Mobilityways security and privacy white paper

This white paper is intended to provide an overview of Mobilityways security and privacy practices in existence on the date of publication of this white paper, which are subject to change without notice. Any description of future plans is subject to change or delay at Mobilityways sole discretion. This white paper is for information purposes only and does not constitute legal advice or be perceived as supplementing or being incorporated into any terms and conditions in any contractual agreements.

Version	1.6
Date of version	November 2026
Date of last review	November 2026
Author	Jonathan Scutt – IT and Compliance Manager
Approved by	Kate Wood – Head of Operations

Document change log

Version	Date	Changes	Author	Approved by
1	October 2024	First published. This replaces the Mobilityways Data Protection and Information Security document.	Jonathan Scutt	Kate Wood
1.1	December 2024	Spelling and typo corrections Appendix E added – compliance certifications New - Data Handling, Storage and Transfer, Scalability and AI and Machine learning added.	Jonathan Scutt	
1.2	May 2025	Typo corrections Cyber Essentials certificate updated 3. Authentication > credentials: Removal of duplicate text and addition of credentials stuffing copy 4. Technical specification added 5. End point security - Addition of technical partners Appendix E added – sub processors	Jonathan Scutt	
1.3	September 2025	Updates include Azure architecture resilience increased, Azure front door and additional region, DB replication New application and network diagrams Supplier name change Sparkposts is now Bird – subprocesses table updated.	Jonathan Scutt Chris Vanderplank Ross Hewitt	
1.4	March 2026	Added exec summary DLP Data Loss and conditional access policies HubSpot supplier Correct Azure locations in Cloud Hosting Cyber Essentials certificate updated Many minor typos and corrections	Jonathan Scutt Chris Vanderplank Ross Hewitt Kate Wood	
	August 2026	*Reframed infrastructure, certification and AI claims around approved evidence and publication control.*	Chris Vanderplank	
1.5	September 2026	*Updated application-security controls and assurance wording to reflect in-house weekly OWASP ZAP scanning, GitHub CodeQL and secret scanning, Dependabot, weekly Codex Security analysis, targeted security tests, API scanning scope, vulnerability-management responsibilities and recent production DAST evidence.* *ISO27001:2022 certificate updated.* *Includes annual document review.*	Jonathan Scutt Chris Vanderplank Ross Hewitt	
1.6	November 2026	*Correction and clarification to sub processor table*	Jonathan Scutt	

Table of contents

Mobilityways security and privacy white paper *1*

Document change log **2**

Executive Summary *6*

Purpose **6**

1. Mobilityways *7*

Our mission statement **7**

Our teams **7**

2. Infrastructure security *7*

Cloud hosting **7**

Cloud infrastructure **8**

Technology Partners 8

Scalability **9**

Network Security **9**

Access control **10**

IP address restrictions **10**

Databases and Environments **10**

File storage **10**

Encryption and key management **11**

Encryption in transit 11

Encryption at rest 11

Segregation of data in Azure **11**

Backup **11**

Service level agreement (SLA) **11**

3. Security features and functionality *12*

Authentication **12**

Credentials 12

Single Sign-On (SSO) 12

Two-factor authentication (2FA) 12

Client data segregation 12

Roles within Mobilityways products **13**

Liftshare for work 13

Mobilityways 13

Dashboard Access 13

Logs **14**

Data imports **14**

The Dashboard **14**

Roles 14

4. Application security ***15***

Secure software development life cycle **15**

Mobilityways app local storage and journey logging **17**

Product technical specification **17**

Vulnerability management **18**

Penetration testing 18

Change management **18**

Encryption **19**

AI and machine learning **19**

5. IT security ***20***

Technology partners **20**

Endpoint security **21**

Password policy and MFA policy **21**

Activity and audit logging **21**

Identity and access management **21**

Email protection **22**

Advanced threat protection **22**

Device and data disposal **22**

Wireless network **22**

6. Operational security ***23***

Access to customer data **23**

Human Resources **23**

Acceptable use **23**

Starters, movers and leavers **23**

Training and awareness **24**

Information Security Management System **24**

Compliance 24

Governance and risk management **25**

Incident response and management **25**

Notification 25

Business continuity and incident response **25**

Data Protection **26**
Data storage and transfer 26
Data retention 26
Data deletion 26
Data Loss Prevention 27
Data destruction 27
Data analysis 27
Monitoring and logs **27**
Supply chain management **28**
Physical security **28**
Mobilityways Office 28
Data centre security **28**
7. Compliance, privacy, and certifications ***29***
Audit assurance and compliance **29**
Privacy policy **29**
Mobilityways.com and GDPR **29**
Internal audits and risk assessments **29**
Appendix A ***31***
Appendix B ***37***
Liftshare for work 37
Mobilityways platform 38
URLs used in the provision of all our services 38
Appendix C ***39***
Appendix D ***40***
Appendix E ***43***
Sub-processors and data storage locations **43**
Appendix F ***44***
ISO27001 ..... **44**

Executive Summary

This Security and Privacy White Paper provides an outline of the technical, organisational, and operational measures implemented by Mobilityways to protect information across its products, services, and internal systems. It is intended to support customers and partners in assessing Mobilityways' security posture, data protection practices, and regulatory compliance.

Mobilityways delivers its services using a cloud native architecture hosted entirely on Microsoft Azure in the UK, with segregated production and development environments located in UK data centre regions. The platform is designed for resilience and availability, utilising multiple active regions, managed platform services, and automated scaling. All data is stored within cloud providers within the EU, no customer or business data is stored on premises.

Information security is governed through a formally implemented Information Security Management System (ISMS) aligned with ISO/IEC 27001:2022, for which Mobilityways is independently certified. Mobilityways also maintains Cyber Essentials certification, demonstrating adherence to recognised cyber security best practice.

Access to systems and data is controlled using role-based access controls, the principle of least privilege, and enforced multifactor authentication for privileged and administrative roles. All data is protected using industry standard encryption in transit and at rest, with customer data logically segregated at both application and database levels.

Mobilityways operates a defence in depth security model supported by continuous monitoring, centralised logging, and security event analysis using Microsoft's security tooling. Clear processes are in place for incident response, change management, and business continuity, with tested plans to ensure service resilience and timely communication.

From a privacy perspective, Mobilityways complies with the UK Data Protection Act 2018 and UK GDPR, acting primarily as a Data Processor on behalf of its customers. Supplier and sub-processor relationships are governed through due diligence, contractual safeguards, and ongoing review. Mobilityways does not use generative AI within its core products, and any analytical use of data is anonymised and strictly controlled.

Purpose

The Information made available in this document is for the benefit of the reader and can be used to make their own independent assessment. It provides the relevant information to sufficiently assess the current Information and Data Protection posture of Mobilityways and its products. This document will be updated as Mobilityways security stance changes and as new technologies and controls are implemented. Any certifications Mobilityways achieves will also be referenced within.

1. Mobilityways

Our mission statement

Mobilityways mission is to make zero carbon commuting a reality by providing large employers with the tools and knowledge to achieve Zero Carbon Commuting.

Our ground-breaking climate tech empowers our clients to measure, reduce and report commuter emissions all in one place.

Our teams

The Mobilityways ISMS Team ensures that applicable regulations and standards are factored into its security frameworks. Mobilityways has multiple policies outlining the proper handling of sensitive, personal and confidential data. All policies are reviewed at least annually.

The Leadership Team at Mobilityways is accountable for information security and needs to formally approve decisions regarding the ISMS. The Leadership Team reviews the ISMS on a yearly basis to verify its actuality and to draft plans to address nonconformities.

Mobilityways does not consider security and privacy to be a single person's responsibility. All employees are responsible for safeguarding company assets. All employees are screened for expertise, experience, and integrity. Anyone who has access to Mobilityways information or assets must adhere to the requirements of the Information Security Policy. Employees receive information on security and privacy during onboarding and throughout ongoing training, knowledge sharing, and awareness communications.

2. Infrastructure security

Cloud hosting

Mobilityways products are entirely cloud-based, with no part of our infrastructure retained on-premise. A key supplier in delivering our services, is Microsoft's best-in-class industry leading Azure platform.

All Mobilityways web applications are hosted in the highly secure managed environments at Microsoft's UK data centre locations. Microsoft are industry leaders with the highest level of security through their secure operational practices and procedures.

In the Microsoft Shared Responsibility Model, Microsoft manages the security of the cloud computing infrastructure, while Mobilityways manages the security of the software and data residing on the cloud computing infrastructure.

https://www.microsoft.com/en-us/trustcenter/compliance/complianceofferings

https://azure.microsoft.com/en-gb/blog/microsoft-azure-leads-the-industry-in-iso-certifications/

For more detail on how Mobilityways uses Microsoft Azure services, see Appendix D.

Cloud infrastructure

Technology Partners

Microsoft Azure

Mobilityways uses Microsoft's Managed Azure services to ensure that we provide the most secure hosting environment for our applications and services. We are fully serverless to reduce the attack surface and ensure the infrastructure is security hardened and always up to date on Microsoft's managed cloud services.

Mobilityways uses the following key Microsoft Azure resources:

- Azure SQL Serverless Auto-Scale
- Azure Redis Cache
- Azure Container instances
- Azure Container Apps
- Azure App Services
- Azure Key Vault
- Azure App Configuration Store
- Azure Blob Storage
- Azure Front Door
- Azure Defender for Cloud
- Azure Log Analytics
- Azure DNS
- Microsoft Sentinel

App Service and Container App are Platform-as-a-Service, which means that the OS and application stack is managed by Azure; Mobilityways manage the application and its data.

Azure manages OS patching on two levels, the physical servers, and the guest virtual machines (VMs) that run the App Service/Container App resources. Both are updated monthly; these updates are applied automatically, in a way that guarantees the high availability of Azure services.

Mobilityways uses a resilient architecture utilising both the UK South and UK West regions. The platform is configured to load balance between the two regions with automatic scaling and robust failover support. The platform uses Azure Front Door to provide edge caching and optimise traffic to the 2 active regions, also providing security and traceability.

Mobilityways uses Microsoft's Azure services best practise security standards, hardening methods, and configuration recommendations.

Please see Appendix D for more information regarding Azure's security and compliance.

Bird (former company name Sparkpost EU)

Email delivery is via a 3rd party email delivery service Bird using their Mail product for outbound transmission of emails originating from the Mobilityways system, their storage servers located in Western Europe. Bird is designated as a permitted sender in the SPF policy, and DKIM authentication is used to indicate emails originating from us. Customer Email services communication content and traffic data are retained for 72 hours. Using opportunistic TLS for outbound traffic, which will depend on whether the receiving SMTP servers supports TLS. The application communicates with Bird Email via TLS encrypted API requests. Bird are ISO27001 certified, SOC 2 Type II, HIPAA and GDPR compliant.

Brevo

Email marketing is via a third-party service Brevo are responsible for the delivery of surveys, campaigns, and marketing materials from Mobilityways. Brevo's email delivery service and data storage are in Western Europe. Brevo is ISO27001 certified, GDPR, and CCPA compliant.

Google Maps and Routing

The web and mobile applications are supported by Google maps and routing APIs which deliver geospatial route calculation and geolocation services used from within the application tier, along with serving graphical map image tiles to client browsers. Google does not store any location data from routing requests.

Scalability

Through manual and automated scaling, we ensure we meet the demands of our clients and ensure a smooth user experience and a performant system. Our Azure SQL database is configured to use Azure Serverless Auto-Scaling model. We have a 2nd active replica database to distribute expensive read operations between databases. Azure App Services and Container Apps allow for automatic horizontal scaling to a pre-determined number of instances to handle spikes in demand. Monitoring is in place to detect and notify Mobilityways of slow performing areas. We operate a dual region resilient architecture to provide the best uptime and availability for the platform.

Network Security

As Mobilityways products are purely cloud-based solution this gives us the advantage of Microsoft's highly secure infrastructure.

Mobilityways uses Microsoft's Defender for Cloud advanced analytics and global threat intelligence to ensure we alerted to attempted malicious activity. Microsoft Azure's DDoS protection defends against the most common, frequently occurring Layer 7 DNS Query Floods and volumetric attacks that target Azure DNS zones.

Mobilityways uses a Security Information and Event Management (SIEM) solution, Microsoft Sentinel, to centrally collect, correlate, analyse and report security events across Azure, Microsoft 365, and endpoint platforms. Shared notifications and real-time threat monitoring from Microsoft's Defender XDR and Log analysis from Sentinel gives us an overview and visibility of our cloud attack surface.

Access control

Access to assets is granted based on role and in accordance with the need-to-access and least privileges principles. All access is assigned to named individual accounts; shared or generic accounts are not permitted.

All access to the Cloud platforms and other critical services is audited regularly, and enforced password strength and enforced MFA ensuring only those that require access have the required access only when they need it.

Access to our Azure estate is managed via Microsoft's Entra services and only key members of the Development Team and IT Manager have elevated privilege access. Using Role Based Access Controls (RBAC) we ensure only those employees that require access for their role have access to only the specific Azure resources required, these roles are managed, reviewed, and logged at least every 6 months or on change of role.

IP address restrictions

Azure Front Door manages access to our platform. We utilise IP Restrictions to key resources like SQL databases, for select Mobilityways Personnel. Where possible, we restrict access to internal Azure Resources using Azure Private Endpoints and deny all external access to increase security and reduce our attack surface.

Databases and Environments

We operate a series of Environments for the platform. Each environment is a full setup with differing data options. Our development environment is built with random seed data. We have a Staging Environment for Pre-Production testing which has an anonymised copy of the production data. All environments and databases have strict access control policies limiting access to select Mobilityways personnel. Database administrators' roles have full access to the database, this is essential for them to perform their role.

Within the web application, data is processed and stored in a SQL Server database, logically partitioned by client community. All data is encrypted at rest. Each environment is fully isolated from each other. Development environments are further separated at the subscription level in Azure to ensure maximum separation and security.

File storage

Microsoft's Azure Front Door provides cached CDN and blob storage that is used at point of delivery to serve some static elements of our application (SVG, PNG, JPG, and video files etc.) directly to client browsers for increased performance.

Encryption and key management

Azure managed secure key vaults are used to manage the encryption keys for services in Azure. Key generation, rotation, and storage are managed by MS Azure. Keys are rotated at least every 90 days. Microsoft's Azure Managed HSM Key vaults use FIPS 140-2 Level 3 validated HSM modules to protect your keys. Each HSM pool is an isolated single-tenant instance key vault.

Encryption in transit

Data in transit across open networks is encrypted using TLS 1.3 (TLS 1.2 at a minimum).

Encryption at rest

All encryption happens at the data access layer apart from passwords which are encrypted in memory using PBKDF2 with HMAC-SHA256, 128-bit salt, 256-bit subkey, and at least 10000 iterations.

TDE encrypts the storage of an entire database using a symmetric key (DEK). On database start-up, the encrypted DEK is decrypted and then used for decryption and re-encryption of the database files in the SQL Server database engine process. DEK is protected by the TDE protector which is a service-managed certificate.

Segregation of data in Azure

Azure is a multi-tenant service, which means that multiple customer deployments and VMs are stored on the same physical hardware. Azure uses logical isolation to segregate each customer's data from the data of others. Segregation provides the scale and economic benefits of multi-tenant services while rigorously preventing customers from accessing one another's data.

Backup

Data backups are encrypted and stored in Microsoft Azure storage with retention policies in place. Point in time restore is available up to one month, and monthly backups are stored for up to two years.

Service level agreement (SLA)

Mobilityways standard SLA is 99.7% availability over a 90-day period.

Planned maintenance will be carried out during the maintenance window of *7.00 P.M. to 2.00 A.M.*

Unscheduled maintenance performed outside maintenance window, provided that the Service Provider has used reasonable endeavours to give Customer at least 8 Normal Business Hours' notice in advance. We aim to release regular feature and change updates but do this when there is limited activity on the websites and use swap deployment slots to ensure no service disruption.

Customer can subscribe to real time status updates here:
https://status.mobilityways.com

3. Security features and functionality

Authentication

Mobilityways supports the following authentication methods:

Credentials

Users registering into a Liftshare For Work community are required to meet a minimum password complexity of 8 characters, at least one number and one uppercase. A lockout process is in place for incorrect passwords.

To enhance security and prevent automated credential stuffing attacks we have implemented rate limiting and account lockouts by restricting the number of login attempts per IP or user within a short period, introducing progressive delays to increase wait times after failed attempts, and temporarily locking accounts after repeated unsuccessful logins.

Single Sign-On (SSO)

OpenID Connect (OIDC) is a simple identity layer, which allows organizations to verify the identity of the end-user based on the authentication performed by an authorization server, as well as to obtain basic profile information about the end-user. This is available for Liftshare for work and the mobile app.

As part of the provisioning process, we will provide a Callback URL for you to whitelist, you will be required to provide an AuthorityUrl, ClientId and your ClientSecret.

Two-factor authentication (2FA)

Mobilityways employee administrator roles are always protected by multifactor authentication, using either a physical token or an authentication app. This control applies to relevant roles within the Liftshare for Work and Mobilityways dashboards.

Mobilityways has the ability for 2FA functionality for client community roles, functionality is limited but will be improved over time.

Client data segregation

All client community configuration and member data are segregated logically within the DB schema and at the application level using unique IDs.

Roles within Mobilityways products

Liftshare for work

The Liftshare for work web application has a user interface for employees to register and enter journey details, search and manage their Liftshare journeys, search for a match, and arrange their trips by messaging their Liftshare match. This is self-managed by the user, they can amend their details, remove journeys, and have functionality to remove themselves.

The Liftshare for work dashboard allows specified customer employees access to the community members to manage users, view journey matching logs, view statistic reports and much more. Community managers have functionality to remove users from the community.

The Mobilityways mobile app offers Liftshare for work functionality for users to be able to match journeys, arrange their trips by messaging their Liftshare match and includes functionality to validate the trip was completed.

Mobilityways

The Mobilityways web application allows users to access surveys and dynamic journey planner maps via links sent by email from the Mobilityways dashboard application. Users cannot register themselves; they must be imported.

The Mobilityways dashboard application has roles which allow functionality such as creating and send surveys, import staff members to the system, and creating journey plans.

Dashboard Access

Only Mobilityways employees can create credentials for both Mobilityways and the Liftshare for work dashboards. Users they cannot add, edit, or remove themselves, changes must be requested through their assigned account manager. Mobilityways Account Managers are also given access to their assigned customers' member data.

For more information about specific roles, please see the reference table in Appendix A.

Logs

Our administration dashboard logs commands with details of who performed them, what was done and when. IP addresses are not logged for dashboard usage. Logs are sanitised to prevent sensitive data, such as tokens and passwords, from being recorded. Our application logs are retained for the lifetime of the clients license.

Azure configuration logs are 180 days. This is not configurable; security event logs are part of the Microsoft services we use. All configuration changes are immutably logged with who, what and when. Microsoft Advanced Threat Protection for 365 and Microsoft Defender XDR have robust logs of all potential events.

Mobilityways uses Microsoft's SIEM tool Sentinel to collect and monitor logs from Azure, Microsoft 365 and Defender, analytic rules monitor security incidents across the services and provides alerts and audits of all activity related to an incident. Sentinel retains these logs for 90 days.

Live notifications are shared across the development and IT teams to ensure that any changes to access or configuration—whether accidental or intentional—are identified and acted upon promptly. In addition, advanced threat alerts are delivered directly to the administrative team, ensuring that critical security events are not missed despite the team's small size.

Log Type	Platform	Retention
Application logs	Mobilityways	180 days
Azure configuration logs	Azure	180 days
Security events (SIEM)	Sentinel	90 days
Error logs	Sentry	30 days

Data imports

Data imports are handled by our team with extreme care, using strict controls and processes. Data import and export functions are limited to specific roles.

The Dashboard

Mobilityways employee dashboard access has enforced 2FA with a physical key or OTP to offer further protection of our customers' data.

Roles

Please see appendix A table 1 showing roles for the dashboard systems.

4. Application security

Secure software development life cycle

Applications are designed, developed, and tested based on the “Security by Design” guidelines.

Mobilityways uses OWASP Top 10 methodology to build in security for our secure software development life cycle

- Secure Coding training and guidelines are provided to all developers.
- Peer Code Reviews to ensure guidelines are adhered to
- Integration Testing
- Static Application Security Testing
- End-to-end Testing
- Security testing combines static source-code analysis, dynamic runtime scanning, secret scanning, dependency monitoring and targeted integration tests.
- CodeQL analyses C# and JavaScript/TypeScript on changes to the main development branches and on a weekly schedule.
- OWASP ZAP scans the running web applications and client API weekly in production, with staging scans included in the production release workflow.
- GitHub secret scanning, Dependabot and weekly Codex Security analysis provide complementary checks for exposed credentials, vulnerable dependencies and application-security weaknesses.
- Best practise is shared, and knowledge sharing is promoted by the team
- All new features have dedicated tests
- Rigorous manual tests are carried out before each major release
- SQL Injection attacks are mitigated with parameterised queries, request filtering, and separating user input from DAL.
- We use anti-forgery tokens on post requests to prevent XSS attacks.

Mobilityways development environments are restricted by IP and all development data is fully anonymous. Security by Design is used throughout development.

Peer code reviews are performed on each pull request, Integration tests and thorough manual tests are carried out before each major release. A development lifecycle process governs how features move from idea through design, development, test writing, code review, integration testing, manual staging testing, release to production and review.

Security defects are tested for through static code analysis integrated into the CI pipeline (SAST) and weekly automated authenticated penetration testing (DAST). Integration tests ensure our system functions as expected, while end-to-end tests confirm that displayed results and actions behave as intended.

Targeted tests provide additional coverage for authentication, authorisation and tenant scoping. Examples include verifying that protected endpoints reject unauthenticated requests and that community-scoped queries exclude data belonging to other communities.

Code analysis and AI-assisted security review provide further ways to investigate weaknesses involving application logic and interactions between components. Together, these controls help identify issues that runtime scanning alone may miss.

For API testing, OWASP ZAP imports the client API's OpenAPI/Swagger definition to discover endpoints and performs passive security checks on the resulting traffic. This is included in the weekly production scan and staging release checks. Targeted integration tests add checks for authentication, authorisation and tenant scoping, while source-code analysis examines API handlers and supporting logic.

The Liftshare for work web application is surfaced by means of our bespoke branding system, presenting our own system to all white-label sites with client-specific branding

.

Mobilityways app local storage and journey logging

Storage is kept to a minimum on the Mobilityways app, operating system level encryption is used to store security related authentication tokens.

When users grant always on location permissions data is transmitted to servers, data unrelated to the commuting activity is discarded.

Trip authentication will store a single location, and this will be transmitted to the servers along with date, time and other meta data related to the journey share.

All data transferred between the mobile apps and Mobilityways API is TLS 1.2> encrypted.

Product technical specification

Platform	Tech Spec	Comments
Liftshare For Work	Vue 2, .Net, MS SQL Server, Redis 6	Traditional MVC application
Mobilityways App	React Native (+ Liftshare API)	React native app powered by the Liftshare API
CommuteBoost	N/A (see comments)	Feature of Mobilityways App and Mobilityways Dashboard
CommuteIQ	N/A (see comments)	Feature of Mobilityways App and Mobilityways Dashboard
Travel Surveys	N/A (see comments)	Feature of Mobilityways Dashboard
PTP	N/A (see comments)	Feature of Mobilityways Dashboard
Liftshare Dashboard	.Net Framework, MS SQL Server, Redis 6	Legacy project actively being replaced by Mobilityways Dashboard
Mobilityways Dashboard	Vite, Vue 3, Tailwind (+ Liftshare API)	SPA powered by Liftshare API
Liftshare API	.Net, MS SQL Server, Redis 6,	REST API

* *Correct at date of document version*

Vulnerability management

Mobilityways uses external security experts for penetration testing when a client-led test has not been completed within a 12 month cycle. Internal vulnerability testing and application-security scanning are also performed throughout the year to identify potential risks quickly.

If a vulnerability is detected in the platform, we will evaluate and score the risk posed to the security of users and their data accordingly. When a suitable patch or mitigation technique has been designed it will be tested and released within the timelines specified.

In some cases, scan results may yield false positives, patches may not be available or applying fixes may not be possible or practical, then other risk mitigation techniques will be used.

Findings from OWASP ZAP DAST, CodeQL SAST, secret scanning, Dependabot and Codex Security feed into the same vulnerability-management process. Findings are reviewed by the technical team to assess validity, exploitability and exposure before an owner and remediation date are assigned. Copies of the reports can be provided under the applicable information-sharing arrangements.

Risk score	Critical	High	Medium	Low	Informational
Remediation time from discovery	48 hours	30 days	60 days	182 days	Waived

Penetration testing

Mobilityways permits client-led penetration tests, or testing by third-party security teams, to be carried out on the web application or supporting infrastructure where required.

Where a client-led test has not been performed within a 12-month period, Mobilityways will commission a third-party penetration test instead.

Prior written approval is strictly required from Mobilityways before any tests are carried out, the results of any testing must be shared with Mobilityways without restrictions or limitations. Previous test results can be shared on request.

Change management

Mobilityways have a clearly defined policy and process in place for change management, the release process requiring any changes to be tested and approved prior to being applied to the production environment. These changes are reviewed in isolated development and staging environments to ensure they do not compromise security. All hotfixes are tested and applied in accordance with this process.

All business requirements are categorised and then prioritised according to business needs. Prior to development work commencing, detailed stories are written and signed off by the appropriate project

owner. A full range of general security and application controls are considered. See secure software development life cycle section above.

Development activities are carried out by our highly skilled team and in accordance with industry best practice.

Encryption

All traffic is encrypted using at least TLS 1.2 to protect all data in transit between the web and mobile applications, API, and the database.

Passwords are stored as hashes using PBKDF2 with HMAC-SHA256, 128-bit salt, 256-bit subkey, and at least 10000 iterations.

AI and machine learning

Mobilityways uses a bespoke Machine Learning Model in our CommuteBoost product. This allows the CommuteBoost product to predict the mode of transport (walking, driving, etc.) based on inputs from our Mobilityways iOS/Android application. It is optional for clients to opt-in to the fine tuning of this model if they'd like to contribute to improving the accuracy of our model.

It is important to note that this implementation is not generative AI, as Mobilityways does not currently utilise generative AI in the delivery of our products.

Machine learning focuses on analysing input data to identify patterns and relationships, enabling accurate predictions and classifications. In contrast, generative AI creates new data that resembles the training data, going beyond prediction to produce entirely new outputs.

While generative AI is not used in our core products, it is used in specific areas of the business in the ongoing creation and production of content, source code, business operations, research and communications as a tool to make our products and service better and to produce them more efficiently.

5. IT security

Technology partners

Microsoft 365 enterprise products provide Mobilityways with a comprehensive suite of advanced cybersecurity features designed to protect our business from various threats. **Some key features Mobilityways has implemented:**

- **Multifactor Authentication (MFA)**: Adds an extra layer of security by requiring users to verify their identity through multiple methods before accessing accounts.
- **Microsoft Defender for Business**: Provides proactive protection against ransomware, malware, vulnerability scanning and other cyber threats across our devices.
- **Microsoft Defender for Office 365**: Protects against phishing attacks and malicious links in emails and collaboration tools.
- **Microsoft Entra ID**: Manages identities and access, helping to prevent unauthorized access to business apps and data, including role based and conditional access.
- **Defender XDR Advanced Threat Protection**: Includes sophisticated scanning of email attachments and AI-powered analysis to detect and block dangerous messages.
- **Microsoft Purview**: Information Protection to classify and protect sensitive data, encrypt messages, and prevent data loss via data loss protection policies.

These and many other products and features collectively help safeguard Mobilityways from cyber threats, ensuring secure access to data and maintaining the integrity of information with the aid of Microsoft knowledge, expertise and secure services.

JumpCloud's enterprise products offer a unified platform for managing identities, access, and devices remotely and is designed to simplify IT management, enhance security, and support hybrid work environments. Below is an overview of the key services Mobilityways uses to ensure our devices are managed securely and access is granted to only those that require it:

- **Cloud Directory**: Centralises user identity management, allowing for seamless integration with various IT resources for instance Microsoft 365.
- **Multi-Factor Authentication (MFA)**: Enhances security by requiring multiple forms of verification before granting access.
- **Device Management**: JumpCloud's MDM solution provides centralised management and security for various devices, including macOS, Windows, iOS, and Android
- **Directory Insights**: Provides detailed reporting and analytics on user activities and access patterns.
- **Patch and Software Management**: Ensures devices are up-to-date with the latest security patches and updates.
- **Security Policy**: enforces configuration by policy on device, allow for screen lockout, external storage, encryption and many other policies to be applied remotely.
- **Password manager:** Provides a robust tool integrated into their platform, offering secure management and sharing of passwords and other sensitive information.

Endpoint security

All employee workstations and mobile devices are remotely managed via our cloud partners MDM/UEM (Unified Endpoint Management) solution. All devices are maintained, monitored by a managed by our internal ICT team.

All employee loaned devices are configured based on industry best practice, some of those controls include:

- Employees use limited privileged accounts
- Unique local administrator credentials for each device
- Strong unique user passwords, lock-out configured to 10 minutes and limited retry attempts
- Remote user binding, lockout, wipe and reset
- All software is supported, signed, and updated, unused applications are removed or disabled
- Remote software installation and enforced patch management
- Remote access deployment and revocation
- Full disk encryption and removable storage disabled
- BYOD mobile devices are remote managed via work profiles segregating business and personal data
- All devices are configured to industry standard security

MDM/UEM (Unified Endpoint Management) and password manager are provided by JumpCloud.

Password policy and MFA policy

Mobilityways password policy and MFA dictates that passwords must be strong and unique to each account. Employees are trained in the best practice use of the supplied password manager, methods of MFA and how to identify cyber security risks.

Regular audits, induction training, refresh training and employee security scoring ensures our cyber security knowledge and credential security are monitored, reviewed, and assessed regularly.

Multi-factor authentication methods are enforced on all cloud service accounts including OTP, physical tokens, SMS, and email verification.

Activity and audit logging

Logging is enabled on all managed loaned devices; automated device insight analytic notifications and reports any unusual activity. Device logs are remotely retained by for 30 days.

Identity and access management

Mobilityways follows the principle of “need to know” and least privilege, role-based access is used where available and conditional access to enforce modern authentication, verifying user identity with MFA, and restricting access based on trusted locations to reduce unauthorised access risks.

Provisioning, change and deprovisioning is overseen by the Operations team. Access is modified with 24 hours of an employee changing role or leaving Mobilityways.

Owners have been assigned for each information asset, and they are responsible for ensuring access is appropriate and reviewed regularly and at least annually for all employees and every 6 months for privileged access.

Email protection

Microsoft's Defender for 365 is active on all employee accounts offering advanced protection from malicious links in emails, Teams, OneDrive, and SharePoint files. It expands on the standard Microsoft 365 prevention tools and adds extra forms of detection and methods of investigation including Real-time detections. DMARC and SPF records are in place.

Employees are trained regularly and are continuously made aware of the phishing avoidance best practices and testing is conducted regularly.

Advanced threat protection

All employee workstations and Microsoft accounts are protected with Microsoft's XDR cloud and end-point security solution providing advanced phishing, antivirus, malware, and ransomware protection. Further to this providing endpoint detection and response, threat, and vulnerability management across Windows, macOS, iOS, and Android devices.

Device and data disposal

Mobilityways uses UKAS accredited – ISO 9001:2008 (incorporating EN15713:2009) third parties for the secure deletion and destruction of physical and electronic data including erasure and destruction of hardware.

Mobilityways uses suppliers adhering to the WEEE directive, who are GDPR compliant and use best practices and sustainable methods for recycling and disposal of IT Equipment.

Wireless network

Mobilityways Norwich office uses industry standard WPA3, DOS, IDS & IP, and web filtering technologies to secure the network and guest, IOT and employee networks to ensure segregation. Mobilityways does not store any business data at this location.

6. Operational security

Access to customer data

All Mobilityways staff contracts outline responsibilities for information security and data protection, and each staff member receives GDPR training along with Mobilityways' GDPR Privacy Policy. Access to customer data by Mobilityways is limited in accordance with our Terms of Service or respective agreement with the customer, on a case-by-case basis.

Human Resources

As part of the recruitment process, Mobilityways conducts character and professional reference checks, along with identity verification and Right to Work checks for the UK, underscoring the importance of ensuring a trustworthy and compliant workforce.

Acceptable use

Access to Mobilityways ICT systems is strictly controlled using unique user ID, passwords and/or tokens. All credentials are uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the Mobilityways ICT systems. All accessed is recorded and reviewed as per our Access Control Policy.

Employees are given clear directions on the extent and limits of their authority regarding Mobilityways systems and data. And are made aware that ICT systems are for business use only and are accountable for their actions.

All breaches of information security policies will be investigated and where investigation reveals misconduct, disciplinary action may follow in line with Mobilityways disciplinary procedures.

Starters, movers and leavers

Prior to new staff joining Mobilityways, the line manager and Head of Operations will approve the access required for the role.

Asset owners are provided with approved levels of access to be granted.

This is reviewed at least annually for all staff, every six months for privileged users, and when a member of staff changes roles or leaves the organisation.

A confidentiality clause is signed and, upon leaving the employment of Mobilityways, an exit process is followed ensuring that all access is removed.

Training and awareness

We consider employees to be our first line of defence, each member of staff is made aware of the fundamentals of information and cyber security during their induction process and during on-going annual security, privacy and awareness training.

Staff are trained to use our internal systems and processes, and to understand the importance of data security under GDPR. Non-disclosure and confidentiality agreements are signed by employees during the recruitment process.

Employees are tested throughout the year with simulated phishing attacks, security quizzes and regular awareness training and updates. Employee security scores are reviewed quarterly as part of the staff appraisal process and are a target for our ISMS objectives.

We encourage our employees to learn and develop their skills and knowledge, each employee has a dedicated Career Development Plan to foster growth and progression.

Information Security Management System

The goal of Mobilityways Information Security Management System (ISMS) is to protect the confidentiality, integrity and availability of information for the organisation, employees, customers and the (authorised) information systems, and to minimise the risks of damage occurring by preventing security incidents and managing security threats and vulnerabilities.

The Mobilityways ISMS is structured in a systematic and well-organised manner to promote ease of use and understanding. Legal and regulatory requirements apply to ensure the confidentiality, integrity and availability of information to the organisation, employees, partners and customers. All these translate into information security policies, procedures, training and guidelines.

The ISMS team are responsible for these policies and for working with each department to ensure procedures allow them to accomplish their tasks while protecting customers' data.

Compliance

Mobilityways' Information Security Management System is certified to ISO/IEC 27001:2022. Policies, procedures and training are continuously improved and communicated to employees.

These policies include: Information Security Policy, Business Continuity Plan, People Policy, Information transfer and classification Policies, Supplier Management Policy, Remote and Hybrid Working Policy, Access Control Policy, etc.

These policies are available upon request.

See Appendix E for compliance certifications, for more information see our website at Mobilityways.com/security

Governance and risk management

Mobilityways maintains an ongoing risk management process intended to proactively identify vulnerabilities within Mobilityways Information assets and assess new and emerging threats to the company's operations. Mobilityways undergoes an annual risk assessment as part of the ISMS and is integral to achieving on-going ISO 27001 certification.

Incident response and management

Clear guidance is given to employees and users of our services on how to report suspected security incidents, escalating them to relevant personnel. Mobilityways Disaster Recovery (DR) team (which includes the ISMS team) may be called upon to convene, evaluate the response, invoke a BCP scenario, action mitigation, and post-mortem analysis in a formalised process.

Mobilityways customer can report suspected incidents to their account manager, through the website ticketing system or straight to our security@mobilityways.com email address.

Disaster Recovery Team (DRT) comprises representatives from Security, Product, Development, Operations, Finance, representatives from other teams may be included on a case-by-case basis

If a potential data breach is identified, Mobilityways will follow the Data Breach Policy to ensure relevant internal and external parties are notified.

Incidents and bugs are reported via our online support ticket system. These are reviewed by the Product Development team in conjunction with our Account Managers and are tracked, tickets are prioritised, fixed, tested and released according to our Change Management Policy. Should the fix be targeted to resolve a security issue, any security implications arising from implementation are escalated to the Management Team if required.

Notification

In accordance with the terms of the Data Processing Agreement after becoming aware of a Data Incident, Mobilityways will notify affected customers without undue delay. Affected customers will be informed of the nature of the breach, the harmful effects of which Mobilityways is aware, actions Mobilityways has taken, and plans to remediate or mitigate the incident at the time of the notification.

Business continuity and incident response

Mobilityways maintains a Business Continuity Plan in alignment with ISO 27001 for dealing with disasters that would affect the business' ability to provide our services and support our customers. These include the restoration of the services, potential data breaches, loss of communication and many scenarios covering all critical functions. Testing is conducted at least four times a year. The Mobilityways DR team smoke-test the plans, assess any changes that might be appropriate, and ensure that we are prepared to deal with the evolving threats that we may face.

A copy of the Mobilityways Business Continuity Plan is available on request.

Data Protection

Data storage and transfer

Mobilityways Supplier Management Policy and risk assessment process ensure our cloud based service providers and sub processors must have suitable controls in place for secure information and data transfer this will be assessed as part of the procurement process, monitored and annually reviewed.

All data transfers to third-party cloud providers or partners must be governed by a data processing agreement (DPA) and/or service-level agreement (SLA) that includes provisions on data security, compliance, and transfer protocols.

Mobilityways suppliers and sub processors must meet our security standards and comply with relevant regulations, such as GDPR and local data protection laws.

Data retention

Mobilityways is required to retain certain personal and business data to fulfil legal and business obligations, as laid out in the Retention Schedule. Unless a valid business reason (or notice to preserve documents for contemplated litigation or other special situation) calls for its continued retention, data will be deleted and removed from all places it is stored when its data retention period ends.

Data deletion

Mobilityways customers retain full ownership of their members data and may modify or delete it using the means available through the service's user interface.

Upon termination or expiry of a contract, operational data is deleted as part of the account-closure procedure, subject to the encrypted backup-retention period described below. When a client's Liftshare for Work community closes, members may be offered the opportunity to move their account to a personal email address and the public Liftshare network.

A member whose email is no longer active due to them leaving an organisation and whose email will be classed as inactive or would bounce will go into a cleaning process. They will be sent a series of emails to ensure the bounce is a permanent and will therefore be deactivated and deleted.

Data stored within the Mobilityways platforms will be retained in encrypted backups for up to 2 years after the end of service provision.

Data Loss Prevention

To protect against data loss, Mobilityways employs a defence-in-depth approach that combines secure cloud architecture with rigorous technical and procedural safeguards. All information is encrypted both in transit and at rest in line with our Cryptography Policy, ensuring that data remains protected throughout its lifecycle. Business data is stored within Microsoft 365 services, where built-in retention and recovery mechanisms ensure that deleted items remain recoverable for defined periods, and endpoint devices synchronise automatically with cloud storage to prevent loss through hardware failure or local corruption. Regular, secure backups of application source code and database records are maintained, with restoration processes periodically tested to validate their reliability, supported further by supplier-level backup controls across all third-party platforms handling our data. These measures work alongside strict access controls and robust endpoint protection to minimise the risk of accidental or unauthorised data loss across the organisation.

Data destruction

Our service is hosted on Microsoft Azure, when customers delete data Microsoft follows strict standards for deleting data, as well as the physical destruction of decommissioned hardware. Microsoft executes a complete deletion of data on customer request and on contract termination.

Please see data destruction at Azure in appendix D for more information.

Data analysis

Mobilityways may carry out research and analysis projects with the data gathered to further explore how we can improve our service and encourage the uptake of more sustainable modes of transport. Any data we use is made anonymous and therefore no individual or organisational data will be identifiable.

Please see Appendix A, Table 2, which shows the data collected from members.

Monitoring and logs

Mobilityways relies on Microsoft Purview Compliance and our MDM solutions to provide detailed logging and activity monitoring tools, furthermore Microsoft's Defender XDR suite provides advanced threat detection, monitoring and remediation tools.

Supply chain management

Mobilityways ensures our suppliers meet our security and support requirements through due diligence processes and ongoing supplier management and reviews.

Mobilityways holds its suppliers and sub-processors to industry standards with respect to data security and privacy and considers both areas as critical in its sub-processors selection process. Among other measures, we have ensured that Data Processing Addendums and other relevant documentation and safeguards are in place with all our sub-processors, and we perform privacy, legal, and information security assessments as well as questionnaire-based audits. Assessments of our sub-processors and suppliers are conducted at least annually.

Mobilityways' documented Supplier Management Policy and process ensure that suppliers meet or exceed requirements for the transfer, processing and storage of data needed to provide and support our applications and services. The locations in which third parties process member data are documented in Appendix E and reviewed against applicable data-protection and transfer requirements.

Physical security

Mobilityways Office

Mobilityways' Norwich collaboration/office space is only accessible to members of staff and is secured with door entry systems and monitored intruder alarms.

All hardware is configured in accordance with our policies and processes to ensure security hardened best practice configurations and limited access to administration functions.

WIFI access is restricted to employees and guests. WIFI networks are separated for Mobilityways managed loaned devices, a guest network and IOT network to ensure segregation.

Traffic is limited by safe category, access is monitored and reviewed, and passwords are changed at least annually. Malicious site blocking, infected device prevention and blocking, IDS and IPS are enabled along with a stateful firewall.

Mobilityways have no on-premises resources, all services and software are cloud based (SaaS or PaaS). All cloud providers are access controlled and have methods of 2FA enforced on all accounts. No data resources, business, client or personal information is stored at this location, and no servers or network storage exists, all storage and backups are cloud based.

Data centre security

Mobilityways relies on Azure's world-class physical and environmental security measures, which results in highly resilient infrastructure. For more information about these security practices, please visit the following links: Overview of Microsoft Azure Security

7. Compliance, privacy, and certifications

Audit assurance and compliance

Mobilityways is compliant with the Data Protection Act 2018, General Data Protection Regulations (GDPR) and all applicable laws and regulations relating to the processing of personal data and privacy. A policy for managing data protection/information privacy is in place and managed by the Managing Director.

Mobilityways is ISO/IEC 27001:2022 certified, certificate 249029.

Mobilityways Limited is registered with the Information Commissioner's Office under number Z5010286. Relevant hosting providers maintain the certifications and assurance reports stated in Appendix E and in their published compliance documentation.

Privacy policy

Mobilityways Privacy policy, which describes our privacy and data processing practices in respect of the personal data can be found here: https://liftshare.com/uk/privacy-policy

Mobilityways.com and GDPR

The GDPR defines and distinguishes between two primary roles when it comes to collecting and processing personal data: data controllers and data processors. A data controller determines the means and purposes for processing personal data, while a data processor is a party that processes data on behalf of the controller.

Our standard position is that we shall act on behalf of our clients as a Data Processor and our clients are the Data Controller. Both parties agree to comply with their respective obligations under all Data Protection Laws.

Where we use the Personal Data outside of the scope of your instructions (e.g. to provide services directly to members (such as a car share to the beach at the weekend) we will process the members personal data as an Independent Controller. Such processing will be at our sole risk.

Further details can be found in Schedule 1 Data Processing Terms of our 2024 Business Terms and Conditions

If you have further questions on GDPR and please read the **Mobilityways GDPR pack**, you will find answers to important questions that we are frequently asked regarding our processing of your data.

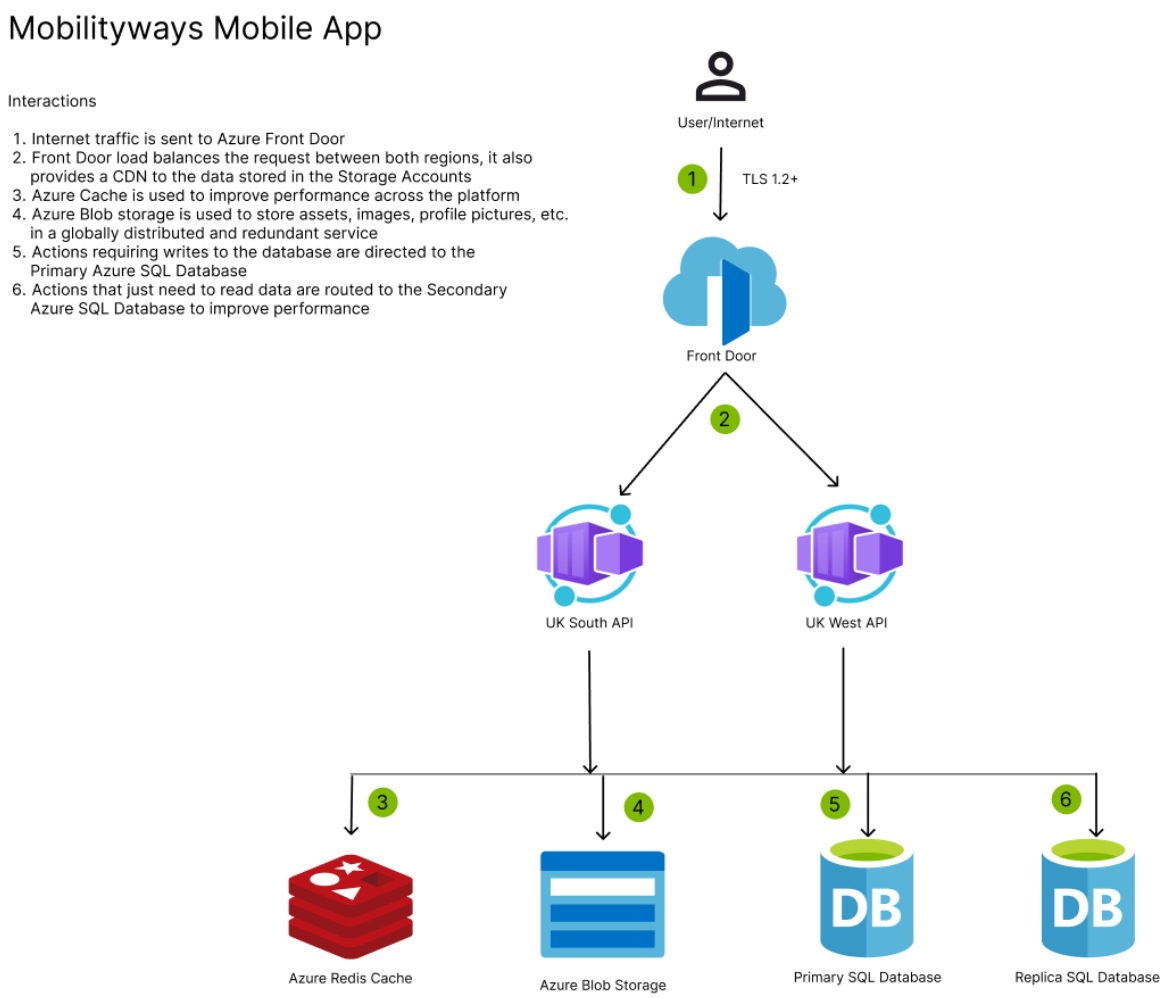
Internal audits and risk assessments

Internal information risk analysis is carried out for information assets. The analysis determines the risk via a business impact assessment and threat and vulnerability analysis. The analysis helps to identify security controls and risk remediations. This is performed under the supervision of the ISMS team who

will then work with the asset owners to track, remediate, and measure the effectiveness of the remediation.

Appendix A

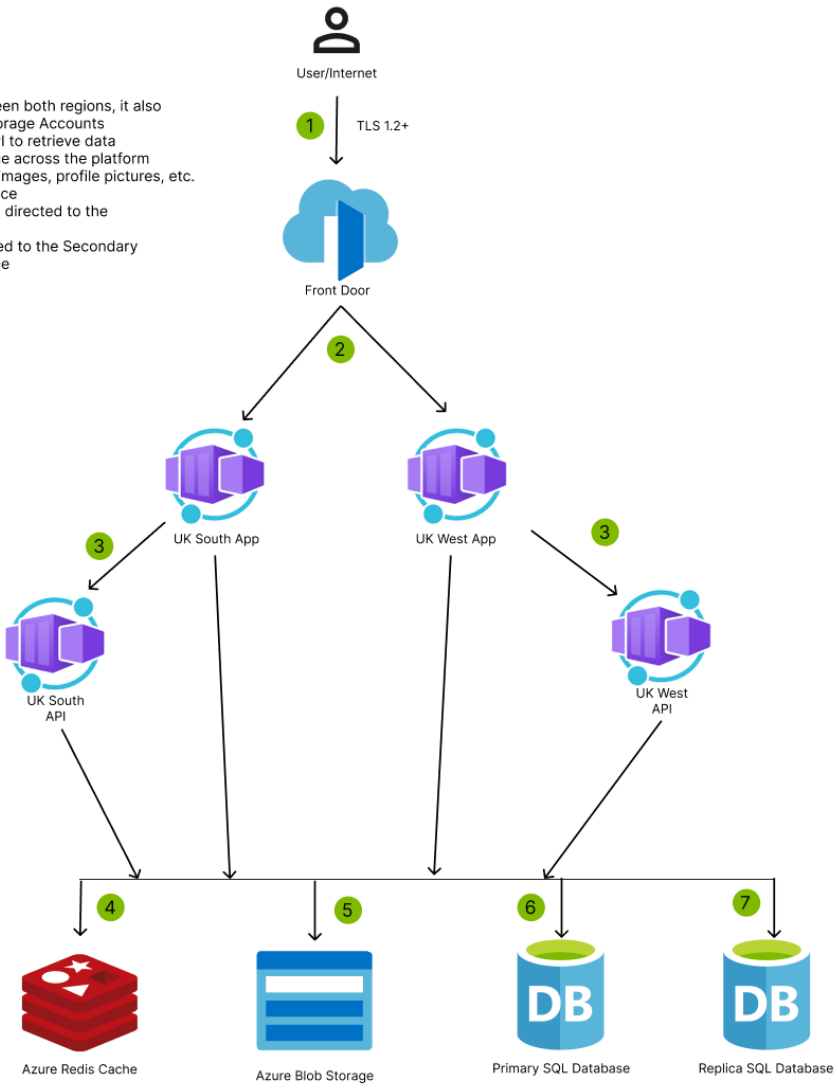
Application flow diagrams and dashboard reference tables



Mobilityways Web App

Interactions

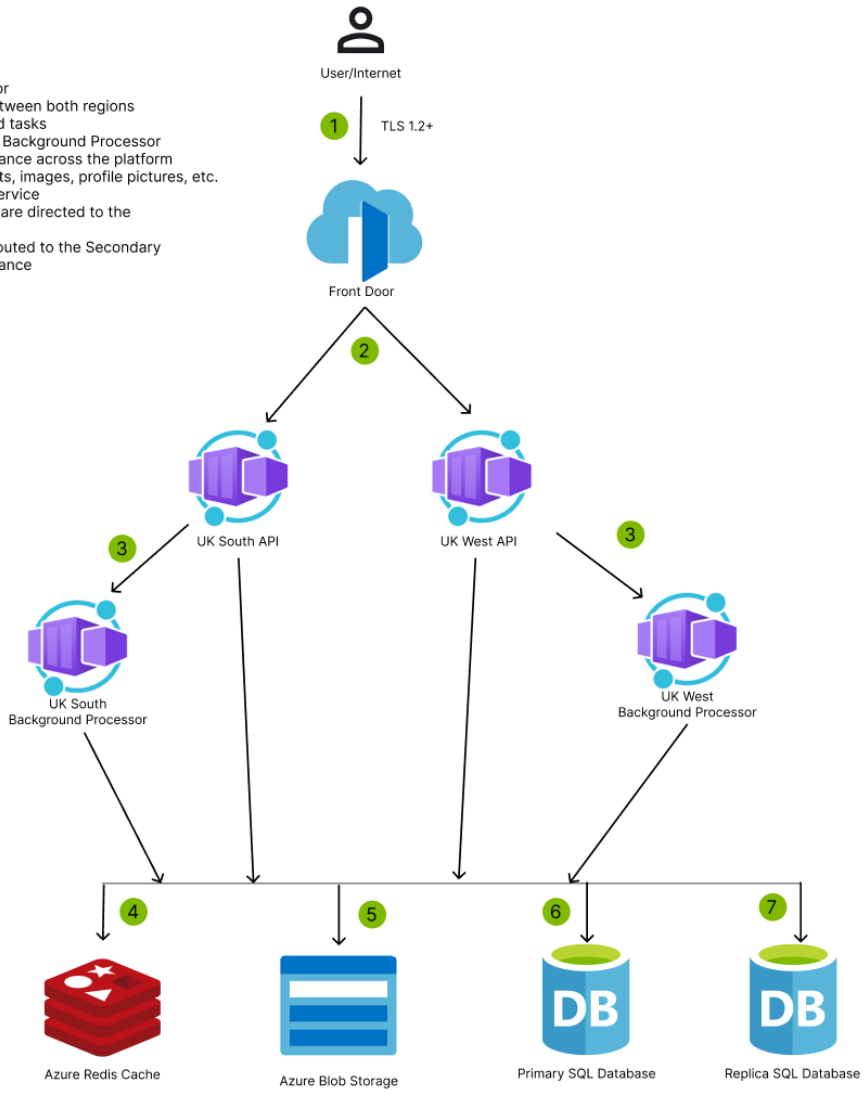
1. Internet traffic is sent to Azure Front Door
2. Front Door load balances the request between both regions, it also provides a CDN to the data stored in the Storage Accounts
3. The Web App will connect to it's regional API to retrieve data
4. Azure Cache is used to improve performance across the platform
5. Azure Blob storage is used to store assets, images, profile pictures, etc. in a globally distributed and redundant service
6. Actions requiring writes to the database are directed to the Primary Azure SQL Database
7. Actions that just need to read data are routed to the Secondary Azure SQL Database to improve performance



API Services

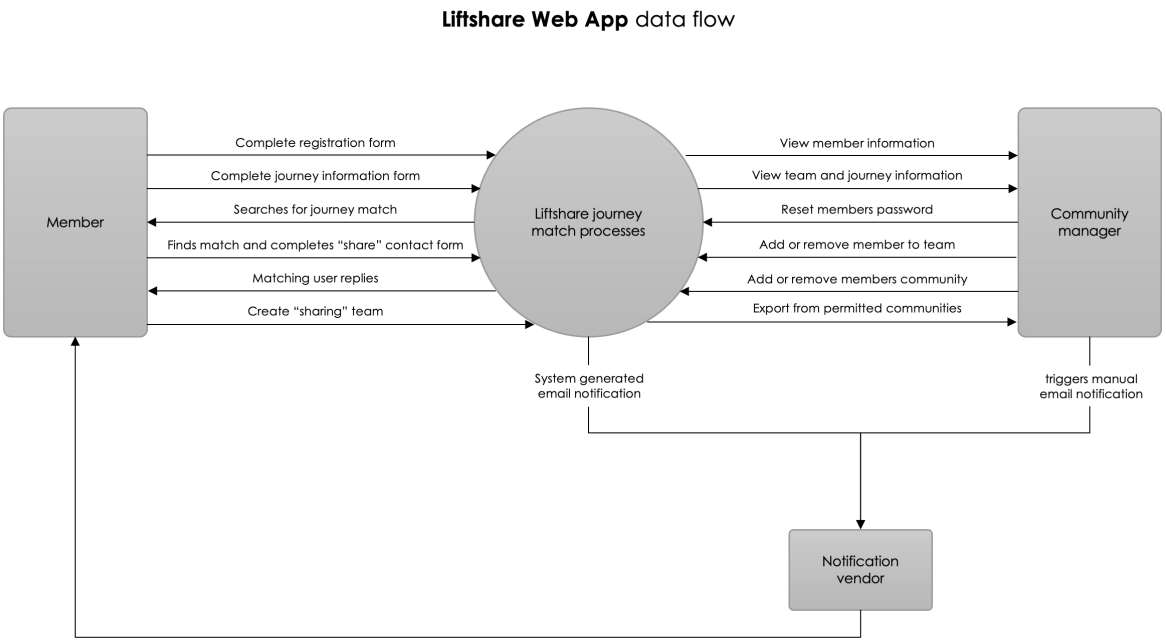
Interactions

1. Internet traffic is sent to Azure Front Door
2. Front Door load balances the request between both regions
3. The API will Queue 3rd Party/Background tasks (Emails, Journey Processing, etc.) via it's Background Processor
4. Azure Cache is used to improve performance across the platform
5. Azure Blob storage is used to store assets, images, profile pictures, etc. in a globally distributed and redundant service
6. Actions requiring writes to the database are directed to the Primary Azure SQL Database
7. Actions that just need to read data are routed to the Secondary Azure SQL Database to improve performance



End-users interact with the web applications and client-specific websites via the public internet using either liftshare.com or mobilityways.com. Other URLs are required for the website to fully function, please refer to the access requirements section.

Liftshare for work high level data flow diagram



Access roles available within the dashboard services

Table 1: Dashboard roles

Role	Description of access
Super Admin	Read and write access to client community configuration, statistics, and products. *Access limited to Mobilityways privileged staff only (Developers and administrators)*
Admin	Read and write access to client statistics and products. *Access limited to Mobilityways privileged staff only (Administrators and account managers)*
Community Admin	Read and write access to a specific communities statistics and systems. *Access available to Mobilityways staff and specified client staff.*
Community Monitor	Read only access to a specific communities statistics and systems, without any personal data shown (E.g. all names and email addresses are removed from view). *Access available to Mobilityways staff and specified client staff.*
Member Export Admin	Allow admin users to export email addresses from the Dashboard. *Access available to Mobilityways staff and specified client staff.*
Community Parking Permit	Allows dashboard user to view parking permit page only. This is used when a Parking Attendant needs to see the status of a parking permit, but no other dashboard pages. *Access available to Mobilityways staff and specified client staff.*
Travel Plan Admin	Access to a specific account Mobilityways Personal Travel Module. *Access available to Mobilityways staff and specified client staff.*
Travel Plan Monitor	Access to high level statistics for an account, no personal data for the PTP Module. *Access available to Mobilityways staff and specified client staff.*
Scoping User	Access to scoping report and map for a specific account, to view CommutelQ reports that are set to private, and to share reports as either Private or Public. *Access available to Mobilityways staff and specified client staff.*
Survey And ACEL Admin	Read and write access to a specific accounts survey and ACEL module. *Access available to Mobilityways staff and specified client staff.*
Survey And ACEL Monitor	Read only access to a specific accounts survey and ACEL module. They can see the survey individual responses, but not the contact they relate to. *Access available to Mobilityways staff and specified client staff.*
Contact Monitor	View-only contacts on a Mobilityways account. *Access available to Mobilityways staff and specified client staff.*
Contact Admin	Read and write access to contact details on Mobilityways. *Access available to Mobilityways staff and specified client staff.*

Table 2: Data Collection

Data Collected	Required	Public
First name, surname, password, email address, preferred contact method	Yes	No
Year of birth	No	No
Telephone number	No	Yes
Member bio	No	Yes
Origin and destination	Yes	Yes*
Frequency, date, and time	Yes	Yes *
If the journey is a private group journey	Yes	No* **
Additional journey comments	No	Yes *

* Members of private communities have the option to keep their entire journey information private to only other members of their community.

** Members of the network will not be shown details of which community a member is in unless they themselves are also in the same community.

Appendix B

Access requirements for our sites and services

The following information is to ensure that all the necessary allowances have been made for the service provided to our clients to work to its full potential.

The system is delivered as a fully hosted managed service, accessed by your users using HTTPS internet protocols with a web browser.

All current versions of mainstream browsers are supported, and we recommend that users install the latest version of Google's Chrome, MS Edge, Firefox, or Safari, along with ensuring all current security updates are applied. We no longer support any version of Internet Explorer, due to its functional limitations and security flaws and we do not recommend using it or any other unsupported browser.

For full use of the system, users also need to have access to an Internet email address capable of receiving emails sent from outside your organisation.

Please ensure your users can access the following URLs.

Liftshare for work

URLs specific to Liftshare for work

- liftshare.com – the main Liftshare software service domain
- *.liftshare.com – API services

Facebook SSO (for public communities)

- connect.facebook.net
- facebook.com

Email

All system notifications are sent from the liftshare.com domain, these should be whitelisted to ensure your employees receive them. We use support@liftshare.com for most transactional emails. However, member communications such as newsletters or information emails may also be sent from other @liftshare.com addresses.

Single Sign On (SSO) – Liftshare for work communities

Allow your employees to log in to your Liftshare for work community with a single pair of credentials from any device, no matter where they are.

OpenID Connect (OIDC) is a simple identity layer, which allows organizations to verify the identity of the end-user based on the authentication performed by an authorization server, as well as to obtain basic profile information about the end-user.

You will be required to provide an AuthorityUrl, ClientId and your ClientSecret. Once we have created the link we will provide Provider ID and Callback URL.

Mobilityways platform

URLs used by Mobilityways platform

- *.mobilityways.com – allow all sub domains
- *.liftshare.com – API services

Email

Travel plans and surveys are sent from the @mobilityways.com domain and if necessary, should be whitelisted to ensure your employees receive them.

URLs used in the provision of all our services

- *.google.com – domains used for Google maps and tag manager
- *.googleapis.com – domains used for Google maps and tag manager
- *.gstatic.com – font delivery from Google
- *.fontawesome.com – for icon provision
- cdn.liftshare.com – fast delivery of static content

Optional for our support systems

- *.hubspot.com
- share.hsforms.com, js.hs-forms.net, js.hsforms.com, js.hs-scripts.com, js.hs-banner.com, js.usemessages.com, js.hs-analytics.com

Optional for improvements to our services

- *.google-analytics.com – analytical tracking, to improve the service
- o267944.ingest.sentry.io – error tracking

- *.hotjar.com – mouse tracking

In all cases the asterisk indicates a wild card character to cover all sub domains.

Email delivery

Mobilityways uses a 3rd party email delivery service provided by Bird's Email PaaS platform (formerly Sparkpost EU) for outbound transmission of emails originating from the Mobilityways system. Brevo's services are used for delivery of marketing campaigns.

Selected emails utilise link tracking to monitor response rates, which requires users to be able to access URLs served from our subdomains. Please ensure all subdomains are allow-listed.

Appendix C

Please view our online policies for the latest versions

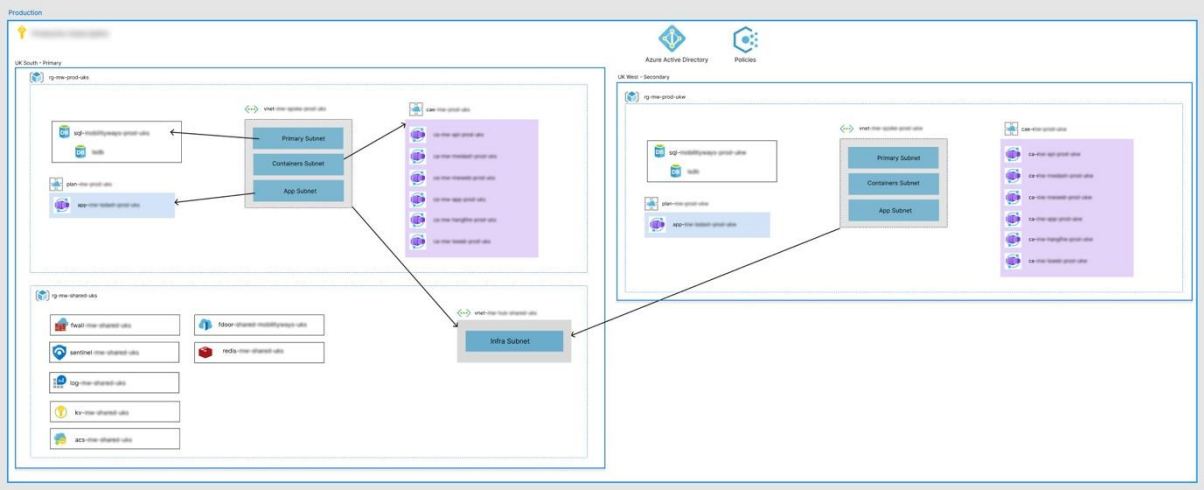
Business Terms and Privacy Policy

Members Terms of Use

Website Terms and Conditions (liftshare.com)

Appendix D

Mobilityways Azure Architecture



Microsoft's Azure platform

Azure offers a broad set global and industry-specific standards and supporting materials for key regulations, including, for example, ISO/IEC 27001 and ISO/IEC 27018, FedRAMP, and SOC 1, 2, and 3 Reports. Azure also meets regional and national standards that include the EU Model Clauses, EU-U.S. Privacy Shield.

A comprehensive library of Azure's security documents can be found here:

Azure security documentation | Microsoft Docs

Azure physical security

Microsoft designs, builds, and operates datacenters in a way that strictly controls physical access to the areas where your data is stored. Data loss is mitigated through highly redundant data backups performed every few minutes. Point in time restore is available up to one month and monthly backups are stored for up to two years. Azure data centre's are also equipped with a full range of environmental and physical security systems to protect hosted equipment from unauthorised physical access, power issues, fire, or flood.

https://docs.microsoft.com/en-us/azure/security/azure-physical-security

Azure network protection

Azure services have basic protection built in: Basic DDoS protection also defends against the most common, frequently occurring Layer 7 DNS Query Floods and volumetric attacks that target your Azure DNS zones. This service also has a proven track record in protecting Microsoft's enterprise and consumer services from large scale attacks.

https://azure.microsoft.com/en-us/blog/azure-ddos-protection-for-virtual-networks-generally-available/

Azure data protection

Access to customer data by Microsoft operations and support personnel is denied by default. When access to data related to a support case is granted, it's only granted using a just-in-time (JIT) model using policies that are audited and vetted against our compliance and privacy policies.

https://docs.microsoft.com/en-us/azure/security/fundamentals/protection-customer-data

Data segregation

Azure is a multi-tenant service, which means that multiple customer deployments and VMs are stored on the same physical hardware. Azure uses logical isolation to segregate each customer's data from the data of others. Segregation provides the scale and economic benefits of multi-tenant services while rigorously preventing customers from accessing one another's data.

Azure data destruction

When customers delete data or leave Azure, Microsoft follows strict standards for deleting data, as well as the physical destruction of decommissioned hardware. Microsoft executes a complete deletion of data on customer request and on contract termination.
https://www.microsoft.com/en-gb/trust-center/privacy/data-management

Azure app services

App Service, including Azure VMs, storage, network connections, web frameworks, management and integration features, are actively secured and hardened. App Service goes through vigorous compliance checks on a continuous basis to make sure that app resources are secured from other customers Azure resources, VM instances and runtime software are regularly updated, all communications are encrypted, 24-hour threat management protects the infrastructure and platform against malware, distributed denial-of-service (DDoS), man-in-the-middle (MITM), and other threats.
https://learn.microsoft.com/en-us/azure/app-service/overview-security

Azure Container Apps

Azure Container Apps is a serverless platform that allows Mobilityways to maintain less infrastructure and save costs while running containerised applications. Instead of worrying about server configuration, container orchestration, and deployment details, Container Apps provides all the up-to-date server resources required to keep your applications stable and secure.
https://learn.microsoft.com/en-us/azure/container-apps/overview

Azure customer data ownership

Microsoft does not inspect, approve, or monitor applications that customers deploy to Azure. Moreover, Microsoft does not know what kind of data customers choose to store in Azure. Microsoft does not claim data ownership over the customer information that's entered into Azure.

Azure compliance

Microsoft design and manage the Azure infrastructure to meet a broad set of international and industry-specific compliance standards, such as ISO 27001, HIPAA, FedRAMP, SOC 1, and SOC 2. Microsoft also meet country- or region-specific standards, including UK G-Cloud and rigorous third-party audits, such as those done by the British Standards Institute, verify adherence to the strict security controls these standards mandate.

https://learn.microsoft.com/en-us/azure/compliance/

Azure encryption at rest and in transit

Mobilityways uses Azure managed secure key vault is used, to manage the encryption keys. Key generation, rotation, and storage are managed by MS Azure. Keys are rotated at least every 90 days. Microsoft's Azure Managed HSM Key vaults use **FIPS 140-2 Level 3** validated HSM modules to protect your keys. Each HSM pool is an isolated single-tenant instance key vault.

https://learn.microsoft.com/en-us/azure/security/fundamentals/encryption-overview

Azure and UK G-Cloud

Every year, Microsoft Azure prepares documentation and submits evidence to attest that its in-scope cloud services comply with the 14 Cloud Security Principles, giving potential G-Cloud customers an overview of its risk environment. As with previous G-Cloud accreditation, the process relies on the ISO/IEC 27001 certification. A GDS accreditor then performs several random checks on the Microsoft assertion statement, samples the evidence, and makes a determination of compliance.

The appointment of Microsoft Azure to the Digital Marketplace means that UK government agencies and partners can use in-scope services to store and process UK OFFICIAL government data, which comprises the vast majority of government data.

https://learn.microsoft.com/en-us/azure/compliance/

Appendix E

Sub-processors and data storage locations

Mobilityways relies on various sub-processors to handle data on its behalf. These providers are carefully selected and regularly reviewed.

Sub Processor	**Type**	**Data Storage Location**
Microsoft Azure Platform	Cloud hosting, data storage and supporting infrastructure managed services.	UK and EU
Bird (formerly SparkPost EU)	Email services	EU, Western Europe
HubSpot	Member helpdesk enquiries	EU, Germany
Google	Mapping and routing services	NA no data stored
Brevo	Email campaign and marketing delivery services	EU – France

Appendix F

ISO27001

Mobilityways is ISO/IEC 27001:2022 certified, certificate 249029.

British Assessment Bureau
Part of the Amtivo group

CERTIFICATE OF REGISTRATION

The management system of certificate number **249029**

Mobilityways Limited
10-12 St Andrews Street, Norwich, Norfolk, NR2 4AF, United Kingdom

has been assessed and certified as meeting the requirements of:

ISO/IEC 27001:2022

The provision of ground-breaking climate tech, empowering large employers to measure, reduce and report their scope 3 commuter emissions globally

This is in accordance with the Statement of Applicability **Version 3.3 dated May 2026**.

Further clarifications regarding the scope of this certificate and the applicability of requirements may be obtained by consulting the certifier.

UKAS MANAGEMENT SYSTEMS
8289

IAF

Valid from:
Initial certification: 19 October 2023
Latest issue: 17 September 2026
Expiry date: 18 October 2029
Subject to annual assessments.

Authorised by

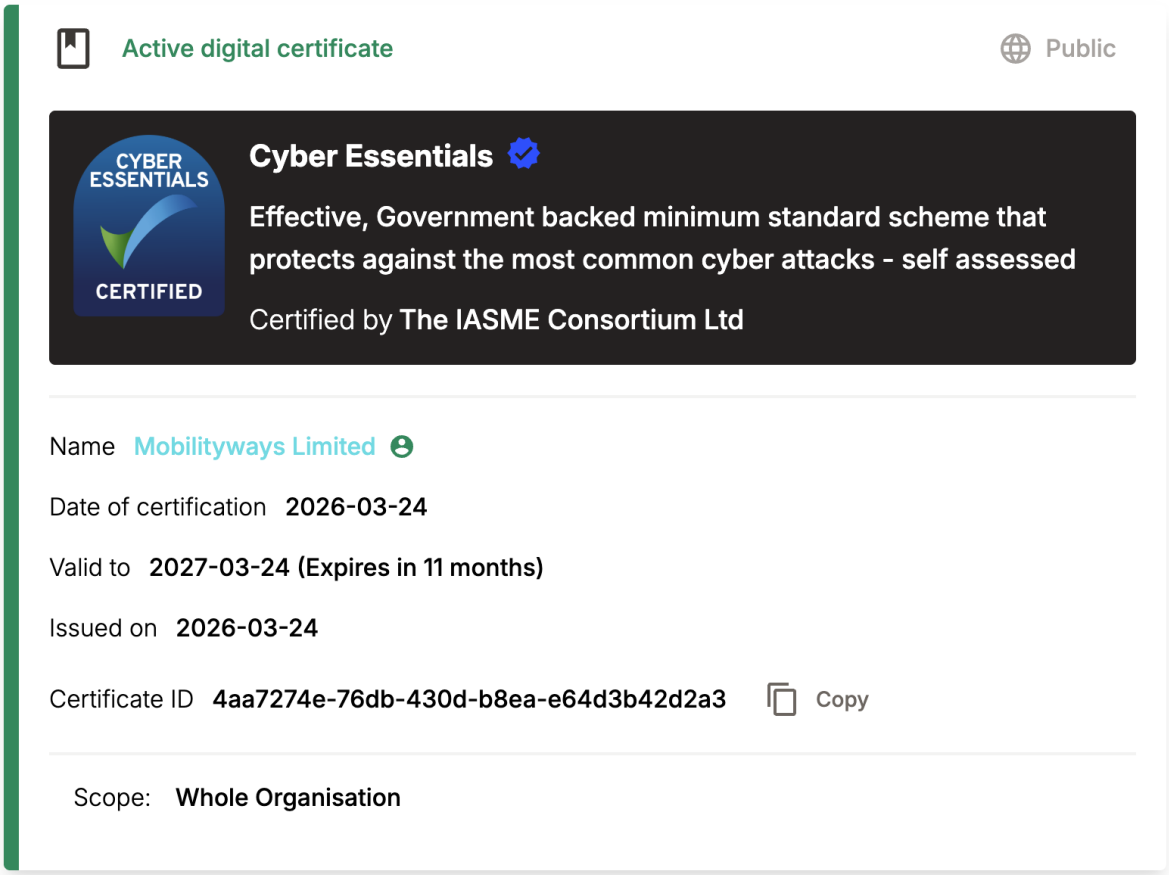
Mike Tims
Chief Executive Officer

british-assessment.co.uk
Certificate issued by British Assessment Bureau Limited.
Certification is conditional on maintaining the required performance standards throughout the certified period of registration.
Amtivo Group Limited. 30 Tower View, Kings Hill, Kent, ME19 4UY.

Cyber Essentials

Mobilityways is Cyber Essentials certified.

Certificate ID: **4aa7274e-76db-430d-b8ea-e64d3b42d2a3**



Digital Certificate

https://registry.blockmarktech.com/certificates/4aa7274e-76db-430d-b8ea-e64d3b42d2a3/