Nmbrs Technology

F.A.Q.

Frequently asked questions about technology information security, availability and development of the system Nmbrs.

MAY 2022

Overview

Nmbrs Technology F.A.Q.

Product & Legal entities covered

This white paper describes the development, maintenance and all other relevant (internal) processes / activities undertaken by Visma Nmbrs and it's associated legal entities, related to providing the product / platform Nmbrs. For the remainder of this paper, Visma Nmbrs and associated legal entities will be referred to as Visma Nmbrs and the product / platform provided, will be referred to as Nmbrs.

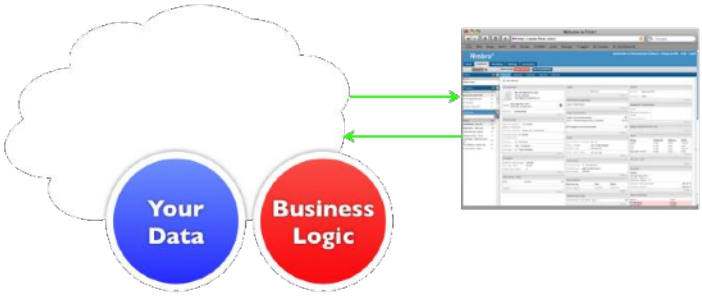
To date, Visma Nmbrs and associated legal entities are comprised out of:

- Visma Nmbrs
- Visma Nmbrs Sweden
- Nmbrs Unip.LDA

Platform & Technology

How is Nmbrs's architecture?

Nmbrs is a SaaS (Software as a Service) / Cloud application, meaning that the entire application runs online without requiring any kind of local or client-side installation. Both your data and the calculations logic are deployed on our cloud infrastructure. You can access the application on any computer with a web-browser.



Architecturally, Nmbrs is composed of a monolithic component and several **micro services**, but for the end-users, only one URL is visible. The micro services run on the Nmbrs-Fabric, which is the layer responsible for security access, logging, communication between services. Technically, the application is divided into several layers with specific responsibilities. The following layers are present in Nmbrs:

- **Presentation Layer:** Manages user interaction, input and display output
- **Service Layer:** Works as the entry point for a stateless application server. Defines the façade of the application and it is where security is implemented.
- **Business Logic Layer:** Contains the classes where application logic is coded.
- **Data Access Layer:** Manages database interaction and works as an abstraction for SQL Server or any other persistence framework

Next to this layering separation, there are following runtime components:

- **Web application:** Web-based user interface.
- **Worker service:** Component where the calculations take place like payroll calculations, report generation, etc.
- **Schedule service:** Background service that handles schedule tasks like signals and workflow execution

On what platforms and technologies is Nmbrs developed?

Nmbrs is mostly developed on Microsoft technologies:

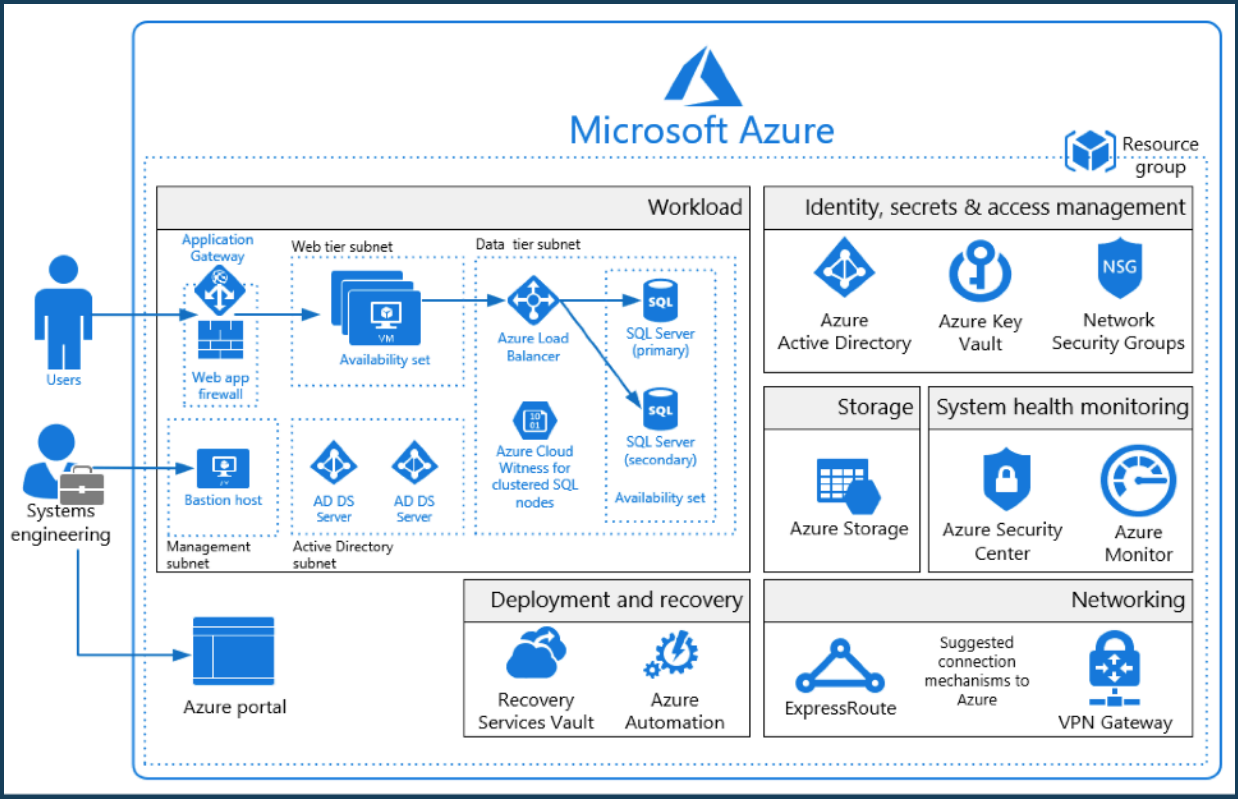
- Back-end: Nmbrs is a .NET application developed in C#. Some micro services are developed in .NET , Core and Python (for Machine Learning)
- Front-end: The presentation layer is mainly built on ASP.NET, JavaScript and HTML5
- Database: For persistent storage, Nmbrs uses Microsoft SQL Server engine.

Hosting & Infrastructure

In what environment is the application deployed (hosting partner)?

Microsoft Azure Cloud

Nmbrs is hosted by Microsoft Azure Cloud, which is composed of a globally distributed datacenter infrastructure, supporting thousands of online services and spanning more than 100 highly secure facilities worldwide.



Infrastructure and Physical Security

Microsoft Azure runs in datacenters managed and operated by Microsoft. These geographically dispersed datacenters comply with key industry standards, such as ISO/IEC 27001:2013 and NIST SP 800-53, for security and reliability. The datacenters are managed, monitored, and administered by Microsoft operations staff. The operations staff has years of experience in delivering the world's largest online services with 24 x 7 continuity.

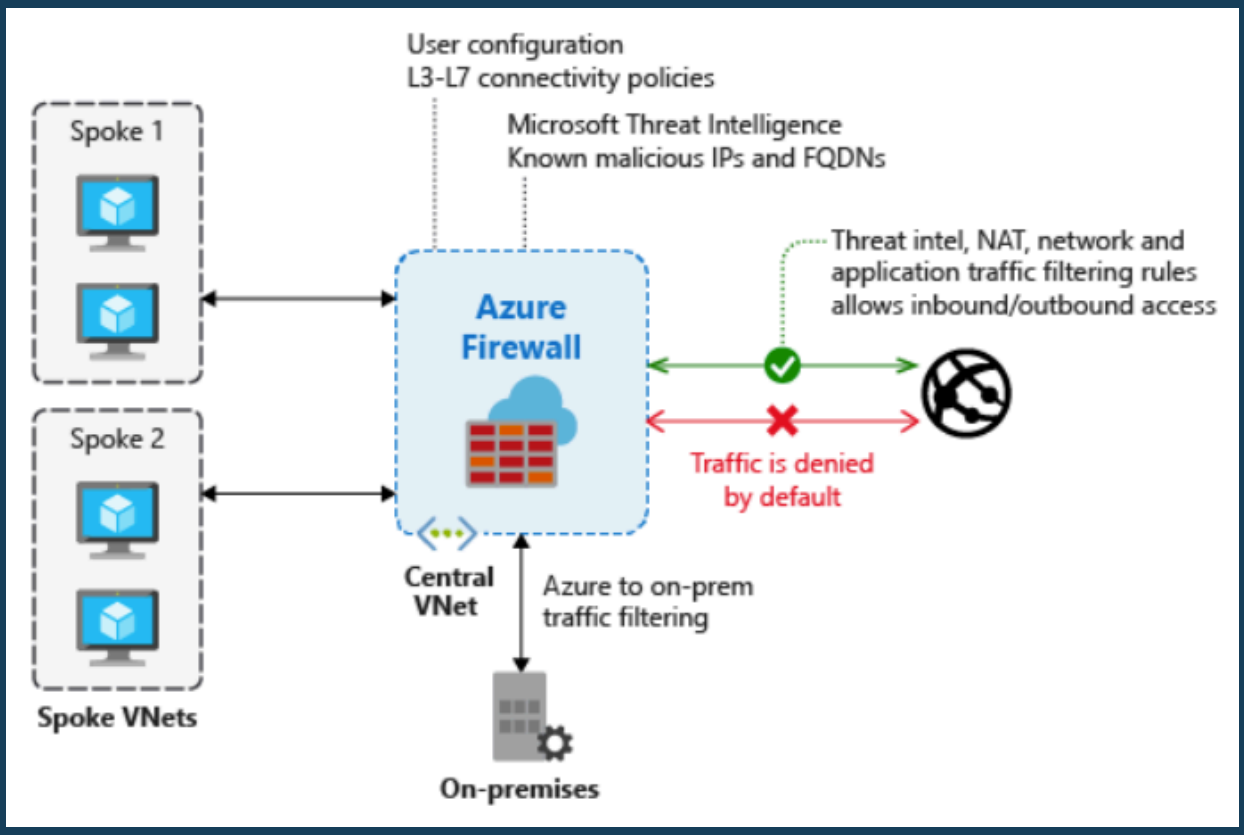
Microsoft designs, builds, and operates datacenters in a way that strictly controls physical access to the areas where your data is stored. Microsoft understands the importance of protecting your data and is committed to helping secure the datacenters that contain your data. Microsoft has an entire division devoted to designing, building, and operating the physical facilities supporting Azure. This team is invested in maintaining state-of-the-art physical security.

Data location

Visma Nmbrs uses the Microsoft Azure platform for the hosting of the Nmbrs platform. All customer data in the Nmbrs platform is stored in the Microsoft Azure region West-Europe. This region is automatically paired with the Microsoft Azure region North-Europe for Business Continuity and Data Backup purposes. The datacenters in use by Microsoft for region West-Europe are located in the Netherlands (Amsterdam) and for the region North-Europe they are located in Ireland (Dublin).

DDoS Protection and Firewall Data location

Nmbrs uses the Azure DDoS Protection and Firewall services. Backed by the Microsoft global network, DDoS Protection brings massive DDoS mitigation capacity to every Azure region. The Azure DDoS Protection scrubs traffic at the Azure network edge before it can impact the availability of your service. Always-on traffic monitoring provides near real-time detection of a DDoS attack, with no intervention required. DDoS Protection automatically mitigates the attack as soon as it's detected. Deployed with the Azure Application Gateway Web Application Firewall, DDoS Protection defends against a comprehensive set of network layer (layer 3/4) attacks, and protects web apps from common application layer (layer 7) attacks, such as SQL injection, cross-site scripting attacks, and session hijacks. The Web Application Firewall comes preconfigured to handle threats identified by the Open Web Application Security Project top 10 common vulnerabilities. The Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources. It's a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability.



Application Requirements

Are there minimum requirements for a user to run Nmbrs?

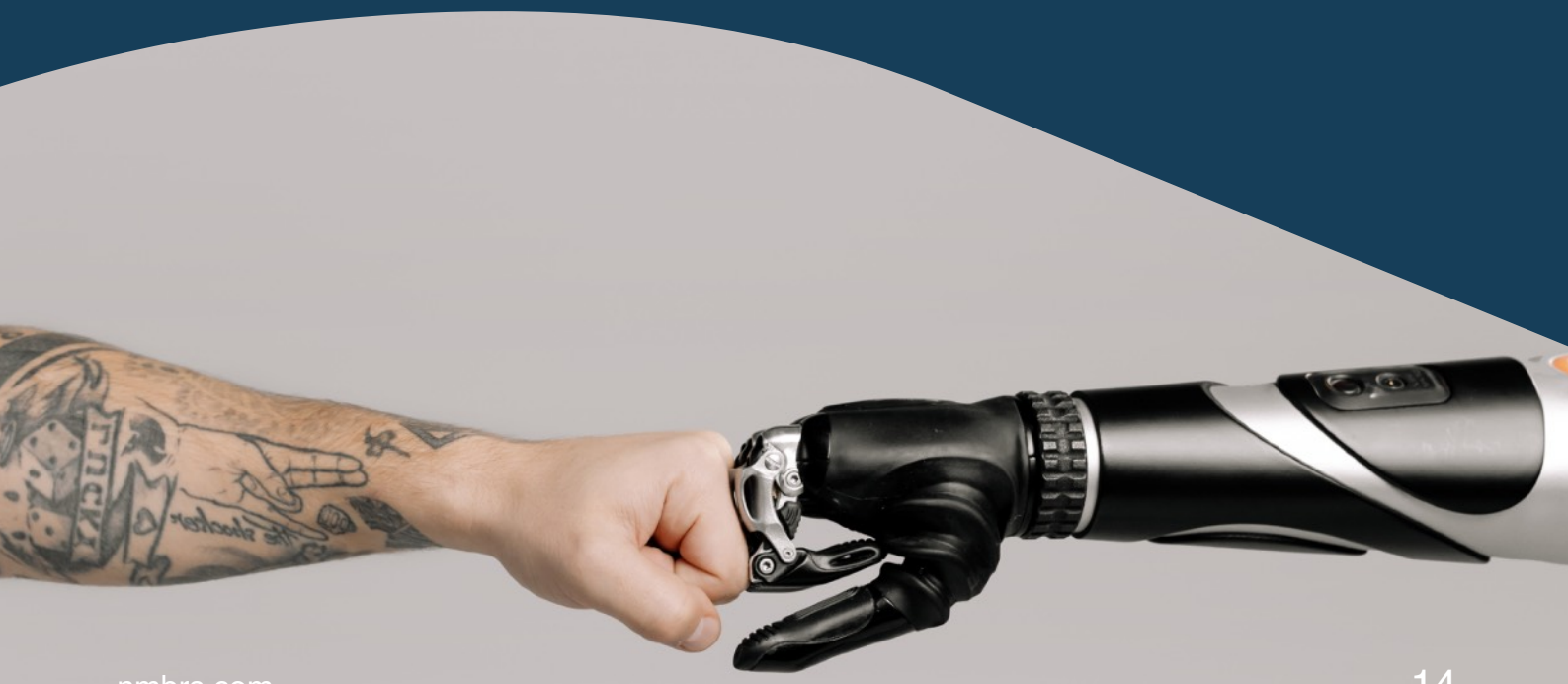
Nmbrs is a Web-based SaaS (software as a service) application; therefore there are no specific operating system requirements since it runs on a Web browser. We do however support and recommend using the following Web browsers.

Minimum requirements:

- Web-browser (Mozilla Firefox, Google Chrome, Safari, Microsoft Edge)
- Internet connection (Cable/ADSL recommended)
- Email account (For user access and management)
- Screen size 1280x800px (Standard 15,6” screen)

💡 ***We recommend the latest versions of these browsers because of possible safety issues***

Development Process

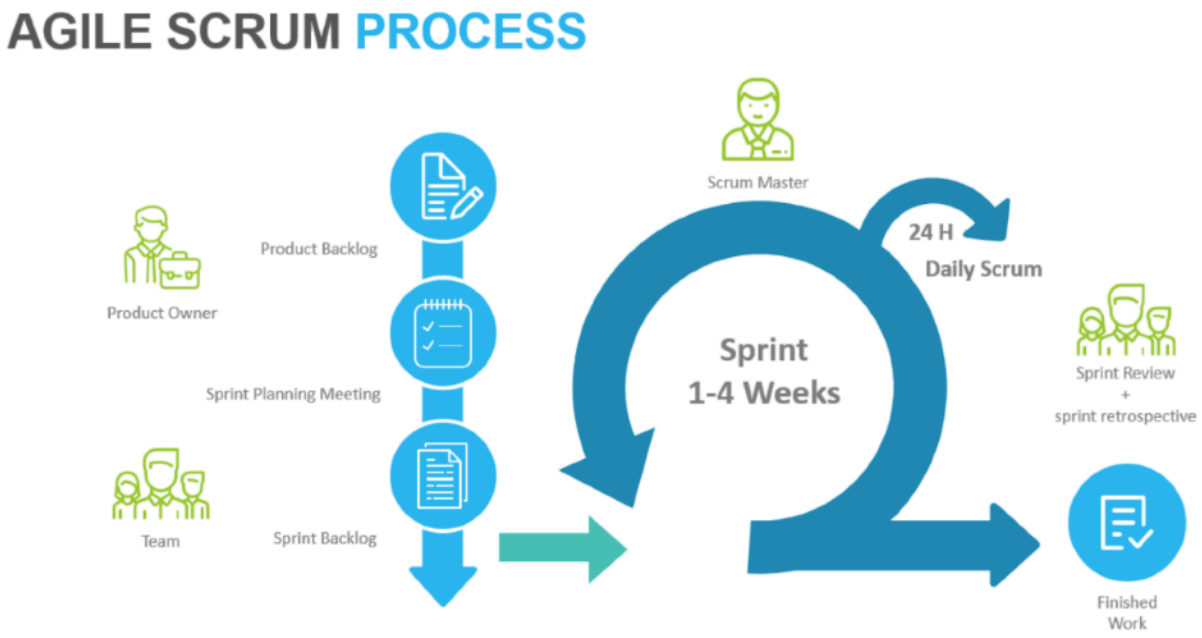


How is Nmbrs's development process?

Development process

The process is based on the Agile / Scrum methodology, these are the main features:

- The development process is iterative and defined by weekly sprints that are composed by several tasks.
- The backlog and product backlog tasks are defined in the Jira system as tickets.
- There are weekly meeting to discuss the work for the week and have an overview on what was done on the previous week



How is Nmbrs's development process?

Testing, QA and Deployments

There are separate development, testing and production environments. Each environment has a different access policy. Before each update, automated regression tests are performed from the delivery pipeline of a test environment. Manual exploratory testing is also performed to ensure proper coverage and high-quality before each update. After update, the QA team verifies that all main processes and features work properly. The application updates are performed by a team of developers, QA engineers and support consultants to ensure updates are properly performed and communicated. The deployment process is automated and performed from the build server and requires no manual intervention.

Application Updates

To ensure optimal performance of the service Nmbrs, periodically maintenance is done, and updates take place. In most cases, maintenance will have limited or no negative impact on the availability and functionality of the service Nmbrs.

If Visma Nmbrs expects planned maintenance to negatively affect the availability or functionality of the service Nmbrs; we will use commercially reasonable efforts to provide at least seven days advance notice of the Maintenance. In addition, Visma Nmbrs may perform emergency unscheduled maintenance at any time. If Visma Nmbrs expects such emergency unscheduled maintenance to negatively affect the availability or functionality of the Service Nmbrs, we will use commercially reasonable efforts to provide advance notice of such maintenance. Maintenance notices noted above will be provided via the Apps Status Dashboard, Admin Console and/or Support Portal. In addition, Customers who subscribe may also be able to receive email and/or RSS Feed notifications of Maintenance.

See more information on the support portal: **support.nmbrs.com** and status.nmbrs.com

Security & Access

How is Nmbrs protected against phishing and other online threats?

Automatic vulnerability scanner

Nmbrs uses the McAfee Web Security Service with accurate vulnerability scanning and reporting technology, which identifies the presence of security vulnerabilities, including dangerous web application risks, and provides the information you need to prioritize and rapidly address risks across business units and IT groups.

Daily security audits are performed in three phases: Port Scanning, Network Services Testing, and Web Applications Vulnerability Testing.

Port Discovery Scan: Phase one is a thorough port scan of the target. Accurately determining which ports on an IP address are open is the crucial first step to a comprehensive security audit.

Network Services Scan: After determining which ports are alive we begin a network services test on each port. During this phase we thoroughly interrogate the service to determine exactly what software is running and how it is configured. This information is leveraged in order to launch additional service specific and generic tests.

Web application Scan: Web application testing is the third phase of our daily security audit. According to industry sources, such as Gartner Group, an estimated 60-75% of all security breaches today are due to vulnerabilities within the web application layer. Traditional security mechanisms such as firewalls are not always sufficient against attacks on your web applications. All HTTP services and virtual domains are tested for the existence of potentially dangerous modules, configurations settings, CGIs and other scripts. The website then is “crawled” to find forms. Forms are exercised in specific ways to disclose all application-level vulnerabilities such as, code revelation, cross-site scripting and SQL injection. Both generic and software specific tests are performed in order to uncover misconfigurations and coding error vulnerabilities.

Pentesting

Visma Nmbrs performs regular penetration testing (pentest) on its infrastructure and the application / service Nmbrs. This is done by a team of external ethical hackers and security experts with a mix of automation and manual testing and by following the OWASP Top 10 web application security standard. Findings are shared with the Visma Nmbrs technical team and solved together with the external experts. The OWASP Top 10 list consists of the 10 most seen application vulnerabilities:

1. Injection
2. Broken Authentication
3. Sensitive data exposure
4. XML External Entities (XXE)
5. Broken Access control
6. Security misconfigurations
7. Cross Site Scripting (XSS)
8. Insecure Deserialization
9. Using Components with known vulnerabilities
10. Insufficient logging and monitoring

Are incidents (Denial of Service attacks or intrusions, information theft or attempts) reported to customers?

Security incident / data breach management

In case of a security incident and or data breach, a standard protocol is followed in order to manage the incident. This protocol ensures proper:

- investigation of the scope and severity,
- timely mitigation / limitation of impact,
- timely communication to all affected parties,
- root cause analysis and (structural) incident resolution.

After the incident has been managed, a full report with incident details including: timeline, root cause, (possible) data exposed; (possible) affected parties; mitigation and preventive measures implemented, will be sent to the account owner(s) affected by the incident. This process is fully described and (annually) audited in the scope of the ISAE 3402 Type II audit.

In what ways is the access to the application secured?

Communication Channel

The browser and API client/Server communication is done with **HTTPS** which guaranties data integrity and prevents data tampering. The SSL certificate used is verified by Trust Provider B.V and the data is 2048 bits encrypted.

Data Encryption

Web application testing is the third phase of our daily security audit. According to industry sources, such as Gartner Group, an estimated 60-75% of all security breaches today are due to vulnerabilities within the web application layer. Traditional security mechanisms such as firewalls are not always sufficient against attacks on your web applications. All HTTP services and virtual domains are tested for the existence of potentially dangerous modules, configurations settings, CGIs and other scripts. The website then is “crawled” to find forms. Forms are exercised in specific ways to disclose all application-level vulnerabilities such as, code revelation, cross-site scripting and SQL injection. Both generic and software specific tests are performed in order to uncover misconfigurations and coding error vulnerabilities.
Data in the Nmbrs platform is **Encrypted-at-Rest** on several “levels”:

1- Encryption of Password fields: within the database the password field, is stored fully encrypted within the database. The user's password itself is not stored in the database, but instead, a salted hash of the password (SHA-2). This is to mitigate the risk of data breaches by unauthorized (logical) access and to mitigate the risk of malicious insider intent.
2- Disk encryption: encryption of the entire OS and database files. This is to mitigate against attempts to obtain physical access to the hardware on which the data is stored, and then compromise the contained data. This is implemented by Azure Transparent Data Encryption (TDE) and it performs real-time encryption and decryption of the database, associated backups, and transaction log files.
3- File storage encryption: of documents uploaded by users in the application. This is to mitigate the risk of data breaches by unauthorized (logical) access and to mitigate the risk of malicious insider intent. This is implemented by Azure Storage where data is encrypted and decrypted transparently using 256-bit AES encryption, one of the strongest block ciphers available, and is FIPS 140-2 compliant.

User Authentication: The authentication is implemented with the ASP.NET Membership authentication framework. The user has to submit a username and password which, when valid, will be registered as an authentication token in the Session of the web application. The user's password itself is not stored in the database, but instead, a salted hash of the password. This prevents password stealing even in case of unauthorized / malicious database access. There is the possibility to force periodical password resets and the use of a pin-code.

IP Validation: Every user has a white list with approved IP addresses to access the system. When the user access the system from a new IP address an email is sent to verify the new IP. It is also possible to restrict access to Nmbrs to a list of IP's or IP ranges.

Multi-Factor Authentication

Nmbrs supports 2-factor and multi-factor authentication. This can be enabled / disabled per Nmbrs subscription (i.e. for all users) as follows:

Step 1 Username (email) and password: This password complies with one of the password policies (standard or strict). There is also the possibility to expire the password after X days. After this authentication there is an IP validation check which the user has to manually approve on his email account to verify the current location.

Step 2, Option 1 - Pincode: In addition to the username and password, this 4 digits pincode can be activate per user type.

Step 2, Option 2 - Pincode: Google Authenticator: In addition to the username and password, an external token has to be validated in the user's mobile app. (2-Factor authentication)

Authorization for features

Nmbrs uses role-based security where each user is linked to a Master-role and one or more User-roles. The Master-role determines the maximum access for the user and is the same for most user accounts. The User-role determines the functionality a certain user has in the system. Each role specifies Deny, None, Read or Write rights to elements of the interface: Navigation Nodes and Area Groups. The server endpoints (handlers) area always linked either to a Popup control or to an Area Group control. In this way, the security system only allows access to handlers from Popups/Area Groups the user can access.

Authorization for entities

In order to determine which entities a certain user can access, every user account has an allow and a deny filter list for each entity (employees, companies, organizations, departments, debtors). In this way, every method of the service layer checks if the caller (user account) can access the entity he wants to read/modify. This is achieved by implementing a pre-call policy injection in the Business Logic Layer methods called from the Service Layer.

Is there logging of whom/when (and for example, from what IP address) accesses and uses the online system?

Nmbrs keeps track of when the user was created, deleted, the status (active / inactive) first login, last login and the user template applied. Also, all approved IP addresses (location) used to login are registered. The user that created and that changed the data within the application is stored in the database. This includes payroll mutations, data imports and mutations performed via the Nmbrs API.

Can Nmbrs employee's access my data?

Organization of Information Security

Visma Nmbrs operates a role based access control policy; utilizing the least privileges principle for all types of access. Customer data may be accessed (view only) by our (support / sales / startup) agents in scope of / in relation to handling (client) support requests. Support access (no access/ read/ write) by our agents to a client environment can be centrally managed by the clients (functional owner).

Direct access to customer data by developers, is only permissible in relation to damage control processes or incident management, when customer data might be at risk due to a software malfunction or a security incident management when that data may be damaged due to a software malfunction. In this case, Visma Nmbrs will always communicate directly with the relevant parties involved. For any other case where customer data access is needed, like customer projects, damage control solution process, access is only granted after this is done by written consent in the form of an agreement / order confirmation of the customer. In the scope of technical support, the account's functional owner and legal owner (both created when the Environment was created) can decide what is Visma Nmbrs' support staff access - no access, view or write access.

In the scope of technical support, the account's functional owner and legal owner (both created when the Environment was created) can decide what is Nmbrs BVs support staff access - no access, view or write access.

Backup & Availability

How is the availability of the online system guaranteed?

Visma Nmbrs provides a minimum level of availability (uptime) of 99.6% on average per month web service outside the exclusions listed in our SLA. The present value of the availability can be requested via the Nmbrs status page. The Microsoft Azure platform provides a minimum levels of availability (uptime) of 99.96% for their services provided to Nmbrs B.V. These services are:

- Application gateway
- Azure SQL servers
- App Services

In the Microsoft Azure platform the Nmbrs data backed up by SQL Database self-service for Point-In-Time Restore (PITR). SQL Database supports self-service for point-in-time restore (PITR) by automatically creating full backup, differential backups, and transaction log backups. Full database backups are created weekly, differential database backups are generally created every 12 hours, and transaction log backups are generally created every 5 - 10 minutes, with the frequency based on the compute size and amount of database activity.

The PITR backups are geo-redundant and protected by Azure Storage cross-regional replication Next to PITR backups also Long-Term Retention (LTR) backups are made. Visma Nmbrs has the following overall backup schedule configured:

- The PITR backups, will be retained for 14 (fourteen) days,
- The Weekly LTR backups, will be retained for 4 (four) weeks,
- The Monthly LTR backups, every last day of the month, will be retained for 1 (one) year,
- The Weekly LTR backup of week 1 of each year, will be retained for 7 (seven) years.

Each backup is compressed and encrypted using AES 256 bits encryption. The backups are stored in a Read-access Geo-redundant Blob Storage in the Microsoft Azure Cloud, located in The Netherlands (Region West-Europe).

Files from the File Manager function will not be considered a backup. Due to the nature of the multi-tenant cloud structure of the application Nmbrs, backups are not performed per customer, but for the whole infrastructure.

The client may request to restore a backup up to six months. This request will be separately invoiced with the applicable fixed fee. Nmbrs B.V. is committed to restore the backup within one working day.

Compliance & Privacy

Is Nmbrs GDPR Compliant?

Visma Nmbrs complies to the General Data Protection Regulation (EU) and more specific to the Dutch General Data Protection Regulation Implementation Act (Uitvoeringswet Algemene Verordening Gegevensverwerking) as Visma Nmbrs is a Dutch based company.

Visma Nmbrs has a Data Protection Officer (DPO). The DPO is a CISA and CIPP/E certified professional and formally registered at the Autoriteit Persoonsgegevens, i.e. the Dutch Data Privacy Supervisory Authority. Contact details of the DPO are publicly published on the website and periodically updated (https://www.nmbrs.com/en/gdpr).

Legal base of processing

In the Nmbrs platform Personal Data is processed on the legal base, contractual obligation. Visma Nmbrs processes Personal Data on behalf of, on instruction and under the responsibility of Subscriber. In this context, Visma Nmbrs either assumes the role of Processor (with respect to the data for which Subscriber assumes the role of Controller), or the role of sub-Processor (with respect to the data for which Subscriber assumes the role of Processor).

Data subjects & type of processing

Within the Nmbrs platform the following types data subjects are (possibly) processed (listing non-exhaustive). Nmbrs subscriber and or it's clients:

- Employees (including potential employees, freelancers and volunteers),
- Former Employees,
- Beneficiaries.

In the context of the services provided, Visma Nmbrs can process the following types of Personal Data of Data Subjects:

- Identification data (incl. Copy ID)
- Occupational data
- Residence Data
- Education & schooling data
- Social Security number (BSN)
- Leave and absenteeism data
- Contact information (telephone number(s), email addresses, etc)
- Performance appraisal data
- Family composition
- Bank account information
- Financial / payroll data
- Employment contract (mutation) data

Date subject rights

Visma Nmbrs has several processes and policies in place to ensure we can fulfill our obligations towards our clients and / or data subjects, in light of the GDPR. Processes are in place to ensure all requests by Data Subjects (under articles 15-22 of the GDPR) are handled in a standardized, timely and correct manner. This process is fully described and (annually) audited in the scope of the ISAE 3402 Type II audit.

Sub-processors

Visma Nmbrs utilizes several sub-processors in providing her services. All relevant sub-processors used are specified on the public website (https://www.nmbrs.com/security/subprocessors). On this website one has the option to register in order to receive notifications pertaining to a proposed change or addition of sub-processors.

Data Processing Agreement (DPA)

Visma Nmbrs has incorporated the required elements of the Data Processing Agreement (DPA) into the general terms and conditions. When starting a free trial and/or confirming your subscription, one is required to read and agree to our general terms and conditions. For further details regarding the elements of the DPA, we refer to section 6 of the general terms and conditions (https://www.nmbrs.com/en/terms).

What "external" audits / testing are available, by whom they are performed and how often they are repeated?

Visma Nmbrs has implemented an internal control framework, defining control objectives and how they are being met. This framework, the controls described and the risks mitigated through use of the control set, is annually evaluated and updated on new risks if needed. Visma Nmbrs is committed to having the design and implementation of these controls annually audited by a certified external auditor in the scope of the ISAE 3402 type II assurance report.

The purpose of this ISAE 3402 type II report is to provide the Visma Nmbrs customers with information to obtain an understanding of the design and implementation of controls implemented by Nmbrs, which are relevant to the control of the user organisation's internal processes for the purpose of the audit of their financial statements. The management of Visma Nmbrs is responsible for the description of the controls and control objectives. The external auditor will report whether the controls in the description are suitably designed to achieve the control objectives set out in the description, and also whether these controls have been implemented and were operating with sufficient effectiveness during the audit period specified.
The Nmbrs internal control framework used for the ISAE 3402 Type II audit is based on COBIT principles due to its suitability IT management and based on thorough risk analysis. For the ISAE 3402 the following processes are in scope:

- Change Management
- Access Security
- Service Level Management
- Backup
- Information Security
- Input controls
- Processing controls
- Reporting / export controls
- Storage
- Managing Master data

This report can be made available (under NDA conditions) to all Visma Nmbrs customers for the use of their own (financial) audit needs as well as those of their clients.

Service & Continuity

What "SLA" is exist, think of: Availability, Response-time support requests, 'Opening', 'Bugs' - Time to Fix?

The service hours of Visma Nmbrs are the office hours (08.30-17.00 CET) from Monday to Friday, excluding official Dutch holidays.

Support requests can be entered 24 hours a day by phone or via our online helpdesk. Visma Nmbrs is automatically notified in case of incidents of Category 10. Nmbrs offers support for all requests during available service hours, in case of incidents of Category 10 also within special Service Hours. We offer the following response times: Category 10 : 2 (two) hours, Category 20: 5 (five) hours, Category 30: 8 (eight) hours and 40 Category: 2 (two) working days.

For more information please refer to our SLA.

Contact information

Visma Nmbrs
Naritaweg 70
1043 BZ Amsterdam

IBAN NL30RABO0140087303
KVK 34150521
BTW NL.8098.44.539

Support: +31 (0)85 888 996
support.nmbrs@visma.com
Sales: +31 (0)85 888 9961
sales.nmbrs@visma.com


Enjoy the ride
Visma
Nmbrs
nmbrs.com