The Motor Ombudsman – Radius Law Webinar
GDPR - What do the new data protection laws mean for the motor industry?
April 2018

Questions & Answers

	Questions	Answers
	Consent	
1	Can a business contact customers to remind them that their MOT / Servicing is due? Do such requirements require consent? Will the business be required to implement any changes to their processes to be compliant with GDPR? Do different methods of communication (e.g. call, letter, email, etc.) need to be treated differently? How about contacting a customer for more general marketing after they have been in for a service / repair?	MOT and service reminders are marketing communications and the regulator recommends that consent is obtained for all marketing. That said, if the reminders are sent by post or by phone, the business could rely on Legitimate Interests rather than consent (see answer to Q15 for more information on Legitimate Interests). For electronic reminders (email/text) then consent will usually be required, but don't forget that for recent customers it's likely that you will be able to rely on the soft opt-in rule. Soft opt-in allows you to send e-communications (without a positive opt-in consent) to recent customers of similar products or services, provided they have always been given the right to opt-out and they have not opted-out.

2	What is the best practice for obtaining, evidencing and recording consent? How can this be achieved in the simplest way possible?	Consent does not need to be in writing (although that's the best evidence). If you take consent verbally, then you will need to be able to demonstrate that you have a robust process e.g. forms on your dealer management system that must be completed to record what consents have been given.
3	Does consent need to be treated differently depending on whether a business is dealing with an existing customer or a prospect?	The only significant difference is that for recent existing customers, you may be able to rely on the soft opt-in rule (see answer to Q 1)
4	How will existing consent be treated under GDPR? If a business has existing consent process for either MOT / service reminders or general marketing, can they continue to communicate with their customers under GDPR as well?	If a business is relying on consent, it must meet the GDPR standard of consent to continue to use it after 25.05.18. Consent under GDPR has more 'bells and whistles' than before (more guidance is available on the Information Commissioner's Office website). In particular, consent needs to be on an opt-in, rather than an opt-out basis. It's unlikely that many businesses will have obtained consent to the GDPR standard and therefore the consents obtained will be redundant.
5	How should customer details captured in a diary as they book in the vehicle treated? Does this require a separate consent?	This does not require consent. If the diary is simply for booking in a vehicle for a service, then you are only recording information that's necessary for the particular job - so would not need consent.
6	At what stage should consent be sought from a potential customer? E.g. when they come in the showroom interested in a vehicle	If you are only going to respond to the prospect's specific enquiry, then you do not need consent. If you plan to send the prospect general marketing in the future then the regulator recommends that you seek consent before doing so. It is however possible to use Legitimate Interests, rather than Consent for postal and phone marketing (see answer to question 1)
7	Is implementing a new form to get customers to opt-in enough? Similarly, is adding a statement to invoices that customers can tick and sign to opt-in enough?	This sounds okay - providing the opt-in statements meet the GDPR requirements and the data capture statement also links to a privacy policy to provide the customer with the detail of your data processing and their rights
8	Do we need to seek consent from all existing customers as well as new ones? Are businesses allowed to contact all customers to ask for consent? Do we need to let all existing customers what information we currently hold for them?	If you are relying on consent (see above answers for more detail) and your current consents do not meet the GDPR standards, then you will need to get the consents refreshed to continue using the data post 25.05.18.

9	Does consent have an "expiry"? Is consent valid for a specific period of time? Does it need to be revisited on a regular basis? Or is it valid until the customer "opts-out"?	It is important to show that you are keeping your database up-to-date, so a process of regularly checking with customers is a good idea.
10	Do we need to record customers consent when sending out estimates, if so what is the best way to record their consent?	If you have been asked to provide an estimate - then by providing the estimate, you are simply responding to the enquiry and consent is not needed.

Re-permissioning

11	What is the definition of re-permissioning? E.g. If we were to suppress an existing customer on our database because we know that existing consents gathered are not valid for GDPR purposes, can we update their consent when they next get in touch with us, or would this be held to be 're-permissioning'?	Yes, we think it is acceptable and a good practice to ask customers when they next contact you, whether they would like to update their marketing consents.
12	If we delete existing customer records, is it OK to then treat them as an entirely new customer if they come back into dealership again (or would this be re-permissioning?)	We recommend that you only delete lapsed customers that have not opted-out of marketing. For customers that have opted out of marketing it is important to retain minimal information about that person to ensure they are not accidently opted back into marketing. With this exception, yes, we think you can treat the customer as an entirely new customer when they come back into the dealership

Soft opt-in

13	Can you clarify what is meant by soft opt-in and how does it work under GDPR?	Soft opt-in allows you to send e-communications (without a positive opt-in consent) to recent customers of similar products or services, provided they have always been given the right to opt-out and they have not opted-out.
14	Is there an acceptable timescale for using soft opt-in after a customer purchase? E.g. Can soft opt-in be used to send direct mail to a customer who bought a vehicle from a dealer 2 years ago?	This is a judgement call and it will depend on what's an appropriate/reasonable time - there is no defined period. Given that customers will often keep cars for 3+ years, we believe that 2 years is a reasonable period to rely on soft opt-in.

Legitimate interest

15	What is legitimate interest?	Legitimate interest is one lawful basis for the processing of personal data. It is an alternative to consent. If you have a genuine and legitimate reason (including commercial benefit) then it can be used, unless this is *'outweighed by harm to the individual's rights and interests'* e.g. it would not be appropriate to use Legitimate Interests to justify marketing to children. In addition, separate data laws state that Legitimate Interests cannot be used for electronic marketing
16	Is sending out MOT / Service due reminders "legitimate interest"? Does the communication method matter (i.e. letters, email, SMS, calls)?	See answer to question 1
17	Similarly, can legitimate interest be used for finance renewal process / PCP to remind a customer that their financial agreement is due to come to an end?	Yes, for non electronic marketing and provided the customer has not opted out of the marketing.
18	Can legitimate interest and consent be applied at the same time, or is it one or the other? For example, can you use legitimate interest for MOT reminders (past sales) but also have a consent form (splitting MOT and sales marketing) for sales from now on? Can a business use legitimate interest for its existing customers and consent for new customers?	Yes, we think that's possible, but may be difficult to manage. Please also note comments already given on the restrictions on use of Legitimate Interests.
19	If a customer exercises the right to be removed, then comes back in 6 months later, can we then use legitimate interest to call them for mot reminders and servicing due?	If a customer has asked for marketing to be stopped, then all marketing including phone calls must be stopped.

Scope

20	Does the regulation apply to companies operating out of the US?	It applies to all businesses providing business in the EEA. A US company would be out of scope if it only provided goods/services in the US

Suppliers / Partners

21	Does a business need to ensure that its suppliers are compliant with GDPR? Does this only apply if the supplier in question has access to customer data (e.g. third party contact centre) / communicates with customers, or to all suppliers?	Yes, if a supplier processes data on your behalf, then you may be liable for its breaches. We recommend that you undertake checks on the supplier's compliance (e.g. has it implemented policies, training and robust security controls?). The GDPR mandates that contracts with specific clauses are implemented. In addition, we recommend that the contract terms require the supplier in these cases to compensate you for their breaches
22	Will GDPR apply to information a business itself hold on its suppliers?	Yes, GDPR applies to all personal data - so keeping the name and telephone number of a business contact is covered. It is however very low risk personal data - so does not need the same level of security as more sensitive data such as a customer's banking details.
23	What if a partner (e.g. manufacturer) is not responding to our GDPR related questions / queries despite several attempts at engaging with them?	A manufacturer is unlikely to be your data processor. Instead, the manufacturer is likely to be a Data Controller and therefore responsible for its own compliance. Nevertheless, it will be important to work together on this topic. Our only advice is to keep trying.
24	If a business is using a number of data capture applications (e.g. dealer management system, showroom enquiry system, finance proposal system, etc.), who is responsible for drawing up GDPR policies / contracts between the business or the system providers? IF there is an existing provider, is it their responsibility to revise existing contracts to ensure GDPR compliance? Should the business send out a Due Diligence Questionnaire to its system providers?	The system providers are likely to be your data processors and therefore you may be liable for their mistakes. Accordingly, we recommend that you take the lead on this topic. By taking the lead it's more likely that you will get your terms in place rather than having to respond to the supplier's terms.

25	If a dealer passes on customer details to the manufacturers for surveys and CRM / marketing purposes, is a 3rd party consent required from the customer? Similarly, what happens if a manufacturer has access to a dealer's data feed / invoices?	Any electronic marketing by the manufacturer is likely to need consent. Surveys may not be marketing, but the regulator's definition of marketing is very wide so they could be caught. Dealers must be clear with their customers that data may be passed to the manufacturer. The manufacturer is responsible at law for its own marketing consents - although it may have mandated that you do this by terms in the franchise agreement.

Cross-departmental working

26	Are there any recommendations for updating of customer situation/issue between departments (i.e. Customer Service looking to obtain an update from dealership)? If this needs to be done via a platform like e-mail, should this be restricted to a job reference code?	Whether email or sending personal data internally is acceptable is a judgement call depending on the nature/risk of the data. Generally, the business should limit the amount of personal data that is shared. If data can be anonymised or transferred in a more secure way than email, then that is better. As an absolute minimum, we recommend all portable devices are encrypted.

Definition of personal data

27	Is a VIN considered to be personal data?	Personal data is anything that can identify a living individual. A VIN number that has not yet been assigned to a customer, will not be personal data, but once it has been assigned to an individual customer, it is personal data.
28	How should we treat vehicle data locked to a customer? If we get a call asking for vehicle data from a third party can this be shared? Eg someone's just bought the car, our stamp is in the service book and they want to know if the timings belts been done	Generally, you should be cautious about releasing any personal data to third parties and are not obliged to do so. That said, in the case that you have mentioned, the data could be released.
29	When we sell a car, we are required to give the customer the V5 showing previous customer details. Is this allowed?	Yes, as this is a legal requirement.

General marketing

30	Can we do follow-up calls or marketing calls to our customers?	Yes, provided you do not call anyone that has opted out. If you have chosen to use consent as your lawful basis for marketing, then you will need to first obtain their consent.
31	How long is the period of time since the last transaction for considering the customer lapsed	This is a judgement call and will depend on the nature of the goods/services. For service customers, we believe 1 year is an appropriate period. For car sales, we believe 3 years and possibly up to 5 years is acceptable
32	Health checks - can we send videos and items identified?	We assume this is a video showing work that has been done or needs to be done when a vehicle has been booked in for servicing. In this case, yes we think it is fine to send.

Paper documentation

33	How should paper records best be dealt with? How long do we have to keep hard copy files? How do they have to be stored?	Records should be retained for as long as can be justified. This will vary depending on the nature of the document. As an example, most businesses choose to keep invoices, order forms and related documents for 7 years for tax and legal reasons. All documents containing personal data should be held securely (e.g. on encrypted systems for soft copy documents and locked cupboards for hard copy data). For more sensitive data, additional security controls should be considered.
34	Is there a timing consideration that needs to be applied to old hard copy records? If such records need to be destroyed, do they need to be passed onto official agencies such as HMRC before being destroyed?	See answer to question above. We are not aware of any documents that need to be passed onto official agencies before being destroyed.
35	A number of businesses use paper forms for areas such as courtesy cards, jobcards, customer invoices, desk diary, etc. How should these be treated moving forward? Will you recommend moving onto an all electronic system to restrict the changes of other customers being able to see these?	Paper records are still acceptable providing there is appropriate security. Nevertheless, we recommend that there is a steady transition to secure electronic documents.

Data Storage

36	How long should different types of data be stored (e.g. electronic vs hard copy, or different types of data about a customer's engagement with a business)? ("this industry is data hungry as we are under constant pressure to deal over supply which leads to boundaries being pushed")	See answer to question 33

Physical Display

37	Do we need to display a notice in our sales/service area that we are GDPR Compliant?	No, but a privacy policy that explains how personal data is managed and the rights of individuals needs to be made available. This will usually be held on business websites. More detail is available on the regulator's (the ICO) website on what needs to be included in a privacy policy.

Practical Help

38	Where can we find a data breach policy, subject access policy and privacy policy?	There is guidance on the regulator's (ICO) website, but not template policies. Law firms such as Radius Law can provide such documents
39	Are there specialist companies who can assist businesses with achieving GDPR compliance?	Yes, Radius Law is an automotive specialist law firm and is regularly advising businesses on GDPR topics. Other consultancies and law firms are also available.

Right to be removed

40	Under the right to be removed, can we keep just the vehicle history - in case of a future new owner, where the previous service history is often asked for by the new owner - and useful to us to diagnose recurring faults?	The right to be removed is unlikely to apply in this case. Where you have a justifiable business reason to retain data then you can resist an application to be forgotten. That said, if the personal data element can be removed, but you keep the vehicle data - then that should be considered.