panagenda iDNA Applications Privacy Policy

This article explains how panagenda iDNA Applications stores, uses and discloses the information it collects.

Data Collection

iDNA Applications collects all its information from local Domino servers.

Data Storage

All collected data is stored and processed within the iDNA Applications virtual appliance - **there is no external data processing!**

By default, all personal data is obfuscated, and therefore compliant with the EU's General Data Protection Regulation (GDPR). Obfuscation can only be disabled by applying a new license.

> Please visit the panagenda Help Center support.panagenda.com if you would like to request a license with a setting that is different from the one in your existing license.

All passwords stored for iDNA Applications are either hashed or encrypted.

Usage Data

panagenda iDNA Applications does not collect any usage data and does not automatically send logs, configurations, statistics, benchmark data, or similar to its data centers.

Data Access

iDNA Applications is delivered as a virtual software appliance that supports VMWare ESX and Microsoft Hyper V. The customer installs iDNA Applications on-premises - thus the customer owns and controls the level of security such as where the virtual appliance is installed, as well as, who has which level of access to it.

iDNA Applications offers two different user roles:

- **Admin** with full access to configuration and data
- **Viewer** with limited access to data and no access to configuration