Introduction

SM Cars Norwich Ltd (the Company) processes the personal data of living individuals such as its staff, Customers, contractors, research subjects and customers. This processing is regulated by the Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR). The UK's regulator for the DPA and GDPR is the Information Commissioner's Office (ICO).

The Company is registered as a Data Controller with the ICO1 and is responsible for compliance with the GDPR and DPA.

1. Key Definitions

This DPA and GDPR contain a number of key definitions which are referenced in this policy such as 'Personal Data, 'Processing' and 'Data Controller. Those definitions are set out in Annex A.

2. Purpose and Objectives of Policy

This policy sets out the Company's commitment to comply with the Data Protection Act 2018 ('DPA'), and the General Data Protection Regulation ('the GDPR').

3. Scope and Status of the Policy

This policy applies to all Company staff, Customers and others who use or process any Personal Data. This policy applies regardless of where Personal Data is held and or the equipment used if the Processing is for the Company's purposes. Further, the policy applies to all Personal Data (including Sensitive Personal Data) held in any form whether manual paper records or electronic records.

Roles and Responsibilities

Board of Directors

The Board of Directors is responsible for approval of the Policy.

Company Executive Group

The Company Executive Group is responsible for the strategic level implementation of the policy, oversight of compliance with the policy and reporting identified risks to the Board.

You can view our registration with the ICO by typing SM Cars Norwich Ltd into the search function accessible via the following link: https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/

Information Asset Owners

The Company will appoint Information Asset Owner (IAO) with local responsibility for data protection compliance for Personal Data processed.

Information Asset Managers

The Company will appoint Information Asset Managers who will hold local responsibility for data protection compliance processed within their teams.

Data Protection Officer

The Company's Data Protection Officer (DPO) is primarily responsible for advising on and assessing the Company's compliance with the DPA and GDPR and making recommendations to improve practice in this area. Further, the DPO acts as the Company's primary point of contact for DPA and GDPR matters.

Legal Services

Legal Services are responsible for providing advice, support and guidance in relation to day-to-day data protection matters.

All staff

All staff, including permanent staff, fixed-term contractors and temporary workers must comply with this Policy, the DPA and the GDPR whenever Processing Personal Data is held by the Company or on behalf of the Company.

All Customers

All Customers are responsible for compliance with the rules and policies made by the Company. Customers must comply with this policy when collecting and Processing Personal Data as part of their course, studies or research.

Contractors and Consultants

Third parties such as consultants, and contractors undertaking work on behalf of the Company involving Personal Data, must adhere to the Company's Data Protection Policy and comply with the DPA and the GDPR. Provision will be made in contracts with external providers to ensure compliance with this Policy, the DPA and GDPR.

4. Compliance with the DPA and GDPR

Awareness & Capability

The Company will implement, and monitor the annual completion of, mandatory Data Protection training for all staff. The content of that training will be reviewed annually.

Privacy By Design

The Company will implement a Privacy By Design Approach to Processing Personal Data by integrating Privacy Impact Assessments into business processes and projects.

Lawful, Fair & Transparent Processing

The Company will provide appropriate information to individuals when collecting their Personal Data by means of privacy notices. The Company will also ensure at least one lawful basis is available before Processing Personal Data.

Purpose Limitation

The Company will clearly set out purposes for Processing Personal Data. The Company will only process Personal Data for purposes notified to individuals and where the new purpose is compatible with an existing purpose.

Data Minimisation

The Company will only collect as much information as is necessary to meet the purposes that have been identified. Personal Data must be adequate, relevant and not excessive.

Accuracy

The Company will ensure that Personal Data processed is accurate and where necessary kept up to date.

Security

The Company will protect the security of Personal Data by maintaining and monitoring compliance with the requirement set up by the GDPR.

Record Keeping & Retention

The Company will maintain a records retention and disposal schedule setting the periods for which records containing Personal Data are to be retained.

External Contractors and International Transfers

The Company will enter into legally binding written contracts with external bodies where those bodies are engaged to process Personal Data on our behalf. The Company will implement adequacy arrangements when transferring any

Personal Data outside of the European Union.

Other Third Party Access

The Company will only disclose Personal Data to third parties such as the police, central government and other educational institutions where there is a lawful basis for doing so and appropriate arrangements are in place with those parties.

Internal Sharing

The Company will seek to ensure that Personal Data is only shared across different teams, divisions or faculties where those areas have a business need for accessing that data.

5. Data Subjects Rights

The Company will comply with requests from an individual to exercise their rights under the DPA, and the GDPR. All individuals have the right to be informed of what information the Company holds about them and to request copies of that information. This is known as a Subject Access Request. Any individual wishing to

submit a Subject Access Request should contact the company in writing.

Under the DPA and GDPR, individuals also have the following rights in relation to their Personal Data:

- The right to request their Personal Data is rectified if inaccurate
- The right to request the erasure of their Personal Data
- The right to request that the Processing of their Personal Data is restricted
- The right of portability in relation to their Personal Data
- The right to object to the Processing of their Personal Data
- The right to object to Processing which involves automated decision making or profiling.

Individuals who wish to exercise the above rights should contact the Company's Data Protection Officer. It is recommended that Individuals submit their request in writing and specify exactly what Personal Data and/or Processing they are referring to and which right they wish to exercise. If you are seeking access to your Personal Data (i.e. making a 'Subject Access Request') then you may find it helpful to review the guidance available on our website.
Any staff member who receives a request from an individual to exercise the above rights under the DPA and GDPR must forward it immediately to the responsible person. All staff are responsible for cooperating with Legal Services to ensure that the Company can comply with an individual's request under the DPA and GDPR within the statutory timescales.

6. Own Personal Data

All staff and Customers are responsible for checking that information they provide to the Company in connection with their employment or studies is accurate and up to date. Any changes to Personal Data provided (e.g. change of address) must be promptly notified, in writing, to the Company.

7. Personal Data Breaches

The Company will respond promptly to any identified Personal Data Breaches and thoroughly investigate those incidents to ascertain whether:

The breach should or must be reported to the ICO

Data subjects should or must be made aware of the breach, and It is necessary to amend processes or introduce new measures to mitigate against any further breaches.

Any staff member who knows or suspects that an actual or potential Personal Data Breach has occurred must immediately notify the responsible. All staff are responsible for fully engaging and cooperating with DPO in relation to their investigation of a Personal Data Breach.

8. Compliance

Compliance with this Policy, the DPA and the GDPR is the responsibility of all members of staff and Customers. Employees must comply with the rules and procedures made by the Company.

Any breach of the policy by a member of staff may result in disciplinary action. Serious or deliberate breaches of the DPA can result in criminal prosecution.

Any breach of the GDPR by the Company may result in a substantial fine or actions imposed upon the Company by the ICO.

9. Further Information

Questions about the interpretation or operation of this policy should be taken up in the first instance with the Data Protection Officer. Any individual who considers that the Policy has not been followed in respect of Personal Data about themselves should also raise the matter with the Company’s Data Protection Officer.

Further information about the DPA and the GDPR can be found on the Information Commissioner’s Office (ICO website). Further guidance for staff can be found on the company’s data protection website. Please see the policy section of the SM Cars Norwich Ltd website for related policies.

Document Data Protection Policy Owner SM Cars Norwich Ltd Approved by Board of Directors

Annexe A Key Definitions

1. Personal Data’ means data which relates to a living individual who can be identified from those data or from those data and other information which is in possession of or is likely to come into the possession of, the Data Controller and includes any expression of opinion about the individual and any indication of the intentions of the Data Controller or any other person in respect of the individual. Under the GDPR, the definition of Personal Data will explicitly extend to IP addresses.
2. ‘Sensitive Personal Data means information:
   a. about an individual’s Special Category Data; and
   b. the commission or alleged commission by an individual of any criminal offence or any proceedings for any offence committed or alleged to have been committed by her or him, the disposal of such proceedings of the sentence of any court in such proceedings.
3. ‘Special Category Data’ means any Personal Data about an individual’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic or biometric data.
4. Processing means any operations or set of operations which is performed on Personal Data whether or not by automated means such as collection, use, disclosure or storage of Personal Data etc.
5. ‘Data Controller means the organisation that, either alone or jointly with another organisation, determines the manner and purpose of the Processing of Personal Data. The Data Controller is responsible for compliance with the DPA and GDPR.
6. ‘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 transmitted, stored or otherwise processed.