iDNA Applications

User Name Pseudonymization

Edition: iDNA Applications · For works councils and data-protection officers

Version: 1.0 · describes iDNA Applications 3.5.0, verified 26 October 2026

1. Introduction

iDNA Applications analyses an organisation's Notes/Domino applications and how they are used, per user, department or location. This note explains the mechanisms iDNA uses to pseudonymize user names and which data is shown with real names on purpose. Pseudonymization is the default. panagenda has worked successfully with works councils this way for many years.

All collected data is stored with real names in the iDNA appliance inside the organisation's network. panagenda has no standing access to it. Access for support or consulting is granted by the organisation under existing agreements. Pseudonymization is applied when iDNA prepares the data for the analyses.

2. What is pseudonymized by default

User names are pseudonymized in the per-user usage analyses: who used which application and when, per-user summaries, the licence analysis and the editor statistics of the content analysis. iDNA replaces each name with a pseudonym derived from it. A person keeps the same pseudonym in every analysis run, so trends over time still work. This also means that a pseudonym can be followed over time without knowing the name. Removing names therefore does not prevent analysis at the level of individuals. The organisation part of the Notes name stays readable.

iDNA has no function that turns a pseudonym back into a name. It is pseudonymization, not anonymization. Anyone who holds the list of names and the method can rebuild the mapping.

Real names appear in these analyses only after the organisation has confirmed in writing that it has taken the necessary internal steps, including with the works council, and is responsible for the processing. Only then does panagenda change the licence. Under a trial licence the usage analysis is always pseudonymized.

3. Departments and locations

Most questions can be answered without names: Which departments and locations use an application? Is it still in use? Who are its stakeholders? How does its usage develop? This is why iDNA also aggregates usage by department and location, and why the content analysis lists document editors by department and location.

While pseudonymization is on, a unit is shown only as a placeholder if fewer user names are assigned to it, including its sub-units, than the threshold requires. The threshold is 15 unless the licence sets another value. The placeholder shows the count and an identifier, for example `*** Pseudonymized: Department too small (12 Users) [ID: 310] ***`. The count is of assigned names, not of people active in an application or period. The row and its usage figures stay, so totals still add up. Each unit is judged on its own count: a small team inside a large department is masked, the department is not.

> A masked row is real usage by a unit too small to be named. It is not missing data.

The threshold hides only the unit's name. People or units may still be identifiable from other information. When pseudonymization is switched off after this confirmation, small units are named like any other. The

threshold is set per installation in the licence. panagenda recommends agreeing it with the works council and the data-protection officer, together with the permitted level of detail, the recipients of reports and the handling of copies.

4. What is shown with names, and why

Some data is shown with real names on purpose. Access-control entries, agent signers and group memberships describe permissions and responsibilities. There is one entry per name, with no record of when or how often a person worked. They identify people, but they are not a record of application use and are not intended for assessing anyone's work.

For each profile document, Notes also stores who changed it and when. iDNA takes these details over as they are. Entries made in iDNA itself, such as owner fields and custom properties, carry the iDNA user's name and their change history.

Also shown with names is who last accessed each application and who last wrote to it. This is recent-use information: one entry per application, without count or history, and not pseudonymized whatever the setting. Across many applications, these entries do show who was last seen where. Person documents from the Domino directory and MarvelClient data are not pseudonymized either.

5. Access, retention and AI

Dashboards, Portal, DataMiner, exports and the AI components work with the prepared data, each with its own access control. The organisation decides who may log in to the Portal and with which role. Per-user views in the Portal show pseudonyms while pseudonymization is on. The Portal's per-database user list uses its own display pseudonym, which differs per application and access date. iDNA deletes raw data after a configurable period and keeps the processed figures. Reports can be exported (see "Data Retention and Cleanup Options" in the product documentation).

AI access is enabled separately in the licence. What an AI assistant retrieves is processed by the organisation's AI platform under the organisation's contract. What the AI components, such as the iDNA Applications Companion, may read under which settings is described in panagenda's AI position paper, available from panagenda.

6. Changing the setting

The setting changes with a new licence, in either direction. Switching it off requires the written confirmation first. The change takes effect in the person directory as soon as the licence is processed, in the usage analyses after the next nightly run, and in the editor statistics once an application's content is collected again. Reports exported earlier are not changed.

> **Applies to:** this note describes the version on its cover, after the nightly run has reprocessed the data. Earlier versions differ in three points. The raw person list shows names not matched to a current user in clear. The person list and the usage analysis use different pseudonyms for the same person. One per-user summary stays pseudonymized even when pseudonymization is disabled.