wflow

# Service Architecture & Security

## Table of content

# 1 Where do we store your data

All data is stored and backed up in Microsoft Azure data centers with the highest possible security at all levels: used technology, physical security of premises and buildings, personnel security and process security.  Each data center uses different keys to encrypt user data on live servers and for backups. Data backups are stored for 35 days.

For added security, the data stored on the wflow.com service is automatically replicated and backed up in two different locations. The primary data center is located in the Netherlands, while the secondary data center is located in Ireland. In the event of a failure, traffic is automatically redirected to the secondary data center within a second, ensuring minimal interruption to the service.

Microsoft is at the forefront of the industry in implementing clear security and privacy requirements and maintaining consistent compliance. Azure meets various international and industry compliance standards, such as the General Data Protection Regulation (GDPR), ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2, as well as country-specific standards such as IRAP (Australia), G-Cloud (UK), and MTCS (Singapore). Strict audits by third parties,e.g. the British Standards Institute (BSI), verify that Azure meets strict security measures required under these standards.

# 2 How do we keep your data safe

## Data encrypting

### Data encrypting in repository

Microsoft Azure employs the use of 256-bit Advanced Encryption Standard (AES) to secure and encrypt data, making it a trusted and secure platform for businesses and organizations. AES encryption is widely recognized and used by the banking sector and the US military, setting a standard for high-level security measures. To provide a seamless and secure data management experience, Microsoft Azure provides transparent encryption, decryption, and key management processes. When data is saved on the Azure servers, it is automatically encrypted and the encryption keys are managed by the Azure KeyVault, ensuring the highest level of security for all stored data.

### Data encrypting in transfer

All transmissions between the server and client are protected through the use of secure TLS/SSL protocols, also known as HTTPS, and is certified by Microsoft's Certificate Authority.  The portal can be accessed both from a PC and a mobile device via a responsive web application

# Data protection

## Data backup

All data stored on the wflow.com service is automatically replicated online between the Primary and Secondary data center (online geo-replication) and then automatically backed up in two locations.

All traffic is routed to the Primary Data Center and in case of its failure, it is automatically redirected online to the Secondary Data Center within a second. Primary data center: Microsoft data center in the Netherlands. Secondary data center: Microsoft data center in Ireland. Data backups are stored for 35 days.

## User access & Access management

For the user authorization the OAuth2 protocol is used, which is a method used to grant access to resources securely. In this instance, the authentication server is managed by wflow.com within the Microsoft Azure environment. For even stronger security measures, it's possible to utilize two-factor authentication through either the Google Authenticator or Microsoft Authenticator mobile applications. This added layer of protection helps ensure that only authorized individuals are able to access the resources in question.

You can ensure the protection of sensitive information by only allowing authorized users to access it. Our service provides the option to customize the level of access and responsibilities of each user through the use of specific roles, permissions, and accesses. This can be accomplished through the organization's settings, which offer a convenient and efficient way to manage user privileges.

# 3 Service

## Service architecture

The wflow.com runs as PaaS (Platform-as-a-Service) on the Microsoft Azure platform. All infrastructure of wflow.com service platform are operated in top-class, certified Microsoft data centers located within the EU (GDPR compliant).

wflow.com was developed using latest technologies, which are being used for e-banking solutions such as:
**Front-end: JavaScript (Angular)**
**Back-end: Azure SQL Server, Azure Cloud Storage, .NET**

## User Data Handling

### Purposes and legal basis for processing personal data:

Carrying out agreement with customer: based on performance of a contract
Improving Platforms and Services: based on legitimate interest of the controller Marketing Services: based on consent of the user.
Keeping Platforms safe: based on legitimate interest of the controller.
Technical data and User data may also be processed for the purposes mentioned above.
Anonymized data is processed for aggregated analytics and research.

Discover more information regarding the handling of user data in the Privacy Policy article. This article outlines the type of personal data that is collected, as well as the purposes and legal basis for its processing.

### Disposal of redundant data

We will store your personal information only if it is legally allowed and necessary for the purposes for which the data was collected, but no longer than 5 years after your last use of our platform.

## Code integrity and security

The application is developed by a skilled team of programmers and relies on the experience of senior team members who have long-term experience.

We are using secure development practices and tools to ensure that code is not compromised or changed without authorization. This includes using secure coding practices and tools such as source code version control systems, secure coding standards and secure coding practices. Every commit is inspected and reviewed by at least one other software engineer.

To reduce the risk of malicious code changes, access to code repositories is restricted to only those of us who really need it. Additionally, code integrity is ensured through regular security audits, penetration tests by an independent third party, and automated tools. Finally, code integrity is enhanced through the use of secure programming languages, secure libraries, and secure development environments.

## SLA

The Service Level Agreement (SLA) for the availability of wflow.com to end customers can be optionally guaranteed at 99.5% under the SLA provided by Microsoft on the Microsoft Azure platform-as-a-service.
The status of the systems is monitored in real time and it automatically prevents possible decrease in service performance.

**SLA for individual services guaranteed by Microsoft:**
Database availability: 99.99%
Availability of the data repository service: 99.99%
Availability of data in the repository: 99.99999999999999%
**The optionally guaranteed SLA for the total availability of the wflow.com service is 99.5%.**

# 4 On-premise deployment & deployment to a different repository

Our service is built on the cloud infrastructure. By utilizing Microsoft Azure services, we are able to benefit from the cloud's inherent security features, including robust physical security measures that surpass those of smaller, on-premise servers. Additionally, our cloud solution allows us to implement optimized network security measures specifically designed for the cloud environment. This enables us to maintain our infrastructure secure and operational 24/7, ensuring that all customers receive reliable service. The servers and databases we use are centrally maintained and updated, allowing us to ensure that our service is always up-to-date and compliant with the latest regulations, such as the General Data Protection Regulation (GDPR) for data storage.

Currently, our service is not available for on-site deployment and cannot be deployed on a repository other than Microsoft Azure.