Nmbrs Payroll Security & Compliance Whitepaper

Frequently asked questions about security, privacy, availability and development of Nmbrs Payroll

Version 28-10-2026

Table of Contents

Product & Legal entities covered **3**

Platform and Technology **4**

What does the architecture of Nmbrs Payroll look like? 4

On what platforms and technologies is Nmbrs Payroll developed? 4

Hosting & Infrastructure **5**

In what environment is the application deployed (hosting partner)? 5

Development process **7**

What does the Nmbrs Payroll development process look like? 7

Security and Access **10**

How is Nmbrs Payroll protected against phishing and other online threats? 10

Are incidents (Denial of Service attacks or intrusions, information theft or attempts) reported to customers? 11

Is data in the application encrypted? 11

In what ways is (the access to) the application secured? 12

Is there logging of whom / when (and for example, from what IP address) accesses and uses the online system? 13

Can Nmbrs Payroll employees access my data? 13

How does Nmbrs Payroll B.V. ensure that its own employees handle information securely? 14

What is the customer responsible for? 14

Backup and Availability **16**

How is the availability of the online system guaranteed? 16

Compliance and Privacy **17**

Is Nmbrs Payroll GDPR compliant? 17

How does the Nmbrs Payroll AI Assistant handle my data? 18

What “external” audits / testing are available, by whom are they performed and how often are they repeated? 19

Service and Continuity **21**

What SLAs exist? Think of: availability, response time on support requests, opening hours, bugs and time to fix 21

Product & Legal entities covered

This whitepaper describes the development, maintenance and all other relevant (internal) processes / activities undertaken by Nmbrs Payroll B.V., related to providing the product / platform Nmbrs Payroll.

Nmbrs Payroll B.V. develops HR / payroll cloud software for accountants and business clients for the Dutch and Swedish market. Nmbrs Payroll B.V. is headquartered in Amsterdam and also has offices in Lisbon and Stockholm.

This whitepaper covers the core HR and payroll processing application, which is developed and maintained internally by Nmbrs Payroll B.V. Additional services referred to as 'Plus-features' are developed by external third-party suppliers and offered as white-labeled services; these fall outside the scope of this whitepaper.

Platform and Technology

What does the architecture of Nmbrs Payroll look like?

Nmbrs Payroll 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.

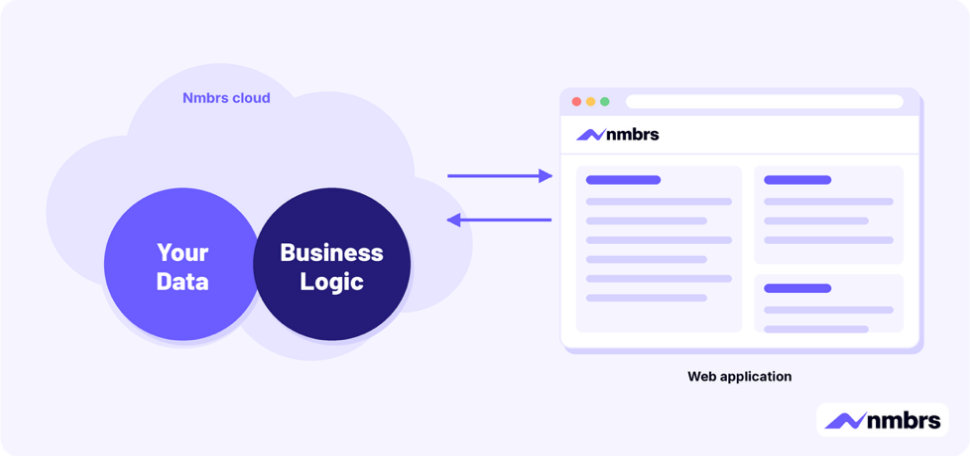


Figure 1: Nmbrs Payroll as a SaaS / Cloud application

Nmbrs Payroll consists of a core application complemented by microservices. For end-users it is a single web application, accessible via one URL. A dedicated platform layer handles security, logging and communication between the services.

On what platforms and technologies is Nmbrs Payroll developed?

Nmbrs Payroll is developed on the Microsoft technology stack and runs on Microsoft Azure platform services (PaaS) for the application, the databases and file storage. All

traffic from end-users enters the platform through an application gateway with a web application firewall.

Hosting & Infrastructure

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

Microsoft Azure Cloud

Nmbrs Payroll is fully hosted in the Microsoft Azure Cloud. Microsoft Azure Cloud is composed of a globally distributed datacenter infrastructure, supporting thousands of online services in 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 27001:2022 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

Nmbrs Payroll B.V. uses the Microsoft Azure platform for the hosting of the Nmbrs Payroll platform. All customer data in the Nmbrs Payroll 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

Nmbrs Payroll B.V. utilizes Azure's comprehensive security services, including Azure DDoS Protection and Azure Web Application Firewall (WAF), to safeguard its infrastructure and applications.

Backed by the Microsoft global network, Azure DDoS Protection provides massive mitigation capacity against network layer (Layer 3/4) attacks. The service scrubs traffic at the Azure network edge before it can impact service availability. Through always-on traffic monitoring and intelligent threat detection, it automatically mitigates DDoS attacks in near real-time without requiring manual intervention.

For application-layer (Layer 7) security, the Azure Web Application Firewall is deployed with the Azure Application Gateway. The WAF protects web applications from common vulnerabilities and exploits such as SQL injection, cross-site scripting, and session hijacking. Its protections are based on a managed rule set, which is kept current with the evolving threat landscape and is aligned with the risks identified in the OWASP (Open Web Application Security Project) Top 10.

Development process

What does the Nmbrs Payroll development process look like?

Development process
Alterations, improvements, or new features regarding the Nmbrs Payroll application are organized, approved and planned by **Product Owners** and **Stakeholders**. These alterations are described in **epics**. Epics are collected in the backlog and are represented by a stakeholder, who can represent both internal and external customers who benefit from the completion of this epic.

Periodically, stakeholders meet with Product Owners and representatives of squads during Product Councils, in order to choose the next epic a squad will work on. Together with the other stakeholders the risk, impact, and business value of each epic is discussed. Based on the outcome of these assessments, the next epic for that specific squad will be chosen to work on. During the building process, there will be regular validations with the stakeholder(s), in order to make sure the development process is on the right track.

Once an epic has finished, it will be demonstrated to the stakeholder(s) and other interested parties. Only after the demo will it be shipped or released to production.

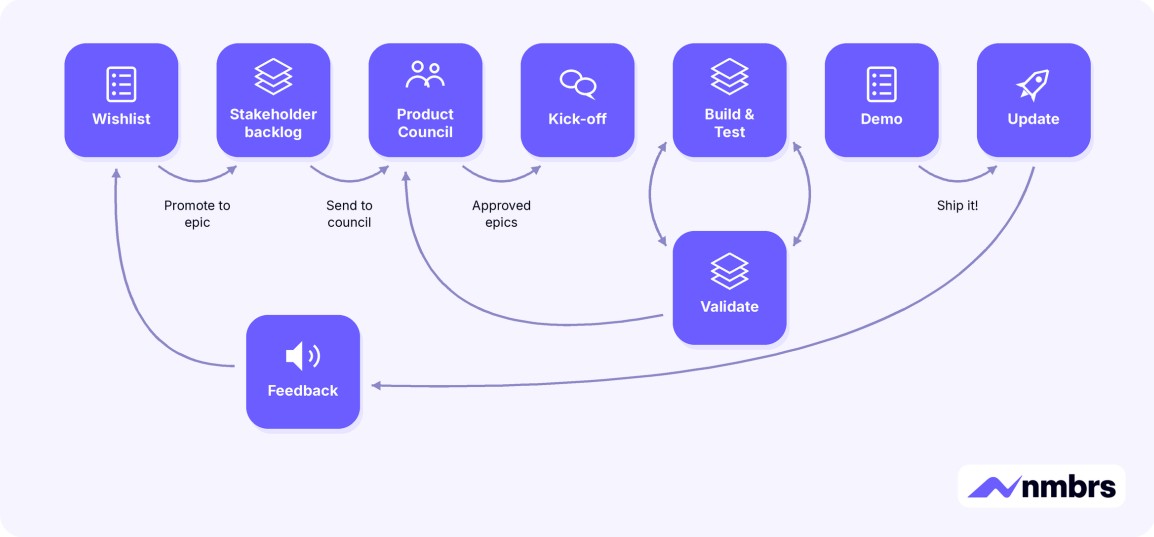


Figure 2: Development process within Nmbrs Payroll B.V.

Testing, QA and Deployments

There are separate development, testing and production environments. Access to these environments is limited to authorized users based on the Nmbrs Payroll B.V. Access Matrix.

Testing is done aligned with the development / deployment cycle and takes place in a separate testing environment. The first testing phase is performed ticket-based to ensure that all new features and improvements are implemented according to specifications and all works as intended. In a second testing phase, QA is performed to ensure that the entire product works with all quality attributes.

The delivery pipeline consists of a continuous integration server where automated testing is performed before each product release. The deployment process is automated to mitigate any risks as a result of manual tasks.

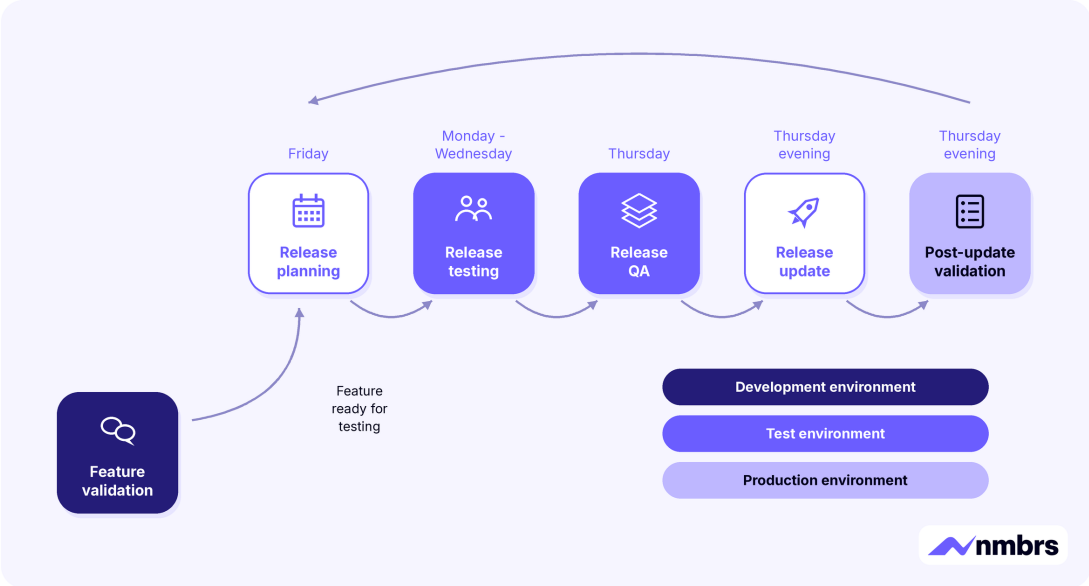


Figure 3: Testing and QA cycle

Application Updates

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

If Nmbrs Payroll B.V. expects planned maintenance to negatively affect the availability or functionality of the service Nmbrs Payroll, we will use commercially reasonable efforts to provide at least seven days advance notice of the maintenance. In addition, Nmbrs Payroll B.V. may perform emergency unscheduled maintenance at any time. If Nmbrs Payroll B.V. expects such emergency unscheduled maintenance to negatively affect the availability or functionality of the service Nmbrs Payroll, 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.payroll.nmbrs.com and status.payroll.nmbrs.com

Security and Access

How is Nmbrs Payroll protected against phishing and other online threats?

Automatic vulnerability scanning
Daily automated vulnerability scans are performed on both the infrastructure and the Nmbrs Payroll application. These scans check for open ports and exposed network services, and test the web application for common vulnerabilities such as cross-site scripting, SQL injection and misconfigurations. Findings are followed up and resolved.

Software Composition Analysis (SCA): Open Source components used in Nmbrs Payroll are continuously scanned for known vulnerabilities and license issues. This identifies which third-party packages pose a security or legal risk and how they should be remediated, in line with the OWASP Top 10 and Open Source license requirements.

Dynamic Application Security Testing (DAST): The running application is automatically tested by simulating real-world attacks, in order to detect vulnerabilities such as cross-site scripting, injection flaws and insecure server configuration before they can be exploited.

Static Application Security Testing (SAST): Source code is automatically analysed for security weaknesses as part of the development process. Findings are made available to developers in their daily workflow, so that issues are resolved before code is released.

Pentesting
Nmbrs Payroll B.V. works with a security specialist company (external party) in order to audit both the infrastructure and the application Nmbrs Payroll for potential security risks. The process takes place periodically, where a team of external ethical hackers and security experts uses a mix of automation and manual testing, following the OWASP Top 10 web application security standard. Findings are shared with the Nmbrs Payroll B.V. technical team and solved together with the external experts.

The OWASP Top 10 list consists of the 10 most seen application vulnerabilities:

1. Broken Access Control
2. Security Misconfiguration
3. Software Supply Chain Failures
4. Cryptographic Failures
5. Injection
6. Insecure Design
7. Authentication Failures
8. Software or Data Integrity Failures
9. Security Logging and Alerting Failures
10. Mishandling of Exceptional Conditions

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 is created with incident details, including: timeline, root cause, (possible) data exposed, (possible) affected parties, and the mitigation and preventive measures implemented. This report can be shared with affected parties upon request. This process is fully described and (annually) audited in the scope of the ISAE 3402 Type II audit.

As part of the Visma group, Nmbrs Payroll B.V. is supported by the Visma Cyber Security Incident Response Team (CSIRT). The CSIRT provides capability for assessing, responding to and learning from information security incidents, including the necessary coordination, management, feedback and communication. Nmbrs Payroll B.V. maintains a

register of security incidents and data leaks, and all reported security incidents are evaluated afterwards.

Is data in the application encrypted?

Data Encryption-in-Transit
Data communication with the Nmbrs Payroll platform is **Encrypted-in-Transit**. The browser and API client / server communication is done with **HTTPS** which guarantees data integrity and prevents data tampering. The data in transit is **TLS 1.2** encrypted, using a certificate issued by a trusted certificate authority.

Data Encryption-at-Rest
Data in the Nmbrs Payroll platform is **Encrypted-at-Rest** on several "levels":

1. **Password protection:** passwords are not stored in the database; instead, a salted hash of the password is stored. 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 Blob Storage where data is encrypted and decrypted transparently using FIPS 140-2 compliant **256-bit AES encryption**.

In what ways is (the access to) the application secured?

User Authentication
Users authenticate with a username and password. 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 database access.

By default, enhanced security settings are applied by enforcing a strong password policy where the user must register a secure password and the use of a pincode. Furthermore, it is possible to force periodic password resets.

IP Validation

When a user logs in from a new IP address, additional verification is required before access is granted. It is also possible to restrict access to Nmbrs Payroll to a list of IPs or IP ranges.

Multi-Factor Authentication

The Nmbrs Payroll platform supports 2-factor authentication as follows:

Step 1

Username (email) and password, in line with the password policy. Passwords can be set to expire after a configurable period. Logging in from a new location requires additional verification.

Step 2

Option 1 – Pincode: In addition to the username and password, a pincode can be activated per user type (Multi-factor authentication).

Option 2 – 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).

In addition, customers can further secure access to their environment by means of IP restriction and/or Single Sign-On (SSO).

Authorization for features

Nmbrs Payroll uses role-based security. Each user is assigned one or more roles that determine which functionality the user can access, and whether the user has no access, read access or write access to specific parts of the application. Access rights are enforced on the server side for every request, so users can only reach the functionality their roles permit. Default user templates with predefined roles are available, and the customer can tailor roles and permissions to its own organisation.

Authorization for entities

In addition to access to functionality, access to data is restricted per user. For every user account it can be defined which entities (such as companies, departments and employees) the user is allowed to access. These restrictions are checked by the application for every read or modification of data.

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

Nmbrs Payroll keeps track of when the user was created and 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 Payroll API.

Can Nmbrs Payroll employees access my data?

Organization of Information Security

Nmbrs Payroll B.V. 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, or when that data may be damaged due to a software malfunction. In this case, Nmbrs Payroll B.V. will always communicate directly with the relevant parties involved. For any other case where customer data access is needed, like customer projects or damage control solution processes, access is only granted after 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 Nmbrs Payroll B.V. support staff access is: no access, view or write access.

How does Nmbrs Payroll B.V. ensure that its own employees handle information securely?

All Nmbrs Payroll B.V. employees agree to comply with the Information Security Policies, which are accessible to all employees and are evaluated on a yearly basis. Every employee and external hire signs a non-disclosure agreement (NDA) in which they state that they have read and will comply with these policies. The policies include, but are not limited to:

- **Information classification and handling:** minimal requirements for handling all work-related information, regardless of whether it is electronic, on paper or shared verbally or visually.
- **Identity and access:** access to applications and infrastructure is granted based on roles, allowing only the minimal rights needed to fulfil one's responsibilities (least privilege, role based access control), while ensuring accountability and traceability of actions and changes.
- **Incident management:** standardized identification, classification and escalation of all types of incidents (support, performance, data leak and security).
- **Mobile device management:** guidelines for working on company devices, such as encrypted hard disks, data storage in backed-up cloud locations, acceptable use and working in public areas.

Access rights of employees are defined per role in the Nmbrs Payroll B.V. Access Matrix. As part of the joiner, mover and leaver processes, access is granted when an employee joins, adjusted when an employee changes roles and revoked when an employee leaves. Users and authorizations are periodically reviewed.

What is the customer responsible for?

Nmbrs Payroll is a very flexible application that allows very different implementations to adapt to diverse customer workflows and environments. This also means that the customer is responsible for a correct use of the system in a manner that will not compromise security, separation of roles and correct workflow. The controls at Nmbrs Payroll B.V. can only achieve their objectives if the customer also has its own controls in place. Taking this into account, the following considerations are relevant:

- The customer is responsible for entering and verifying the correct payroll input,
- The customer is responsible for revoking access when needed,
- The customer is responsible for the security settings of its environment, including the use of 2-step authentication by means of a pincode, IP restriction and/or Single Sign-On,
- The customer is responsible for keeping their means of authentication (passwords, pincodes) safe and personal, specifically in case of shared user accounts (users with the same email),
- When not using the default roles and permission settings, the customer is responsible for the correct implementation of permission settings to provide correct access,
- When not using the default workflow settings, the customer is responsible for the correct implementation of a correctly working workflow and signal settings for its own environment.

The customer should notify Nmbrs Payroll B.V. immediately when it suspects or has determined that a security incident has occurred at its side, which could lead to unauthorized access, alteration or deletion of the data within its Nmbrs Payroll environment.

Backup and Availability

How is the availability of the online system guaranteed?

Nmbrs Payroll B.V. 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 Payroll status page. The Microsoft Azure platform provides a minimum level of availability (uptime) of 99.96% for their services provided to Nmbrs Payroll B.V. These services are:

- Application Gateway
- Azure SQL servers
- App Services

In the Microsoft Azure platform the Nmbrs Payroll data is 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 backups, 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. Nmbrs Payroll B.V. 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 Payroll, backups are not performed per customer, but for the whole infrastructure.

Compliance and Privacy

Is Nmbrs Payroll GDPR compliant?

Nmbrs Payroll B.V. complies with the General Data Protection Regulation (EU) and more specifically with the Dutch General Data Protection Regulation Implementation Act (Uitvoeringswet Algemene Verordening Gegevensbescherming), as Nmbrs Payroll B.V. is a Dutch based company.

Nmbrs Payroll B.V. has a Data Protection Officer (DPO). The DPO is 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/).

Legal basis of processing
In the Nmbrs Payroll platform Personal Data is processed on the legal basis of contractual obligation. Nmbrs Payroll B.V. processes Personal Data on behalf of, on instruction and under the responsibility of Subscriber. In this context, Nmbrs Payroll B.V. 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 Payroll platform the following types of data subjects (of the Nmbrs Payroll subscriber and / or its clients) are (possibly) processed (listing non-exhaustive):

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

In the context of the services provided, Nmbrs Payroll B.V. 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

Data subject rights
Nmbrs Payroll B.V. 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
Nmbrs Payroll B.V. utilizes several sub-processors in providing her services. All relevant sub-processors used are specified on the public website (https://www.nmbrs.com/nl/security). 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)
Nmbrs Payroll B.V. 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 information we refer to our general terms and conditions available on the Nmbrs website. Please visit https://www.nmbrs.com/nl/algemenevoorwaarden for the product in the Dutch market and https://www.nmbrs.com/se/villkor for the product in the Swedish market.

How does the Nmbrs Payroll AI Assistant handle my data?

Data location

The AI Assistant runs entirely within the Microsoft Azure environment of Nmbrs Payroll B.V., in the same resource groups as the rest of the Nmbrs Payroll platform, in the Azure region West-Europe. For the language model, Azure OpenAI is used with an EU deployment, not the public OpenAI API. Prompts, answers, conversation history and log files are stored within the European Economic Area.

Retention

Prompts, answers and log files are retained for six months. This allows users to resume a conversation and allows Nmbrs Payroll B.V. to monitor the quality of the answers. After this period the data is permanently deleted.

Suppliers and sub-processors

Microsoft (Azure) provides the hosting and the language model (Azure OpenAI) and acts as a sub-processor. Microsoft does not use customer data or prompts to train models, and OpenAI has no access to them. If a user explicitly asks the Assistant to create a support ticket, a summary of the conversation, including the company, employee and period concerned, is sent to our support system Zendesk. This only happens at the explicit request of the user.

Processing of data from your Nmbrs Payroll environment

For knowledge questions, for example about the Payroll Tax Handbook (Handboek Loonheffingen), collective labour agreements (cao's) and the help center, only the content of the question is processed. In addition, the Assistant can perform tasks in Nmbrs Payroll, such as creating new employees. For these tasks personal data is processed, for example from an uploaded contract or identity document, or from the data of an employee. The following safeguards apply:

- The Assistant only works with data the logged-in user already has access to and follows exactly the same rights as in Nmbrs Payroll,
- Every change requires an explicit confirmation by the user; this cannot be disabled,
- Users without write permissions can only submit a mutation form that has to be approved by the payroll administrator,

- All data remains within the Azure environment of Nmbrs Payroll B.V. in Europe and is not used for model training.

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

ISAE 3402 Type II Assurance Report
Nmbrs Payroll B.V. 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 on new risks and updated if needed. Nmbrs Payroll B.V. is committed to having the design and operating effectiveness of these controls annually audited by a certified external auditor in the scope of the ISAE 3402 Type II assurance report. The audit is currently performed by Forvis Mazars N.V. (IT-Audit & Advisory) in accordance with ISAE 3402, as issued by the Nederlandse Orde van Register EDP Auditors (NOREA), and covers the period of a full calendar year.

The purpose of this ISAE 3402 Type II report is to provide Nmbrs Payroll B.V. customers with information to obtain an understanding of the design and implementation of controls implemented by Nmbrs Payroll, 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 Nmbrs Payroll B.V. 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 effectively during the audit period specified. Nmbrs Payroll B.V. uses Microsoft Azure as a subservice organization for housing and hosting; the controls at Microsoft Azure are excluded from the scope of the report (carve-out method).

The Nmbrs Payroll internal control framework used for the ISAE 3402 Type II audit is based on COBIT principles due to its suitability for IT management and based on thorough risk analysis. For the ISAE 3402 the following processes are in scope:

- Risk Management
- Change Management

- Incident Management
- Access Security Management
- Service Level Management
- Backup and Recovery Management
- Information Security Management
- Input & Processing Controls
- Master data
- Privacy & GDPR

There are no reporting / export controls included in the framework. This is due to the design of Nmbrs Payroll, where all input and processing of data is controlled by both end-user and application controls, effectively preventing (unintentional) faulty export / reporting.

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

ISAE 3000 Type II Assurance Report
Next to the ISAE 3402 Type II report, Nmbrs Payroll B.V. has an ISAE 3000 Type II assurance report. Unlike the ISAE 3402 report, the ISAE 3000 report can be shared with customers without NDA conditions.

Service and Continuity

What SLAs exist? Think of: availability, response time on support requests, opening hours, bugs and time to fix.

The service hours of Nmbrs Payroll B.V. are the office hours (08:30-17:00 CET) from Monday to Friday, excluding official Dutch holidays.

For the applicable service levels, including availability and response times on support requests, please refer to our SLA.