Visma Draftit

Information security -

Visma Draftit AB

Last updated 02/03/2023

Content

1. Our information security

Draftit's goal is to maintain a high a level of data privacy as demanded by our customers and to meet current GDPR requirements. With our geographical location of data storage, information security is subject to Swedish legislation.

2. Subcontractors

Draftit uses subcontractors for parts of our IT operations and for some development. We have signed data processing agreements and confidentiality agreements with them.

3. Operational setup

Our environment consists of two parts. One traditional with servers in data centres. And one cloud based. The cloud part is located inside EU/EES.

Login for end users in all our products is handled in a cloud service, but no user information is stored there except username and IP address in log files that are continuously cleared after three months.

See 3.1 and 3.2 for information on storage of user data.

Products where all parts exist in a cloud environment are Whistleblow Incident and our Expert products, where code is executed and data stored in the cloud.

The cloud setup is redundant with replication over multiple regions inside EU/EES. We also have backup routines as an extra safety measure, also within EU/EES.

For all other products see 3.1 and 3.2 below.

3.1. Data centres

The data centres we use are located in Sweden.

The data centre setup follows modern standards for physical access control, fire protection, USP's, monitoring, firewalls, antivirus, patching etc.

Our operations partner is certified for ISO 9001, 14001 and 27001.

The environment has a redundant setup and is isolated from other customers environments. We have our own dedicated servers and network segments.

The data centres are compliant with Swedish security specifications SSF 130:6, intrusion alarm class 2, SSF 200:3 class 2 for physical intrusion protection, class 3 or higher as stated in SS3522. Fire alarms are as in Svenska Brandskyddsföreningen's recommendations (SBF 110:6)

3.2. Backup

A full backup of our databases is performed every 24 hours. We also do a transaction log backup every hour. Full backups are saved for ten days. On top of that, the first backup every month is saved for two months.

Restores, if needed, should be initiated within an hour according to our SLA.

Backups are made to a geographically separated data centre, but still in Sweden.

Our backups are done on a system level, they cannot be used to roll back changes made by an individual customer or user.

4. Operations

We have an uptime guaranteed from our partner to be 99.9.
Uptime for our end users is approximately 98,5%. Updates and maintenance are made during evenings or weekends.
Draftit and our operations partner are working together to continuously improve stability, monitoring etc to avoid problems and incidents

5. Information security

5.1. General

Communication client/server through https/TLS.
Encryption of passwords and other sensitive data in our databases through modern industry standard algorithms.
Role based access to our applications and their functions.
Increased password complexity for roles with higher permissions.
Logging of customer data changes.
MFA/2Fa possibilities.
Penetration tests done on a regular basis.
Internal routines and education to prevent social engineering and other similar attack types.

We follow the recommendations from OWASP for our code and development work: (https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project).

Permission to our systems for Draftit employees is given based on the actual needs for everybody's role in the organization. The ones given a higher level of access are typically technicians responsible for operations and development, content editors and the ones working with customer support.
All Draftit personnel have a non-disclosure agreement built in to the employee contract we use. This is also included in the agreements we sign with any subcontractor.

5.2. Log on and passwords

Accounts are locked after repeated log on attempts with wrong password.
If a customer so wishes, we can set up dedicated password rules for them including number of digits, number of non-alphanumeric characters, minimum length and if MFA should be mandatory.
All users with a personal account can activate MFA in their personal profile settings.
MFA needs an app installed on the user's mobile phone.

5.3. User accounts

When a new account is created, we will send out an email to the user with a link they must use to set their password. We also have password reset functionality through email showing a link to the reset page.
Both these types of links are valid for a limited amount of time.

6. Support

Draftit has two levels of support:
Support Level 1 is staffed by our support specialists in CS (Customer Success), who will identify the incident, open an incident case and initiate action and handle incidents that require more in-depth expertise.
Support Level 2 is staffed by our developers. Support Level 2 is the final stage for escalation and for action in case of an incident.
The process flow for incident management follows the ITIL model for IT Service Management:

1. A user calls or sends an email message to CS to report an incident.
2. An issue is registered.
3. CS confirms by email to the user/contact person that the incident has been registered.

4. Diagnosis of the incident is conducted, troubleshooting or escalation occurs.
5. If the support engineer who has received the case can solve it, she will assign the case to herself, solve it and then notify and verify the functionality with the user.
6. If the support engineer cannot solve the case, the case will be escalated to support level 2.

Draftit also conducts daily measure of the following parameters:

- Response time
- Call recording
- Action time
- Number of calls per month
- Average call duration
- Level of support and technical expertise