# Compliance built-in

## Activity and data logging (optional)

Activity and Data Logging includes the automatic creation of a series of log files. Logging can be set up for each entity in an application providing insight and transparency in relation to: user activity, creation, changes and status of different records in an application.

- **Access Log**: Can be activated on an entity in an application. This automatically generates a log of which users have accessed and/or edited a given record.
- **Status Log**: Can be activated for an entity in an application. This automatically generates a log of the history of the created records, which shows how long a record has been in each status
- **Change Log**: Can be activated for an entity in an application. This automatically generates a log of what changes have been made to the individual records. Including who has changed what and when (timestamp).

**How to:** Each option is activated on the entity Advanced page.

**Pro tip:** Especially the status log can be used for setting up performance charts on dashboards, as it can give detailed information of how much time was spent in each step.

## Versioning (optional)

By default file versioning is supported on the "Documents" and "Files" field types. In addition, data revisions can be supported on each entity. This automatically builds an audit log for each record.

In addition data revisions can be supported on each individual entity.

**How to:** Data revisions is activated on the entity Advanced page.

## GDPR Deletion Policies (optional)

For each entity in a TS Application, a GDPR Deletion Policy can be set up, enabling automatic deletion or anonymization in accordance with the specified rules. The application will thus automatically delete or anonymize data and files in the application, cf. specified criteria.

**How to:**

1. Set up an action on a entity status
2. Check of deletion policy
3. Choose between anonymization or deletion
4. Optionally select log data to also be deleted

In case you choose "anonymization" you should define how each field should be handled

1. Click on a field
2. Click on Assignment
3. Check of anonymization
4. Optionally set value after change

# Event and System Logging (recommended)

When Event and System Logging are turned on for an application, the following events are logged automatically:

- User logins
  - Successful normal user logins are hidden
  - Also contains client IP (used for MFA)
- System events
  - User errors
  - Scheduled services
  - Administrator logins

Error events will include stacktraces if available.

The eventlog can be cleaned automatically on a regular schedule.

---

Revision #2
Created 3 April 2025 13:21:54 by Theis Villumsen
Updated 13 October 2025 13:01:44 by Max Gøtske