the agreement is accepted when ordering. For other packages, it forms part of the signed order or contract. 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 Tarumo 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 the 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.

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. Tarumo'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, the invitation, the start and end of access and the choice on new-invoice notices. The accountant's actions are logged.	As long as the person is the accountant or until the organisation's data is deleted. Log entries for the retention period of the log.
Sign-in events and sessions	Sign-in events 90 days, sessions at most 30 days
Key person data: name, job title, starting year, departure date and its confirmation, knowledge areas, criticality and whether they are the only expert	For the term of the contract; an archived key person remains as a card's source
Interview questions and answers (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
Dictation audio (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, the source (expert and date), versions, archived versions and reports of outdated information	For the term of the contract. Cards are not deleted but replaced, and the version history is kept. 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.

Data	Retention
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 draft pack proposals (visible only to the expert), and pack proposals sent under 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 erased, their choices and drafts are deleted.
Incentives: a person's points, level and achievements (visible only to them), their reward choices, rewards notified 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 without the reader's identity and users' own "useful" marks	For the term of the contract
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 (section 10).	For the term of the contract
Notifications and reminders (email or Teams)	Tarumo does not store their content 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 Tarumo'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 asked 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 of filtering per day and reason for each organisation is recorded, without the person or the content. If the AI is unavailable, an interview answer or a card edit that has passed the word lists is stored awaiting review (section 7).
- **Special categories:** the Customer instructs that no special categories of personal data (Article 9 of the GDPR) and no data on criminal offences (Article 10) are stored in the service. The content filter does not currently recognise such data. That is why the expert checks the draft before approving it, and the Customer instructs experts to describe practices rather than individual people (section 6 a).
- **Backups:** in production, the encrypted backups are kept in Helsinki, and an encrypted, locked copy is kept in Paris (Scaleway). The locked copy cannot be changed or deleted before its retention period ends. All backups are gone at the latest 36 days after they were made, so deleted data leaves the backups within 36 days at the latest. The database service also keeps its own encrypted backups for up to 15 days. Dictated audio is not included in the backups.

6. The Customer's instructions

- Tarumo processes personal data, including transfers outside the EU and the EEA, only on the Customer's documented instructions. 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 audio retention period, the sign-in methods, switching on incentives, Mapping, enabling the Teams app and the HR integrations. The instructions also include the principles of section 7, such as interviews being visible only to the interviewee and the deletion of interview texts under section 5.
- The Customer gives further instructions in writing through its administrators, and Tarumo keeps them.
- By accepting this agreement, the Customer also instructs Tarumo
  - to record card views and card reports to investigate the security of the service, and to deliver a person's own rows to them under section 13 (section 10);
  - to 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;
  - to transfer data as set out in section 12.
- If EU or Finnish law requires Tarumo to process data otherwise, Tarumo informs the Customer before the processing, unless the law prohibits it.

- If Tarumo considers that an instruction infringes data protection law, it informs the Customer without delay and may refrain from carrying out 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 processing being lawful. In particular, the Customer:

determines the legal basis. Processing employees' data is usually based on the Customer's legitimate interest in passing on know-how, 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 needed to pass on know-how: a departure that has been agreed or that the employee has announced, not estimates of the employee's age, health or intentions;

informs employees and key people about the use of the service before it is introduced (Articles 13 and 14 of the GDPR). Tarumo provides the information about the service needed for this;

handles the introduction with the staff: in a company with at least 50 employees in the dialogue under the Finnish Co-operation Act and, where needed, in change negotiations; in a company with 20–49 employees in the dialogue under section 7 a of that Act; and in a smaller company by hearing the employees when section 21 of the Act on the Protection of Privacy in Working Life requires it;

assesses whether a data protection impact assessment is needed. In Tarumo's view it usually is, because the service processes employees' data with AI. Tarumo provides material for it (section 15);

does not use the service or its data to evaluate, score, compare or monitor employees' performance or for decisions on employment (section 3 a of the terms of service). The service's own incentives are allowed as they work in the service (section 3 b of the terms of service);

instructs experts to describe practices rather than individual people and not to store data on health, trade union membership or other special categories of personal data;

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

decides who its accountant is and removes the accountant when their task ends (section 7 a of the terms of service).

7. Principles of the processing

Tarumo 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 measures the risk of knowledge being lost, not how people perform.
- **The interview belongs to the interviewee.** In the service, interview answers are 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 Tarumo's staff.
- **Published only with approval.** A knowledge card is published only with the expert's approval. 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. 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.** An outdated or incorrect card is archived when a corrected version is approved, and the version history is kept. The 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

- Tarumo uses the Customer's data only to provide the service. **Tarumo never uses the Customer's data to develop or train AI models**, and this includes the diagnostic data mentioned below.
- Tarumo is the provider of the service's AI system and the Customer its deployer (section 3 a of the terms of service). The service tells users when they are interacting with AI, and AI output is marked visibly and in a machine-readable way. The service makes no decisions about people based solely on automated processing (Article 22 of the GDPR). The risk radar is a rule-based calculation of the risk of knowledge being lost, not an assessment of a person.
- 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.
- 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 Tarumo's staff

- Tarumo ensures that personal data is processed only by those of Tarumo's people who need it to provide, maintain or support the service, and that they have committed to confidentiality or are under a statutory obligation of confidentiality.
- Tarumo's administration panel shows only counts and states of organisations, not Customer content or users' names.
- Tarumo's named administrators hold database administration credentials. Interview texts are technically restricted so that Tarumo's administration tools and scheduled jobs cannot reach them. The texts are read only in a disclosure under section 13, for which the restriction is lifted separately and the disclosure is logged. The database superuser account, the servers' root access and the backup keys nevertheless give technical access to all of the Customer's data, including interview texts, until they are deleted under section 5. They are held only by two named people who are bound to confidentiality, and they are used only to maintain the service, to investigate security and for actions the Customer has asked for (for example data export and data subjects' requests). The backups contain the interview texts for no longer than section 5 allows.

10. Security

Tarumo implements the technical and organisational measures required by Article 32 of the GDPR, in particular:

- **Separation of customers:** every row of data belongs to one organisation, and the row-level security (RLS) of the PostgreSQL database prevents seeing or changing other organisations'

data. The separation is checked by automated tests on every change. The accountant has a 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:** the database, the servers' disks and the backups are stored encrypted with keys managed by the provider. Tarumo's own backups are also encrypted with Tarumo's keys before they are stored.
- **Access control:** roles (administrator, manager, expert, reader) and the principle of least privilege, also in the database roles. Sign-in by email link or code or with a Microsoft or Google account. Tarumo's administration panel can be accessed only with two-factor authentication, and the servers only with personal SSH keys.
- **Log:** the service records what is viewed, changed, approved and exported. The Customer's administrators can see the log and export it, except card views and card reports. No role in the application sees those rows, not even an administrator, so that the log does not tell who read or reported what. They are used only to investigate the security of the service on the Customer's instruction (section 6) and are delivered only to the data subject themselves on their access request (section 13). The log cannot be altered afterwards.
- **Backups:** the production database is backed up every night. The backups are encrypted and kept in Helsinki, and an encrypted, locked copy is kept in Paris. Restoring is tested monthly, and opening the stored backups quarterly.
- **Environments:** the Customer's data is not processed in the test environment.
- **Incidents:** Tarumo records security incidents, investigates their extent and notifies 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 never sees the encryption key.

Tarumo may update the measures provided that the level of protection does not decrease.

11. Sub-processors

The Customer gives Tarumo general authorisation to use the sub-processors listed below. Tarumo binds them in writing to the same data protection obligations as in this agreement and is responsible for them as for itself.

Sub-processor	Task	Location and transfers
UpCloud Oy	Servers, the PostgreSQL database and its own backups, Tarumo's encrypted backups and storage of audio recordings	Helsinki, Finland. No transfers outside the EU.
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 (Object Storage)	Paris, France. No transfers outside the EU.
Zoho Corporation B.V.	Tarumo'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; the transfer is based on the EU standard contractual clauses.
Microsoft Ireland Operations Ltd	Only if the Customer enables the Teams app: Azure Bot Service, which passes messages between Tarumo and the Customer's Teams	The bot is 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).

- **Services the Customer chooses itself** are not Tarumo's sub-processors: Microsoft Entra ID and Google sign-in and user synchronisation (SCIM), where authentication takes place in the Customer's or the user's own account under the provider's terms, the HR systems from which the Customer brings data, and the Customer's own Microsoft 365 environment.
- Stripe processes only Tarumo's own customer and billing data, so it is not a sub-processor under this agreement. The privacy notice describes it.
- **Changes:** Tarumo notifies the Customer's administrators of a new or replaced 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, the location and the basis of any transfers. The Customer may object to the change on reasonable data protection grounds during that time. If the matter cannot be resolved, the Customer may terminate the contract to end before the change, and the unused part of a period paid in advance is refunded.

- On request, Tarumo gives information on the sub-processors' own subcontractors, as far as it is available to Tarumo, and a copy of a sub-processor's data protection terms. Trade secrets may be redacted. Tarumo informs the Customer if a sub-processor fails to meet its data protection obligations.
- **Teams:** the Teams app is off by default, and the Customer's administrator decides whether to enable it. When the service is integrated into the Customer's Teams, Microsoft processes the messages under the agreement between the Customer and Microsoft. A copy of the chat stays in the Customer's Microsoft 365 environment, where the Customer's administrators may be able to access it, for example with an eDiscovery search. Text that Tarumo filters out also stays in the copy. Tarumo is not responsible for that 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 the user about the copy before their first interview answer in Teams.

12. Location of data and transfers

- The data in the service is stored in the EU: servers, database, backups and audio recordings in Finland; the locked copy of the backups, AI, speech recognition and sending emails in France. The same information is at tarumo.fi/en/data-location.
- Tarumo itself does not transfer the Customer's personal data outside the EU and the EEA. A sub-processor's group company in a third country may, however, access the data in exceptional cases, for example for technical support, and only on the basis of an adequacy decision of the Commission or standard contractual clauses with any necessary supplementary measures. These cases are marked in the list in section 11: Zoho's technical support from India and Microsoft's Teams services. By this agreement, the Customer instructs Tarumo to carry out these transfers.
- If the Customer enables Microsoft or Google sign-in, these providers process the sign-in data under their own terms.

13. Data subjects' rights

- Tarumo helps the Customer respond to data subjects' requests (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. Tarumo gives this help within five business days of the Customer's request at the latest, so that the Customer can reply to the data subject within the time required by law.

- When a data subject asks for access to their data, Tarumo, on the Customer's instruction, delivers the person's own card view and card report rows directly to them. Tarumo tells the Customer only that the rows have been delivered.
- At the Customer's request, Tarumo deletes an individual person's data: the texts of their interviews, their audio recordings and their unapproved drafts 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 leaves the backups as set out in section 5. The Customer then decides whether the cards the person published stay under their name or the source is changed to "Former expert".
- Interview texts and audio recordings are visible only to the interviewee (section 7). The person sees them in the service for as long as they are kept. Tarumo does not disclose them to the Customer except as set out in the next item.
- **Disclosure under a statutory obligation.** Tarumo may disclose interview texts or audio recordings that still exist to the Customer only on the Customer's written, justified request, and only when the Customer's statutory or employment-law obligations strictly require it, for example in an authority's investigation. Tarumo discloses them to an authority when the law or an authority's order requires it. In either case:
  - only what is strictly necessary is disclosed;
  - Tarumo tells the interviewee about 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 the content filter is never stored, so it can never be disclosed.
- If a data subject contacts Tarumo directly, Tarumo forwards the request to the Customer without delay and does not respond to it without the Customer's instruction.
- This assistance is free of charge unless the requests are exceptionally numerous.

14. Personal data breaches and security incidents

- Tarumo notifies the Customer of every personal data breach concerning the Customer's personal data without undue delay and at the latest within 48 hours of becoming aware of it. The notice is given whether or not Tarumo assesses the breach as a risk. Within the same time, Tarumo notifies the Customer of a security incident that materially affects the Customer's data or the availability of the service.

- The notice is sent to the contact person the Customer has named and to its administrators. It describes at least what happened, which categories of data and people are affected and how many, Tarumo's contact person, the likely consequences and what Tarumo has done or will do. The information may be given in phases as it becomes available.
- The Customer is responsible for notifying the supervisory authority and the data subjects. Tarumo does not notify them on the Customer's behalf without the Customer's instruction, unless the law requires it. Tarumo helps the Customer with the necessary information, documents breaches and gives the record to the Customer.

15. Impact assessment and prior consultation

On request, Tarumo gives the Customer free of charge the material for a data protection impact assessment: a description of the processing, the data flows, the retention periods, the sub-processors, the transfers, the security measures and the identified risks with their mitigations. Tarumo updates the material when the service changes materially, and also gives the information for any prior consultation (Articles 35 and 36 of the GDPR).

16. Audits

- Tarumo gives the Customer the information that shows compliance with this agreement and the obligations of Article 28. This is done primarily in writing, for example by answering the Customer's security questionnaire. On request, Tarumo also gives its sub-processors' security certificates and reports, as far as they are available to it.
- In addition, the Customer may audit the processing once a year with 30 days' notice, or at once if there is a specific reason such as a personal data breach. The audit is carried out by the Customer or by an independent auditor of its choice who is bound by confidentiality. The Customer bears its own costs.
- Written answers and answering a reasonable, standard security questionnaire are free of charge. If an audit requires substantial work from Tarumo, Tarumo may charge for its assistance at its normal hourly rates, unless the audit reveals material shortcomings in Tarumo's processing.
- An audit must not endanger other customers' data or the security of the service. A supervisory authority's right of inspection always applies.

17. Return and deletion at the end of the contract

- When the contract ends, the Customer chooses whether the data is returned or deleted. The 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.
- After the contract ends, the Customer has an export period of at least 30 days. If the Customer has requested a switch to another service or the porting of its data, the service first continues for a 30-day transition period, and the export period begins only after it (section 12 a of the terms of service).

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, Tarumo 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 Tarumo'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.

On request, Tarumo delivers card read counts and the numbers of "useful" marks as figures per card in JSON within 14 days at the latest.

The structure and formats of the exported files are described at tarumo.fi/en/export. If a request is made within the export or retrieval period, Tarumo delivers the data even if the delivery falls after that period ends, and does not delete the data before delivering it.

Data not exported

- Interview texts and audio recordings, undecided card drafts and draft mapping proposals. They are visible only to the interviewee and are deleted after a short time. This is how the Customer, as controller, has given instructions, and data protection law takes precedence over the Data Act.
- Personal points, levels, achievements and reward choices. They are visible only to the person themselves.
- The card view rows (who opened which card) and who reported a card. They are not shown to the Customer, so that the log does not tell who read or reported what.
- Filtered content, which is not stored.
- The service's internal workings: the AI's prompts, the intermediate results of the risk calculation, the search index vectors and the service's technical log. They are Tarumo's trade secrets or tied to Tarumo's implementation.
- Tarumo's general knowledge packs, which are Tarumo's intellectual property. The Customer's changes to them are exported.

Deletion

- After the export period, Tarumo permanently deletes the Customer's personal data within 30 days at the latest and confirms the deletion in writing on request. It leaves the encrypted backups at the latest 36 days after the deletion.
- Interview texts, audio recordings and unapproved drafts are deleted without being returned, because they are meant only for the interviewee and are deleted after a short time in any case.
- When the contract ends, Tarumo asks Scaleway to delete the metadata of the emails sent to the Customer's users.
- Tarumo keeps only what the law requires or what is Tarumo's own data:
  - the invoices, vouchers and billing records that belong to Tarumo's own bookkeeping. They are kept for the time required by chapter 2, section 10 of the Finnish Accounting Act and

section 209 n of the Finnish VAT Act, at most until the end of the seventh year after the invoice year. The invoices contain the name and contact details of the billing contact;
  - the organisation's name and identifier and the record of the deletion;
  - its own administration log, described in the privacy notice;
  - the record of erasures (identifiers without names or addresses) for at most 40 days, so that an erasure can be repeated if the database is restored from a backup;
  - the suppression list of bounced email addresses, which holds only a keyed hash and a masked hint of each address.
- 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. Neither this agreement nor the terms of service limit that liability between a data subject and either party. Each party is liable for the administrative fines imposed on it.
- Between the parties, the limitations of liability in section 14 of the terms of service apply. Breaches of data protection and breaches of confidentiality are subject not to the general cap but to a separate cap. Per contract year, it is three times the fees on which the general cap is based (the fees the Customer has paid, or that have fallen due, for the service in the 12 months before the damage; for a package with a one-off fee, the one-off fee) or €15,000, whichever is greater.
- The separate cap also covers, as direct damage, compensation a party has paid to data subjects under Article 82 for a breach for which the other party is responsible and which it claims back under Article 82(5), as well as 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.
- Liability is not limited for damage caused intentionally or by gross negligence, or where mandatory law prohibits limiting it.

19. Term and changes

- The agreement remains in force as long as Tarumo processes the Customer's personal data.
- Tarumo may change the agreement on the same conditions 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. Changes to sub-processors follow section 11.

- 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 period paid in advance is refunded.
- If Tarumo ceases its business or is declared bankrupt, the Customer has the right to receive its data by export and to require its deletion. Tarumo arranges this with its sub-processors too.
- Each online order records which version the person ordering accepted.

20. Contact details

Tarumo Oy (business ID 3664892-5)
Artturintie 4, 43500 Karstula, Finland
Email: sales@tarumo.fi

Questions, requests and notices concerning data protection can be sent to the same address. Tarumo sends its notices to the Customer's administrators by email. The Customer names in the order, or tells Tarumo, a contact person for data protection or security, to whom the notices under section 14 are sent in addition to the administrators.