GDPR Workshops
FAQs – updated April 2018

This document is a consolidation of questions arising from the GDPR Workshops held by TGB during October and November 2017 and emailed to TGB since. It is not intended to be fully comprehensive and is not intended to form legal advice. Please seek legal advice if you need assistance on the issues raised in this document.

This document is based on the General Data Protection Regulation which comes into effect on 25 May 2018.

This document is confidential to the recipient Centre and must not be circulated outside of the Toyota/Lexus Centre to which it is sent.

***

1. *To recap: What is "personal data" and "sensitive personal data"?*

> *"Personal Data" is any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who 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;" (Article 4 (1) GDPR)*

The GDPR refers to "sensitive personal data" as "special categories of personal data". These categories are broadly the same as those under the current law (racial or ethnic origin, religious and political beliefs, trade union membership, physical/mental health, sexual orientation, actual or alleged criminal offence and proceedings), but updated to include:

(a) genetic data;

(b) biometric data where processed to uniquely identify an individual.

Tip:

- Remember: If you have CCTV within your premises, images constitute personal data. Consider putting in place a CCTV policy that explains why you collect images and what you do with them

2. *How does the approach to GDPR differ from the existing law?*

One of the most significant additions to the new law is the **accountability principle**. The GDPR requires you to show **how** you comply with the principles, for example by **documenting** the decisions you take about a processing activity.

In addition to emphasising this, the Information Commissioner has emphasised the need to improve data protection in the UK by engendering in organisations a '**privacy by design**' culture.

GDPR also refreshes and updates the rules on consent for marketing:

> *"Consent should be given by a **clear affirmative act** establishing **a freely given, specific, informed and unambiguous indication** of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement." (GDPR Art 32)*

Tip:

- Demonstrate accountability by ensuring all decisions about the processing of data are documented: document **what** you are doing and **why**. This should include ensuring you can demonstrate consent for marketing, whether given or withdrawn. Consider any changes to your systems that may be required to ensure you can provide an audit trail.

- When designing a new process, system or project that involves personal data, consider how you will protect that data from the outset. Importantly, **document** how you are demonstrating that data protection is being considered and baked into the activity/project from the outset.

- Remember: in some cases it is possible to market to someone based on "legitimate interest". Care should be exercised in using this lawful basis as it places an obligation on the Centre to carry out a balancing exercise between commercial interests and the rights of the data subject.

3. What about data that may be left on in-car systems, either on a part-exchange vehicle, test drive or courtesy car?

Caution should be exercised with regard to personal data contained within in-car systems and phone books. For example, navigation systems may include a customer's address (personal data) or addresses of frequently visited locations. By way of example, a sat nav could contain the address that indicates the customer has visited a trade union office or meeting. This specific detail includes sensitive personal data.

Tip:

- Create a process for clearing down data held on any used vehicle purchased and frequently on test drive/courtesy vehicles.

- If a vehicle is purchased in part exchange, ask the customer to ensure all data is deleted and document that this request has been communicated.

- In addition to the steps above, remind customers to check the vehicle is emptied of all personal effects. Document this.

4. *"We follow up customers with a courtesy call following their purchase of a vehicle. Is this OK?"*

In principle yes, providing the call is a routine customer service communication and does not contain a marketing message. If the message contains a marketing message then you must comply with the rules on telephone marketing.

Tip:

- Under GDPR you need a lawful basis for processing data. It would be prudent to inform the customer, for example in your Privacy Notice at the point of data capture, that as a business you will follow up their purchase in this way.

5. *We purchase marketing lists from third party organisations. Where does the responsibility for compliance with data protection legislation sit?*

Where you are using data for your own marketing activities, you (the Centre) are responsible for ensuring you are using that data in a fully compliant manner. For example, you must satisfy yourself that the data subjects in that list have agreed to receive email marketing from you before using the list for that purpose.

Tip*:*

- Ensure you document the basis on which you are purchasing the marketing list and where liability rests for any breach of data protection legislation, by entering into a suitable contract with the seller of the marketing list.

6. *"I am not confident marketing permissions held within my database are GDPR compliant. How can I update my marketing permissions without breaching the law?"*

There is no comprehensive answer to this question. Be aware that a blanket approach by email to your entire database to check you have permission to market to them by email, is likely to be interpreted as a marketing communication in itself and is likely to fall foul of the law. The ICO has recently levied fines in these circumstances.

Tip: Good data governance is an opportunity! Consider a multi-layered approach depending on a gap analysis of the current status of your database:

- if you are confident you have permission under current law to market to an individual by email, you could consider seeking GDPR-compliant consent by email from those individuals (only)
- a substantial number of customers will visit your Centre between now and 25 May 2018. Use this as an opportunity to open up a conversation with them about obtaining compliant consent.

- Use your web presence to advertise the need for customers (and others) to update their preferences and give them an easy-to-use method to do that, for example by using a dedicated telephone number.
- Put notices up in the Centre asking customers to update their details by speaking to a sales advisor.

7. *Does everyone in my organisation need to understand GDPR?*

It is prudent to provide a basic level of training to all members of staff; GDPR doesn't just affect customer-facing staff. You may however wish to provide different levels of training depending on different roles performed. The ICO recommends around 2 hours of training per person per year.

Tip:

- Consider an ongoing training programme to ensure knowledge is refreshed and 'new starter' programmes.

- A training module will be developed by the Academy to support Centres ongoing compliance programmes.

8. *What happens if a laptop or other device is stolen or lost and it contains personal data? Are we responsible?*

Yes. Data held on mobile devices/laptops must be encrypted or otherwise secured. The GDPR requires "*appropriate technical and organisational measures to guard against unlawful processing*"

Tip:

- Consider purchasing encryption software, which is now widely available and relatively inexpensive. The ICO is very likely to levy fines in circumstances where there is a loss of data with no encryption.

- Consider issuing written guidance about the use of mobile devices outside the office.

9. *What about home working?*

Whilst there can be many benefits to working from home/working remotely, there are some challenges that should be considered.

There include:

- Removal of hard copy documents/files from the office that may contain personal data
- The potential risk of being overheard or 'shoulder surfing' when working in an open environment, such as a café or airport lounge
- Using open wifi hotspots that may not be secure

Tip:

- Consider a written policy on remote working, ensuring it is kept up to date and enforced**.**
- 'Privacy screens' can be temporarily attached to monitors/laptop screens to limit visibility of screens to others.

10. ***What about staff using their own devices for work purposes?***

The ICO has issued guidance on BYOD which can be found here: https://ico.org.uk/media/for-organisations/documents/1563/ico_bring_your_own_device_byod_guidance.pdf

Note: this Guidance is based on the existing law (pre-GDPR). It is however unlikely to change substantially and contains useful practical information.

11. ***Can we keep customers date of birth on personal mobile devices and send 'birthday texts'?***

This question raises a number of considerations.

One of the GDPR principles is "proportionality". Consider whether obtaining (and retaining) a customer's date of birth is proportionate for the purposes for which it is obtained. In other words, is it proportionate to obtain DOB when the key purpose of obtaining and processing the customer's data is to market new products and services? Could this aim be achieved by obtaining and retaining less classes of data? Would a customer want (and expect) a text on their birthday?

Consider also the specific risk of the data being held on a personal mobile device. Is this device secure? Could it be accessed by anyone else? Is the device used for social media?

12. ***One delegate also asked whether there was a distinction between retaining data of friends who have become customers, and vice versa, on their personal mobile.***

If the data held can identify a living individual then it is "personal data", regardless of the original source of the data (friend or customer).

However, determining the basis on which the data is collected, processed and stored will depend on other factors. It is relevant to consider the purpose for which the data was originally collected but also, the purpose to which you intend to put the data. If you wish to market products and services to a contact who was originally a friend then the usual consent rules apply.

Tip: Consider having a short internal policy statement that ensures staff are clear on this point.

13. *Do the rules on consent apply to business contacts?*

A distinction should be drawn between contacts who are representatives of limited companies or PLCs and those who are sole traders or partners in a partnership. The updated requirement for consent under GDPR applies to this latter category (sole traders and partnerships), although no organisation or individual should be marketed to where they have expressly opted out.

In addition, many employees have personal corporate email addresses (eg firstname.lastname@xxx.com) and individual employees have a right to request that marketing is not sent to that type of email address.

Further changes are expected in this area when the E-Privacy Regulation is finalised, which is expected to come into effect sometime after GDPR on a date to be announced by the Government.

Tip:

- Whilst awaiting the final version of the E-Privacy Regulation, it may be good practice to periodically confirm the correct details and consents are held where Centres are communicating to customers on a B2B basis.

14. *Could you give us some basic pointers on how to deal with Subject Access Requests (SARs)?*

The position on SARs is changing under GDPR and will provide less time for organisations to respond.

The purpose of SARs is to enable data subjects to make themselves aware of and to verify the lawfulness of the processing.

Can I charge a fee for dealing with a subject access request?

You must provide a copy of the information free of charge. The removal of the £10 SAR fee is a significant change from the existing law.

YOU MAY charge a 'reasonable fee' when a SAR is manifestly unfounded, excessive and/or repetitive. Any fee must be based on the administrative cost of providing the information.

How long do I have to comply?

You must answer the SAR with the requested information without delay and within one month of receipt.

In what format should I provide the information?

Usually you should provide the information in the same format in which it was provided, so if made in writing you should provide the information in a written format.

Tip:

- Satisfy yourself using 'reasonable means' that the person making the SAR is the data subject themselves. For example, by asking for proof of identification.
- Prepare a simple process document that sets out how you will deal with a SAR and ensure staff are familiar with it. You only have a month to respond to a SAR and it will demonstrate that you have considered the importance of managing such Requests properly.
- Remember: a SAR can take any form and may not be immediately identifiable as such. The Request could, for example, be contained within a longer piece of correspondence on another issue.

15. *Will TGB be providing a template Privacy Policy?*

No. TGB will provide a Fair Collection Notice however.
Each Centre (or Group) is likely to need a different Privacy Policy as it relates to each Centre/Group's own requirements, including topics such as security and the identity of data processors. The Fair Collection Notice provides a space to link both a Centre's and TGBs Privacy Policies.

16. *Retailers with multiple different OEM franchises. Can we share personal data obtained in one franchise to another or to the Group (holding co.) for the purposes of direct marketing?*

As the data is to be shared for the purposes of direct marketing, consent will need to be obtained from the data subjects for this purpose.

Under the Addendum to the Toyota and Lexus Centre Agreements, it is not permissible to obtain consent from a Toyota Group customer/prospect to prospect a product from a competitor franchise.

17. *Can we market customers with MOT and Service Reminders? Do we have a "legitimate interest" in contacting them without specific consent?*

Where a customer has purchased a vehicle or had a vehicle serviced, it is possible that "legitimate interest" will be an adequate lawful basis for contacting them about other services related to their vehicle: it is a type of processing which they may reasonably expect their data to be used for and which should have minimal privacy impact.

If you rely on "legitimate interest" however (as opposed to explicit informed consent), you must be able to demonstrate you have identified in whose interests you intend to process the data and that you have undertaken an exercise to balance commercial interests with the interests of the data subject.

If you cannot use legitimate interest, you need another legal basis for consent. You may be able to base consent as "*necessary for the performance of a contract with the data subject*" for example, if the customer has purchased a service plan or other product that includes an MOT. Alternatively, you will need explicit, informed consent for this category of marketing.

18. ***Will the OnebyOne system be impacted by GDPR?***

The current basis for marketing for the One by One system is the consent that the customer gives at point of sale through Finance@ / NGage.

Under GDPR consent will still be relied upon and consent will still be obtained at point of sale. That said, under GDPR TFS will be expanding the categories of consent to marketing for the customer, and OnebyOne customer contact will be covered by one of these categories. In the same way as now, OnebyOne will continue to include an opt out tick box so that if the customer retracts their consent during a call made by the dealer, the Centre will be able to record this on the system.

In this case there shouldn't be any network impact.

19. ***Is Google Docs / Sheets a sufficiently secure environment to store personal data?***

For any documents containing personal data it is advised that password protection is always applied. The TGB Systems department are reviewing the security features of platforms such as Google Docs and will advise in the near future.

20. ***Does the current Centre Standard requiring Retailers to capture a core level of customer data comply with GDPR regulations?***

TGB are currently reviewing this Standard in relation to 2018 and will communicate in due course as to whether this will be continued in its current form or amended accordingly.

21. ***What is the process within Value Chain After Sales marketing to ensure we only include customers who have previously provided consent?***

In principle the selection of customers to be included in any form of marketing / campaign should be based on the consent provided by the customer or where it can clearly be demonstrated that a legitimate interest to market exists.

22. ***A query has been raised by a couple of Centres about the physical Centre environment (for example, use of consultation pods) when handling personal data.***

This is less a question about GDPR and more one of general confidentiality. Centres should use sensible measures to protect confidentiality such as locking screens when

Centre staff are away from their desks, not leaving documents containing personal data unattended and consider investing in privacy screens.

23. ***Does the current Retailer Agreement cover the filming of Centre staff for the purposes of TGB's Mystery Shop programme?***

The personal data in question here belongs to the individual Centre staff member being filmed. In that case, the Centre will need to address this with their staff and decide the basis on which they can collect and process this data. Consent may not be a valid legal basis as the staff member probably has no real prospect of disagreeing to this data capture and processing. The Centre may be able to rely on the legal basis of "legitimate interest" as they are required to take part in the Standards programme of which this is part, but would need to make this clear to staff.

24. ***Where else can we get help?***

- The Information Commissioners Office **–** ***www.ico.org.uk***

There are already a number of resources on the ICO website (ico.org.uk) to help organisations prepare for the GDPR.

On 1 November 2017, a new phone line (primarily for small business employing less than 250 people) will offer additional, personal advice to small organisations that still have questions. The ICO helpline can be contacted on 0303 123 1113/option 4.

As well as advice on preparing for the GDPR, callers can also ask questions about other legislation regulated by the ICO including electronic marketing and Freedom of Information.

- In addition, the ICO has published its “12 steps to take now”, to help business prepare. This is available at the following location:

https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf