Data Protection Policy

Author
Legal Services

Owner
General Counsel

Committee Sign-off
RMC

Sign off date
November 2025

Issue date
November 2025

Next review date
October 2026

Motability Operations

1. About the policy

1.1 Motability Operations Ltd is fully committed to compliance with the requirements of the UK General Data Protection Regulations and the Data Protection Act 2018 (***Data Protection Laws***). We recognise that the correct and lawful treatment of this Personal Data will maintain confidence in Motability Operations and will contribute to its success.

1.2 This Data Protection Policy defines the standards and guidelines for accessing corporate systems and data and expectations for maintaining the security of employees', customers', suppliers, other third parties' data and business information, and the process for reporting and managing suspected or actual data security breaches.

2. Scope of Policy

2.1 This policy applies to all employees, contractors, consultants, temporary staff and other workers (Data Users).

2.2. Data Users are obliged to comply with this policy when processing Personal Data on behalf of Motability Operations. Any breach of this Policy by employees may result in disciplinary action. Motability Operations reserves the right to take appropriate action against any third party, including (but not limited to) removal from the premises and/or termination of any contractual arrangement, if they are in breach of this Policy.

3. Guiding Principles

3.1 Through this policy and our approach to data protection and data retention, we aim to ensure that:

1 any processing of Personal Data is lawful, fair and transparent;
2 Personal Data is only used for the purpose for which you acquired it;
3 we only collect the minimum amount of Personal Data that is necessary;
4 we have a process in place to ensure it is accurate;
5 Personal Data is not retained it for longer than is necessary;
6 any Personal Data held will be held securely;
7 not transferred to another country without appropriate safeguards in place (transfer limitation); and
8 made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data (data subject's rights and requests).

4. Roles and responsibilities

4.1 **Responsibility of all Data Users.** We aim to comply with the laws, rules, and regulations that govern our organisation and with recognised compliance good practices. All employees must comply with this policy, the Data Retention Policy, any communications suspending data disposal and any specific instructions from the Legal Department. An employee's failure to comply with this policy may result in disciplinary sanctions, including suspension or termination. It is therefore the responsibility of everyone to understand and comply with this policy.

4.2 **Executives and Senior Leadership Team.** . Each Executive and Senior Leader is responsible for identifying the data that they wish to collect, retain and process, and determining, in collaboration with the Legal Department the lawful basis for collecting such data and the proper period of retention.

4.3 **Data Protection Officer.** Our Data Protection Officer (DPO) is responsible for advising on and monitoring our compliance with data protection laws which regulate personal data. The Data Protection Officer is General Counsel.

5. Types of data and data classifications

5.1 **Formal or official records.** Certain data is more important to us and is therefore listed in the Record Retention Schedule. This may be because we have a legal requirement to retain it, or because we may need it as evidence of our transactions, or because it is important to the running of our business. Please see the Data Retention Policy for more information on retention periods for this type of data.

5.2 **Disposable information.** Disposable information consists of data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose and/or data that may be safely destroyed because it is not a formal or official record as defined by this policy and the Record Retention Schedule. Examples may include:

9 Duplicates of originals that have not been annotated.
10 Preliminary drafts of letters, memoranda, reports, worksheets, and informal notes that do not represent significant steps or decisions in the preparation of an official record.
11 Books, periodicals, manuals, training binders, and other printed materials obtained from outside sources and retained primarily for reference purposes.
12 Spam and junk mail.

5.3 **Personal Data.** Both formal or official records and disposable information may contain personal data; that is, data that identifies living individuals. Data protection laws require us to retain personal data for no longer than is necessary for the purposes for which it is processed (principle of storage limitation).

5.4 **Confidential information belonging to others.** Any confidential information that an employee may have obtained from a source outside of Motability Operations Ltd, such as a previous employer, must not, so long as such information remains confidential, be disclosed to or used by us.

5.5 **Data Classifications.** Some of our data is more confidential than other data. Our Information Classification and Handling Policy explains how we classify data and how each type of data should be marked and protected.

6. Retention Periods

6.1 Details of our approach to data retention and relevant data retention periods are set out in our Data Retention Policy and Record Retention Schedule.

7. Managing Personal Data

7.1 **Processing.** All Personal Data should be accessible only to those who need to use it and we must have a lawful basis to process the Personal Data. The lawful basis for processing Personal Data is limited to one or more of the following purposes:

1. the identified or identifiable individual (Data Subject) has given their ***consent***;
2. the processing is necessary for the performance of a ***contract***;
3. to meet our ***legal and regulatory*** compliance obligations
4. to protect the ***vital interests*** of the Data Subject:
5. to pursue our ***legitimate interests*** where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects

7.2 **Disclosure**. Data Users have a duty to ensure that Personal Data is not improperly disclosed to unauthorised third parties. Before any Personal Data is disclosed Data Users must ensure that the agreed verification questions (see Appendix A) have been confirmed by the party seeking disclosure and in the case of data relating to a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, sex or sexual orientation (Special Categories Data) that the disclosure is strictly permitted under the Data Protection Laws.

This does not apply to requests from the following parties, subject to receipt of a written request on appropriate letter headed paper, which confirms the specific exception in the Data Protection Act on which the party seeks to rely:

1. The Police
2. Other government departments e.g. Citizen's Advice Bureau, Department for Business, Energy & Industrial Strategy, DVLA and the Financial Conduct Authority;
3. Where information is sought in relation to legal proceedings; and
4. Credit reference agencies.

7.3 **Data subjects' right and requests.** All Data Subjects have rights and obligations under the Data Protection Laws in relation to the processing of Personal Data and access to such information. These include the rights to:

1. Withdraw consent to the processing at any time, where consent is the lawful basis for processing;
2. Receive a copy of Motability Operations' relevant Privacy Notice (see Appendix B and Appendix C);
3. Request access to Personal Data we hold;
4. Ask us to erase Personal Data if it is no longer necessary in relation to the purpose for which it was collected or Processed or to rectify inaccurate data or to complete inaccurate data;

5 Restrict Processing in specific circumstances;
6 Challenge Processing which has been justified on the basis of Motability Operations' legitimate interests or in the public interest;
7 prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;
8 be notified of a Personal Data Breach which is likely to result in a high risk to their rights and freedoms;
9 make a complaint to a supervisory authority.

Any Data Subject who wishes to exercise their right to access Personal Data we hold must make a request in writing to:

The Data Protection Office
Motability Operations Limited
6th Floor,
22 Bishopsgate
London
EC2N 4BQ

All Data Subjects are responsible for:

- Checking that any Personal Data they provide to Motability Operations is accurate and up to date; and
- Informing Motability Operations of any changes to the information they have provided.

7.4 **Systems, equipment and access.** Access to systems and the use of equipment (desktop, laptop, mobile phone or associated hardware) is role dependent and controlled through use of user accounts and passwords. Personal Data may only be accessed via Motability Operations' approved and installed software. Requests for access to systems, equipment, software or applications should be:

- made via the IT Support Helpdesk by an authorised approver (individual designated by a Head of Function) using the Starter, Leaver, Mover form; and
- limited to those Information Systems required to perform the particular role.

7.5 **Data Protection Impact Assessment (DPIA).** A DPIA describes a process designed to identify risks arising out of the processing of personal data and to minimise these risks as far and as early as possible. DPIAs are important tools for negating risk, and for demonstrating compliance with the Data Protection Laws. A DPIA must be completed when implementing major system or business change programmes or onboarding a new third party supplier where the engagement will involve the Processing of Personal Data. The DPIA, a copy of which is at Annex D includes:

- a description of the Processing, its purpose and Motability Operations' legitimate interest (if appropriate)
- an assessment of the necessity and proportionality of the Processing in relation to the purpose;
- an assessment of the risk to individuals; and
- the risk mitigation measures in place and demonstration of compliance.

The Data Protection Officer or the Legal Services Team should be approached if assistance is required in completing the DPIA. A copy of the DPIA must be sent to the Legal Services Team as part of the supplier onboarding process (as more fully set out in the Purchasing Policy) and/or project implementation.

8. Data management and security (Prevention of unauthorised access)

8.1 **General.** Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage. Maintaining both electronic and paper copies of Personal Data is not advisable. In general, all documents should be retained in electronic format.

8.2 **Electronic Data.** Where there is a specific business requirement to store/retain data outside of our core systems, the following should be observed in the interests of ensuring the safety and integrity of the Personal Data:

- All Personal Data should be stored on the network file servers i.e. Q or S drives, and not on local hard drives. Personal Data should not be stored on your C: drive permanently.
- Where Personal Data is confidential or sensitive due consideration should be given to whether it should be encrypted or password protected to prevent unauthorised access.
- User accounts and passwords must not be shared and should be changed regularly.
- Ensure that your PC is locked when away from your desk.
- Do not just "turn off" your laptop at the end of the day. To ensure that you do not lose Data that hasn't been saved you should select the "Log Off" or "Shutdown" option from the Start menu.
- Laptops and/or mobile phones should not be left unreasonably unattended, whether it is in the office or outside of the office i.e. on public transport.
- Any malfunctions of systems or equipment should be reported to IT Support Helpdesk.
- Any suspected theft or loss of equipment should be reported to both your leader and the IT Support Desk.
- Any suspected theft, loss or unauthorised disclosure of Personal Data should be reported to your leader and Legal Services Team.

8.3 **Hardcopy files.** If there is a distinct business reason to retain a hardcopy file, it should be stored appropriately to provide the level of protection that is required and should be reviewed on a regular basis, with closed files archived.

8.4 **Email, internet, intranet and phones.** None of these communication methods should be used for:

- political, business or commercial purposes not related to Motability Operations;
- sending, forwarding or replying to chain letters, hoaxes or jokes;
- accessing pornographic, illegal or other improper material;
- subscribing to chat rooms, messaging services or social networking sites, except for sites used for official Motability Operations duties;

- sending, forwarding or leaking company confidential business or customer information;
- for purposes not related to official Motability Operations duties.

Messages that disparage Motability Operations, shareholder banks, scheme partners, customers, Motability (the Charity), any organisation associated with the Motability Scheme, or any individual working at Motability Operations must not be posted anywhere in any format. Motability Operations reserves the right to take disciplinary action if it becomes aware of such postings.

9. Data Security Breaches

9.1 **General.** We hold a large amount of information, both in hard and soft copy. This includes Personal Data and company information, some of which may be commercially sensitive or confidential ("Information"). Care should be taken to protect Information to ensure that it is not changed (either accidentally or deliberately), lost, stolen or falls into the wrong hands, that its authenticity and integrity is maintained. In the event of a suspected or actual breach, it is vital that appropriate action is taken to minimise associated risks.

9.2 **What is a breach?** A data breach is an incident in which any form of Personal Data is compromised, disclosed, copied, transmitted, accessed, stolen or used by unauthorised individuals, whether accidentally or on purpose. Some examples:

- Accidental loss, or theft of equipment on which data is stored;
- Human error such as emailing data by mistake;
- Failure of equipment and hence data held on it;
- Loss of data or equipment through fire or flood;
- Hacking attack;
- "Blagging, where information is obtained by deceiving Data Users.

9.3 **Reporting a breach.** Data security breaches (including suspected breaches) must be reported within 24 hours or as soon as reasonably practicable to Legal Services, Business Risk and Compliance and the IT Service Centre. The report should include full and accurate details of the incident, including who is reporting the incident, what type of data is involved, if the data relates to people, how many people are involved.

9.4 **Investigation and risk assessment.** Together the Legal Services Team, the Chief Information Security Officer and the Head of Business Risk and Compliance will facilitate that an investigation will be started within 24 hours of the breach being discovered, where possible.

The investigation will establish the nature of the breach, the type of data involved, whether the data is Personal Data, and if so, who are the subjects and how many are involved. The investigation will consider the extent of the sensitivity of the data, and a risk assessment performed as to what might be the consequences of its loss, for instance whether harm could come to individuals or to Motability Operations.

9.5 **Containment and recovery.** The Legal Services Team together with the Chief Information Security Officer, Head of Business Risk and Compliance and relevant business functions will determine the appropriate course of action and the required resources needed to limit the impact of the breach. This might require isolating a compromised section of the network, alerting relevant staff or shutting down critical equipment or invoking the Cyber Incident Response plan.

Appropriate steps will be taken to recover data losses and resume normal business operation. This might entail attempting to recover any lost equipment, using backup mechanisms to restore compromised or stolen data and changing compromised passwords. Advice from experts may be sought if deemed necessary or appropriate.

9.6 **Notification.** The Executives will be notified, as soon as reasonably possible, of all reported incidents and, with the support of the Data Protection Officer and the Legal Services Team will make a decision based on the nature of the breach whether it is necessary to inform any external organisation, such as the police or other appropriate regulatory body. The Risk Management Committee and the Audit Committee will also be advised of any breach reported to a regulatory body, at the next scheduled committee meetings, unless it is deemed appropriate to inform the committees before that date.

If a Personal Data breach has occurred, the Data Protection Officer will inform the Information Commissioner's Office, if necessary, based on the extent and nature of the breach. Notice of the breach will be made to affected individuals to enable them to take steps to protect themselves. This notice will include a description of the breach and the steps taken to mitigate the risks, and will be undertaken by the Legal Services Team.

9.7 **Review.** Once the breach is contained a thorough review of the event will be undertaken by Business Systems, Business Risk and Compliance and the Legal Services Team, to establish the cause of the breach, the effectiveness of the response and to identify areas that require improvement. Recommended changes to systems, policies and procedures will be documented and implemented as soon as possible thereafter.

10. Monitoring

10.1 **General.** Motability Operations reserves the right to audit systems and monitor Data Users on a periodic basis to ensure compliance with this policy or where there is suspected misuse of Information systems or equipment. For further information please speak to HR or refer to the Communications Monitoring procedure.

10.2 **Asset Register.** An asset register of equipment shall be maintained by Business Systems. The Executives or Senior Leaders are responsible for the regular verification of the asset register.

10.3 **Unacceptable conduct.** Motability Operations deems the following to be unacceptable:

13 Offensive and/or disparaging statements made on any basis, including race, sex, sexual orientation, age, disability, religion or religious beliefs.
14 The commission of any criminal offence.
15 Sending or receiving sexually explicit or other inappropriate material.
16 Sending, receiving or leaking confidential business or customer information.
17 Defamatory comments about people or organisations.
18 Repeated visits to Internet sites that are considered by the Company to be offensive, pornographic, criminal or which may lead to embarrassment, distress or offence to other Employees.
19 Excessive personal use of Information Systems.
20 Downloading software from the Internet unless authorised to do so by Business Systems.
21 Sending or posting offensive, defamatory or confidential company information to third parties.
22 Sending confidential information to unauthorised third parties or your personal email address.

This list is not exhaustive and the Company reserves the right to include any other circumstance at its sole discretion. Employees found to be engaged in the above may be subject to disciplinary action and/or dismissal.

11. Related Documents

11.1 The following documents should be read in conjunction with this policy:

- Data Retention Policy and Data Record Schedule
- Information Security Management Policy
- Information Classification and Handling Policy
- Acceptable Use Policy

Appendix A: Data Protection Security Verification

Customer or appointee

Essential information

- Full name
- Current address and postcode
- Date of birth
- Telephone number

If the individual is unsure of the above – suitable alternatives include:

- CRN
- ARN
- Vehicle registration

Nominee / Disabled person (if different from above)

Essential information

Full name of Customer or Appointee

Current address and postcode of Customer or Appointee

Date of birth of Customer or Appointee

Password (if applicable)

If the nominee or Disabled Person is not aware of the above, it should be established whether the Customer or Appointee is available to provide verbal consent. If so, take the Customer or Appointee through the usual checks before accepting their consent to speak to the Nominee or Disabled Person.

It is suggested that the verification process is also followed where outbound calls are made to customers and/or third parties.

Third Parties

Personal data should not be disclosed to a third party without the express consent of the Customer. Exception, subject to receipt of a written request on appropriate letter headed paper, which confirms the specific exception in the DPA on which the party seeks to rely:

Police

Other government departments e.g. Citizen's Advice Bureau, Department for Energy & Industrial Strategy, the DVLA or the Financial Conduct Authority (FCA)Where information is needed for legal proceedings

Credit reference agencies.

Appendix B: Motability Operations Worker Privacy Notice

Privacy Notice

Maintaining the security of your personal information is a priority for Motability Operations Ltd, ("MO", "we", "us", "our") and we are committed to respecting your privacy rights. We are also dedicated to ensuring that your data is processed lawfully and fairly and being transparent about what data we collect about you and how we use it.

This privacy notice describes how we collect and use personal information about you during and after your working relationship with us.

What personal data do we collect?

We will collect, store, and use the following categories of personal information that you have provided through the application and recruitment process and the ongoing working relationship:

- Personal details: name, date of birth, gender, national insurance number, passport number and identity documents
- Contact details: address, telephone number (including mobile number) and email address
- Marital status and dependents
- Next of kin and emergency contract information
- Bank account details, payroll records and tax status information
- Salary (including compensation history), pension and benefit information
- Copy of driving licence (if applicable)
- Recruitment information (including references and other information included in a CV or cover letter or as part of the application process)
- Right to work documentation
- Employment records (including job titles, work history and working hours)
- Performance information
- Disciplinary and grievance information
- CCTV footage and other information obtained through electronic means such as access card records
- Information about your use of our information and communication systems
- Photographs.

We may also collect, store and use the following "special categories" information:

- Information about your race or ethnicity, gender, gender identity and sexual orientation
- Information about your health, including any medical condition, health and sickness records
- Information about criminal convictions and offences.

We may sometime collect information from third parties including former employers, educational institutions, credit reference agencies or other background checking agencies.

How we use it

We use your personal data:

- Performance of the contract we have entered into
- Checking you are legally entitled to work in the UK
- Paying you and, if you are an employee deducting tax and National Insurance contributions
- Providing you with benefits, including private medical aid and travel insurance (if applicable)
- Liaising with the benefit providers
- Business management and planning, including accounting and auditing
- Conducting performance reviews, managing performance and determining performance requirements
- Making decisions about salary reviews and compensation
- Gathering evidence for possible grievance and disciplinary hearings
- Ascertaining your fitness to work and managing sickness absence

- To monitor your use of our information and communication systems to ensure compliance with our information security policies
- Equal opportunities monitoring
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests
- To comply with legal and regulatory requirements
- For crime and fraud prevention, detection and related purposes.

We may also use your personal data in the following situations, which are likely to be rare:

- Where we need to protect your interests (or someone else's interests)
- Where it is needed in the public interest or for official purposes.

If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Who we share your personal information with

We may share your personal data with third parties as set out below:

- Companies or organisations that we have engaged to provide services on our behalf. The following activities are carried out by third party providers; payroll, pension administration, benefits provision and administration
- Any law enforcement agency, court, regulator, government authority or third party where we believe this is necessary to comply with a legal or regulatory obligation, or otherwise protect our rights or the rights of any third party
- Providers of back-up and storage services, cloud service provider, software services provider.

All our third party service providers are required to take appropriate security measures to protect your personal information. We do not allow our third party service providers to use your personal data for their own purposes. We only permit them to process your personal information for specified purposes and in accordance with our instructions.

Transferring information outside the United Kingdom ("UK")

We may transfer your personal information to countries outside of the UK, where this is necessary for the purposes for which we collected it. Whenever we transfer your personal data outside of the UK, we ensure a similar degree of protection afforded to it by implementing at least one of the following safeguards:

- We will only transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data by the European Commission and/or the UK Data Protection Authority
- Where we use certain service providers, we may use specific contracts approved by the European Commission and/or the UK Data Protection Authority which give personal data the same protection as it has in the UK or obtain contractual assurances from the third party given access to your personal information that your personal information will be protected by standards which are equivalent to those that protect your personal information when it is in the UK.

How we protect your data

We are committed to keeping your personal information safe and secure. Our security measures include:

- Security controls which protect our infrastructure from external attack and unauthorised access
- Regular cyber security assessment and business continuity exercises to ensure we are ready to respond to cyber security attacks and data security incidents
- Internal policies and procedures relevant to data and data security.

In addition, we limit access to your personal information to those employees, agents, contractors and third party service providers who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

Data retention

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting purposes and in line with our internal policies.

Your rights relating to your personal data

It is important that you know your rights to be able to request from us what you need and help us to keep the personal information accurate and current. Please keep us informed if your personal information changes during your relationship with us.

You have the following rights:

- to ask what personal data we hold about you at any time
- to ask us to update and correct any out-of-date or incorrect personal data that we hold about you
- to object to processing of your personal information

You can exercise any of the above rights at any time by contracting us

- If we are using legitimate interest to process your personal information you always have the right to opt out if there is something about your particular situation which makes you want to object to processing on this ground.

Data protection officer

We have appointed the General Counsel to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact the Data Protection Officer (DPO) by writing DPO at Motability Operations Limited, 6th Floor, 22 Bishopsgate, London, EC2N 4BQ.

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

Changes to this privacy notice

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

Appendix C: Motability Scheme Privacy Notice

Privacy Notice

Motability Operations Limited takes data privacy very seriously and this notice is designed to help you understand how we use your personal data.

1. About us

We are Motability Operations Limited. Our registered address is Level 6, 22 Bishopsgate Level 6, 22 Bishopsgate, London, England EC2N 4BQ and we are authorised and regulated by the Financial Conduct Authority under reference number 735390.

Our main business is operating the Motability Scheme and the Family Fund Mobility Support Scheme ("the Schemes") which enable eligible individuals to lease new vehicles from us (such as cars, wheelchair accessible vehicles, scooters and powered wheelchairs).

2. About this privacy notice

This is our main general privacy notice that applies across our business (including our operation of the Schemes), although we may publish additional privacy statements that apply to specific services that we offer from time to time.

3. Updating this privacy notice

We may update this privacy notice from time to time. You will always be able to find the up-to-date version of this notice on our main website at **motability.co.uk**. This version is dated November 2025.

4. What is personal data?

Personal data is information that relates to you or allows us to identify you. This includes obvious things like your name, address and telephone number but can also include less obvious things like analysis of your use of our websites.

There are different types of personal data. The most important types for you to know about are:

- **Special categories of personal data:** for example health, race, religion or biometric data.
- **Criminal convictions data:** information about offences or alleged offences.

5. Our responsibility to you

We process your personal data in our capacity as a controller. This means that we are responsible for ensuring that we comply with relevant data protection laws when processing your personal data.

6. Data Protection Officer

We have appointed a Data Protection Officer to oversee our data protection compliance. If you have any questions about this privacy notice or how we handle your personal data, please contact the Data Protection Officer by email at **dataprotection@mo.co.uk** or in writing to the Data Protection Officer at Motability Operations Limited, 22 Bishopsgate, 6th Floor, London EC2N 4BQ.

7. Why are we collecting personal data about you?

We only collect personal data about you in connection with operating the Schemes and running our business. We will hold information about you if:

- You enquire about a Scheme.
- You enter into a Scheme hire agreement with us.
- You are the disabled person who ultimately benefits from a Scheme hire agreement (even though you may not have entered into the agreement yourself).
- You are a named driver of a Scheme vehicle.
- Your information is provided to us or we otherwise obtain your information in connection with the operation of the Schemes or our business. For example, you are a witness to an accident involving a Scheme vehicle.
- You provide services to us (or you represent a company which provides services to us).
- You represent a regulator, certification body or government body which has dealings with us.
- You attend our events, receive our updates, visit our office or use our websites.

8. What personal data do we collect about you?

The types of personal data that we process about you may include:

- **Individual details:** name, date of birth, gender, nationality, details of your mobility allowance and your contact details, including address, telephone number (including mobile number) and email address.
- **Identification details**: identification numbers issued by government bodies or agencies such as your national insurance number, driving licence number and identification through facial recognition and other relevant technologies.
- **Financial information:** bank account or payment card details.
- **Credit, anti-fraud and sanctions data**: credit history, credit score and information received from various anti-fraud and sanctions databases relating to you.
- **Criminal convictions data**: information relating to your criminal convictions and offences, including driving offences.
- **Information on your use of a Scheme vehicle:** VIN number, registration number and connected vehicle data including but not limited to mileage data, technical vehicle data, driving behaviour data, charging data and location data.
- **Identifiers:** information which can be traced back to you, such as an IP address, a website tracking code or electronic images of you.

9. Where do we collect your personal data from?

We collect your personal data directly from you, for example, when you make an application to join a Scheme, set up an on-line account with us or send an email to our customer services team.

We also collect your personal data by actively obtaining your data ourselves, for example through the use of website tracking devices, and from various third parties and publicly available sources, including:

- Your employer.
- Our customers.
- Our service providers.
- Credit reference agencies.
- Anti-fraud databases, sanctions lists, court judgements and other databases.
- Government agencies and publicly accessible registers or sources of information.
- Other third parties, such as witnesses to accidents involving Scheme vehicles.

Which of the sources apply to you will depend on why we are collecting your personal data.

10. How do we use your personal data?

In this Section we set out in more detail the main purposes for which we use your personal data and the lawful bases upon which we are using your personal data.

Purpose	**Lawful basis**
Risk management and other legal obligations We use personal data about Scheme hirers, drivers and others for risk management purposes and also to help us comply with legislation on money laundering, terrorist financing, and sanctions. In relation to hirers, this includes verifying the identity of hirers and carrying out credit checks, including periodic credit checks during the term of their Scheme hire agreement. We may also use certain information, such as credit check and fraud information, for risk assessment purposes, including risk assessments relating to Scheme insurance, Scheme hire agreements and determining whether to install telematics in a Scheme vehicle. We may also share your personal data in order to help prevent fraud and money laundering, for example by uploading your data onto relevant anti-fraud databases. In some cases, the personal data processed will include special categories of personal data and criminal convictions data.	For all information **- compliance with a legal obligation** or **legitimate interests** . As a firm regulated by the Financial Conduct Authority, we have a legitimate interest to manage risks responsibly. For example this means using information to decide whether to enter into and manage Scheme lease agreements, help prevent and detect fraud or money laundering, check and confirm the identity of hirers and drivers, trace and recover debts, if needed. These activities help us protect both our customers and our business For special category and criminal data - **preventing or detecting unlawful acts**, **regulatory requirements** and **suspicion of terrorist financing or money laundering**
Operating the Schemes We use personal data to operate the Schemes. This includes processing applications to join a Scheme, entering into Scheme hire agreements, providing hirers with an online account and communicating with hirers and drivers (including via our Website's live chat function).	For all information - **to take steps to enter into a contract with you/fulfil our obligations under the contract** and **legitimate interests**. We have a legitimate interest in operating the Schemes and providing Scheme vehicles and associated services and assistance.

It also includes providing hirers with a Scheme vehicle and related services and assistance, such as roadside assistance. We also use Scheme vehicle data, together with other personal data (which may include special categories of personal data) that we hold about hirers and drivers, to support the Schemes and the servicing, maintenance and repair of Scheme vehicles.	For special category data – **explicit consent**.
Monitoring Scheme vehicle data and location We may monitor driving behaviour using DriveSmart app and the DriveSmart fitted box Telematics, as set out in the relevant Scheme hire agreement and DriveSmart terms and conditions, which will be made available to hirers and drivers where relevant. We do not generally look to collect special categories of personal data and criminal convictions data for this purpose.	**To fulfil our obligations under the contract** and **legitimate interests**. We have a legitimate interest in ensuring Scheme vehicles are driven appropriately and in tracing and recovering Scheme vehicles, where applicable.
Research and analysis We may use third party providers to contact you on our behalf to ask you for your opinion and feedback on the operation of the Schemes. They may combine the data that you provide to them as part of the survey with data from other sources to study it and produce reports and advice that helps us to understand our customers' point of view, so that we can improve the way we work as a business and our operation of the Schemes. We also process data relating to us/the Schemes which you have shared via a public platform (such as an X feed or public Facebook page) and information that you provide voluntarily on our social media pages. We also analyse information that we collect from our third party service providers (such as Google, Facebook, X and Instagram) to understand how you engage with our services to help us to understand your preferences and improve our services. We use all of this information for customer insight, internal analysis and research purposes.	For all information - **legitimate interests** We have a legitimate interest in carrying out research and analysis, including surveys, to better understand the needs of our customers and your views on the operation of the Schemes, to help us to improve our services and to develop new services. We also have a legitimate interest in understanding how you engage with us and our services. For special category data – **research and analysis**, or where that lawful basis does not apply **explicit consent**.
Marketing We may use your details to provide information to you in relation to the Schemes, including news and developments. In particular, we circulate a monthly Scheme newsletter to hirers (unless they have opted out) and to other individuals on request. We may also provide targeted Scheme related updates, news and advertising to Scheme hirers via our websites and the social media platforms they use. We may also use images and footage of individuals such as individuals who attend our events for promotional and marketing purposes, including on our websites and on social media. Please see 'Events' below	For all information - **legitimate interests.** We have a legitimate interest in keeping you informed about updates, news, and developments that may be relevant to you. This may include sending marketing communications or showing you Scheme-related updates and advertising on our website or social media platforms. When we do this, we follow the specific laws that apply to marketing

for further information on our use of personal data in this context.	and advertising, as well as data protection laws. You can choose to stop receiving marketing communications or targeted advertising from us at any time — every message we send includes an easy way to opt out. Please note that social media platforms also have their own settings that let you control the advertising you see when using their services. We may also rely on our legitimate interests to use photographs and video footage from our events to promote the Scheme or create marketing materials. For all information - **consent** Where we cannot rely on our legitimate interests to process your personal data for any of these purposes, we will do so only with your consent. For special category data – **explicit consent**.
Events We organise several Scheme related events in different locations throughout the year. For example, we hold events which enable visitors to explore a range of adapted cars and to speak to experts about their particular needs.	For all information - **legitimate interests**. We have a legitimate interest organising and running events in relation to the Schemes. For special category data – **explicit consent**.
Visitors to our website We use analytics tools to understand your preferences and to make your experience on our websites smoother and more relevant. Some areas of our websites ask you to provide personal information — for example, when you complete a form or make an enquiry. We'll only use the information you give us for the specific purpose you provided it. Our websites also use a small number of non-intrusive cookies to help them run efficiently and to tell us how people use them. This helps us improve our websites over time. In particular, we use Google Analytics, which places small text files (known as "cookies") on your device to collect information about how you use our websites. Google also processes this information in line with its own privacy policies and may store it on servers in the United States. You can control or delete cookies through your browser settings, or by using browser add-ons. To find out more	**Legitimate interests** - we have a legitimate interest in providing to you the facilities on our websites that you have requested and in understanding how our websites are used and the relative popularity of the content on our websites. We also have a legitimate interest in improving the browsing experience of visitors to our websites. **Consent** - where we cannot rely on our legitimate interests to process your personal data for any of these purposes, we will do so only with your consent.

about how we use cookies, please read our separate cookies notice. We do not generally collect any special category data (such as information about your health or beliefs) or criminal convictions data through our websites.	
Visitors to our offices We have security measures in place at our offices to help keep everyone safe. These include building access controls and, in some areas, CCTV monitoring. CCTV images are stored securely and are only accessed when necessary — for example, to investigate an incident. Recordings are automatically deleted after a short period unless they need to be kept for an investigation (such as a theft). When you visit our offices, you'll be asked to sign in at reception. We keep visitor records securely for a short period and only access them when needed, such as to look into an incident. We do not usually collect special category data (such as health information) or criminal convictions data for this purpose.	For all information - **legitimate interests**. We have a legitimate interest in making sure our offices, and the people that visit and work at them, are safe and secure. For special category and criminal data - **preventing or detecting unlawful acts**.
Service providers We collect information about you in connection with your provision of services to us or your position as a representative of a provider of services to us. We do not generally look to collect special categories of personal data and criminal convictions data for this purpose.	**Legitimate interests.** We have a legitimate interest in contacting and dealing with individuals involved in providing services to us.

11. Failure to provide your personal data to us

Where we need to collect your personal data by law or in order to provide you with our services or perform a contract we have with you and you decide not to provide that information when requested, we may not be able to provide our services or perform the contract we have or are trying to enter into with you. In other circumstances where you choose not to provide us with your personal data when we request it, your decision not to provide us with your personal data may affect our ability to provide you with our services.

12. Consent

We do not generally process your personal data based on your consent/explicit consent (as we can usually rely on another lawful basis). Where we do process your personal data based on your consent/explicit consent, you have the right to withdraw your consent at any time. To withdraw your consent please contact the Data Protection Officer using the details set out in Section 6.

If you want to opt out of receiving Scheme news and updates you can do so by following the opt out links on any communications we send to you. Alternatively, please contact the Data Protection Officer, using the details set out in Section 6, to opt out.

Please note that you cannot opt out of receiving service-related communications from us – for example, communications we send to hirers about their Scheme vehicle. However, you can still choose how you prefer us to provide you with service-related communications.

13. Who do we share your personal data with?

We do not sell your information nor make it generally available to others. But we may share your information with the following third parties:

- Third parties we use to help us operate the Schemes effectively. For example, we share personal data with our Scheme vehicle manufacturers and dealers, our Scheme insurers (currently Direct Line), our Scheme roadside assistance providers (currently RAC) and with energy suppliers where we arrange the installation of a charging point for a Scheme electric vehicle at a hirer's home.
- Research agencies.
- Service providers we use to help us run our business efficiently, particularly in relation to our IT systems. Some of these services (such as email hosting and data backups) involve the service provider holding and using personal data.
- Trusted third parties, such as specialist consultants, for the purposes of developing and improving our services and innovation.
- Governmental departments or bodies, such as the Department for Work and Pensions, Veterans UK, Social Security Scotland and the Driver Vehicle Licensing Agency.
- Relevant third parties as part of our efforts to prevent fraud, which includes third parties that have access to relevant anti-fraud databases onto which we may upload your personal data.
- The Motability Foundation, which has appointed us to operate the Motability Scheme. The Motability Foundation also has its own privacy notice setting out how it processes your personal data and which can be found at www.motabilityfoundation.org.uk.
- Family Fund Trust, which has appointed us to operate the Family Fund Mobility Support Scheme. Family Fund Trust also has its own privacy notice setting out how it processes your personal data and which can be found at www.motability.co.uk.
- Legal and other professional advisers.
- Any law enforcement agency, court, regulator, government authority or third party where we believe this is necessary to comply with a legal or regulatory obligation, or otherwise to protect our rights or the rights of any third party.
- In the event of termination of our appointment to operate the Motability Scheme, we will share your personal data with the Motability Foundation and the new operator of the Scheme in connection with the continued operation of the Scheme.
- In the event of termination of our appointment to operate the Family Fund Mobility Support Scheme, we will share your personal data with Family Fund Trust and the new operator of the Scheme in connection with the continued operation of the Scheme.

14. Organisations engaged to provide services on our behalf

Certain third parties we use to help us operate the Schemes, such as our Scheme vehicle manufacturers and dealers and our Scheme insurers, will be responsible to you, in their capacity as controllers, for how they use your personal data that we share with them. These third parties have their own privacy notices informing you how they will use your personal data. More information about how our Scheme insurers use your personal data can be found in the Scheme insurance cover booklet.

Other third parties we use to help us operate the Schemes, such as our Scheme roadside assistance providers, act as our processors when processing your personal data in relation to the Schemes. This means that we are responsible to you for how they process your personal data and they only process your personal data in line with our instructions.

All our third-party providers are required to take appropriate security measures to protect your personal data and the personal data we share with them is limited to the information they require to provide their services to us.

15. Transferring information outside the United Kingdom

As part of operating the Schemes and running our business, we may transfer your personal data to countries outside of the UK. Where we transfer your personal data outside of the UK, we will protect your personal data by ensuring that the transfer is made in compliance with all applicable data protection laws.

In most cases, this means we will only transfer your personal data to third parties located in:

- Countries that have been deemed to provide an adequate level of protection for personal data by the UK Government.
- Other countries only when we have put specific contracts in place with those third parties approved by the Information Commissioner's Office ("ICO"), the UK supervisory authority for data protection issues, which obtain contractual assurances from the third party that your personal data will be protected by standards which are equivalent to those that protect your personal data when it is in the UK.

If you would like further details of how your personal data is protected when transferred from one country to another then please contact the Data Protection Officer using the details set out in Section 6.

16. How we protect your personal data

We are committed to keeping your personal data safe and we implement appropriate steps to help maintain the security of our information systems and processes and prevent the accidental destruction, loss or unauthorised disclosure of the personal data we process secure. Our security measures include:

- Security controls which protect our infrastructure from external attack and unauthorised access.
- Regular cyber security assessment and business continuity exercises to ensure we are ready to respond to cyber security attacks and data security incidents.
- Internal policies and procedures relevant to data and data security.

17. Profiling and automated decision making

We do not use profiling (where an electronic system uses personal data to try and predict something about you) or automated decision making (where an electronic system uses personal data to make a decision about you without human intervention).

18. Data retention

We keep your personal data in accordance with our data retention policy which categorises all of the information held by us and specifies the appropriate retention period for each category of information. Those periods are based on the requirements of relevant data protection laws and the purpose for which the information is collected and used, taking into account legal and regulatory requirements to retain the information for a minimum period, limitation periods for taking legal action, good practice and our business purposes.

Further information in relation to our data retention processes may be obtained by contacting the Data Protection Officer using the details set out in Section 6.

19. Your rights relating to your personal data

Under certain conditions, you may have the right to require us to:

- Provide you with further details on how we use your personal data.
- Provide you with a copy of the personal data we hold about you.
- Update any inaccuracies in the personal data we hold about you.
- Delete any of your personal data that we no longer have a lawful ground to use.
- Restrict how we use your personal data, for example, whilst a complaint is being investigated.
- Where processing is based on consent, stop that particular processing by withdrawing your consent.
- Object to any processing based on our legitimate interests unless our reasons for undertaking that processing outweigh any prejudice to your data protection rights.
- Transfer your personal data to a third party in a standardised machine-readable format.

In certain circumstances, we may need to restrict your rights in order to safeguard the public interest (e.g. the prevention or detection of crime) and our interests (e.g. the maintenance of legal privilege).

You can exercise any of these rights at any time by contacting the Data Protection Officer using the details set out in Section 6.

We are obliged to keep your personal data accurate and up to date. Please help us to do this by advising us of any changes to your personal data.

20. Your right to complain

If you are not satisfied with our use of your personal data or our response to any request by you to exercise your rights, or if you think that we have breached any applicable data protection laws, you have the right to make a complaint at any time to the ICO. The ICO can be contacted on **0303 123 1113** or via the website at **ico.org.uk**.

Appendix D: Data Privacy Impact Assessment

Data Privacy Impact Assessment

The Data Privacy Impact Assessment (DPIA) is our way of verifying that we can use and share data in a way in which our employees or customers have consented to, or in a way we have told them we will use their data (or as they would expect us to use it).

You should fill out the template:

- at the start of any major project involving the use of personal data or implementing a new system;
- if you are making a significant change to an existing process (you are proposing to process data in a way that you or your department has not previously done);
- if you are onboarding a third party supplier who you will or propose to share personal data with.

This is not an exhaustive list.
Please see notes at the end of the template to assist you in completing the document. If you are unsure whether you need to complete a DPIA please contact the Legal Team at [redacted]

Step 1: Supplier Details

Name of supplier:	
Is the supplier a data controller or a data processor: If the supplier cannot use the data for their own business purposes and only for the purposes we allow them to use it, they will be a data processor and MO will be the data controller	
Title of project:	
Business Owner:	
Department:	
Date:	

Step 2: Identifying the need for a DPIA

Explain broadly what the project or activity aims to achieve and what type of processing it involves.		
What does the project aim to achieve?		
What types of data processing are involved?		
Type of processing	**Yes/No**	**Explanation**
Collection of personal data		
Use of personal data		
Erasure of personal data		

Storage of personal data		

Step 3: Describe the processing

Describe the nature of the processing	
Nature of processing:	
How will the data be collected:	
How will the data be used:	
Where will the date be stored:	
How and when will the data be deleted:	
Describe the scope of the processing	
Nature of the personal data: What data are you collecting	
Special category data: For example, race, religion or belief, sex or sexual orientation, disability or heath data	
Criminal offence data:	
Geographic data: **Data** that contain either coordinates that reference a geographic location or area or attribute data that can be related to a geographic area or location	
Describe the context of the processing	
What is the nature of your relationship with the individuals (data subjects):	
How much control will they have over what we do with their data?	
Do they include children or other vulnerable groups?	
Describe the purpose of the processing	

What do you want to achieve?
Intended effect on individuals?
The benefits of processing?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality		
What is the lawful basis of the processing (tick as appropriate)		
Basis	**Yes/No**	**Explanation**
Performance of a contract The processing an individual's personal data to meet our obligations under a contract		
Consent The individual has consented to the use of their personal data		
Legal obligation This is where you are legally obligated to share personal data (outside of the contractual obligations). For example, sharing information with the police.		
Vital interest You can collect, use or share personal data in emergency situations, to protect someone's life		
Legitimate interest Processing of personal data is necessary for MO or a third party involved in delivering the Scheme. For example, using personal data for internal analysis and research in the commercial interests of improving our services.		*Purpose test*: Why it is necessary to process the PII in that way? What is the benefit from processing in this way? *Necessity test:* Is it proportionate/can it be done in any other way? *Balancing test:* What is the impact to the customer (does it impact their rights and freedoms)?

Step 5: Identify and assess risk(s)

Describe any risks and the potential impact on individuals

Source of the risk	**Controls**	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Example: Customers may object to the use of their data	opt outs managed via data cleansing before processing occurs	Low	Low	Low

Step 6: Sign off and recommended outcomes

Summary of DPO advise
Which lawful basis of processing has been fulfilled?
Further considerations (if any)
Is the processing deemed fair and reasonable?

For further information contact:

The Legal Department

Motability Operations