Version 2025.06

TinQwise Policy

005.1

Data Segregation & Retention

TinQwise B.V. | Mussenstraat 15 | 1223 RB | Hilversum | The Netherlands | +31 35 538 5656
CoC Hilversum 32082603 | VAT NL809771287B01 | IBAN NL26 INGB 0006679651 | SWIFT / BIC INGBNL2A | tinqwise.com

tinQwise

Validity and document management

Version	Date	Author	Description
01	2021-06-08	Simon Kennedy & Wim Van Dessel	Document creation
02	2022-11-02	Simon Kennedy & Elena Neagu	Annual review and policy update.
03	2022-11-27	Reinoud van Dommelen	Update to align with standard customer contract set. Renumbering.
04	2023-01-04	Simon Kennedy & Emil de Valk	Updated with detailed data segregation architecture
05	2023-11-02	Emil de Valk, Okke Formsma	Annual review & policy update
07	2023-12-12	Emil de Valk	Annual review

This document is valid as of January 1st, 2025.

The owner of this document is the C.O.O., who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- Number of (potential) data segregation related findings arising from regular and ad-hoc security reviews and penetration testing
- Number of (potential) data segregation incidents arising from failed security / access controls built into the systems

TinQwise reserves the right to update this Policy to reflect changes in our practices and regulatory requirements. Data subjects will be informed of material changes. Previous versions of this procedure will be stored for a period of 5 years, unless specified otherwise by legal or contractual requirement.

tinQwise

Table of Contents

tinQwise

1. Relevant to

Management	Finance / Legal	HR	Office Management	Marketing, Sales and Account Management	Professional services	IT Support	Product & Engineering	DevOps	Support & Maintenance
X	X				X	X	X	X	X

2. Purpose

The purpose of this document is to offer a detailed overview of how we segregate and retain data – i.e. how we keep Client's data separated from each other, safely, structurally, and by design. Additionally, we cover administrator rights and how data is accessed.

3. Scope

This policy applies to all data within TinQwise Platform.

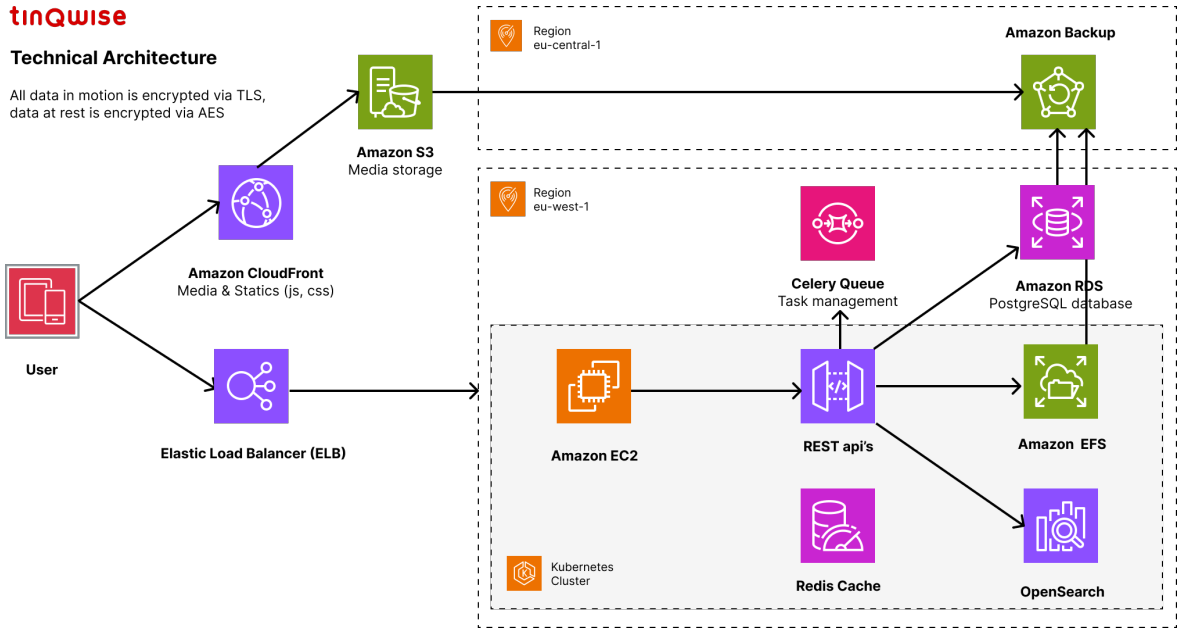
4. Compliance to this policy

The C.O.O. is responsible for verifying compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits. Any exception to the policy is subject to the Information security exceptions management process.

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Application Architecture

TinQwise Platform is a fully scalable, cloud-native SAAS Application, built using the most modern and secure technology available, and hosted in ISO 27001 and SOC2-certified European data centers of Amazon Web Services.



6. Data minimization

Data Privacy is critical to TinQwise, and we are constantly working to ensure that we are GDPR compliant.

One of our standard principles is data minimization, using only essential data. We make use of the bare minimum of Personal Data to ensure a functional user experience. Users removed from a Platform are automatically anonymized after an agreed retention period. Once projects are closed out and a Platform deleted, all associated Users and all instance data are permanently deleted from the SAAS Application.

7. Data segregation mechanism

TinQwise Platform is a multitenant SAAS Application. The software is architected with multi-tenancy on “platform” level. Separating Client data occurs on software level, backed by an extensive set of unit tests to ensure segregated datasets in any future adjustment of platform logic.

Access to Personal Data and confidential data in a particular Platform is only granted to administrators with appropriate administrative rights in the system, following our Access Control Policy. Users can be easily removed from the Platform by Administrators or automatically suspended from the system through integrations with Client HR or identity management systems.

tinQwise

Software level data-segregation

The SAAS Application uses a software-level segregation model. All tenants share the same database. TinQwise chose software-level segregation for reasons of simplified and scalable security, data backup and recovery processes, as well as reduction of database management overhead and volume-related risks.

The SAAS Application data model segregates every tenant with a unique “platform” object. All related objects like users, groups, learning content, comments, answers and so on are connected to this unique platform object using database foreign key relations.

Every platform has a “domain” attached to it. All incoming traffic can only be handled by the chosen domain for that “platform” tenant. All API handling for any given tenant is filtered for that “platform” domain. E.g. every platform has a set of APIs available at a URL like: https://tinqwise.platform.co.nl/api/v3/public/.

In the API layer and the data layer underneath we use application-level filters to ensure that each tenant only sees their own data. We do this by adding filters with the platform domain to all database queries to ensure that they only retrieve data belonging to the requesting tenant. Data segregation is tested via a suite of unit tests, as well as third party code analysis and testing during our yearly penetration test cycle.

Role based access to data via application

We use role-based access control to restrict access to certain parts of the application based on the user’s role. We do this by getting the requesting user from either:

- An active session via cookies
- An active session via a JSON Web Token (JWT)
- An active session via an OAuth requested token

First the SAAS Application determines the role based on the database level relation object to the “platform” tenant. That relation describes their role in the platform. Roles determined like this are: staff user, platform administrator and regular user.

Second, the SAAS Application determine optional additional “permissions” over groups or objects that grant access to (parts of) the reporting capabilities. Roles determined like this include Trainers, (team-)Managers and Content creators.

A small set of ‘Super Administrators’ (specifically C.O.O., head of Engineering, technical architect and back-end engineers) have access to all instances, in accordance with our Access Control, Data Privacy and Secure Development Policies.

Scope based access to data via API’s

Our external APIs are all managed by oAuth based scoped “applications”. Each application is attached to a single “platform” tenant. Each application gets an explicit list of scopes for different resources and the required action (e.g. v3:users:read). Access to the resource can be requested following the OAuth 2 standard protocol with a Key and Secret shared by TinQwise Staff only.

Tenant based access to assets

Access to tenant specific assets is limited to the domain attached to a tenants “platform” object. Access is only granted when assets are requested with a valid “media token”. This is effectively a JSON Web Token that can only be used to request assets. Requesting the same media without a “media token”, or from another tenant’s domain is blocked. Media tokens invalidate after 10 minutes.

Tenant onboarding

During the onboarding of a Client a new “platform” is created with a unique domain. In most cases, provisioning of users, groups and permissions is automated with a scheduled background process that loads the current set of users that should have access to the SAAS Application from the source provided by the Client. The scheduled background process is running exclusively for this tenant. Some Clients buy off-the-shelf content from TinQwise. That content is copied and can be adjusted to the Clients’ liking without affecting the source content. The same goes for the reverse route, adjustments in the source of the content will never get published automatically to the tenant's copy.

Monitor and maintain

We ensure that the data-segregation mechanisms are properly implemented and tested to prevent unauthorised access or data leaks by:

- Covering the data access layer and all API endpoints with extensive unit tests
- Running bi-weekly quality assurance tests
- Running annual independent security tests

8. Access rights for TinQwise Staff

Access rights of TinQwise Staff to system data is covered by our Access Control Policy. Per above TinQwise Administrators only have access to those instances specifically needed for the completion of their duties, for the time needed for said completion. The access rights of all TinQwise Staff to the SAAS Application and other systems supporting the SAAS Application is revoked and removed upon termination of their employment, contract or agreement or adjusted upon change in role (description).

9. Data retention

When a User is deleted, all Personal Data as defined in TinQwise Data Processing Terms that can identify a User is removed. Learning progress of the deleted user is saved for customer reporting purposes, but this progress data is anonymized.

Following TinQwise standard Data Privacy Policy, when the project or Client contract ends, the applicable Client instance is permanently removed and all Personal Data and learning progress data is permanently and irrevocably deleted.

tinQwise

10. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Procedures for data segregation and retention	SharePoint and / or GitLab	C.O.O.	Only TinQwise Staff can access these files	2 years