Data Protection & Information Security

Version	9.2
Date of version	May 2024
Date of last review	May 2024
Author	Jonathan Scutt – IT and Compliance Manager
Approve by	Julie Furnell – Managing Director

Document change log

Version	Date	Changes	Author/Approved by
3	April 2019	Update to Privacy Policy	Jonathan Scutt, Julie Furnell
4	May 2019	Update to cloud diagram and removal of Amazon	Jonathan Scutt, Julie Furnell
5	March 2021	Review of online services, addition of SharePoint and Mobilityways, updated password security	Jonathan Scutt Julie Furnell
6	Feb 2022	Annual review, addition of FAQs table and references. Web application architecture and data flow diagrams.	Jonathan Scutt Julie Furnell
7	Jan 2023	Access requirements updated Dashboard admin roles added Additional Azure Physical security information SSO details Sparkposts EU supplier change Mobilityways company name change	Jonathan Scutt Julie Furnell
8	September 2023	collaboration space at St Andrews location removal of Duke St office Addition of JumpCloud services Restructure for customers to better understand our security posture – many sections added, renamed and content moved. Many corrections, clarifications and amends based on recent changes to processes and policies. Addition of Microsoft Defender services. Clarification of : • pen test and vulnerability tests • encryption methods • antimalware usage • starters, movers and leavers process • development roles internal and external	Jonathan Scutt Julie Furnell
9	October 2023	ISO 27001 certification Links to security page ISMS Policy table Typo corrections	Jonathan Scutt Julie Furnell
9.1	January 2024	Small Corrections and formatting consistency Collab space changes Microsoft Sentinel Clarification of dashboard roles	Jonathan Scutt
9.2	April-May 2024	Addition of Brevo supplier details Policy versions removed Update suppliers in supporting services and cloud hosting ISO27001 certificate updated Spelling and typo corrections Cyber Essentials renewal certificate	Jonathan Scutt

Table of Contents

Data Protection & Information Security *1*

Document change log 2

Introduction **5**

Scope 5

1. Purpose **5**

2. Compliance **5**

3. Information Security Management System **5**

4. Security and privacy awareness **6**

5. People security **6**

Starters, movers and leavers 7

6. Security policies and procedures **7**

Compliance 7

7. Incident Management **7**

8. Infrastructure Security **8**

Collaboration space 8

9. Change management **9**

10. Encryption **9**

11. Access Management **10**

12. Acceptable Use **10**

13. Data Retention and Classification **10**

14. Application Security **11**

Cloud app services 12

Penetration testing 12

15. Supplier Risk Management **13**

16. Business Continuity and Disaster Recovery **14**

Risk Assessment and Treatment 14

Service Level Agreement 14

17. Data security **15**

Data accessibility within Mobilityways web applications 15

Data security in development and hosting 15
Developers and Database admins 16
Support systems 16
Audit logs 16
18. Device security 16
Device and data disposal 17
Appendix A 18
Web application flow diagrams 18
Liftshare for work high level data flow diagram 21
Access roles available within the dashboard services 22
Appendix B 24
Access requirements for our sites and services 24
Liftshare platform (Liftshare for work) 24
Mobilityways platform 25
All platforms (must be included for Mobilityways and Liftshare) 25
Optional for our support systems 25
Optional for improvements to our services 25
3rd Party suppliers 26
Appendix C 26
Appendix D 26
Appendix E 28
Frequently Asked Questions 28
Appendix F 31
ISO 27001:2022 certificate no 249029 31
Mobilityways ISMS policies 32
Cyber essentials certificate 33
Reference 34

Introduction

Mobilityways has clear and robust leadership from the senior management team in respect to information security. These members have specific operational responsibility for information and systems.

The Information made available in this document is for the benefit of the reader and can be used in order to make their own independent assessment. It provides the relevant information to sufficiently assess the current Information and Data Protection posture of Mobilityways and it's 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.

Scope

This document covers the entirety of the Mobilitways organisation, its remote and hybrid workers, contractors, devices, products and platforms.

1. Purpose

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

2. Compliance

Mobilityways is compliant with the General Data Protection Regulations. 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. See appendix F for certifications.

Mobilityways complies with all legal and regulatory requirements for data protection and audit procedures.

Mobilityways acts as the Joint Data Controller and Data Processor and as such is a registered member of the Information Commissioner's Office under number Z5010286.

All hosting services are SOC 2 Type II complaint and ISO/IEC 27001:2013 certified.

See appendix F for certifications.

3. Information Security Management System

The goal of Mobilityways Information Security Management System (ISMS) is to protect the confidentiality, integrity and availability of information to 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 Team ensures that applicable regulations and standards are factored into its security frameworks. Mobilityways has many policies which refer to how sensitive personal and customer data should be handled. All policies are reviewed at least annually.

The Leadership Team of 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 are informed about security and privacy at the on-boarding stage, as well as by regular training and other knowledge sharing and awareness communications.

4. Security and privacy awareness

Security and data protection training sessions are carried out during onboarding. There are mandatory team/role specific sessions as well. Mobilityways has an ongoing annual security and privacy awareness training for all employees.

Staff are trained to use our internal system and process, and to understand the importance of data security under GDPR.

Non-disclosure and confidentiality Agreements are signed by employees during onboarding.

Secure Coding training and guidelines are provided to all developers.

5. People security

All Mobilityways staff contracts specify responsibilities regarding information security and data protection and all staff are issued with Mobilityways's GDPR Privacy Policy.

Each member of staff is made aware of the fundamentals of information security during their induction process and during on-going security and awareness training. Employees are trained in how to access and use our information systems securely, at induction and refreshers throughout the year staff are trained to ensures the use of strong secure passwords and to use the password manager provided to ensure they maintain a strong security score.

Security scores are reviewed quarterly as part of the staff appraisal process.

Employees are tested throughout the year with simulated phishing attacks, security quizzes and regular awareness training and updates.

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

Methods of multi-factor authentication are enforced on all accounts, devices, services and websites including but not limited to OTP, physical tokens, SMS and email verification.

Mobilityways carries out character and professional reference checks on all employees as part of the recruitment process together with identity checks and the right to work in the UK.

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, if or when that member of staff changes roles or leaves the organization.

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

6. Security policies and procedures

The Mobilityways ISMS is set up in a systematic and well organised way. Legal and regulatory requirements apply to ensure the confidentiality, integrity and availability of information to the organization, 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 ISMS is ISO27001:2022 compliant and certified. Policies, procedures, and training are continuously being improved and communicated to our employees.

Some of the policies: 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 F for certifications.

Further information is available on Mobilityways.com/security

7. Incident Management

Clear guidance is given to employees on how to report suspected security incidents. The DR team (which includes the ISMS team) may be called upon to convene and evaluate the response. Any incidents will be reviewed by the ISMS and/or DR teams.

Mobilityways will follow the Data Breach Policy to ensure relevant internal and external parties are notified.

Internal security incidents are reported through Teams or via email, this process is communicated to all employees.

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 them are escalated to the Management Team if required.

There is an up-to-date Disaster Recovery plan in place, which enables a fast and effective response to serious attacks. For more detail see section 16 Business Continuity and Disaster Recovery

8. Infrastructure Security

Mobilityways applications and services are hosted on Microsoft Azure Platform.

Microsoft Azure App Services is a Platform-as-a-Service, which means that the OS and application stack are managed for you by Azure. Please see appendix D

All systems are fully isolated in development, staging and production environments. Customer data is logically segmented. Some of the controls are:

- Multi-factor authentication
- Vulnerability management
- Data encryption
- Bi-weekly vulnerability and web application scans
- Central device management and hardening
- Microsoft advanced threat protection for real time monitoring of all resources
- Microsoft defender for cloud

See appendix D for further information on Microsoft's Azure services used by Mobilityways.

Collaboration space

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

Mobilityways have no on-premises resources for staff to access, all services and software are in the cloud (SaaS or PaaS). All cloud services have forms of MFA enforced on all accounts.

WIFI access is restricted to employees and guests. Internet traffic is monitored and limited by safe category, access is monitored and reviewed, and passwords are changed at least annually. WIFI networks are separated for Mobilityways managed loaned devices, a guest network for employee's personal devices and guests, and another for IOT devices to ensure segregation of devices. Notifications are sent to administrators of various events including new device connections, configuration changes, policy violations and more.

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

Routers area configured with malicious site blocking, infected device prevention and blocking, IDS and IPS enabled.

Stateful firewall is enabled, denying all new inbound traffic, it keeps track of "established, related". All requests are tracked and maintained, so that responses coming back are properly identified and cannot be manipulated.

No data resources, business, client or personal information is stored at this location, no servers or network storage.

9. Change management

Mobilityways have a clearly defined change management and release process requiring any system changes to be tested and approved prior to being applied to the production environment. These changes are reviewed in development and staging environments to ensure they do not compromise security. Hotfixes are tested and applied in accordance with change management procedures.

All business requirements are categorised and then prioritised according to business needs. Prior to development work commencing, detailed project briefs are written and signed off by the appropriate project owner. A full range of general security and application controls are considered when designing the system under development.

Information security requirements for the system are taken into consideration when designing the system. System build activities are carried out by trained individuals and in accordance with industry best practice. Proposed changes are inspected thoroughly to identify changes that may affect security controls.

All elements of a system are tested before promotion to the production environment using automated testing, integration testing and manual testing. Tests are conducted in an isolated development environment as well as a staging environment mirroring production.

Code goes through static and dynamic vulnerability testing as well as manual testing before signing off.

Results are documented, approved by internal users, and signed off by the project owner.

10. Encryption

All Mobilityways devices with storage functionality have encryption enabled.

All traffic is TLS 1.2 encrypted to protect all data while in transit, between the web application as well as connectivity between the web application and the API.

All data is encrypted at rest and during transit.

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.

Passwords are never stored in plain text; Within the web application, data is processed and stored in a SQL Server database, logically partitioned by the client community. Passwords are stored as hashes using

PBKDF2 with HMAC-SHA256, 128-bit salt, 256-bit subkey, and at least 10000 iterations. Original passwords cannot be retrieved.

11. Access Management

Mobilityways follows the principle of "need to know" and least privilege. Role-based access is used where available. Provisioning and deprovisioning is overseen by the Operations team, with MFA and strong unique passwords by default.

Employees are trained in the best practice use of the supplied password manager, methods of MFA and how to identify cyber security risks.

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.

IP restrictions are in place for privileged access and UK IP restrictions are in place for more general access.

All SaaS/PaaS services are configured to send live notifications to multiple admin staff of anomalies to configurations and access.

Access is revoked on the same day an employee leaves Mobilityways, who no longer require access, or they are on prolonged leave.

12. Acceptable Use

Access to Mobilityways ICT systems is controlled using User ID, passwords and/or tokens. All Usernames and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the Mobilityways ICT systems.

Line managers must ensure that individuals are given clear directions on the extent and limits of their authority regarding Mobilityways systems and data.

Use of Mobilityways internet and email is intended for business use. All individuals are accountable for their actions on the internet and email systems.

All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with Mobilityways disciplinary procedures.

Mobilityways staff are provided with and trained to use a Password management service and secondary physical authentication token. Employees are requested to carry out an online security challenge every three months to ensure strong passwords are maintained.

13. Data Retention and Classification

Mobilityways is bound by various obligations regarding the documentation and electronic data it retains. These obligations include the period of retention for documentation and when/how this documentation is disposed of.

The Data Protection Legislation Article 5 (1)(e) states "personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed". The Data Handling Policy (available on request) ensures that necessary records, documents, and electronic data stored and processed by Mobilityways are adequately protected, archived, and disposed of at the correct retention period. This policy will provide all staff with clear instructions regarding the appropriate retention and disposal of such information.

Data classification

Data classification, in the context of information security, is the classification of data based on its level of sensitivity and the impact to Mobilityways Ltd, its clients and users, should that data be disclosed, altered, or destroyed without authorisation.

The classification of data helps determine what baseline security controls are appropriate. In the context of Mobilityways Ltd, every document generated must contain at least one data classification.

Confidential Data
Data is classified as confidential when the disclosure, alteration or disposal of data could cause significant risk to Mobilityways Ltd its clients, employees and users.

Internal/Private Data
Data is classified as internal/private when the disclosure, alteration or disposal of that data could result in a moderate level of risk to Mobilityways Ltd and its clients, employees and users.

Public Data
Data is classified as public when the disclosure, alteration or disposal of that data would result in a little to no risk to Mobilityways Ltd and its clients, employees, and users. Whilst minimal or no controls are required to protect the confidentiality of public data, some degree of control is required to prevent unauthorised modification or disposal of public data.

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

14. Application Security

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

- Peer code reviews are undertaken to ensure best practice and secure guidelines such as OWASP
- Rigorous manual tests are carried out before each major release
- The development lifecycle process governs how features move from idea through development, automated testing, code review, integration testing, staging testing, release to production and review.
- Bi-weekly automated web application and vulnerability testing allows us the ability to catch any new vulnerability early and quickly action any mitigation developments.
- These will be actioned by the team, tested, released, and then triggering vulnerability will be re-tested. Penetration test reports are provided on request.

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 undertaken, and thorough manual tests are carried out before each major release. A development lifecycle process governs how features move from idea through development, unit testing, static code analysis, code review, integration testing, manual staging testing, release to production and review. Security defects are tested for by static code analysis, this is integrated into the CI pipeline (SAST) and bi-weekly automated authenticated penetration testing (DAST). Integration tests ensure our system works as expected.

The Liftshare for work web application is surfaced by means of a white-label theme system, presenting the same underlying system to all white-label sites with client-specific branding, colours, images, and text where appropriate. All community configurations and member data is segregated virtually within the DB schema and within the application structure.

Cloud app services

Mobilityways key supplier in delivering our services is Microsofts's Azure platform, our web applications are hosted in a highly secure managed environment located at the UK south data centre. Microsoft are industry leaders in ISO certifications which ensures the highest level of security through Microsoft's secure operational practices and procedures.

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

Penetration testing

Mobilityways uses the services of external security experts to carry out scheduled vulnerability and web application penetration testing. Every 2 weeks automated penetration scans ensure any potential risks with website security and hosting infrastructure are identified and resolved.

The web application scanner is designed by experienced penetration testers, making it more thorough and accurate at identifying complex issues. The crawling engine uses a combination of application modelling techniques and subtle heuristical cues to automatically discover the complete attack surface of any given application in the shortest time possible. The algorithms are designed to model how a penetration tester or attacker would explore the application, to detect subtle vulnerabilities that other tools often miss and

opening up attack vectors that are inaccessible to less sophisticated crawlers."

source: https://appcheck-ng.com/

AppCheck identifies the top 10 OWASP vulnerabilities and helps to mitigate risk: https://appcheck-ng.com/appcheck-the-owasp-top-10-privacy-risks

After 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 risk mitigation techniques must be considered.

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

Penetration test reports are provided on request. We welcome client-led penetration tests and are always happy to work with internal or third-party security teams to facilitate additional web application or infrastructure testing if required. Prior written approval is strictly required from Mobilityways before any penetration tests are carried out. The results of any testing must be shared with Mobilityways without restrictions or limitations.

15. Supplier Risk Management

To deliver our applications and services we require the services of top-tier suppliers. Mobilityways ensures our suppliers meet our security and support requirements through due diligence processes and ongoing supplier management and reviews.

Mobilityways documented supplier management policy and process ensures that our suppliers meet or exceed requirements for the transport, processing and storage of data required to provide and support our applications and services. Mobilityways ensures all our supporting services are located within the EEA.

Microsoft Azure managed services

Mobilityway's web applications are hosted in a highly secure managed environment provided by Microsoft, physically located at the Azure UK South data centre. Using Microsoft's Managed Azure App Services, managed SQL database, key encryption vaults and Defender for Cloud we ensure that we provide the most secure hosting environment for our software services.

Microsoft Azure CDN/blob storage 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.

Google routing and maps API

The application is supported by Google Maps Business 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.

Email delivery

Email delivery is via a 3rd party email delivery service Sparkpost EU for outbound transmission of emails originating from the Mobilityways system, their storage servers are located in Western Europe. Sparkpost EU is designated a permitted sender in the SPF policy and DKIM authentication is used to indicate emails originate from us. Sparkpost EU use opportunistic TLS for outbound traffic, which will depend on whether the receiving SMTP servers supports TLS. The application communicates with Sparkpost EU via API requests via TLS 1.2.

Email marketing is via 3rd party service Brevo are responsible for the delivery of surveys, campaigns and marketing materials from Mobilityways. Brevo's email delivery service and data storage is located in Western Europe. Brevo is ISO27001:2013-certified, GDPR, and CCPA compliant.

16. Business Continuity and Disaster Recovery

Mobilityways maintains a comprehensive business continuity plan that covers the following key areas:

- defining and prioritising the critical functions of the business
- identifying the threats and the potential impacts on the business
- forming a plan to mitigate and minimise the threats we face
- detailing the agreed response to an emergency
- identify key contacts and provide useful resources during an emergency.

Through focusing on these important items, Mobilityways have been able to identify and take mitigating actions against the event of a major incident or disaster, and where possible minimise the potential impacts.

Furthermore, the Mobilityways disaster recovery team meet quarterly to 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 BCP is available on request.

Risk Assessment and Treatment

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.

Service Level Agreement

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.

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

17. Data security

Data accessibility within Mobilityways web applications

Liftshare for work

The web application has a user interface for employees to register and enter journey details and search and manage their Liftshares. Users can also chat with other members to arrange journey matches. This is self-managed; the user can edit their details and remove themselves from the platform. The Liftshare mobile app offers functionality for users to be able to match journeys and chat with their Liftshare, functionality to validate the Liftshare journey match.

Liftshare for work administration dashboard

Allows specified employees access to the community member data to perform management processes this includes user and journey details. Super users create access credentials for Dashboard users they cannot add, edit, or remove themselves. Changes must be requested through their assigned account manager who also has access to the community member data.

Mobilityways dashboard

Dashboard application, user cannot register themselves they must be created by a super user. Dashboard user import staff members to the system. User can access a survey page and dynamic journey planner via links sent by email from the application.

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

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

Please see appendix A table 2 showing what data is collected from our members.

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

Data security in development and hosting

Cloud hosting security

Microsoft Azure Defender is employed to protect and give advanced detection of unauthorised access, this covers all of Mobilityways software services in the cloud Azure App services, MS SQL databases. Administrator and developer access is limited to UK IPs, MFA is enforced with strong passwords. Development environments are further limited by restricted specific IPs.

Software services 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.

Source code is stored in source control provided by GitHub, access is limited to those that require it for their role.

Developers and Database admins

All data within of our development environments is fully anonymised. Database administrators have full access to the data stored in the database this is essential in perform their roles.

Support systems

Software development and bug tracking is handled by GitHub Projects. CRM is provided by HubSpot.

Mobilityways's business data and staff collaboration tools are provided by Microsoft 365 platform including Sharepoint, Exchange, Teams, OneDrive, Entra, Defender and many more. DLP control policies are applied across Microsoft 365 services to ensure common data types are detected eg. GDPR, UK finance data, EU finance data etc.

Audit logs

Audit logs are stored for 180 days and live notifications are shared across the development team ensuring changes to access or configuration accidental or otherwise are quickly actioned.

Microsoft's SIEM tool Sentinel is used to store and analyze Azure, Microsoft 365 and Defender logs, 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.

18. Device security

Devices are configured based on industry best practice, some controls include:

- All default accounts are removed or changed
- Drivers and firmware updated to manufacturer's recommend requirements
- No end of life or unsupported operating system or software are allowed
- All software is supported, signed and updated, unused applications are removed or disabled

- Unique local administrator credentials for each device
- BYOD mobile devices are remote managed via work profiles segregating data
- Remote managed security policies including:
    - Lock screen timeout
    - limited privileges
    - full disk encryption
    - removable storage disabled
    - malware/anti-virus signatures
- Remote lockout, wipe and reset
- Remote enforced patch management
- Remote access deployment and revocation
- Remote managed software
- Includes Windows, MacOS, iOS and Android

UEM (Unified Endpoint Management) and password manager are provided by JumpCloud a lead provider of device and access management.

Logging is enabled on all managed devices.

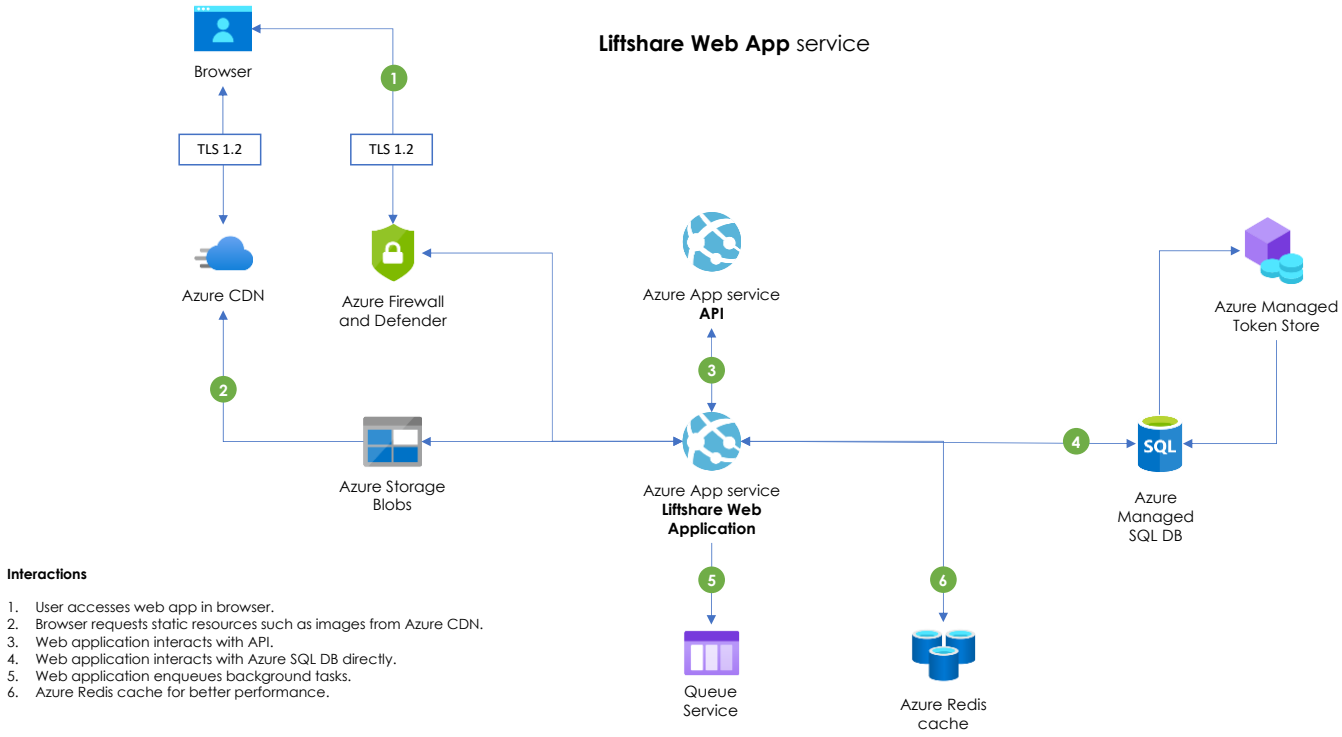
Device and data disposal

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.

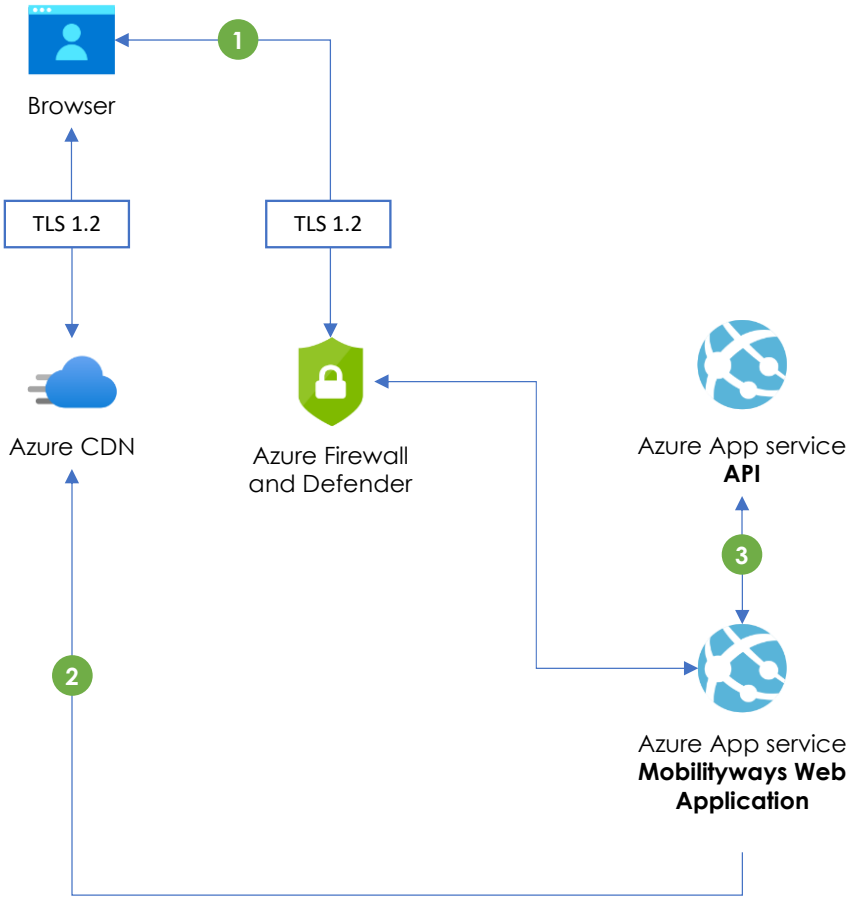
Mobilityways uses suppliers adhering to the WEEE directive, who are GDPR compliant and use best practices and sustainable methods for recycling and disposal of IT Equipment.

Appendix A

Web application flow diagrams

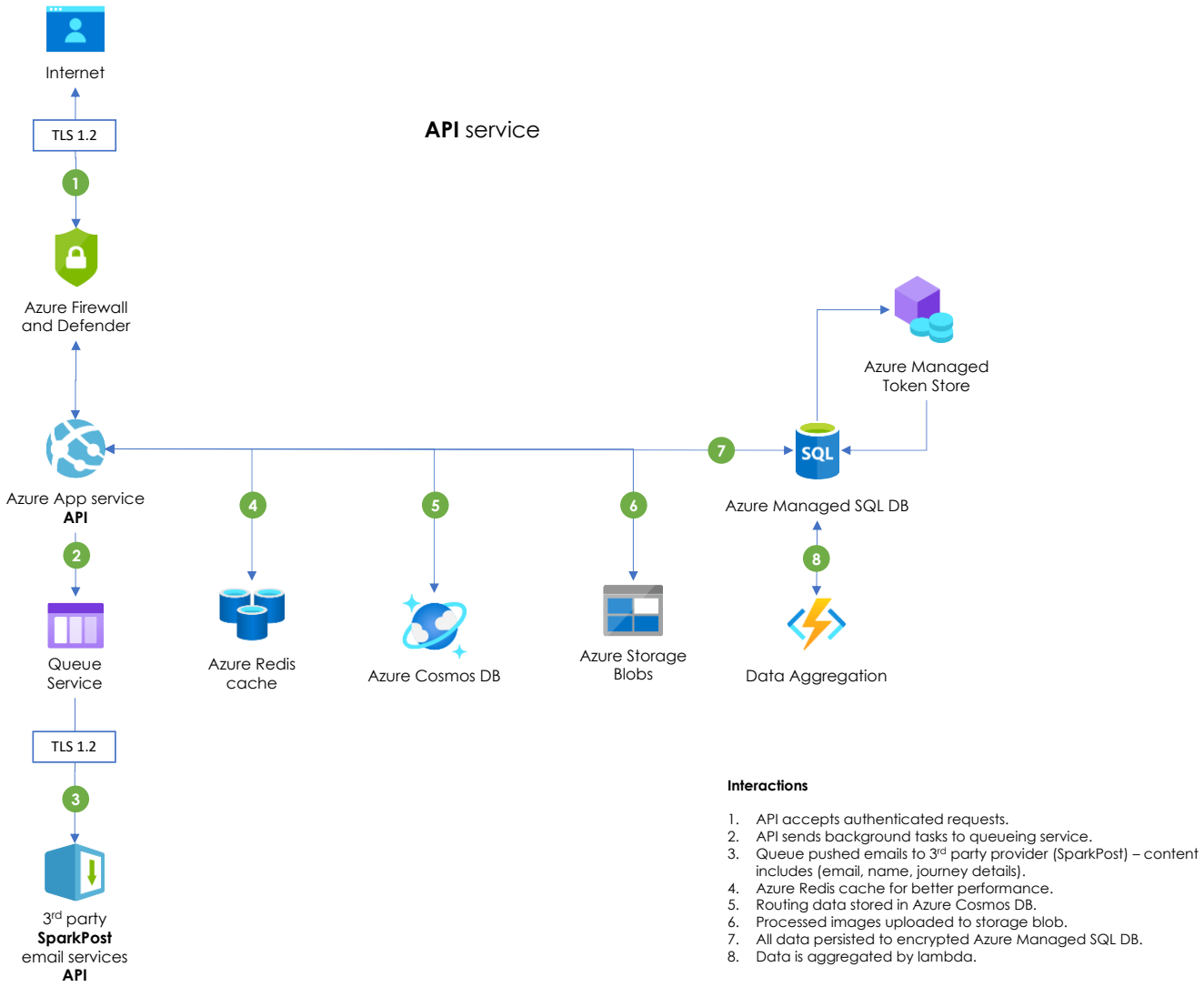


Mobilityways Web App service



Interactions

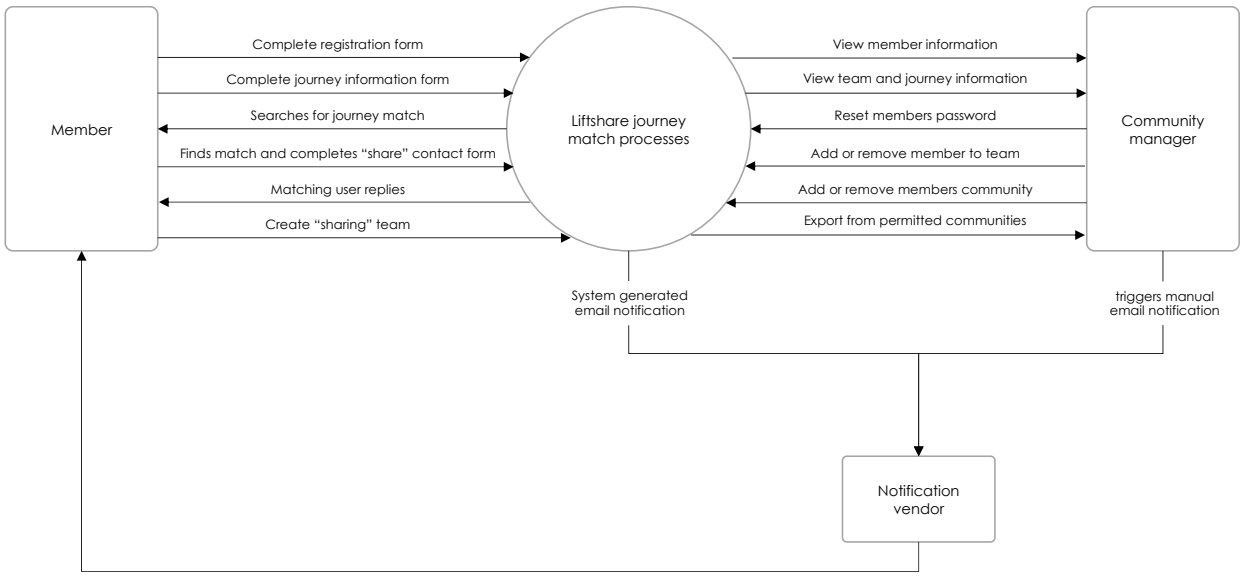
1. User accesses web app in browser.
2. Browser requests static resources such as images from Azure CDN.
3. Web application interacts with API.



End-users interact with the web applications and client-specific websites via the public internet using either liftshare.com, mobilityways.com or a client-specific URLs. 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

Liftshare Web App data flow



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 CommuteIQ 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
Personal Information	First name, surname, password, email address, preferred contact method	Yes	No
	Year of birth	No	No
	Telephone number	No	Yes
	Member bio	No	Yes
Journey Information*	Origin and destination	Yes	Yes*
	Frequency, date, and time	Yes	Yes *
	If the journey is a private group journey	Yes	No* **
	Additional 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 through any network level firewalls, malware scanners and spam filters.

Liftshare platform (Liftshare for work)

- liftshare.com – the main Liftshare software service domain
- *.liftshare.com – API services
- Including domains under all platforms below

Facebook SSO

- connect.facebook.net
- facebook.com

Email

All system notifications are sent from the liftshare.com domain, which should ideally be allow-listed in any email security systems. 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. If possible, please allow-list *@liftshare.com rather than individual 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

- *.mobilityways.com – allow all sub domains
- *.mobilityways.co.uk – allow all sub domains
- *.liftshare.com – API services
- Including domains under all platforms below

Email

Travel plans and surveys are sent from the @mobilityways.com domain this should be whitelisted in any email security systems to ensure your staff receive them.

All platforms (must be included for Mobilityways and Liftshare)

- *.google.com – many domains are used for Google maps and tag manager
- *.googleapis.com – many domains are used for Google maps and tag manager
- *.gstatic.com – font delivery from Google
- *.fontawesome.com – for icon provision
- liftshare.blob.core.windows.net – for static resources – photos, icons, etc
- 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

*The asterisk indicates a wild card character to cover all sub domains (e.g., scripts.liftshare.com, images.liftshare.com, e.liftshare.com etc).

In addition, if you have purchased a custom domain (Website Address) for your site please ensure that this is added to the above list. Custom domains are non HTTPS, the custom domain redirects to the secure Liftshare application with the correct community and branding initialised

3rd Party suppliers

Mobilityways uses a 3rd party email delivery service called 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

Privacy policy

Members Terms of Use

Website Terms and Conditions (liftshare.com)

Appendix D

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 datacentres 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

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. For more information, see Data management at Microsoft.

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

We 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. We also meet country- or region-specific standards, including Australia IRAP, UK G-Cloud, and Singapore MTCS. Rigorous third-party audits, such as those done by the British Standards Institute, verify adherence to the strict security controls these standards mandate.

Azure encryption at rest and in transit

An 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 vaults.

Appendix E

Frequently Asked Questions

Question	Response
Do you have a password policy? Please describe the passwords standards required, including minimum characters, complexity, expiration, application timeout, and reuse.	Service: New users a 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. Administrator/Management roles are enforced with MFA. Internal: Staff are trained and must use a supplied password manager to create and store all passwords, this is periodically checked for a minimum-security score and usage. All default accounts are removed or disabled on new devices. multiple forms of MFA are enabled where available and enforced on all accounts. Employees are requested to carry out an online security challenge every 3 months to ensure secure passwords and safeguards are always in place. Periodic checks by IT staff ensure that staff are meeting a minimum score and are encouraged to improve.
Do you have DDoS protection in place?	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 record of accomplishment 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/
Is all network traffic over public networks to the production infrastructure sent over cryptographically sound encrypted connections?	TLS 1.2 encryption is used to protect all data while in transit between client browser and our servers as well as connectivity between applications and databases. 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.
Is all data encrypted at rest and during transit? What type of encryption is used and what level? How are keys managed?	Keys are managed by CTO or in the case of the TDE protector, by a service-managed certificate. Within the web application, data is processed and stored in a SQL Server database, logically partitioned by client community. Passwords are stored as hashes using PBKDF2 with HMAC-SHA256, 128-bit salt, 256-bit subkey, and at least 10000 iterations. All data is encrypted at rest and in transit. Keys rotated at least every 90 days. Keys are stored in an Azure Key Vault. Keys are accessed via the azure portal by privileged admins with MFA enforces. Application access to key vault via service principal managed identity. TDE encrypts the storage of an entire database by 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. TDE protector is a service-managed certificate. All encryption happens at the data access layer with the exception of passwords which are encrypted in memory using PBKDF2 with HMAC-SHA256, 128-bit salt, 256-bit subkey, and at least 10000 iterations
Do you perform penetration testing? If so, what is the frequency, scope, and methodology used?	AppCheck – is an automated web application and vulnerability scanning platform, scans are executed on each web app every 2 weeks.

	Site testing is staggered by a week to allow time for scans to complete. We use App checks full web application scans - "More basic vulnerability scanners may solely identify CVEs – common cybersecurity vulnerabilities that are identified based on recognised patterns and software versions. However, AppCheck's web application scanner is designed by experienced penetration testers, making it more thorough and accurate at identifying complex issues. The AppCheck crawling engine uses a combination of application modelling techniques and subtle heuristical cues to automatically discover the complete attack surface of any given application in the shortest time possible. The algorithms are designed to model how a penetration tester or attacker would explore the application, to detect subtle vulnerabilities that other tools often miss and opening up attack vectors that are inaccessible to less sophisticated crawlers." Whilst Mobilityways does not perform our own external manual tests on the platform, throughout the year several client-initiated tests will be performed. We welcome clients to have their own penetration test performed, prior approval is required from Mobilityways before any penetration tests are carried out.
Are audit logs centrally stored in a secure platform and retained for a minimum of 180 days? How do you log and alert on relevant security events?	MS Azure configuration logs are 180 days this is not configurable. Security event logs are part of the Microsoft services that we use. Azure Dev Ops, GitHub and Microsoft 365 all have detailed event logs. All configuration changes are immutably logged with who, what and when. Microsoft SIEM tool Sentinel is used to store and analyze Azure, Microsoft 365 and Defender logs, Sentinel retains these logs for 90 days. Microsoft Advanced Threat Protection and Microsoft Defender have robust logs of all potential events. Application usage logs exist for the lifetime of the client. Our administration dashboard also logs all commands run with who, what and when. IP addresses are not logged for dashboard usage. Logs are sanitized to make sure passwords are not logged. Logs are maintained and stored for a minimum of 180 days.
Do you have a structured patch management program in place with capability to patch vulnerabilities across all of your systems?	Mobilityways uses Microsoft's Managed Azure services to ensure that we provide the most secure hosting environment for our software services. We are fully serverless and all management or services are provided by Microsoft's top-tier service. Excerpt from Microsoft Documents: App Service is a Platform-as-a-Service, which means that the OS and application stack are managed for you by Azure; you only manage your application and its data. More control over the OS and application stack is available you in Azure Virtual Machines. With that in mind, it is nevertheless helpful for you as an App Service user to know more information, such as: Azure manages OS patching on two levels, the physical servers and the guest virtual machines (VMs) that run the App Service resources. Both are updated monthly, which aligns to the monthly Patch Tuesday schedule. These updates are applied automatically, in a way that guarantees the high-availability SLA of Azure services. When severe vulnerabilities require immediate patching, such as zero-day vulnerabilities, the high-priority updates are handled on a case-by-case basis. https://docs.microsoft.com/en-us/azure/app-service/overview-patch-os-runtime

Do any third parties have access to personal data? If so, are these third parties contractually obligated to comply with a set of security standards for data processing? How do you verify compliance to such standards?	Mobilityways uses a 3rd party email delivery service called Sparkpost EU for outbound transmission of emails originating from the Mobilityways system. Sparkpost EU is designated a permitted sender in the SPF policy and DKIM authentication is used to indicate emails originating from us. Sparkpost EU uses opportunistic TLS for outbound traffic, which will depend on whether the receiving SMTP servers supports TLS. SparkPost EU is SSAE-16 SOC II Type 2 Certified and GDPR ready. Email marketing is via 3rd party service Brevo they are responsible for the delivery of surveys, campaigns and marketing materials. Brevo's email delivery service and data storage is located within Western Europe. Brevo is ISO27001:2013-certified, GDPR, and CCPA compliant.
Is MFA required for employees/contractors to log in to production systems supporting the services provided?	MFA is required on all systems our employees' access, including our own bespoke backend. We are a small team, and some responsibilities are shared, in these cases shared authentication is secured via password a password management system and MFA. Mobilityways staff are provided with a Password management service and accounts, it is company policy to use the service to generate and store all account information.
Do employees/contractors have ability to remotely connect to your production systems? What controls are in place to limit access and data security in our development environment?	All privileged role access is logged and technical controls including IP restriction, physical token authentication, time-based MFA and various other forms of MFA. Our bespoke admin/backend system also employee similar methods. Source control, database access, dev ops is restricted to development staff. Access roles are in place to further limit certain functionality to super admins. New staff are allocated access based on role requirements, change of role also has to undergoing same requirements. Staff are only given access to systems that are required for their role. All development environments are hosted in the cloud via MS azure app services, controls are in place to limit access to authorised developers.. All development data is fully anonymised.
Does Mobilityways use a VPN or Proxy service to access it services?	Mobilityways employees no longer use a VPN to access any resources, we have relocated all our hosting services, business functions and storage to cloud providers. No business functions or data is stored at our Norwich location. Many controls are in place to control access to our SaaS/PaaS services including IP restriction, enforced MFA methods, managed strong unique password, live notifications of non-conformities to policy. This has allowed Mobilityways to leverage the supplier's superior security and resilience, allowing our small team to concentrate on the controls to securely manage and control access to these services. An exception to this is a VPN service to allow remote administration of our office WIFI router, this access is restricted privileged IT admin.

Appendix F

ISO 27001:2022 certificate no 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

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 in the UK.

This is in accordance with the Statement of Applicability **Version 1 and is dated 22/6/2023**.

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: 19 October 2023
Expiry date: 18 October 2026
Subject to annual assessments.

Authorised by

Mike Tims
Chief Executive Officer

british-assessment.co.uk
Certificate issued by Amtivo Group Limited T/A British Assessment Bureau Ltd.
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.

Mobilityways ISMS policies

- Acceptable Use Policy
- Access Control Policy
- Business Continuity Plan
- BYOD Policy
- Change Management Policy
- Clear Desk and Screen Policy
- Cryptography Policy
- Data Breach Policy
- Data Handling Policy
- Data Protection and Information Security
- Information Backup and Restore Policy
- Information Transfer Policy
- Operations Security Policies and Procedures
- Password and MFA policy
- Patch and Vulnerability Management Policy
- People Policies
- Physical and Environmental Security Policy
- Remote and Hybrid Working Policy
- Secure Systems Engineering Principles
- Supplier Management Policy
- User endpoint device policy

Cyber essentials certificate

CYBER ESSENTIALS

CERTIFICATE OF ASSURANCE

Mobilityways Ltd

10-12 St Andrews Street Norwich NR2 4AF

COMPLIES WITH THE REQUIREMENTS OF THE CYBER ESSENTIALS SCHEME

NAME OF ASSESSOR : Nathan Warren

CERTIFICATE NUMBER : 5b2828b0-f9d1-4e56-a9de-b9a0860fea8b

DATE OF CERTIFICATION : 2024-05-03

PROFILE VERSION : 3.1 (Montpellier)

RECERTIFICATION DUE : 2025-05-03

SCOPE : Whole Organisation

SCAN QR CODE TO VERIFY THE AUTHENTICITY OF THIS CERTIFICATE

CERTIFICATION MARK

CYBER ESSENTIALS CERTIFIED

CERTIFICATION BODY

reformit Technology Peace of Mind

CYBER ESSENTIALS PARTNER

IASME CONSORTIUM

The Certificate certifies that the organisation was assessed as meeting the Cyber Essentials implementation profile and thus that, at the time of testing, the organisations ICT defences were assessed as satisfactory against commodity based cyber attack. However, this Certificate does not in any way guarantee that the organisations defences will remain satisfactory against a cyber attack.

Reference

Microsoft 365 Teams security

https://docs.microsoft.com/en-gb/microsoftteams/teams-security-guide

Microsoft Azure Managed apps patching
https://docs.microsoft.com/en-us/azure/app-service/overview-patch-os-runtime

AppCheck penetration scanning platform

https://appcheck-ng.com/

Sparkpost EU – polices

https://www.sparkpost.com/policies/

Brevo

https://www.brevo.com/features/data-security/

https://www.brevo.com/legal/privacypolicy/

Microsoft services compliance

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

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

Google services compliance

https://cloud.google.com/security/compliance/compliance-reports-manager#/Industry=Industry-agnostic&Region=Global&ProductArea=Google_Cloud