Visma Severa Information Security Statement

Visma **Severa**

Visma Severa is a modern and visual professional services automation tool that brings together CRM, work hour entries, projects and invoicing. It is provided as Software as a Service (SaaS). Visma Severa-service is provided by Visma Solutions Oy and it's responsible for delivering the service to the customers. In this document, we have described how Visma Severa service is being delivered to our customers and we also pinpoint the main aspects from information security viewpoint.

Visma Severa service delivery

Visma Severa service is hosted in Microsoft Azure. Data centers are located in the North Europe region (Ireland). Microsoft Azure is a GDPR compliant cloud hosting provider with certifications such as ISO 27001 and ISO 9001.
More information can be found from:
https://azure.microsoft.com/en-gb/overview/trusted-cloud/compliance/

We do not offer any separate SLA for our service to our customers. Visma Severa service is updated frequently and these updates are performed without service breaks. On certain occasions we need to have a planned service break. These are performed outside business hours and all planned service breaks are informed in advance to our customers via https://status.visma.com/. Our service availability track record from the previous years has been approximately 99,99%.

Visma Severa service is monitored by our Service Delivery Team during business hours and by Visma's Central Operations team during other times. Service Delivery team works closely together with Customer Service to provide our customers information regarding possible incidents in our service. In case of an incident, we provide frequently updated information to our customers via https://status.visma.com/.

Authentication mechanisms and user identity

Visma Severa user accounts are always personal and should not be shared. Visma Severa user account is actually managed by Visma Connect, which means that you can log in to multiple Visma services with the same username and password. Our mobile apps also use the same credentials. Users can enable 2FA authentication from their personal settings and they also have the possibility to authenticate with their Google or Microsoft credentials.

Security and risk management

Data protection in Visma Severa

- **Encryption at rest:** protects customer data from a system compromise or data breach by encrypting data while it's stored to the database. All Visma Severa customer data is protected with AES-256 bit encryption.
- **Encryption in transit:** protects customer data when data moves between your computer, mobile phone or other devices and Visma Severa. This protection is achieved by encrypting the data before transmission; authenticating the endpoints; and decrypting and verifying the data on arrival. All data transferred from and to Visma Severa support and requires usage of the latest TLS 1.2 encryption whenever possible(*).

(*) SOAP API service supports TLS 1.0/1.1 for compatibility reasons.

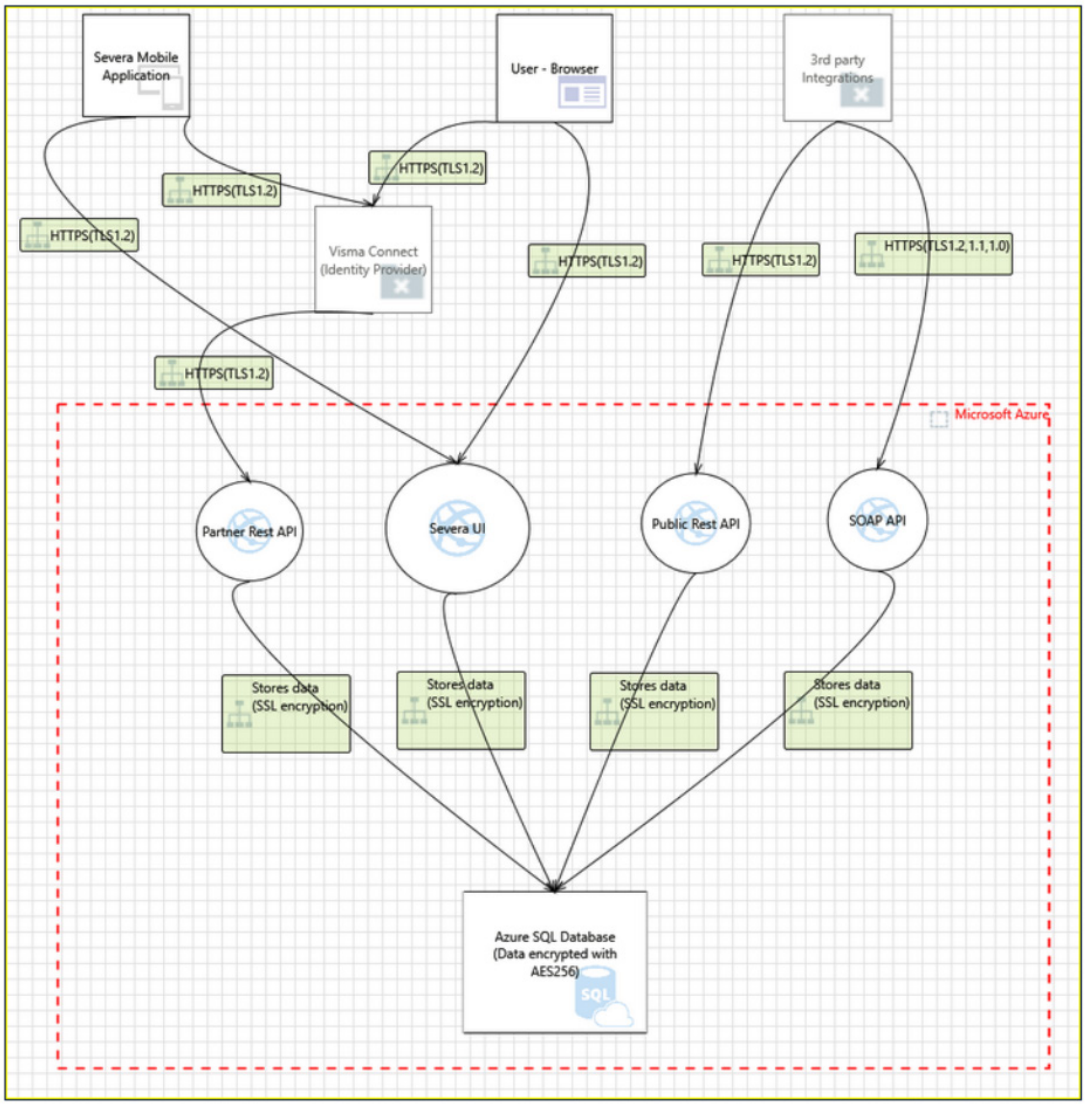

Diagram: Severa Data Protection

Platform security

Visma Severa is hosted in Microsoft Azure which comply with key industry standards, such as ISO/IEC 27001:2013 and NIST SP 800-53, for security and reliability. Visma Severa uses security services such as threat detection and security center provided by Microsoft Azure which monitor our services 24/7

Infrastructure security

All of our services are hosted as PaaS (Platform as a Service) or IaaS (Infrastructure as a Service). Benefit of this hosting model is that our cloud provider Microsoft Azure always provides the latest security patches and technologies to all infrastructure we use.

Risk assessments are done yearly through security standard ISO 27001 which we enforce in our processes.

Application security

Visma Severa code base is continuously scanned with leading SAST (Static Application Security Test) and ATVS (Automated Third-party Vulnerability Service) tools. Any issues discovered by the tools are fixed immediately.

Visma has a Responsible Disclosure Policy which states transparent rules for submitting vulnerabilities to our team with a responsible disclosure policy.
Please find more information from: https://www.visma.com/trust-centre/smb/security-and-privacy/operational/responsible-disclosure

Visma has a separate security team, which offers a lot of training and support for development teams and also performs annual manual application vulnerability assessments for Visma Severa. This service is designed to identify application level weaknesses and vulnerabilities, most of which are covered in OWASP Top 10.

Connections to external services

Visma Severa-service has a SOAP and 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 multiple levels including user and company access checks.

Backups and error recovery

Customer data is backed up into secure geo-redundant service that ensures that data is backed up and available even if the Azure data center is unavailable. Backups are taken nightly and stored for the past 30 days.

Visma Severa has a multitenant databases which means that restoring a full backup is not really an option if data corruption occurs only for one customer in a shared database. Instead, we compare the original data in the backup to the corrupted production data and fix manually only the corrupted data. This way customers do not lose all the work they did during the previous day. Separate databases can be offered to large organizations with the possibility for full backup restore.

Privacy

All data, which we handle as a data processor, stays always within the EU/EEA area.

We also handle some personal information as a data controller (for monitoring, errors, logging etc.) and we use subcontractors (eg. AppDynamics, Raygun) for this. Therefore some personal data may be exported outside the EU/EEA area. 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.

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. We are GDPR compliant.

More information

More information about Visma-level standards regarding security and privacy can be found from 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/.