DATA PROTECTION POLICY

May 2018

Data Protection Policy

This is a statement of the Data Protection Policy adopted by M J Warner ARC and M J Warner Volkswagen

Introduction

This policy forms part of a suite of policies and procedures that support a data management and governance framework.

The business needs to hold and to process large amounts of personal data about its customers, potential customers, suppliers, employees, job applicants, contractors and other individuals to carry out its business operations. This includes current, past and prospective individuals and entities with whom we conduct business. Personal information, or data, must be dealt with properly however it is collected, recorded and used – whether on paper, electronically, or other means.

Responsibility for updating and dissemination of this policy rests with the compliance function and senior management. The policy is subject to regular review to reflect changes in legislation. All colleagues are required to understand, apply and abide by the policy and if in any doubt to seek advice. All colleagues, regardless of department, job title or seniority must receive General Data Protection Regulation training as part of a signed induction process.

Data protection law defines personal data as any information relating to an individual or identifiable person ("data subject"); an identifiable natural person is one who can be identified whether that is directly or indirectly or by reference to an identifier such as a name, an identification number, through using location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Purpose

Our purpose is to ensure that we handle personal information in accordance with the law. Compliance with legislation will be achieved through the implementation of controls and responsibilities including measures to ensure that:

1. Personal data is processed lawfully, fairly and transparently;
2. Personal data is processed only for the purposes for which it was collected;
3. Personal data is adequate, relevant and not excessive for the purposes for which it was collected;
4. Personal data is accurate and where necessary kept up to date;

5. Personal data is not kept for longer than is necessary;
6. Personal data is processed in accordance with the integrity and confidentiality principles

The business must take all reasonable and proportionate measures to ensure that personal data, both manual and digital are subject to an appropriate level of security when stored, used and communicated by the business in order to protect that data against unlawful or malicious processing and accidental loss, destruction or damage. It also includes measures to ensure that personal data transferred to or otherwise shared with third-parties have appropriate contractual provisions in place.

We will ensure that:

- The design and implementation of the company's systems and processes make adequate provision for the security and privacy of personal data
- Personal data will not be transferred outside the European Economic Area ("EEA") without the appropriate safeguards in place
- All colleagues receive adequate and effective GDPR training both at induction and on a regular ongoing basis
- We review and update our data protection policy as new legislation emerges
- We understand what personal data we hold, where it's held and where it goes
- We have a legal basis for our data processing activities
- We understand and properly define our processing activities
- We have enforceable written personal data handling agreements with all third party suppliers
- We carry out appropriate due diligence on all third party suppliers
- We attend to any subject access requests (SAR) in a timely manner (less than one month)
- We review and update our information security policy on a regular basis
- We update our annual registration with the ICO
- We align ourselves, as much as possible, with the objectives and requirements of ISO 27001
- We meet the requirement of the Cyber Essentials accreditation
- We check that all the above is kept in order via an appropriate compliance programme
- Additional conditions and safeguards will be applied to ensure that more sensitive personal data (defined as special category data) is handled appropriately by the business.

Data Subject Rights

Personal data must be processed in accordance with the rights of individuals. All data subject requests are handled by the compliance function and all requests must be referred to compliance immediately upon receipt. These rights are:

1. The right to be informed

2. The right of access (“Subject Access Request”)
3. The right to rectification
4. The right to erase
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

1. The Right to be Informed

All data subjects have a right to be informed as to how their data is being processes and whether it is being transferred to any third parties. We inform data subjects of our processing activities through the provision of our **Privacy Notice** which is available externally on the website www.mjwarner.co.uk and www.mjwranerarc.co.uk .

2. The Right of Access (“Subject Access Request”)

This is a right for an individual to obtain confirmation whether a data controller processes personal information about them and if they do, to be provided with details of that personal information and access to it.

3. The Right to Rectification

This is a right for an individual to obtain rectification without undue delay of inaccurate personal data that the data controller holds about them. For example if a customer notified you that you had inputted the wrong date of birth onto your systems then they would have the right to have this incorrect data amended with the correct date of birth.

4. The Right to Erase (Right to be Forgotten)

This is a right for an individual to require a controller to erase personal information about them on certain grounds. A customer (who has not bought a car) may wish to have their contact details removing from the marketing database. This is a reasonable request and must be actioned. The right to be forgotten however not an absolute right and in some circumstances the right will be refused on lawful grounds.

5. Right to Restrict Processing

This is a right for an individual to require a data controller to restrict processing of personal information about them on certain grounds.

6. Right to Data Portability

The data subject can request that all their data is transferred from one provider to another in a structured, commonly used and machine readable format and to transmit the information to

another controller.

7. **Right to Object**
   This is a right for an individual to object on grounds relating to a particular situation to a controller's processing of personal data about them if certain grounds apply.

8. **Rights in relation to Automated Decision Making and Profiling**
   If a decision has been made about a data controller using automated means or the data subject has been profiled then they have the right to have access to speak with a human being about this.

Special category data

Special category data is defined as personal data relating to an individual's:

- Race or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Health
- Sex life or sexual orientation
- In addition similar extra conditions and safeguards also apply to the processing of the personal data relating to criminal convictions

Most areas of the business will not be handing or processing special category data. If however you have a **motability customer** and you collect specific information about their physical or mental health or disability then this would be classed as special category data. Handling financial information is not classed as special category data but still needs to be sufficiently protected and kept secure.

Scope

This Policy applies to:

- All personal data held by the business whether held in a manual form (eg. in a filing cabinet or in a deal file) or held in a system Na
- All colleagues who work for or in M J Warner such as employees or workers regardless as to whether they are permanent, temporary, agency workers, casual, voluntary and/or

apprentices (the list is not intended to be exhaustive) and those working remotely from home

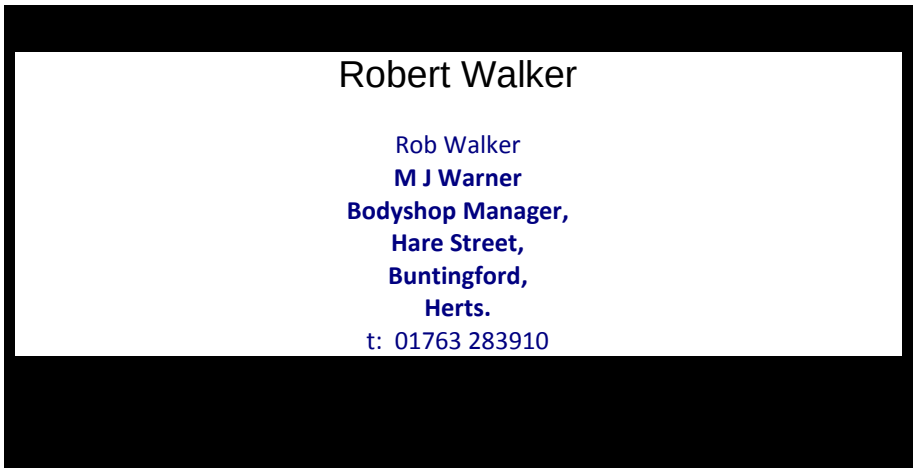
- All locations including dealerships, head office, all offices, buildings and other locations

Removal from the Marketing Database

If you receive a request from a customer to remove their details from the company's database as they no longer wish to receive marketing communications (whether by email, post, telephone or any other means) then simply email the details to reception@mjwarner.co.uk

Advice, support and assistance

Anyone who needs help with understanding and applying any of the data protection/GDPR policies and procedures must contact the company's **Data Protection Officer** whose details can be found below:



Resources and the full suite of data protection and procedures are available in the compliance Folder

Responsibilities and compliance framework

You must report the following to the compliance function in the business immediately upon become aware of the issue

1. Data protection complaint
2. Data protection breach or security incident
3. Data Subject request

You can contact the Data Protection Officer directly if you want to discuss a data protection issue by simply sending an email to Robert.walker@mjwarner.co.uk

All manual data must be disposed of in a confidential manner whether that is via use of a shredder or through the use of a confidential waste disposal unit. If you do not have access to either of these facilities please report this to compliance by email bodyshop@mjwarner.co.uk immediately.

You are expected at all times to comply with the M J Warner's GDPR Guidelines (see **"Schedule 1**"). They are there to help you achieve data protection compliance each and every day.

The company could be fined up to 4% of annual turnover if it breaches the data protection/GDPR principles. Therefore compliance with this Policy is of the upmost importance.

Colleagues must note that a breach of this Policy may be treated as misconduct under the company's relevant disciplinary procedures and could lead to disciplinary action or sanctions. Serious breach of this Policy may constitute gross misconduct and lead to summary dismissal or termination of contract.

Monitoring compliance

This Data Protection Policy and its implementation are subject to internal monitoring and auditing as part of the company's compliance monitoring framework. The outcomes of any auditing is intended to improve practices and ensure a high standard of regulatory compliance.

Review of Policy

This Policy will next be reviewed in **December 2019** or when any significant changes in data protection legislation occurs.

Schedule 1

GDPR Guidelines

1	Familiarise yourself with the company's IT and data protection policies
2	Lock you PC when leaving your desk.
3	Don't share or write down passwords.
4	Don't leave personal data on an open desk, or other open, accessible or public area.
5	Dispose of confidential data by shredding it or placing it in one of the secure confidential waste bins provided – never recycle it and never put it in a waste paper basket.
6	Don't write anything in an email about a customer or colleague that you wouldn't want them to read.
7	Check the identity of any caller that is requesting information.
8	If a third party makes contact on behalf of someone else, makes sure the data subject has provided "consent" for that third party to act on their behalf (this includes external organisations).
9	Do not underestimate the importance of data protection and its potential consequences – you could be fined personally in addition to the company if a breach occurs.
10	Respect others people's data in the same way that you would expect other people to respect yours – keep it secure at all times.
11	Remember that a loss of data can lead to identity theft, fraud and money laundering offences, so take care.
12	If a customer wants to be removed from the marketing database then please email reception@mjwarner.co.uk providing full details.
Contact COMPLIANCE immediately for any of the following:	
13	You become aware of a security incident or personal data breach
14	You receive a data protection complaint
15	You want some advice and assistance on a GDPR/data protection issue
16	An individual makes a data subject request relating to one of the a data subject right (see below)

	Compliance contact details: Robert Walker Rob Walker **M J Warner** **Bodyshop Manager,** **Hare Street,** **Buntingford,** **Herts.** t: 01763 283910	**Data Subject Rights:** • The right to be informed • The right of access • The right to rectification • The right to erasure • The right to restrict processing • The right to data portability • The right to object Rights in relation to automated decision making and profiling
