Pendragon | PLC

Adopted: 02 May 2018

DATA PROTECTION & PRIVACY, INFORMATION AND CYBER SECURITY POLICY 2018 – 2019

Pendragon PLC and the Pendragon Group, which includes our businesses trading as Evans Halshaw, Evans Halshaw Car Store and Stratstone (together, "Pendragon", the "Company", "we", "us" or "our") take the issues of information security, cyber security and data protection and privacy very seriously. We are committed to protecting the privacy and security of our customers, team members, suppliers, online visitors and other third parties during the course of our activities. We have adopted this Data Protection & Privacy, Information and Cyber Security Policy (the "Policy") setting out the principles and approaches by which we will manage information technology, cyber security and data security risks.

DATA PROTECTION & PRIVACY POLICY

We collect, store and process Personal Data belonging to our customers, potential customers, suppliers, team members and other third parties ('Data Subjects') during the course of our activities. Data protection laws give our Data Subjects rights to control how their Personal Data is used. We follow the principle that Personal Data belongs to Data Subjects, not to us, and Data Subjects should be able to control and be comfortable with everything we do with their Personal Data. We are committed to being transparent about how we collect, store and process the Personal Data of our Data Subjects. We believe that Data Subjects should feel both informed and empowered when it comes to how we handle and use their Personal Data.

DEFINITIONS USED IN THIS POLICY

The definitions used in this Policy shall have the same meanings as used in the General Data Protection Regulation (Regulation (EU) 2016/679) and any applicable UK legislation that modifies, implements or applies it (the "General Data Protection Regulation" or "GDPR" for the purposes of this Policy):-

Controller in most instances in this Policy, the Controller will mean us, but it may also include another natural or legal person such as another company or agency we work with. The Controller will determine the purpose and means of Processing Personal Data, or in other words, will decide what Personal Data will be Processed for, and how it will be done.

Consent of the Data Subject means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes.

Data Subject means an identified or identifiable natural person, and references to "you" or "your" in this Policy are intended to be references to Data Subjects, unless the context requires otherwise.

Pendragon Group means Pendragon PLC and any company over which Pendragon PLC has exercised or is entitled to acquire direct or indirect control over that company's affairs, control to have the same meaning as in section 450 of the Corporation Taxes Act 2010.

Personal Data means any information relating to a Data Subject, where a Data Subject can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, 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.

Processing or Process means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organising, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processor means a natural or legal person who Processes Personal Data on behalf of the Controller.

Profiling means any form of automated Processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to a natural person.

Special Categories of Personal Data means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, data concerning a natural person's sex life or sexual orientation.

OUR DATA PROTECTION PRINCIPLES

In accordance with the GDPR, we apply the following principles relating to the processing of Personal Data belonging to our Data Subjects.

Data Protection Principles

We adhere to the following principles in relation to Personal Data, and ensure that Personal Data is:-

(a) processed lawfully, fairly and in a transparent manner in relation to the Data Subject;

(b) collected for specified, explicit and legitimate purposes;

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

(d) accurate, and where necessary, kept up to date. Pendragon will take every reasonable step to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

(e) kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are Processed;

(f) processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures;

(g) Recognised as belonging to our Data Subjects, not to us, and ensure that our Data Subjects are able to control and be comfortable with everything we do with their Personal Data.

TRANSPARENCY AND PRIVACY NOTICES

We remain committed to protecting the privacy of our Data Subjects, which is why being transparent and informing our Data Subjects how we collect Personal Data, why we collect Personal Data, how we share Personal Data, for how long we keep Personal Data, what rights our Data Subjects have with regard to their Personal Data and our approach to information and cyber security is fundamental to our approach. Informing you of what we are doing with your Personal Data is important to allow you to provide valid consent for its use, allow you to exercise your rights or ultimately, helping you decide whether or not to provide Personal Data. We will provide clear, accessible, specific and plain language privacy notices to our Data Subjects, in addition to the information contained within this Policy.

HOW DO WE COLLECT PERSONAL DATA?

In any interaction a Data Subject may have with us, we collect Personal Data in three main ways:-

- **When a Data Subject directly gives Personal Data to us (Directly Provided Data)**

  When you are a customer or potential customer and visit one of our websites, purchase our products, supply us with goods and services, join Pendragon as a team member or otherwise communicate with us, you may choose to voluntarily give us certain Personal Data. All this information requires a direct action by a Data Subject in order for us to receive it.

- **When a Data Subject gives us permission to obtain it from other accounts or information (User Authorised Data)**

  In some situations, depending on the settings or privacy policies for other online services, a Data Subject may give us permission to obtain information from an account with those other services. For example, social media is becoming an increasingly important part of how our businesses interact with our customers. In using certain social media services, you may provide us with permission to access Personal Data in that social media channel or in other services. So, if you did choose to link your social media account to us, this may enable us to obtain information and content from those accounts. The Personal Data we obtain from services in this way will depend on the settings for that service or their privacy policies. Data Subjects should regularly check what these are. Similarly, if you are an existing customer and have provided Personal Data to one of our dealerships, you may have already authorised for it to be shared with our other businesses.

- **As our Data Subjects use our websites or apps, or use websites or apps that are connected to us, our systems may collect information or data (System Collected Data)**

  Often, when you use a website, app or other internet service, certain information is created and recorded automatically by the IT system that is used to operate that site, app or service. The same is true when you use our websites, apps and services. For example, when accessing our websites, we use “cookies” to make it easier for you to use our websites and improve your online interaction and experience. Cookies allow us record and log data relating to the pages you visit, the vehicles or products you have viewed and the activities carried out during your visit. Further details of our cookies policies can be found on our websites and within our privacy notices.

WHY DO WE COLLECT PERSONAL DATA AND HOW MIGHT WE USE IT?

Doing business with our customer and prospective customers

Personal Data belonging to our customers and prospective customers is collected in order to establish, execute and terminate contracts to buy vehicles, parts and other services from our dealerships.This may also include advisory services for our customers if this is related to the contractual purpose. We may also collect Personal Data to prepare purchase orders or to fulfill other requests of prospective customers prior to concluding a contract.

Advertising and Marketing activity

If a Data Subject contacts us to request information, for example about a particular vehicle or offer, we will have a legitimate interest for Processing Personal Data. In some circumstances, our customers or prospective customers may consent to us contacting them with follow up information, details about customer loyalty schemes, invitations to launches and events or to allow us to conduct market and opinion research. We will always seek to ensure that we have a clear, unambiguous consent from a Data Subject to process their Personal Data or contact them for advertising and marketing purposes unless we have a legitimate interest to make contact otherwise. We will not share Data Subject's Personal Data with third party advertisers or ad networks without having obtained your express consent to do so.

Employment and Human Resources

Personal Data may be Processed by our human resource and recruitment teams for a number of reasons. For existing team members, we may Process Personal Data to allow us to maintain accurate records and contact details of our team members and for HR and business administration purposes where it is in our legitimate interest to do so. In addition, we will Process Personal Data if we need to initiate, carry out or terminate employment contracts with our team members or prospective team members. Initiation of an employment relationship will require the processing of a prospective team member's Personal Data. If a prospective team member is rejected, his/her Personal Data is held for the required retention period, unless the prospective team member has agreed that the Personal Data can remain on file for a future recruitment and selection process. Team member Personal Data gathered during the employment relationship is held on the individual team member's personnel file (in written or electronic format) and on human resource systems. The periods for which Pendragon holds human resource related Personal Data are contained in its privacy notices to team members.

HOW DO WE SHARE PERSONAL DATA?

It is Pendragon you are trusting with your Personal Data, not another company or third party. However, there are some occasions where for us to be able to carry on our business with our Data Subjects, we need to work with a number of third parties with particular expertise. Such situations may involve the sharing of Personal Data for the performance of a contract, for the purposes of complying with a legal obligation of which we are subject or for the purposes of pursuing our legitimate interests. In this regard, we are always very careful who we choose to share your Personal Data with, and will never share Personal Data with a partner, company or other third party who cannot evidence that they have in place a data protection and privacy policy of an equivalent or better standard to this Policy. The following provide examples of the typical instances where we may share Personal Data:-

- We share Personal Data internally within the Pendragon Group when required for our business to function: As a large, nationwide business, Pendragon does not operate as a single company, but is made up of a group of companies. It may be necessary to disclose Personal Data of our Data Subjects to any of our group companies, in order to operate our business. For example, if you a Customer using our Move Me Closer (MMC) scheme, Personal Data may be shared between the dispatching dealership and receiving dealership, which maybe under separate legal entities.

- Customer Personal Data may be shared with our manufacturer partners: For example, in order to register and activate a warranty on a new vehicle purchased by one of our customers, we may need to share Personal Data with our manufacturer partner.

- Customer Personal Data may be shared with service plan providers: if you are a customer who has purchased a service plan with a vehicle, this may be administered by an external company on our behalf, and we will share Personal Data with them for the purposes of administering and managing your plan.

- Customer Personal Data may be shared with finance providers: our dealerships act as the introducer or broker of finance products and solutions provided by third party lenders or providers, which allow customers to purchase vehicles with the assistance of finance.

In order to propose customers to our third party lending partners for finance products, it is necessary to share customer Personal Data with such providers and subsequently credit reference agencies.

- Team member Personal Data may be shared with the providers of our payroll and employee benefit platforms: our payroll, pensions and team member training and learning platforms maybe provided by third party companies, with whom we may share team member Personal Data.

- We share Personal Data when we're required to comply with a legal request: from time to time, we may be required to share Personal Data in order to comply with a legal obligation to which we are subject. For example, if we have sold a vehicle to a customer which is later involved in a motoring offence, we may be obliged to share the Personal Details of that customer with the Police or other law enforcement agency or investigatory body in accordance with due legal process. Similarly, certain regulators or other law enforcement agencies may require us to share Personal Data with them, under law or pursuant to a court order. Where we do come under a legal obligation to share Personal Data in order to comply with legal obligations, we will share such Personal Data where we believe it is reasonably necessary to comply. However, where we consider disclosure requests to be vexatious, spurious, vague or have been made without proper authority, we reserve the right to dispute the same and may resist the disclosure of Data Subjects' Personal Data accordingly. We will always attempt to notify our Data Subjects of a legal or regulatory demand for disclosure of Personal Data, unless to do so would prejudice an investigation or where we are prevented from doing so by law or court order.

- We share Personal Data for the purposes of detecting, investigating or preventing suspected or actual illegal activities or fraud: to assist in the detection, investigation or prevention of fraud or other illegal activities, investigate or defend ourselves against third-party claims or allegations, protect the security and integrity of our business and services or otherwise in order to protect our legitimate interests we may share Personal Data.

We will **never** sell Personal Data or share it with third-party advertiser or ad networks without having obtained the express consent of a Data Subject to do so.

HOW LONG DO WE KEEP PERSONAL DATA?

To protect our legitimate interests, we need to be able to produce documents and supporting paperwork relating to the transactions our businesses have done. Contracts formed with our Data Subjects and other documentation will invariably contain Personal Data. Our objective is only to retain Personal Data of our Data Subjects for so long as the information is necessary to perform our contracts, or comply with our statutory or other legal obligations. We will also retain Personal Data if we are legally required to do so or if it is reasonably necessary to meet regulatory requirements, resolve disputes, prevent fraud and abuse or enforce our terms and conditions.

WHAT RIGHTS DO DATA SUBJECTS HAVE IN RELATION TO PERSONAL DATA?

We recognise that our Data Subjects have a number of rights attaching to their Personal Data. Some of these rights are existing rights, and others are new rights arising from the GDPR. We recognise all our Data Subjects' rights, and will process Personal Data in accordance with GDPR as follows:-

- **The right to be forgotten**: we recognise that our Data Subjects have the right to request that we delete their personal data in certain limited circumstances. The right to have Personal Data erased without undue delay applies only where (a) the retention of Personal Data is no longer necessary for the purposes for which they were collected or Processed; (b) the Data Subject withdraws consent on which the Processing is based (only applicable to those situations where the Data Subject has given clear, unambiguous affirmative consent to the Processing of Personal Data; (c) there is no other legal ground for the Processing; (d) the Data Subject objects to the Processing in conjunction with the right to object (see below) and there are no overriding legitimate grounds for the Processing; (e) the Data Subject objects to the Processing for direct marketing purposes; (f) Personal Data has been unlawfully processed; (g) Personal Data has been erased to comply with a legal obligation. Where we receive a request to erase Personal Data within one of the grounds (a) – (g) outlined above, and we have made Personal Data public, we will take reasonable steps, including technical measures, to inform any other Controller or Processor who is Processing the Personal Data that the Data Subject has requested deletion of any links to, copies or replication of the Personal Data.

- **The right to rectification:** Our Data Subjects have the right to request that we correct, without undue delay any inaccurate Personal Data we hold about them. This means that if we hold incomplete Personal Data, we will complete it.

- **The right to restrict processing**: Our Data Subjects have the right to request the restriction of Processing of Personal Data where (a) the accuracy of the Personal Data is contested for a period enabling us to verify its accuracy; (b) the Processing is unlawful, the Data Subject opposes the erasure of the Personal Data and requests the restriction of its use in the alternative; (c) the Controller no longer needs the Personal Data, but it is required by the Data Subject for the purposes of establishing, exercising or defending legal claims; (d) the Data Subject objects to the Processing on the basis that the Controller does not need to process the Personal Data for a purpose in the Controller's legitimate interest, pending verification of the same. If Processing has been restricted for any of the above reasons, such Personal Data shall only be Processed with the Consent of the Data Subject.

- **The right to object to direct marketing:** Our Data Subjects have the right to object to the Processing of Personal Data for direct marketing purposes, including for Profiling purposes where the Profiling is related to direct marketing.

- **The right to data portability:** we recognise the right of our Data Subject to receive Personal Data concerning them which they have provided to us in a structured, commonly used and machine readable format, and will use our reasonable endeavours to transmit Personal Data to another non-Pendragon Controller should a Data Subject request that we do so, and provided it is technically feasible.

- **Data Subject access requests**: Our Data Subjects are entitled to make a subject access request to obtain a copy of their Personal Data. We will not charge for the first data subject access request, but may do so if you ask for further copies of Personal Data. Please note that if we consider that a Data Subject makes excessive requests, or the request is manifestly unfounded or excessive, we reserve the right to refuse to respond to the request. If you wish to make a data subject access request, you should specify exactly what information or processing the request relates to. Under GDPR, we have one month to respond to a data subject access request, although we may extend this by a further two months if the request is complex or we are dealing with a large volume of requests. We reserve the right to withhold the disclosure of Personal Data in circumstances where disclosure would adversely affect the rights and freedoms of others, for instance things that might adversely affect our business including disclosure of information which may adversely affect our intellectual property rights, trade secrets or confidential information.

- **The right to object to Profiling**: Our Data Subjects have the right not to be subject to decisions made automatically that produce legal effects or which significantly affect them. In terms of our business, Profiling may include some online tracking and behaviourial advertising, such as the use of cookies for the purposes of delivering targeted advertising to you. These cookies will also limit the number of times a Data Subject sees an advertisement, to help us measure the effectiveness of our marketing campaigns. If you wish to object to Profiling, you have a right to do so and we will not use Personal Data for this type of activity if you object. We will always tell you at the outset if we are Profiling, and we will conduct a data protection impact assessment before carrying out any Processing that uses new technologies that is likely to increase the risk to our Data Subjects in the use of Personal Data.

As a predominantly consumer facing business, we recognise that our Data Subjects may wish to exercise one or more of a combination of these rights. We will always do everything we can to empower our Data Subjects and ensure that they retain control over their Personal Data. If you wish to exercise any of the above rights, please e-mail either dataprotection@evanshalshaw.uk.com for our Evans Halshaw and Evans Halshaw Car Store businesses, dataprotection@stratstone.uk.com for our Stratstone businesses or otherwise dataprotection@pendragon.uk.com We will send you a Data Subject Rights Request Form accordingly. Please note that we will endeavour respond to a request within one month, although in some cases, where the request is complex or we are dealing with an excessive volume of requests, we may extend this period to two months.

HOW DO WE STORE PERSONAL DATA?

We store our Data Subjects' Personal Data in accordance with data security measures as detailed in our the Information and Cyber Security section of this Policy below. As a large business, data security (including Personal Data) remains a priority, and we have taken a number of steps to secure our systems.

SPECIAL CATEGORIES OF PERSONAL DATA

We will not process Special Categories of Personal Data unless a Data Subject has given explicit consent to the Processing of it or the Processing is necessary for the purposes of carrying out certain of our employment, social security and social protection law obligations. Special Categories of Personal Data are most likely to be processed in the context of our team member Personal Data. Team member Personal Data gathered during employment will be held in the individual's personnel file (in written or electronic format) and on our HR systems.

DATA PROTECTION OFFICER

The company secretary of the Company acts as the Data Protection Officer, and monitors compliance with the GDPR and this Policy. The Data Protection Officer remains entirely independent from our internal audit function, which has responsibility for day to day monitoring of procedures and processes at Dealership level to ensure compliance with this Policy.

If you have a complaint about how we have handled your Personal Data, or wish to raise any concerns about the way this Policy has been applied, in the first instance, please e-mail either dataprotection@evanshalshaw.uk.com for our Evans Halshaw and Evans Halshaw Car Store businesses, dataprotection@stratstone.uk.com for our Stratstone businesses or otherwise dataprotection@pendragon.uk.com

INFORMATION & CYBER SECURITY POLICY

Pendragon implements appropriate technical and organisational measures to ensure information we hold and receive, including Personal Data is protected against loss, accidental destruction, misuse or disclosure. In addition, we treat all Personal Data as confidential information, and have processes in place to prevent any unauthorised collection, processing or use of Personal Data by our team members that has not been authorised as part of a team members' legitimate duty. Team members may have access to Personal Data as appropriate to their role and function, for a specific task or activity, and are made aware of, and trained in aspects of this Policy accordingly. As soon as we receive information, we implement various security features and procedures, to try and protect information and Personal Data provided, and prevent unauthorised access to it. For example:

- Our technology company, Pinewood Technologies Plc is ISO27001 accredited, which is an internationally recognised best practice standard in information security management;
- We expect all suppliers with whom we may share Personal Data to achieve ISO27001 or equivalent accreditation;
- To protect information, including Personal Data stored on our servers, we regularly monitor our system for possible vulnerabilities and attacks, as well as carrying out penetration testing on our systems as part of a process of continuing and never ending improvement and enhancement of our protections;
- We offer secure "https" access to the transactional parts of our system, such as payments under our Move Me Closer (MMC) scheme;
- We have implemented two-part encryption and authentication for internal team member communications.

Data security is a priority for our business, and we will do everything we can to protect information provided to us through measures such as the above. However, our Data Subjects should also do whatever they can to keep Personal Data and information secure by using strong passwords, reviewing privacy settings and be aware that when communication methods such as instant messaging and emails are not always encrypted, so should not be used for confidential communications.

DATA BREACHES AND CYBER ATTACKS

If we discover that there has been a breach or violation of our systems, such that information or Personal Data is unlawfully accessed or obtained by a third party, we will report the breach to the Information Commissioner within 72 hours of its discovery. We will record all data breaches regardless of their effect.

If we consider that the data breach is likely to affect our Data Subjects' individual rights and freedoms, we will inform them of the nature of the breach without delay.

Data breaches and cyber attacks are dealt with in accordance with our tiered Data Breach Response Plan (DBRP), which has clearly delineated escalation levels in the event of a data breach or cyber attack. Each incident and a proportionate response will be considered in light of the prevailing facts and circumstances. Although we consider all incidences of data breach or potential cyber attack with seriousness, our DBRP is designed to avoid over reaction to relatively minor incidents.

- First tier response: relatively minor incidents will be dealt with autonomously by a team member of the appropriate level of responsibility, with assistance from Group Legal and the Data Protection Officer where required.
- Second tier response: for more serious incidents, we will convene a dedicated data breach incident response team, who will be appointed to manage the incident. The leader of the data breach incident response team will be on an appropriate level of seniority and expertise, be immediately available and have the authority to draw on the resources of the business, including specialist team members, to manage the incident.
- Third tier response: for major or significant incidents, the Company's Risk Control Group will be convened made up of the chief operating officer, finance director, company secretary and Group heads of information technology and internal audit, plus other specialist team members as appropriate, together with external advisors (where necessary), to deal with both the immediate response as well as assessing the extent of the data breach and cyber attack and its cause.

STATUS OF THE POLICY

This Policy is adopted by the Company. It may be varied or withdrawn at any time, in the Company's absolute discretion. We encourage you to regularly check our website for any updates or changes to this policy.