Mobilityways Data Protection and Information Security Policy

Signed:  Date: 26/01/2023

Name & Job Title: Julie Furnell
Managing Director

Table of Contents

Document Version History

Revision	Date	Changes
Draft A	April 2018	GDPR compliance
Draft B	October 2018	Azure migration
VLS003	April 2019	Update to Privacy Policy
VLS004	May 2019	Update to cloud diagram and removal of Amazon
VLS005	March 2021	Review of online services, addition of SharePoint and Mobilityways, updated password security
VLS006	Feb 2022	Annual review, addition of FAQs table and references. Web application architecture and data flow diagrams.
VLS007	Jan 2023	Access requirements updated Dashboard admin roles added Additional Azure Physical security information SSO details Sparkposts EU supplier change Mobilityways company name change

1. 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.

Scope

This document is communicated to all company personnel who all receive the necessary training during the induction process to ensure they are aware of their responsibilities for information security.

2. Human Resources Security

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

Each member of staff is made aware of the fundamentals of information security during their induction process and during on-going job-related training. Business users are trained in how to run & access our systems correctly and the IT team ensures the use of secure passwords to help prevent unauthorised access.

MFA (multi-factor authentication) is enforced on accounts, devices and websites where available.

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/Leavers

Prior to new staff joining Mobilityways, the IT department are presented with a process form outlining the access controls to be available to that candidate and this will be reviewed if or when that member of staff changes roles or leaves the organisation. A Confidentiality Clause is signed and, upon leaving the employment of Mobilityways, the IT department are presented with an exit process form ensuring that access controls are removed. Key members of staff with restricted access privileges retain access control only whilst they remain in a position requiring such access.

Internal Mobilityways policies include -

- BYOD (Bring Your Own Device)
- Data Security Policy
- Privacy Notices for Employees and Contractors
- Environmental Policy
- Homeworking Policy
- Corporate Social Responsibility Policy
- Physical Security Policy.

3. Physical & Environmental Security

Software cloud environment

Our software applications are hosted in a highly secure managed environment provided by Microsoft, physically located at the Azure UK South data centre. Microsoft are industry leaders in ISO certifications which help to ensure the security of Mobilityways's systems through 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/

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 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/

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.

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.

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.

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.

Business cloud collaboration

Mobilityways's business data and staff collaboration tools are provided by Microsoft 365 platform including Sharepoint, Exchange, Active Directory and more. Software development and bug tracking is handled by Atlasssians JIRA and Confluence applications. CRM is provided by HubSpot. Password management and account sharing is provided by LastPass.

Staff are trained to use each application and to understand the importance of data security under GDPR. All accounts have very strong passwords and MFA enforced.

Office environment

Mobilityways's Norwich office is only accessible to members of staff and is secured with door entry systems, monitored intruder alarms & CCTV. All internal office file servers, infrastructure components are in a secure environment with access restricted to key members of staff. Internal servers are only accessible on the internal private office network, VPN access is restricted to key IT staff.

Usage of external storage devices is prohibited by company policy and Windows policies, only privileged IT admins can store specific information on encrypted secure device (encryption keys, password backups, etc) and these are stored in a fireproof safe within the secured server room.

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.

4. Personal Data Breach Reporting

Mobilityways recognises a Personal Data Breach

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than about losing personal data and includes, but is not limited to:

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a controller or processor
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity, or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted, or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

Addressing Personal Data Breaches

On becoming aware of a breach, Mobilityways will endeavour to contain it and assess the potential adverse consequences for individuals. Mobilityways staff are equipped to escalate a security incident to the appropriate person within our organisation to determine whether a breach has occurred. If a breach of personal data has occurred, said breach will be addressed and the ICO notified within 72 hours if required, even if we do not have all the details yet. An investigation will be conducted to determine whether the breach was a result of human error, or a systemic issue and steps put in place to ensure such a recurrence is prevented.

Reporting a Personal Data Breach

The potential detriment to individuals is the overriding consideration in deciding whether a breach of data security would be reported to the ICO. Detriment includes emotional distress as well as both physical and financial damage. Detriment includes but is not limited to:

- exposure to identity theft through the release of non-public identifiers
- information about the private aspects of a person's life becoming known to others.

The extent of detriment likely to occur is dependent on both the volume of personal data involved and the sensitivity of the data. Where there is significant actual or potential detriment because of the breach, whether

because of the volume of data, its sensitivity, or a combination of the two, Mobilityways will report. Where there is negligible risk that individuals would suffer significant detriment, for example because a stolen laptop is properly encrypted or the information that is the subject of the breach is publicly available information, Mobilityways will not report. The volume of personal data lost / released / corrupted: Mobilityways will report to the ICO where a large volume of personal data is concerned and there is a real risk of individuals suffering some harm. In relation to deciding on what constitutes a large volume of personal data, Mobilityways will consider on its own merits.

In the event the Mobilityways data controller is unsure whether to report, the breach will be reported. The sensitivity of the data lost / released / corrupted: Mobilityways will report to the ICO where smaller amounts of personal data are involved, the release of which could cause a significant risk of individuals suffering substantial detriment, including substantial distress. This is most likely to be the case where that data is sensitive personal data as defined in section 2 of the DPA.

Serious breaches will be reported to the ICO using the DPA security breach helpline on 0303 123 1113 (open Monday to Friday, 9am to 5pm), alternatively, we may report in writing using the DPA security breach notification form.

Information to be Reported to ICO in the Event of a Personal Data Breach:

- Mobilityways organisation details - to include the details of Mobilityways Data Controller and full contact details.
- Details of the Data Protection Breach - to include a full explanation of the incident:
- how and when the incident happened
- explanation for any delay in reporting
- measures Mobilityways have taken to prevent an incident of such nature occurring
- extracts of policies and procedures considered relevant to the incident with explanation of which of these were in place at the time of the incident together with dates on which they were implemented
- Personal Data Placed at Risk – specifying if any financial or sensitive personal data has been affected together with details of the extent.
- The number of affected individuals.
- Whether the incident has been reported to the affected individuals.
- Details of potential consequences or adverse effects on the individuals.
- Whether or not any affected individuals have submitted complaints to Mobilityways about the incident.
- Containment and Recovery – steps Mobilityways have taken to minimise / mitigate the effect on the affected individuals; whether the data placed at risk has been recovered together with full details of such implementation; steps taken to prevent recurrence of such an incident.
- Training and Guidance – provide extracts of Data Protection Act Training and Guidance provided to all staff together with confirmation of whether this training is mandatory and whether the staff members involved in the incident had received training and when.
- Previous Contact with ICO – details of any previous reported incidents to the ICO within the past two years together with details of such an incident and the ICO reference number.
- Details of whether other international data protection authorities have been notified.

- Details of whether the police have been informed of the incident. If so, provide details and specify the force concerned.
- Details on any other regulatory bodies reported to.
- Details of any media coverage.

Informing Affected Individuals about a Personal Data Breach

If Mobilityways has an obligation to inform the affected individual about a Personal Data Security Breach, the following specifics will be offered without undue delay:

- Nature and details of risk
- Specific, clear advice on steps they can take to protect themselves
- Contact details for Mobilityways
- Description of the consequences of the personal data breach
- Details of the measures taken, or proposed action to be taken, to deal with the personal breach and including any measures taken to mitigate any possible adverse effects.

Documentation of Breaches

All breaches are documented regardless of whether they needed to be reported or not. Documentation will include the facts relating to the breach, the effects and remedial action taken. This will form part of Mobilityways's Business Continuity Plan and will be recorded as such.

Data Protection Impact Assessment

Mobilityways does not process data in situations where individual's data is at substantial risk in terms of protection.

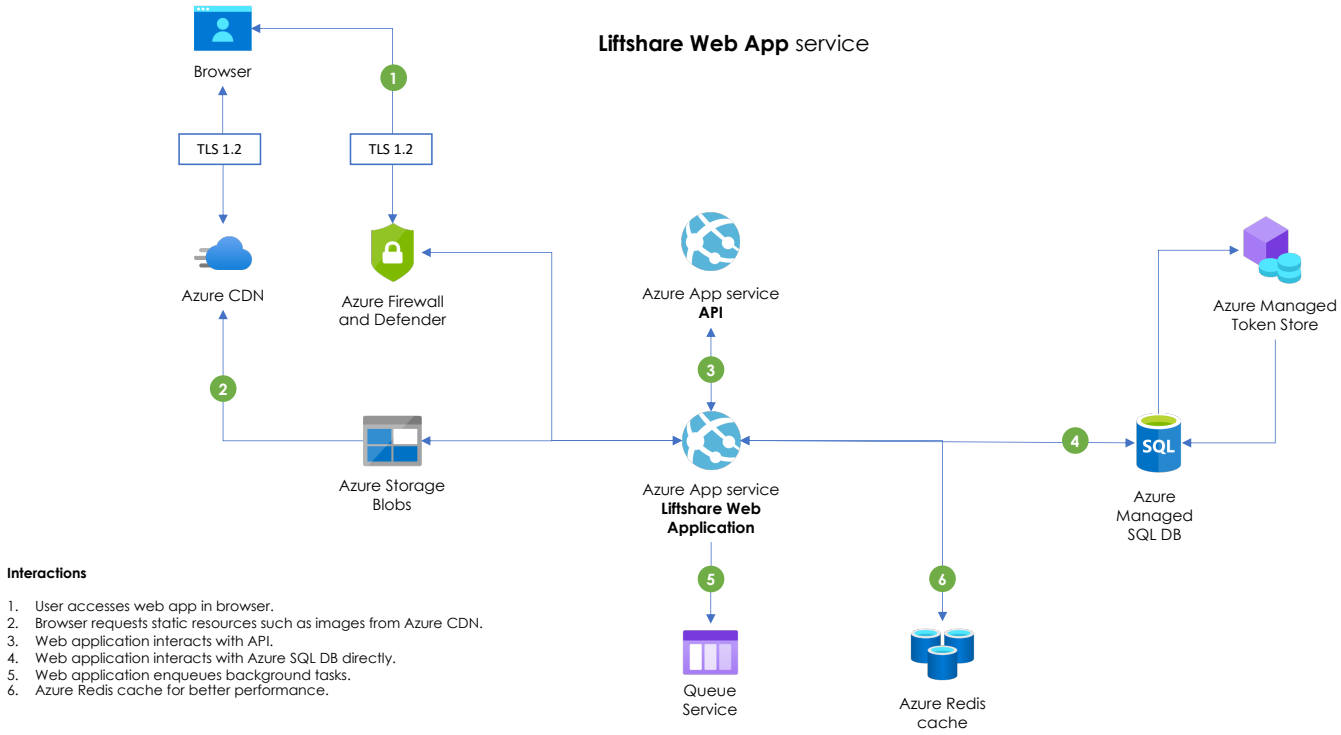
Mobilityways only uses well established and well vetted technologies stacks and does not have any plans or intentions to use any other technology at this point.

Mobilityways are not, and have no plans to, use profiling in a way that uses sensitive data.

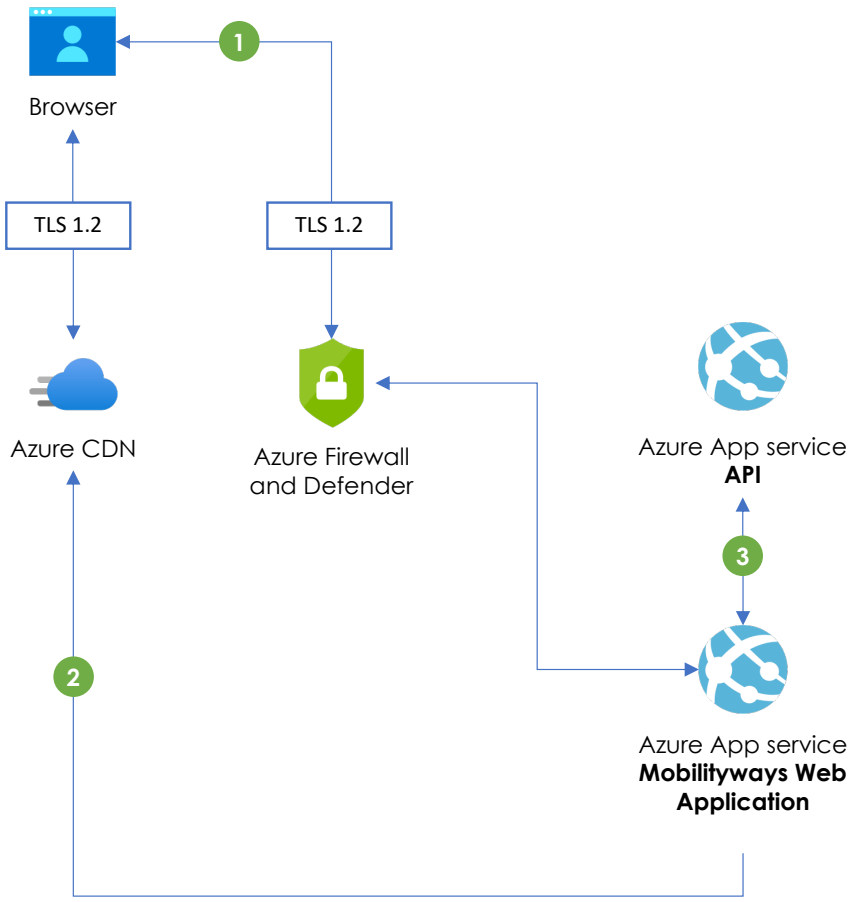
Mobilityways does not store or process any special category data, nor has any plans or intentions to do this.

If any of the above changes, we will carry out a DPIA in accordance with GDPR. This will be completed by Mobilityways's Chief Technical Officer, Head of Product, and our Managing Director.

5. Web application topology

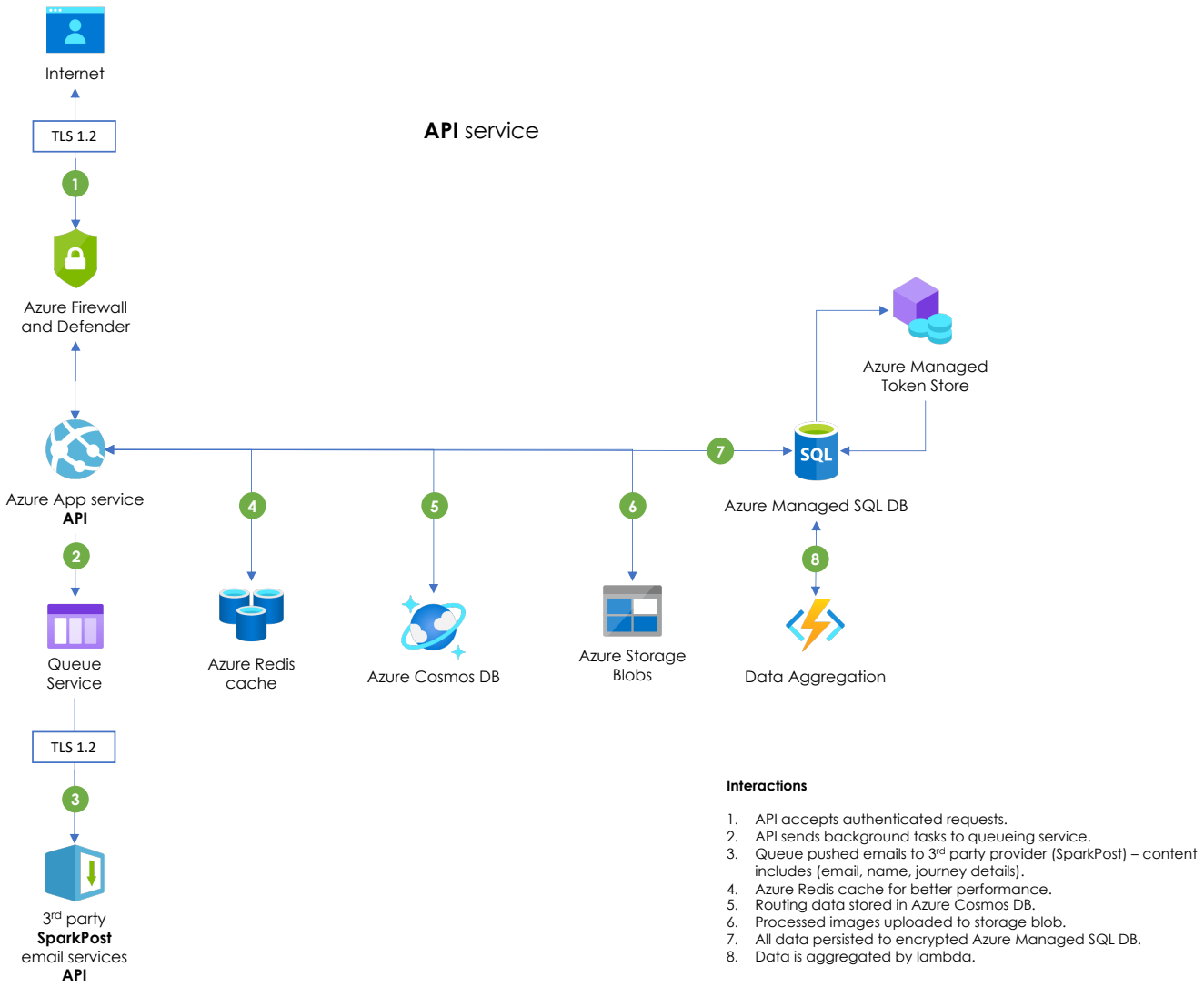


Mobilityways Web App service



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.

Encryption and Passwords

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

All data is encrypted at rest and during transit.

Azure managed keys are used, encryption keys are stored in a secure key vault, key generation, rotation, and storage are managed by MS Azure. Keys are rotated at least every 90 days.

Passwords are never stored in plain text; 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. Original passwords cannot be retrieved.

Security by Design

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.

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, automated testing, code review, integration testing, staging testing, release to production and review.

Bi-weekly automated, authenticated penetration test of web applications and infrastructure 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.

The Liftshare for work web application is surfaced by means of a white-label theming 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.

How is data accessed

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.

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 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.

Developers and Database administrators

All data within of our development environments is fully anonymised. Database administrators have full access to the data stored in the database to perform their roles. Access logs are stored for 90 days and live notifications are shared across the development team ensuring changes to access or configuration accidental or otherwise are quickly actioned.

Supporting services and suppliers

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

Managing our suppliers

Mobilityways has a documented supplier management process to ensure only that all suppliers meet or exceed our requirement for transport, processing and storage of any data required to provide and support our applications and services.

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

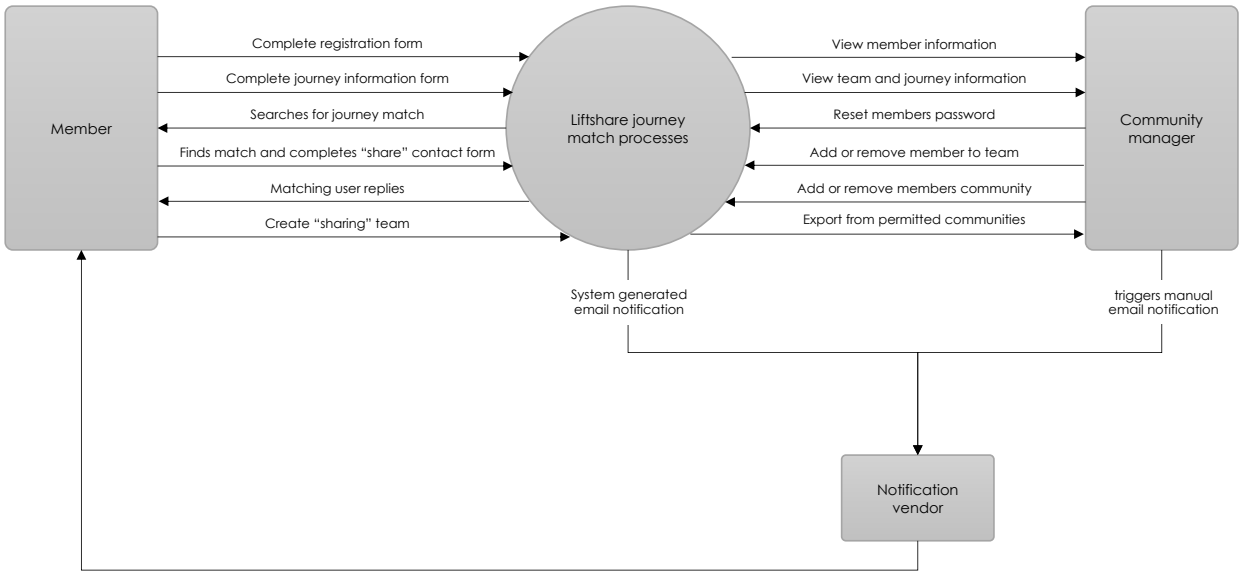
The application is supported by Google Maps Business APIs which deliver geospatial route calculation and geolocation services used from within the application tier, along with serving graphical map image tiles to client browsers.

Sparkpost email delivery

Email delivery is via a 3rd party email delivery service 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 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.

Liftshare for work high level data flow diagram

Liftshare Web App data flow



Access roles available within the dashboard services

Role	Description of access
SuperAdmin	Developer access, read and write access to client statistics and products
Admin	Read and write access to client statistics and products
CommunityAdmin	Read and write access to a specific communities statistics and systems
CommunityMonitor	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)
MemberExportAdmin	Allow admin users to export email addresses from the Dashboard
CommunityParkingPermit	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.
TravelPlanAdmin	Access to a specific accounts Mobilityways Personal Travel Module
TravelPlanMonitor	Access to high level statistics for an account, no personal data for the Personal Travel Plan Module.
ScopingUser	Access to scoping report and map for a specific account. Has access to create a sharing link for the map.
SurveyAndAcelAdmin	Read and write access to a specific accounts survey and ACEL module.
SurveyAndAcelMonitor	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.
ContactMonitor	Access to view-only contacts on a Mobilityways account
ContactAdmin	Allows admin to see, create, edit and delete contact details on Mobilityways

6. Access Control

Mobilityways implements access control across its office network, IT systems and services to provide authorised personal with only the access they require to perform their role. We have the following four roles:

- Guest users - Limited to Mobilityways's office guests, limited access to internet traffic.
- Standard users - Mobilityways provides each member of staff with access to the office internet, Microsoft 365 services and our client administrative systems. All user activity is monitored and each device has limited privileges preventing any software from being installed.
- Privileged users - Are trusted members of staff who are responsible for user access to external systems, these users are responsible for the day to day running of all services and thus have access to user account management and all essential services.
- Administrators - A higher level role with access to all systems and services used for generating accounts and high-level administrative functions for onboarding and off-boarding users, role assignment to systems and services. These users are responsible for overall security and are accountable for any security issues.

IT Personnel are required to perform regular audits of the network infrastructure to check for common vulnerabilities and ensure devices such as routers, firewalls, servers, etc are using up to date and justified access control rules, devices and systems are up to date with firmware and security patches.

Device configuration

Newly acquired devices are assessed as part of installation and new configuration process. As part of industry best practise, all default accounts are removed or changed on any new device. Any necessary ports or exceptional access requirements are evaluated and approved by a business case. All devices are driver/firmware updated and OS patched according to manufacturer's recommend requirements. All software is supported, signed and updated. All unnecessary applications are removed or disabled. All devices are again reviewed by the IT team in accordance with this process before being reassigned to other staff members.

- Unique administrator credentials are created for each device, Limited access local accounts are created for employees with Group policies to enforce security configuration.
- Employees have to register BYOD device and comply with the BYOD policy. They are instructed to only use the device to access business communication systems.
- Mobilityways 's bespoke Dashboard are protected by enforced 2FA with a physical key which is allowed only on their provided device. Passwords are unique and strong and are managed.

Device Encryption

All devices with storage capacity have encryption enabled as part of new device configuration process and are checked as part of the re-assignment process.

Secure backups

Backups of Microsoft 365 business data are stored within the office network in a centralised enterprise level NAS with multiple levels of redundancy. Data is stored on encrypted volumes and access is restricted to privelages individuals. External access is provided to administrators only to manage backups.

No backups exist at our office location for any data stored within the sites and services we provide.

BOYD and home working

Each user is bound by the Mobilityways acceptable use policy (including the BOYD and Home Working Policies) present in the staff handbook which covers the use of Mobilityways networks, users are also bound by both the Data Protection Act 2018 as well as The Computer Misuse Act 1990.

Internal password policy

Company policy dictates that any password to access all websites, systems or services is generated and stored using our Enterprise level 3rd party password management service provider. This is monitored and audited on a regular basis to ensure staff are using it and that staff are exceeding a set minimum security score based on complexity and other criteria. The top tier service provider is built on AES-256bit encryption with PBKDF2 SHA-256 and salted hashes to ensure data protection in the cloud.

The provider operates on a zero-knowledge security model, data is encrypted at the device level with AES-256 encryption before syncing with TLS to protect from on-path attackers.

The password manager account is further protected by a 2FA physical device provided to all employees.

7. 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 make 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

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.

Facebook SSO

- connect.facebook.net
- facebook.com

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. 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. 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.

8. Incident Management

Incidents are reported through our support ticket system, tickets are prioritised, fixed, tested and released according to our change management policy.

Emergency fixes are reviewed by the Product Development team in conjunction with our account managers and are tracked through our IT ticketing system.

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 emergency response process in place, which enables a fast and effective response to serious attacks.

9. Business Continuity Management

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 monthly 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.

Risk Assessment and Treatment

Internal information risk analysis is carried out for critical systems and environments. The analysis determines the risk via a business impact assessment and threat and vulnerability analysis. The analysis helps to identify security controls and evaluate the costs of these and determine the limit of such controls.

The following Security measures are in place to mitigate risk

Security Metric	Monitoring Frequency	Reported to
Penetration Tests	every 2 weeks	Product Manager
Security Patching	Monthly	Management Team
Infrastructure Compliance Monitoring	Quarterly	Management Team
Network Security Device Change Control	Quarterly	Management Team
Application Code Change Control	Fortnightly	Product Manger
Password standards	Quarterly	Management Team
User management	Bi-monthly	Office manager

Use of external storage devices is prohibited by company policy and local configuration policy. Sharing of business data is controlled via limited accounts in Microsoft 365 and company policy.

Organisation data is stored in Microsofts SharePoint cloud, access is limited to only the document libraries required to complete their role. All accounts have 2FA enforced and strong unique passwords managed by our password manager service.

Data Loss Prevention policies are applied across Microsoft 365 services to ensure common data types are detected eg. GDPR, UK finance data, EU finance data etc.

Microsoft 365 data is backed up on change to our office-based enterprise NAS, minimising the risk of any loss of data if Microsoft is either in accessible or has multiple failures.

Employees work from Microsoft OneDrive accounts to minimise business downtime in the event of hardware failures and to allow continuous backup of critical data.

All privileged role access is logged and technical controls including IP restriction, physical token authentication and various other forms of MFA. Our bespoke admin/backend system also employee similar methods of control.

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 Microsoft Azure Devops, access is limited to our internal development team.

10. Communications and Operations Management

Mobilityways have implemented processes that ensure that key staff can share knowledge with other team members to enable robust succession planning. New software features are planned and developed in a collaborative, agile manner; ensuring internal knowledge & key decisions are documented & retained within our teams.

Systems are fully scalable and designed with sufficient capacity to cope with anticipated surges in traffic. Systems are secured by using a range of inbuilt, platform & network security controls including full auditing and Microsoft Advanced Threat Protection. Microsoft Advanced Threat Protection allows us to monitor user, device, and resource behaviour, and detects anomalies right away with learning-based analytics, as well as identify and investigate suspicious user activities and advanced attacks.

Computer systems & networks are monitored to identify potential security breaches. System monitoring and scanning is carried out on known vulnerabilities by port scanning and commercially released vulnerability checkers.

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 company procedures.

Third parties who have approved access to systems are uniquely identified and are supported by contractual agreements. Personal computers used by staff working in remote locations are tested prior to use and are bound by the Home Working Policy.

All staff are made aware of the requirement for secure disposal of confidential and sensitive information. Procedures for handling and storage of information are in place. System documentation is protected against unauthorised access by passwords.

11. Acquisition, Development and Maintenance

System development activities are performed in a development environment, separate from the production environment. Development environments are further protected by IP restrictions.

Microsoft advanced threat protection for real time monitoring of all our systems, which will alert and log any activity off baseline (e.g. admin login attempts from a new IP).

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 Product 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 sign off.

Results are documented, approved by internal users, and signed off by the Product Owner.

Penetration testing

Mobilityways sources 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/

The articles below outline how AppCheck identifies the top 10 OWASP vulnerabilities and helps to mitigate risk.

https://appcheck-ng.com/appcheck-vs-owasp-top-10

https://appcheck-ng.com/appcheck-the-owasp-top-10-privacy-risks

Penetration test reports are provided on request. We welcome client-led penetration tests and are always happy to work with internal or 3rd party security teams to facilitate additional web application or infrastructure testing if required. Prior approval is required from Mobilityways before any penetration tests are carried out.

12. 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 complies with all legal and regulatory requirements for data protection and audit procedures. All staff are given data protection training both during their initial corporate induction and on an on-going basis.

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.

It is a legal requirement for Mobilityways and its employees to always comply with these principles in its information-handling practices. Each employee holds the following responsibilities in relation to personal information they may handle as part of their work, and the following guidelines are always complied with. Data must be:

- Processed fairly, lawfully, and not be processed unless certain conditions are met in relation to personal data and additional conditions are met in relation to sensitive personal data.
- Obtained for one or more specified and lawful purpose, and not processed in a manner incompatible with these purposes.
- Adequate, relevant, and not excessive. Only data which is needed is collected. Historic data will be checked to ensure there is a sound business reason requiring the information to be held.
- Accurate and up to date.
- Not kept for longer than is necessary. Distinct categories of data will be kept for retained for different periods of time, depending on legal, operations, statistical and financial requirements.
- Processed in accordance with the rights of the individual.
- Secure, technical and organisations measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss or disposal of, or damage to, data. Data stored on external storage is prohibited by company policy and configuration policy. All employees are responsible for the security of their own devices. Sensitive information held electronically will be stored confidentially by means of password protection, encryption or coding and only authorised employees have access to that data. All electronic business data is automatically backed up to mirrored file servers off-site to protect against loss or corruption.
- Not transferred to a country or territory outside the European Economic Area unless that country ensures an adequate level of protection of the processing of personal data.
- Do not give out confidential personal information except to the data subject. It should not be given to any other unauthorised third party unless the data subject has given their explicit consent.

- Be aware that those seeking information sometimes use deception to gain access to it. Always verify the identity of the data subject and the legitimacy of the request, particularly before releasing personal information by telephone.
- Ensure any personal data you hold is kept securely, either in a locked filing cabinet or, if computerised, it is password protected and/or encrypted.

Compliance with the Act is the responsibility of each employee and any breach could be subject to disciplinary proceedings.

Please see Table 1 (below) 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. Passwords set by members are not stored.

Table 1: 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.

Cyber Essentials

Mobilityways holds Cyber Essentials certification. The Cyber Essentials scheme is aimed at highlighting security controls that will help organisations mitigate the risk to their IT systems from internet-based threats. It is administered by the UK government and helps to protect personal data in our IT systems from the most common cyber threats. As there is no solitary product that can provide complete security for a business, Cyber Essentials covers 5 areas

for keeping information secure:

- boundary firewalls and internet gateways
- secure configuration
- access control
- malware protection
- patch management and software updates.

By having certified cyber security, we have a clear picture of our organisations cyber security level and promise our customers that we have cyber security measures in place.

Microsoft's 365 services

Operating a global cloud infrastructure creates a need to meet compliance obligations and to pass third-party audits. Auditable requirements come from government and industry mandates, internal policies, and industry best practices. Continuous compliance refers to our commitment to evolve the Office 365 controls and stay up to date with IT standards and regulations.

As a result, Office 365 has obtained independent verification, including ISO 27001, ISO 27018, and SSAE 16 audits; is able to transfer data outside of the European Union through the EU Model Clauses; is willing to sign a HIPAA Business Associate Agreement (BAA) with all customers; has received authority to operate from a U.S. federal agency under FISMA; and has disclosed security measures through the Cloud Security Alliance's public registry. Office 365 extends the controls implemented to meet these standards to customers who are not necessarily subject to the respective laws or controls.

Microsoft's Azure platform

Azure offers a broad set of key 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 document library for all the Azure's security advantages.

Azure security documentation | Microsoft Docs

13. Asset Management & Data Handling

Access to critical information is restricted to authorised individuals through password protection and role-based access control. Authorised individuals are aware of their responsibility for critical information via their job descriptions and our corporate induction process. Essential information (unique identifiers, version numbers & physical locations) pertaining to hardware and software are logged by the IT team.

An asset register of all IT equipment that includes devices that can store data, are registered, and managed via an asset management register. Regular audits are conducted to ensure this register is maintained.

All Mobilityways staff as part of their data protection training is required to acknowledge and sign an agreement that they have read and understood the Mobilityways data security policies. As part of the briefing process there is a high emphasis on data handling and transmission as this is critical for data security.

Mobilityways ensure that the transmission of personal or commercially sensitive data is not permitted without the appropriate level of encryption applied. Data must only be stored within the Mobilityways provided services and not stored or transmitted via any other unauthorised services. This includes but is not limited to:

- External storage devices
- unauthorised third-party services
- storage on mobile devices
- on any other un-encrypted device.

Under no circumstance should personal sensitive data be printed physically, if this occurs the physical copy must be destroyed immediately via the Mobilityways document disposal procedures.

Commercially sensitive data if printed physically must be stored securely in a locked cabinet and destroyed immediately once the document is no longer required via the Mobilityways document disposal procedures.

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, 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, every document generated must contain one of the following data classifications:

- Confidential Data

    - Data is classified as confidential when the disclosure, alteration or disposal of data could cause significant risk to Mobilityways its clients and users. An example of confidential data includes unencrypted commercially sensitive client and user information. Any client data exports taken from Mobilityways systems should be classified as confidential and be handled in line with any confidentiality agreements in place.
    - Access to confidential data is managed from inception to disposal. Access to this data will be granted only to those who require access to perform their job role. Access to this data is approved on a case-by-case basis by the network administrator who is responsible for the data.
    - Confidential data is classified as extremely sensitive and may have personal privacy considerations, be restricted by confidentiality agreements and/or by law. The negative impact on Mobilityways its clients and users should this data be incorrect, improperly disclosed, or not available when needed is typically severe.
- 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 and its clients. An example of internal/private data includes commercial discussions between Mobilityways /client, scheme statistics. All data that is not explicitly classified as confidential or public data should be treated as internal/private data. Reasonable levels of security controls should be applied to internal data.
    - Access to this data will be granted only to those who require access to perform their job role. Access to this data is approved on a case-by-case basis by the network administrator who is responsible for the data.
    - Internal/private data is classified as moderately sensitive. Often, internal/private data is used for decision making, and therefore it is important this information remains accurate and up to date. The risk for negative impact on Mobilityways and its clients should this information not be available when needed is typically moderate.
- 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 and its clients 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 Disposal

The disposal of any data is dependent upon which medium it is stored, the following table outlines the mechanisms used to deliver data disposal:

Media Type	Data Removal Methods
HDD/SSD	Pattern wiping*, disintegration/incineration**
Optical Media	Pattern wiping*, disintegration/incineration**
Paper Based	Shredding***, incineration

*Pattern wiping is the process used to erase data, using multiple patterns of data, rendering lower layers of data unreadable and non-recoverable.

**Disintegration/Incineration is the process used to physically destroy mediums used to store data after pattern wiping is performed. This involved the physical disintegration/incineration of the device. The appropriately accredited third parties are utilised to carry out this process.

***Paper Based is the process used to physically destroy paper copies that contain data. This is destroyed via shredding of the physical copies and incinerated by an appropriately accredited third party.

14. Acceptable Use and Password Policy

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.

Individuals must not:

- allow anyone else to use their user ID/token and password on any Mobilityways system
- leave their user accounts logged in at an unattended and unlocked computer.
- use someone else's user ID and password to access Mobilityways systems.
- leave their password unprotected (for example writing it down)
- attempt to access data that they are not authorised to use or access
- exceed the limits of their access authorisation
- connect any non- Mobilityways authorised device to the Mobilityways network
- store Mobilityways data on any non-authorised Mobilityways equipment
- give or transfer Mobilityways data or software to any person or organisation outside Mobilityways without the authority.

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

Internet and Email conditions of use

Use of Mobilityways internet and email is intended for business use. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to Mobilityways in any way, not in breach of any term and condition of employment and does not place the individual or Mobilityways in breach of statutory or other legal obligations.

All individuals are accountable for their actions on the internet and email systems.

Individuals must not:

- use the internet or email for the purposes of harassment or abuse
- use profanity, obscenities, or derogatory remarks in communications
- access, download, send or receive any data (including images), which Mobilityways considers offensive in any way, including sexually explicit, discriminatory, defamatory, or libellous material
- use the internet or email to make personal gains or conduct a personal business without prior consent from Mobilityways
- use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam
- place any information on the Internet that relates to Mobilityways, alter any information about it, or express any opinion about Mobilityways, unless they are specifically authorised to do this
- forward Mobilityways mail to personal email accounts.
- make official commitments through the internet or email on behalf of Mobilityways unless authorised to do so
- download any software from the internet without prior approval of the Mobilityways IT Department.

Working Off-site

It is accepted that equipment will be taken off-site. The following controls must be applied:

- equipment and media taken off-site must not be left unattended in public places and not left in sight in a car
- laptops must be carried as hand luggage when travelling
- information should be protected against loss or compromise when working remotely (for example at home or in public places)
- particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones, and tablets. They must be protected at least by a password or a PIN and, where available, encryption.

External Storage Devices

External storage devices such as memory sticks, CDs, DVDs, and removable hard drives are prohibited by company and configuration policy.

Telephony Equipment

Use of Mobilityways telephony equipment is intended for business use. Individuals must not use Mobilityways's voice facilities for sending or receiving private communications on personal matters, except in exceptional circumstances or with prior consent.

Individuals must not:

- use Mobilityways's voice for conducting personal business
- make hoax or threatening calls to internal or external destinations
- accept reverse charge calls from domestic or International operators unless it is for business use.

Actions upon Termination of Contract

All Mobilityways equipment and data, for example laptops and mobile devices including telephones, smartphones, must be returned to Mobilityways at termination of contract.

All Mobilityways data or intellectual property developed or gained during the period of employment remains the property of Mobilityways and must not be retained beyond termination or reused for any other purpose.

Monitoring and Filtering

All data that is created and stored on Mobilityways computers is the property of Mobilityways and there is no official provision for individual data privacy, however wherever possible Mobilityways will avoid opening residual personal data.

IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. Mobilityways has the right (under certain conditions) to monitor activity on its systems, including internet and email use, to ensure systems security and effective operation, and to protect against misuse.

This policy must be read in conjunction with:

Computer Misuse Act 1990

Data Protection Act 2018

It is your responsibility to report suspected breaches of security policy without delay to your line manager.

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

Password policy

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 six month to ensure secure passwords and safeguards are always in place.

Every password is required to be unique, at least 12 characters, a mixture of letters, numbers and specials characters are enforced by policy.

15. Privacy policy, terms of use and conditions

Please view our online policies for the latest versions

Privacy policy

Members Terms of Use

Website Terms and Conditions (liftshare.com)

16. 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 minumum password complexity of 8 characters, at least one number and one uppercase. A lockout process is in place for incorrect passwords. Administor/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 minumum 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 six month 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 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/
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 manged 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 – scanning platform Scans are executed every 2 weeks 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."
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 90 days this is not configurable. Security event logs are part of the Microsoft services that we use. Azure Dev op, Microsoft 365 all have detailed event logs. All configuration changes are immutably logged with who, what and when. 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 store for a minimum of 180 days
Do you have a structured patch management programme 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 and all management or services is provided by Microsofts 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 originate from us. Sparkpost EU use opportunistic TLS for outbound traffic, which will depend on whether the receiving SMTP servers supports TLS. 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. SparkPost EU is SSAE-16 SOC II Type 2 Certified and GDPR ready.
Is MFA required for employees/contractors to log in to production systems supporting the services provided?	MFA is required on all system our employees access, including our own bespoke backend. Employees are trained to use We are a small team and some responsabilites 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 account along with a physical authentication token (hardware based multi-factor authentication). It is company policy to use the service to generate and store all web-based 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?	VPN access is limited to IT staff to monitor network and backups at the Norwich office location. All privelaged 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 system 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 UK IP addresses, further IP restrictions are in place to limit development applications. All development data is fully anonymised.

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/

Microsoft services complaince

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 complaince

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