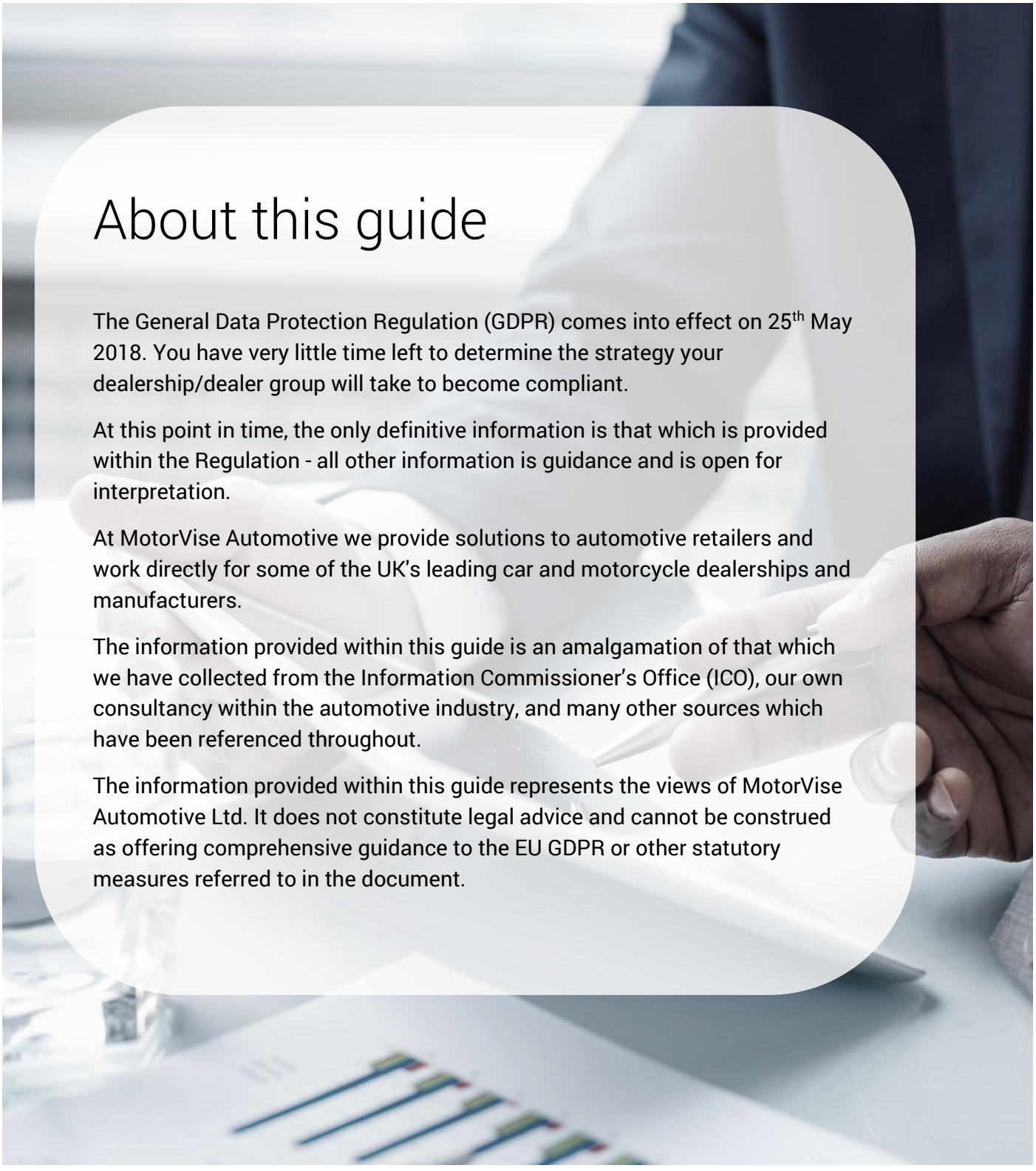
MotorVise

Guidance on the impact of the EU General Data Protection Regulation within the Automotive Industry



About this guide

The General Data Protection Regulation (GDPR) comes into effect on 25th May 2018. You have very little time left to determine the strategy your dealership/dealer group will take to become compliant.

At this point in time, the only definitive information is that which is provided within the Regulation - all other information is guidance and is open for interpretation.

At MotorVise Automotive we provide solutions to automotive retailers and work directly for some of the UK's leading car and motorcycle dealerships and manufacturers.

The information provided within this guide is an amalgamation of that which we have collected from the Information Commissioner's Office (ICO), our own consultancy within the automotive industry, and many other sources which have been referenced throughout.

The information provided within this guide represents the views of MotorVise Automotive Ltd. It does not constitute legal advice and cannot be construed as offering comprehensive guidance to the EU GDPR or other statutory measures referred to in the document.

Table of Contents

Introduction

After four years of preparations and debate, the GDPR was approved by the European Union (EU) Parliament in April 2016. The enforcement date agreed across member states is 25th May 2018 requiring each state to individually enact their own legislation in accordance with the Regulation.

In September 2017, the United Kingdom (UK) Parliament published the Data Protection Bill which, when enacted, will replace the outdated Data Protection Act 1998 and integrate GDPR into UK law. In accordance with the EU Regulation, Parliament must enact this Bill, conveying it into the UK by 25th May 2018.

As time is of the essence for businesses across all EU member states, including the UK, preparations have already begun. Countless groups and individuals are offering their own interpretations of how GDPR will affect the future of data in the business realm, particularly regarding marketing.

We initially compiled this guide with the intention of providing it to our existing consultancy clients to keep them informed as to the progressing direction of the ICO.

However, as the information contained within this document appears to not yet be openly shared within the public domain, we felt the need as an industry-leading supplier to publicly publish this information.

The information contained within this guide is targeted at the automotive industry. While much of the information will be applicable to other industries, this guide has been created with the intention of providing car dealerships with the most accurate and applicable information for their business.

If you have any questions regarding the information contained within this document, please do not hesitate to get in touch.

Telephone: 01325 776410

Email: customerservice@motorvise.com

Overview of changes introduced by General Data Protection Regulation

The most significant change introduced by GDPR over the Data Protection Act (DPA) 1998 is the greater emphasis on the documentation that data controllers must keep to demonstrate accountability.

The requirement for increased accountability regarding data can be achieved by taking action in multiple areas throughout a business. This includes ensuring:

- Records are kept of where personal data is held, where it came from and who it is shared with.
- Staff exercise increased vigilance when dealing with customer data.
- All Display Screen Equipment (DSE) displaying data should not be in view of anyone not authorised to view it.
- Hard copy documents used at workspaces are kept out of sight of unauthorised personnel.

An extensive checklist of these actions can be found in Appendix A. At MotorVise we offer a consultancy service for car dealerships to ensure such actions are planned and taken.

Nevertheless, the biggest issue affecting marketing departments is that concerning the right to continue marketing to their database.

“Do all future marketing communications need to be restricted to customers who have opted in?” “Do I need to send out a communication to all customers requesting consent to email and text communications?” “Should my business simply delete our database and start over?”

Let us look at the implications of GDPR on the future marketing to your customer database.

GDPR (Article 6)– What it says for future marketing

A crucial element of GDPR affecting car dealerships concerns data processing for marketing purposes. Article 6 of GDPR states:

> *Processing shall be lawful only if and to the extent that at least one of the following applies:*
>
> *a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;*
> *…*
> *f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.*

Until recently, the consensus regarding lawful processing of data for the purposes of direct marketing was that consent (point (a)) would be the only viable option for businesses.

In response, businesses took different approaches to the issue. As an example, last year following an ICO investigation, Honda Motor Europe Ltd was found to have sent 289,790 emails to customers who had previously opted out of communications asking to confirm this decision. Following these findings Honda received a £13,000 penalty notice.

Additionally, national restaurant chain Wetherspoons announced they had chosen to delete their entire customer email database as a result of GDPR. This was done to develop a less intrusive relationship with their customers and to perform a hard-reset on their database to ensure all customer records regarding opt-in consent would be accurate.

So, what has changed?

Legitimate Interest (Recital 47) – It's not all doom and gloom

If we look back to point (f) of Article 6 of GDPR which states:

> *Processing shall be lawful only if and to the extent that at least one of the following applies:*
>
> 1. *processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data…*

For clarification as to what a Legitimate Interest is we must look to Recital 47.

> *(47) The legitimate interests of a controller … may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller…*
>
> *Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller…*
>
> *The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.*

Until recently, the Legitimate Interest basis for processing customer data was largely overlooked by businesses in comparison to gaining customer consent. It is unclear as to why this has been the case, however a previous lack of focus on this within the guidance provided by the ICO, the Data Protection Network and other data specialists is likely to be a contributing factor.

Whilst the Regulation is open to interpretation until precedents are set after May 2018, the best source of guidance for businesses is that given by the ICO which has offered a 3-stage test businesses must follow when processing customer data on the basis of Legitimate Interest. We look at this next.

3-Stage test – What dealerships must prove to rely on Legitimate Interest

To rely upon the principle of Legitimate Interest, it must be shown that there is a balance between the interests of the business and the rights and freedoms of the individual.

The method provided by the ICO is that of a 3-stage test.

1. *Identify a Legitimate Interest*
2. *Carry out a Necessity Test*
3. *Carry out a Balancing Test*

1) Identify a Legitimate Interest

A wide range of interests may be considered as Legitimate Interests. The questions to ask are:

- What is the purpose of processing personal data?
- Why is it important to you as a business?

The ICO explicitly states this can include commercial interests.

Whilst trivial interests may also fall within the scope of what can be identified, most will be overridden in the balancing test.

2) Carry out a Necessity Test

The second stage requires that you consider whether the processing is necessary for the purpose outlined previously.

The Data Protection Network stated that 'Necessary' should be interpreted as that the processing must be "…a targeted and proportionate way of achieving the purpose." Legitimate Interest cannot be relied upon if there is another more reasonable and less intrusive way of achieving the same result.

3) Carry out a Balancing Test

The third and final stage requires that you must balance your business interests against the individual's interests. You should consider whether the individual would reasonably expect you to use their data that way, or whether it would cause them unwarranted harm.

The nature of the interests, the impact of processing and safeguards in place (e.g. opt-out options) are all different factors to be considered.

Don't forget PECR!

Due to many factors (including lack of enforcement), many businesses are wholly unaware of the Privacy and Electronic Communications Regulations (2003). These regulations placed specific rules on sending marketing emails, text messages or conducting telemarketing calls.

PECR will not be overridden by GDPR and will instead run alongside the new regulations.

PECR states that in order to send marketing emails/texts to specific individuals, consent must have been obtained unless an exemption applies.

One of the exemptions known as 'soft opt-in' allows for marketing communications to be sent if the following conditions are met:

- *You have obtained the contact details in the course of a sale (or negotiations of a sale) of a product or service.*
- *You are only marketing your own similar products and services.*
- *You provided a simple opportunity to refuse or opt-out of the marketing when you first collected the contact details and in every subsequent communication.*

Therefore, according to PECR you may be able to email or text your own customers without consent providing the above conditions are met. This will not apply to prospective customers, bought-in lists, and generally does not apply to non-commercial promotions.

It must be noted that in order to rely upon Legitimate Interest as an alternative to Consent under GDPR, the rules and guidance under both GDPR and PECR must be followed.

We understand that many of the rules may seem unclear and difficult to truly apply to your car dealership. Consequently, we have created our own Legitimate Interest Assessment document to help you assess your qualification to use Legitimate Interest as an option in Appendix B.

APPENDICES

A – GDPR Preparations Checklist

B – Legitimate Interest Assessment

Appendix A:

GDPR Preparations Checklist

Aside from the specific changes regarding how data is processed for communication purposes (e.g. Consent, Legitimate Interest), much of what GDPR reiterates is the need for increased accountability. Therefore, many of the points mentioned below may seem obvious or common-place.

Nevertheless, it must be ensured that all the necessary actions mentioned below are taken to show your car dealership is taking the new regulations seriously. It is also recommended that all actions and information are recorded for future reference.

Data Compliance

- ☐ Create a privacy statement and add to your website.
- ☐ Appoint a data controller for customer contact.
- ☐ Staff to be asked to re-sign new data protection policy explicitly authorising storage and use of their data and confirming they understand the importance of data security
- ☐ All staff to be given presentation and have GDPR explained to them
- ☐ Review your storage of customer and staff data and ensure it is secure and if stored on remote servers are they in the EU – if not, acquire a certificate of compliance with GDPR
- ☐ Send out questionnaire to all people you share customer or staff data with and get them to sign your data agreement and check the responses you get to the due diligence questionnaire
- ☐ Request all companies you share your customer and staff data with to agree to a new data sharing agreement in line with GDPR
- ☐ Conduct a Legitimate Interest Assessment (LIA) to ensure customer communications are valid within the scope of GDPR and PECR

Showroom/Office Compliance

- [ ] Ensure all staff to be vigilant when dealing with any customer data (e.g. driving licences, proof of address documentation, phone numbers, e-mail details etc.)
- [ ] All Display Screen Equipment (DSE) should not be in view of anyone not authorised to view the data you are viewing or processing
- [ ] All company equipment should be locked (Ctrl+Alt+Delete – Lock) when unattended or when you are with someone who is not authorised to view the content
- [ ] 2 minutes automatic screen lock to be applied on all laptops and desktops
- [ ] Documents should not be left at the printer
- [ ] Hard copy documents used at your workspace should only be viewable if you are working on them and individuals who are not authorised to view them are not present
- [ ] Hard copy documents carried around the premises should be carried in such a way (e.g. a folder) so the information on the document is not in view of any unauthorised people

Appendix B:

Legitimate Interest Assessment

Please note, there is no standard format provided by the ICO for a Legitimate Interest Assessment (LIA). However, guidance can be found at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/

We have outlined some of the more notable points to consider when conducting your own LIA. We recommend using our guidance below alongside that which the ICO has provided to generate your own comprehensive LIA. You should keep a record of your LIA and record the outcome as to help show you have shown due diligence in terms of the decision making and justification behind processing data under Legitimate Interest.

If you are relying on legitimate interests for direct marketing, the right to object is absolute and you must stop processing when someone objects.

	Identifying a Legitimate Interest		
	Question	**Guidance**	**Answer**
1	What is the purpose of processing personal data?	This is to identify the Legitimate Interest. What is the reason for processing data? ICO has explicitly stated this can be a commercial interest such as direct marketing.	
2	Who benefits from the processing and how important are those benefits?	If the processing is needed to achieve a lawful business objective (such as direct marketing) then it is likely to be legitimate for these purposes.	
3	Would your use of the data be unethical or unlawful in any way?	This is very much in relation to processing sensitive data regarding criminals, children etc. In terms of using customer data for marketing purposes this would not be considered unlawful or unethical.	

	Necessity Test		
	Question	**Guidance**	**Answer**
1	Does the processing help to further the interest identified?	There must be a connection between the interest identified and the method of processing used. If this connection is weak, it will unlikely be found necessary. Necessary is not synonymous with 'indispensable' but should neither be considered as wide as 'reasonable' or 'useful'.	
2	Is there another, less intrusive way to achieve the same result?	If there isn't then the processing shall be deemed necessary. If there are other methods but require disproportionate levels of effort, then processing will still be deemed necessary. It is unlikely to find a scenario in which processing is unnecessary where it has been identified to achieve a stated business objective.	

	Balancing the Interests		
	Question	**Guidance**	**Answer**
1	What is the nature of your relationship with the individual?	If you are following the Legitimate Interest option as a means to marketing, all personal data being processed should be that of previous customers and/or customers which have negotiated a sale.	
2	Is any of the data particularly sensitive or private?	Data regarding customers should not extend beyond their contact details and make/model. No details should be held of children or other sensitive data (e.g. criminal convictions).	
3	Would people expect you to use their data this way?	If individuals would expect this processing to take place (e.g. you informed them so at point of sale with an opt-out option) then they are likely to have already considered and accepted this. If they have no expectation, then the impact is greater and given more weight in the balancing test.	
4	Are some people likely to object or find it intrusive?	Processing should be targeted and specific. It should be justified based on the nature of the relationship (e.g. existing customer). It should be considered how the data is processed (e.g. large scale mass marketing or whether due diligence is taken on who is being processed).	

		The more unusual and unexpected the processing is, the more intrusive it will be regarded.	
5	Has the personal information been obtained directly from the individual, or indirectly?	If the personal data was collected directly with the individually expecting their data to be processed, this points in favour of a Legitimate Interest. However, if data is obtained indirectly, there will need to be more compelling information in favour of a Legitimate Interest to overcome this.	
6	Can you offer an opt-out?	The individual should have complete control throughout processing to opt-out. At the point of collection, they should be informed that they may opt-out and given the opportunity to at every other point of processing (e.g. email opt-out).	