Visma Sign Information Security Statement

Visma Sign is a cloud based digital signature software, which is provided as Software as a Service (SaaS) by Visma Solutions Oy. Visma Solutions Oy is responsible for delivering the service to the customers.

In this document, we have described how Visma Sign -service is being delivered to our customers and we also pinpoint the main aspects from information security viewpoint.

Visma Sign service delivery

Visma Sign -service is hosted by two different service providers, UpCloud Oy and Google Cloud Platform. Both service providers are dedicated to providing continuity services for mission critical systems.

Google Cloud Platform data center which is used in Visma Sign is located in Hamina, Finland. Visma Sign uses Google Cloud Platform for storing encrypted documents and hosting a small part of our functionality there, related to handling uploaded documents.

UpCloud data center which is used in Visma Sign is located in Helsinki, Finland. We are hosting most of our functionality in UpCloud.

Communication between our two data centers (UpCloud & Google Cloud Platform) is always encrypted and VPN is also used as an added layer of security when uploaded documents are being handled.

Our service availability track record from previous years has been approximately over 99,99%, which means that we have under one hour of unexpected downtime in extended business hours (07.00 - 20.00) during one calendar year. We don’t offer any separate SLA for our service to our customers.

Visma Sign -service is updated frequently and these updates are performed without service breaks. In certain occasions (eg. updates to our platform infrastructure), we need to have a planned service break. These are performed outside extended business hours and all planned service breaks are informed in advance to our customers.

Visma Sign -service is monitored by our Service Delivery Team and they work closely with the whole product team to provide our customers information regarding possible incidents in our service.

Authentication mechanisms and user identity

Visma Sign user accounts are always personal and cannot be shared. Visma Sign -service uses strong 2FA authentication to identify users. Available authentication mechanisms:

- For Finnish customers is Open ID login which supports all Finnish Banks and also strong mobile authentication mechanism from Finnish mobile operators (https://mobiilivarmenne.fi/).
- For Norwegian and Danish customers the available authentication mechanism is Open ID login with Bank ID.
- For Swedish customers the available authentication mechanism is SAML login with Bank ID.

For the first login customer has to register themselves using available authentications methods above. During registration the customer will give an email address and password which can be used in following logins to Visma Sign.

When customers authenticate themselves, we will store their social security number using a one-way hashing algorithm in our database. Visma Sign has to store social security numbers for service to operate correctly in following cases:

- Customer registers herself again, so we can check if the customer already has an account and not to create a new one.
- When a customer signs a document using strong 2FA authentication, we have information who the customer is and save the signed document to their private archive.

Security and risk management

Visma Sign handles security in several levels including:

- Transport level security in encrypted connections to the service
- Infrastructure security is enforced with common good practices:
    - Network level security: reverse proxy, firewall, VPN used when communicating with different services between UpCloud and Google Cloud Platform
    - OS and middleware level security: operating system and software patches, all uploaded documents are scanned for viruses
    - Application level: mitigation against web application security threats, internal web application security auditing

In overall, Visma Sign works actively to identify and eliminate relevant risks. Unavoidable risks are controlled so that the total risk level is kept on an acceptable level, while ensuring that the information systems and work procedures remain efficient.

Visma Group has a security framework, which all Visma product lines are required to follow. This framework includes eg. multiple levels of security testing (including dynamic and static application security tests, penetration tests and automated vulnerability scans), mandatory training provided to all personnel and an open culture of sharing experiences both internally and externally by Visma employees regarding security issues. More information regarding the Visma-level security approach is at https://www.visma.com/trust-centre/.

Connections to external services

Visma Sign is connected to multiple third party services to provide our customers secure and useful functionality. Some of the connections are built-in to Visma Sign and these connections are monitored for exceptions by the Visma Sign Service Delivery Team. These connections include connections to a payment provider, HSM service and authentication providers. All of these connections use secure protocols for data traffic.

Visma Sign -service also has a REST API, which our customers can use to implement connections to third party services. All API calls are done over encrypted connections and API authentication is implemented on organization level access checks.

Backups and error recovery

Customer data is backed up every hour and transferred to Google Cloud Platform for storing purposes. Backups are stored in multiple different physical locations, other than actual production servers. In the very unlikely event of a major incident, where the current state of database data would be destroyed, maximum data loss would be one hour.

For a fee Visma Sign can offer data recovery services for customers in cases where there has been accidental changes to the data by the customer's own user or user of a third party partner. In these matters, please contact our Customer Support (tuki.sign@visma.com).

Privacy

Visma Solutions Oy provides Visma Sign service to our customers as a cloud service, which means that customers of Visma Sign are the data controllers of the data they input to the system and Visma Solutions is the data processor for this data. We utilize subcontractors to run Visma Sign service. Some of these sub-processors are used for providing us the needed data center services and some are for example helping us monitor our system. All of the subcontractors we use are carefully selected and we have done thorough checks to make sure they are able to provide the level of quality that our customers deserve.

Visma Group has strict policies regarding the agreements with the subcontractors so we can be sure that all of them meet the legal and regulatory requirements. When using subcontractors, we will always enter into a data processing agreement (DPA) in order to safeguard our customers' privacy rights and to fulfil our obligations towards our Customers. Some of the sub-processors are used only to handle technical data, meaning that they don't handle our customers' personal information at all. All of the sub-processors that handle personal data, are located within the EU/EEA area. Full list of our sub-processors can always be found from https://privacy.vismasolutions.com/.

We also handle some personal information as a data controller (for customer service, billing, sales etc.) and we also use subcontractors (eg. Zendesk) for this. Therefore some personal data may be exported outside the EU/EEA area. Just like when we are the data processor, always when we use subcontractors as a data controller, we will always enter into a data processing agreement (DPA) in order to safeguard our customers' privacy rights and to fulfil our obligations towards our Customers.

If the subcontractor is in the US, we make sure that they are certified to the EU/US Privacy Shield framework or we will have a Data Processing Agreement based on the EU Standard Contractual Clauses with this subcontractor. We follow European data protection and privacy regulations and directives and Finnish law.

More information

More information about Visma Solutions and Visma-level standards regarding security and privacy can be found from https://privacy.vismasolutions.com/ , https://www.visma.com/trust-centre/ and https://www.visma.com/privacy-statement/.

If you have any questions or concerns or you need detailed information regarding our security measures, please contact our Customer Support. Contact details are listed in our Community at https://community.vismasolutions.com/.