GDPR Centre Checklist

Oct-17

This checklist is provided as a thought starter for Centres to consider in preparation for GDPR compliance for May 2018. Whilst it may reference GDPR concepts it should not be taken as Legal advice or counsel.

	Touchpoint	Channel	GDPR Consideration	Centre Status / Next Steps
1. Vehicle Purchase Journey	Lead Capture	Online : Centre / Group Websites Centre Event Contact Centre : Inbound In Centre : Walk In	**Data Privacy Policy and Fair Collection Notice** needs to reference : > Data Retention Policy - How long do we keep customer data? > Purpose for holding the data - Why? > Who the data is shared with > Where the data will be stored/accessed (whether inside or outside EEA) > Alignment of Data Privacy policy wording with TGB > Same Privacy wording across all Centre channels **Consent Capture** (Additional to Lead Capture / Data Privacy Notice) : > informed and freely given - No default Opt In for email marketing > Consent captured across 4 standard categories > Evidence recorded of consent captured / consent changed > Consent validated with Customer / Prospect	Capture: 1. current situation 2. gaps toward GDPR 3. proposed countermeasure actions (prioritised) 4. discuss and share progress with TGB field team in Q1 2018
	Sales Journey : Qualification, Test Drive, Choose, Quote, Purchase	In Centre : Face to Face	At any of the Sales Journey touchpoints a customer can provide new, or update existing Permission/Preference data. As with the initial Lead capture process we are looking to capture consent across 4 categories : 1). Reminders 2). Offers 3). Surveys 4). Events Once the consent data is captured the following actions will be required : > Consent Data to be stored in local DMS &/or local SMS, and shared to TGB > Record of the change date / time to be recorded and stored in DMS &/or local SMS and shared to TGB > Customer to be emailed with details of the changes made, and requested to validate that the changes are correct. Customer should be prompted / able to click on a link in the email and sent to a validation web page. This validation step is not required if the customer 'directly' entered the consent data themself (e.g. via an iPad). > Status of change to be recorded as 'Unvalidated' until Validation process completed.	
	(NOTE : Similar expectations exist in respect of Data Privacy Notice and Consent Capture for After Sales Customer Journey touchpoints)			
2. Customer Communication	Outbound Customer Communication (Reminders, Marketing Offers, Surveys and Events)	Email / Letter / SMS / Phone	All local communications to customers generated by the Centre must ensure that they are sent within the permissions as defined by the customer. There should be two steps applied to ensuring that the inclusion of the customer into the communication is correct : 1). Check the local Centre DMS/SMS for previously provided consent permissions 2). (When available) additionally check the central Subscription Centre system for confirmation of consent settings at a more granular level (based on the 4 consent categories). If there are no details held within the central Subscription Centre revert to the local DMS/SMS information	
3. Customer Rights	Customer Rights Management	Inbound (to Centre) Customer Requests	Customers may at any time trigger any of the 8 Customer Rights requests as follows : 1). Rights to Access: Information confirming what Personal data is captured and who has access to it 2). Rights to Portability : Ability for a customer to receive in an electronic, machine readable format, a copy of the personal data held against them 3). Right of erasure: Ability for customer to get their personal data removed (there are exception around legal obligations that mean this cannot always be completed). 4). Right to be informed : Requirement to inform a customer of what processing takes place with their data. Typically provided via a privacy notice at the point of capture. 5). Automated profiling and decision making: right not to be subject to a decision that is based on automated processing that has a significant effect on the data subject 6). Right to rectification: Customer has right to correct data held 7). Right to restrict processing: Customer can request no further processing 8). Right to object: Customer can object to processing in certain limited circumstances. The execution of the Customer rights request can be manual (system automation not required), but there must be a record of every request made, including requesting customer details, date, time and resulting actions taken.	
4. Data Security	Data Security Management	Data Breach	Any data breach that is "likely to result in a risk to the rights and freedoms of individuals" must be reported to (in this order) : 1). TGB DPO immediately (within 24 hours) 2). UK Authorities - ICO (within 72 hours) 3). Work with TGB on response to customers where risk to "rights and freedoms" is HIGH There must be an audit log of each Data Breach occurrence, including overview of date / time, volume of customer records impacted, listing of impacted customer details, outline of actions taken to inform the authorities, understanding of root cause and repair actions completed. Consider Data Breach Policy to map process to be followed.	
5. Consent	Consent Validation	Customer Contact - In Centre or via other communication	Review consent held against each customer records held within DMS / SMS systems. Consider : 1). Dialogue with customer as and when they are in contact with you - validate information at Service, Repair, Vehicle Purchase touchpoints 2). Non solicited communication - but be careful - Do Not link to any marketing message / campaign	
6. Training	Staff Training & Awareness	In Centre	Consider company policy towards data management : > No emails including customer information either within email text > Email attachments (containing customer details) to be secured by Password - Password to be sent under separate cover > No storing of Customer records on mobile devices (laptops, memory sticks...) that are not encrypted > consider risk of paper records and remote working General training on six principles of GDPR to all staff	