

Data Processor Questionnaire

Please complete the following questionnaire fully and completely. Please note the following instructions:

- For the purposes of this questionnaire, references to **personal data** mean the personal data you receive or will receive from <insert dealerships> (or one of its affiliates) in the provision of services to <insert dealerships> plc (or one of its affiliates).
- References to **you** mean the entity or entities that will be processing the personal data; please ensure your answers to the questions below reflect this.
- Do not leave questions blank; if you are unable to answer a question please explain why.
- If your response refers to documents (eg policy documents), please also provide a copy of each relevant document when you return the questionnaire.

1.	Your details	
1.1	Organisation name (please list all entities within the organisation that will receive and process personal data):	
1.2	Name of person completing this form:	
1.3	Position held within the organisation:	
1.4	Contact details for this person:	
1.5	Date this questionnaire was completed:	

2.	General	
2.1	Who is your Data Protection Officer or most senior person responsible for data protection issues?	
2.2	What relevant accreditation / standards / certifications / codes of practice / codes of conduct relating to data protection or information security have you been awarded or does your organisation comply with?	
2.3	What steps have you taken / are you currently taking to ensure your organisation's processing of personal data will be compliant with the European General Data Protection Regulation when it enters into force in May 2018?	
2.4	Have you prepared a privacy impact assessment in relation to your processing of personal data? If so, please provide a copy.	
3.	Compliance and incidents	
3.1	Please confirm that you comply with all applicable laws and regulations relating to data protection, the processing of personal data and privacy (collectively data protection law).	
3.2	Please confirm that you have not received any complaints or been the subject of any investigations, regulatory enforcement	

	action or litigation in relation to compliance with data protection law.	
3.3	Please confirm that you have never had any data security incidents or breaches (eg data thefts, unauthorised access, data losses).	
4.	Physical and technological security measures	
4.1	What physical measures have you put in place to restrict and monitor physical access to locations containing personal data and to protect the personal data? (Eg CCTV or controlled entry)	
4.2	What technological measures have you put in place to protect personal data and prevent unauthorised access? (Eg encryption, pseudonymisation, security monitoring systems, routine security assessments and testing, controlling access, minimum password standards, remote access by multi factor authentication, firewalls, anti-virus software etc)	
4.3	How often are these physical and technological measures tested, reviewed and updated?	
5.	Organisational arrangements	
5.1	What organisational arrangements have you put in place to protect personal data?	

	<p>These could include:</p> <ul style="list-style-type: none"> • Policies on data protection, information security, use of employees' own devices, home working, company devices being used away from the workplace, etc • Staff training • Routine security assessments and testing • Information governance structure 	
5.2	What steps do you take to ensure the reliability of staff who have access to personal data?	
5.3	Please describe your starters and leavers process, including the process for revocation of physical and logical access on departure.	
5.4	What policies and procedures do you have in place to detect and investigate a data security incident or breach?	
5.5	What policies and procedures do you have in place to govern your response to a data security incident or breach?	
5.6	How often are the arrangements referred to in your response to questions 5.1 to 5.5 (inclusive) tested, reviewed and updated?	
6.	Business continuity and data retention	
6.1	Please explain your business continuity and disaster recovery arrangements.	

6.2	How do you ensure personal data is not retained for any longer than is necessary?	
6.3	What steps do you take to ensure secure disposal or return (as the case may be) of personal data upon the conclusion of the data processing activities?	
7.	Data transfers and data sharing	
7.1	<p>Please confirm that all personal data is stored, processed and accessed within the UK.</p> <p>If data is transferred outside the UK or accessed from outside the UK, please provide details.</p>	
7.2	<p>Please confirm that personal data is not shared with, or processed by, subcontractors.</p> <p>If you do share personal data with subcontractors, please provide details and explain how you ensure that the subcontractors keep that data secure and in accordance with the measures described in this questionnaire.</p>	
7.3	Please confirm that personal data is never removed from your premises.	

End of questionnaire