The General Data Protection Regulation (GDPR)

- things you need to look out for

A JudgeService White Paper

JudgeService

business.judgeservice.com

Introduction

The General Data Protection Regulation (GDPR) changes will come into effect on 25th May 2018. The new laws will make unprecedented changes to marketing consent.

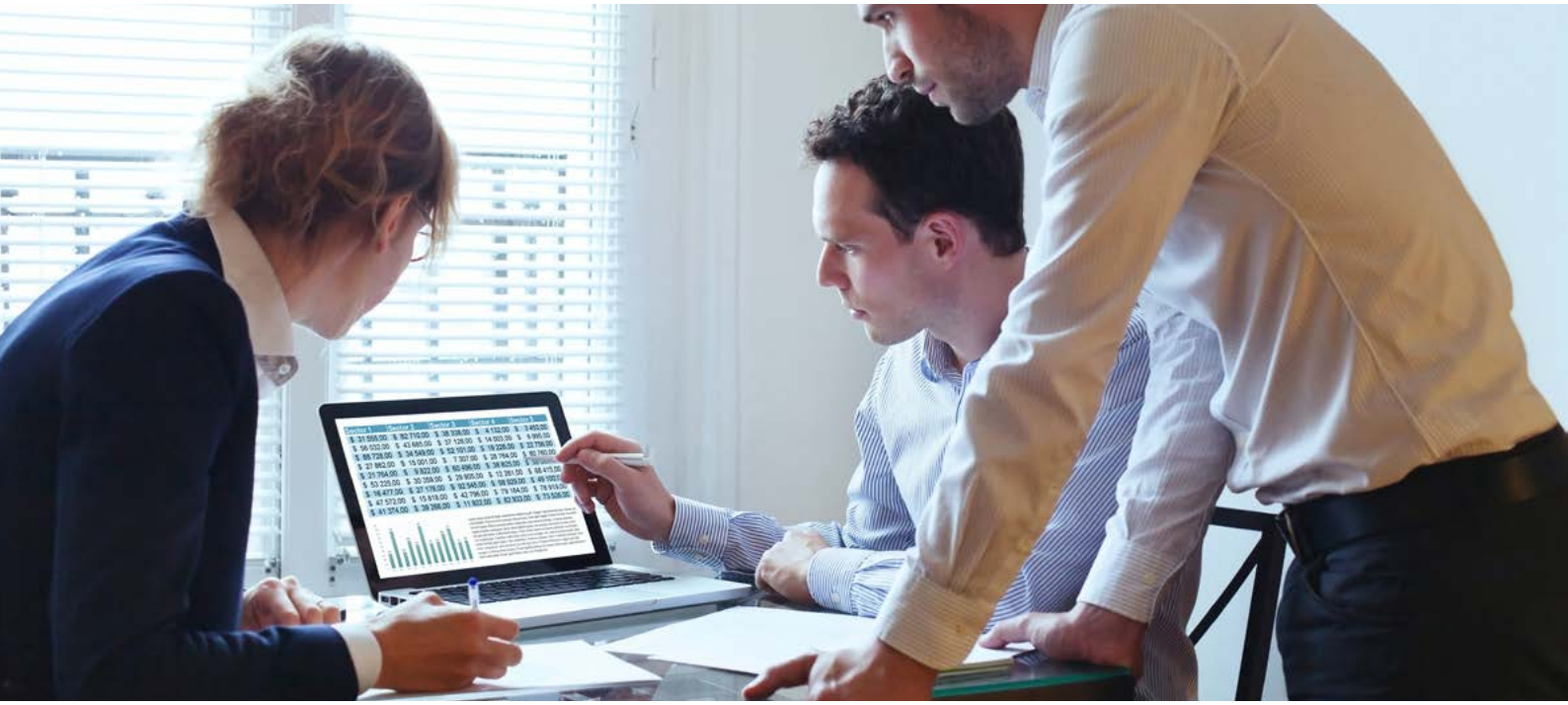
Although May 2018 may seem to be a generous transition period, the scale of the changes imposed by the GDPR means that all companies affected by the new rules will need to take steps to move toward compliance without delay.

In fact, GDPR is now in force, and will be unaffected by the UK leaving the EU. You have until 25th May 2018 to fully implement new requirements. Preparing for compliance will take significant time and resources, and failure to comply can result in fines of up to 4% of annual turnover, or €20 million, whichever is higher.

Putting in place a GDPR implementation programme is therefore a critical priority to ensure that you can continue to use and share data in compliance with applicable laws.

"The General Data Protection Regulation promises the biggest shake up to European privacy laws for 20 years."

Linklaters.



Implications of the GDPR

In comparison to the existing EU and UK data protection rules, which are part of UK law under the Data Protection Act 1998, the GDPR places greater emphasis on the obligations of data controllers (those who determine when, how and for what purpose personal data is to be processed). It also imposes a significant number of new requirements directly on data processors (those who process data on behalf of data controllers).

One of the biggest changes, which means actions need to be taken by all businesses, is a new accountability principle. This will require companies that process personal data to create and maintain records demonstrating their compliance with the relevant GDPR requirements.

In some cases, significant business process and even business model change will be required to meet the new obligations. Data Protection Impact Assessments will need to be carried out, and will need to be fully and accountably recorded. National Data Protection Authorities will have audit and investigatory powers to ensure that the requisite procedures are being followed.

The GDPR will reinforce and expand the data privacy rights of individuals in a number of important ways. At the same time, it will subject data controllers and processors that fail to comply with the GDPR requirements to potentially severe fines. The maximum penalties will be €20 million or 4% of annual worldwide turnover, whichever is the greater. This compares with just £500,000 now.

Does the GDPR affect your Company? The GDPR will affect every business and public body that processes the personal data of EU residents, including:

- Every employer in the EU, including the UK!
- All businesses that offer goods or services to individuals in the EU or that monitor their behaviour.
- All businesses that process the personal data of EU individuals on behalf of other businesses.

What is the source for this, and its date?

One in four businesses in the UK say they have cancelled all preparations for the EU General Data Protection Regulation in the misunderstanding that it will not apply after Brexit, new research reveals.

A survey of IT decision makers at UK companies by information management firm *Crown Records Management* in April 2017 found 24% are no longer preparing for the regulation. A further 4% had not even begun to prepare. Alarmingly, a massive 44% of those surveyed said they didn't think the regulation will apply to UK business after Brexit. *THIS IS NOT THE CASE.*

GDPR will affect all companies processing data in the UK and the EU. The UK government made clear in November 2016 that it would continue to enforce GDPR before and after Brexit.

The focus

The new Regulations, among other things, focus on:

Collecting and using personal data

The GDPR introduces more stringent requirements in terms of the information to be provided to individuals to make the processing of personal data fair and lawful. All processes for collecting personal data need to be reviewed and changes made to privacy notices and documentation containing information about how an individual's data is processed to ensure that new mandatory provisions are included.

You should review the way you obtain consent to confirm it meets the requirements of the Regulation. For example, ensuring that you are not using pre-ticked boxes and that ensuring the request for consent is separate from other matters, and gives fuller information.

Use of personal data for marketing purposes

When you process personal data for marketing purposes, you will need to ensure that you obtain the consent of the individual to process their personal data. The requirements for consent under the GDPR are much higher than under current data protection legislation, therefore, if you wish to continue to use personal data already collected and personal data you will collect in the future you must ensure that the consent of the individual has been obtained in accordance with the requirements of the GDPR.

The Regulation imposes onerous requirements on consent and seeking consent will only be appropriate if the individual has a genuine choice over the matter, for example, whether to be sent marketing materials.

You need to obtain explicit consent to use data for contacting an individual, be it for customer satisfaction surveys, marketing follow-up or finance enquiries. Whereas previously the customer was given the option to opt OUT, this is no longer enough. Customers should now be asked to opt IN in order for you to contact them.

On top of this, not only must you gain consent, but actually be able to demonstrate HOW you have lawfully obtained it. Failure to do so can result in a breach of the new Regulations.

Data sharing arrangements

Consent is a freely-given, specific, informed and unambiguous indication of the individual's wishes. A data controller must keep records so they can demonstrate that consent has been given by the relevant individual. In addition:

- A request for consent must be in an intelligible and accessible form in clear and plain language and, if applicable, in accordance with the Directive on unfair terms in consumer contracts.
- Where the request for consent is part of a written form, it must be clearly distinguishable from other matters.
- The consent must consist of a clear affirmative action. Inactivity or silence is not enough and the use of "pre-ticked boxes" is not permitted.
- Consent will not be valid if the individual does not have a genuine free choice or if there is a detriment if they refuse or withdraw consent.
- Consent might not be valid if there is a clear imbalance of power between the individual and the controller, particularly where the controller is a public authority.
- You cannot "bundle consent". Where different processing activities are taking place, consent is presumed not valid unless the individual can consent to them separately.
- Consent is presumed not valid if it is a condition of performance of a contract.
- The individual can withdraw consent at any time and must be told of that right prior to giving consent. It should be as easy to withdraw consent as it is to give it.

Source: Linklaters' The General Data Protection Regulations : A Survival Guide

You must only use data processors which take such security measures and comply with all other requirements of the GDPR. You must also ensure that when appointing a third party to process personal data (for example an IT provider) or sharing personal data (for example with a manufacturer) there are adequate contracts in place containing mandatory processing clauses.

You need to review all your data sharing arrangements to ensure that adequate contractual provisions are in place and if not, that appropriate clauses are drafted and contracts amended or re-negotiated.

New and expanded individual rights

The GDPR gives individuals a new "right to be forgotten" (have their personal data removed), a new right of data portability (have their personal data copied and transmitted to another organization for further use, including competitors) and enhanced data subject access rights. Individuals will also have expanded rights to object to processing, including an absolute right to object to direct marketing, which might have significant implications for businesses that rely on data analytics.

The Regulation preserves the right for individuals to object to direct marketing. When an individual exercises this right, you must not only stop sending direct marketing material to the individual, but also stop any processing of that individual's personal data for such marketing. For example, if you receive an objection, you should stop profiling that individual to the extent related to direct marketing.

You will also need a process to manage requests to withdraw consent. In particular, what channels will you make available for a withdrawal of consent? How will you record and act on that withdrawal? If consent is withdrawn, are there any other conditions you can rely on?

Businesses will need to implement both technical and organisational measure to show compliance. Putting these in place will take time, and is likely to need review and changes to existing systems. This cannot therefore be left until late.

Compliance and accountability

There will be new limitations on data profiling, including a requirement to obtain prior consent to profiling, strict notice obligations regarding profiling and a duty to honour individuals' right to object to profiling, as previously noted.

The GDPR also sets out specific information to be included in privacy notices and requires individuals to be given clear information as to what is done with their data in an easily accessible form.

You must be able to demonstrate compliance with the GDPR. If you fail to do so you may be liable for a fine for non-compliance under the Regulations. Demonstrating compliance can be done in many ways.

You will need to consider whether you need a data protection officer or other responsible individual to manage data protection compliance in the dealership, and to understand what the needs of those roles are. They should be at Board level – this isn't an IT function.

You will need to put in place measures to ensure that a record of the personal data processed is maintained, that there are adequate policies and procedures in place relating to the collection and use of personal data and that all people responsible for processing personal data are trained on their obligations under the GDPR. You will need to carry out Data Protection Impact Assessments (and know how to do so, and what they entail), and implement "Privacy by Design" into your products and services.

Can we carry on using existing DPA consents?

You are not required to automatically 'repaper' or refresh all existing DPA consents in preparation for the GDPR. But it's important to check your processes and records in detail to be sure existing consents meet the GDPR standard.

Recital 171 of the GDPR makes clear you can continue to rely on any existing consent that was given in line with the GDPR requirements, and there's no need to seek fresh consent. However, you will need to be confident that your consent requests already met the GDPR standard and that consents are properly documented. You will also need to put in place compliant mechanisms for individuals to withdraw their consent easily.

On the other hand, if existing DPA consents don't meet the GDPR's high standards or are poorly documented, you will need to seek fresh GDPR compliant consent, identify a different lawful basis for your processing (and ensure continued processing is fair), or stop the processing.

ico.
Information Commissioner's Office

Essentially, if you don't have explicit permission by 24th May 2018, YOU WILL NO LONGER BE ABLE TO CONTACT YOUR CONTACTS / LEADS!

You can check with the *Information Commissioner's Office*, who regulate these laws and publish marketing guidance, to understand what you need to do to be legally compliant.

A controller must ensure the processing of personal data complies with all six of the following general principles:

- Personal data must be processed lawfully, fairly and in a transparent manner.
- Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Personal data must be adequate, relevant and limited to what is necessary in relation to purposes for which they are processed.
- Personal data must be accurate and, where necessary, kept up to date. Inaccurate personal data should be corrected or deleted.
- Personal data should be kept in an identifiable format for no longer than is necessary.
- Personal data should be kept secure and confidential.

The Regulation places much stronger controls on the processing of sensitive personal data. While there are a number of processing conditions, those conditions are narrower. Any processing of personal data must satisfy at least one of the following conditions:

- The individual has given explicit consent.
- The processing is necessary for a legal obligation in the field of employment and social security law or for a collective agreement.
- The processing is necessary in order to protect the vital interests of the individual or of another natural person.
- The processing relates to personal data which is manifestly made public by the data subject.
- The processing is necessary for reasons of substantial public interest.
- The processing is necessary for archiving, scientific or historical research purposes or statistical purposes.

The best ways to avoid trouble and embrace opportunities with GDPR are awareness, vigilance and pre-planning.

Discover More

To find out more about how JudgeService can help you, and why we are able to boast over 750,000 reviews, visit business.judgeservice.com or email sales-enquiry@judgeservice.com

This document is NOT intended to provide legal advice. It is a guide about the implications of the GDPR.

Readers should check with their own legal advisors or the Information Commissioner's Office, who regulate these laws and publish guidance, to understand what they need to do to be legally compliant

JudgeService

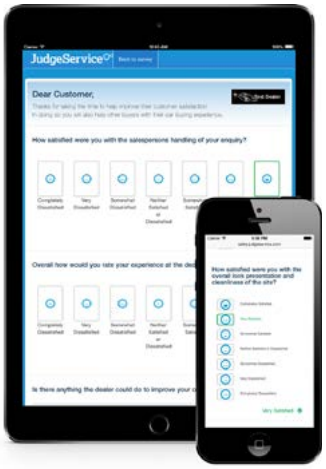
About JudgeService.

JudgeService is the UK's most effective automotive online review provider and understands how powerful reviews are in influencing buyer behaviour and aiding a conversion. We help car buyers find great car dealers.

Our surveys are developed from market demand and our expertise in the automotive sector. Over 25 years' motor trade experience has enabled us to ensure the questions we ask customers provide answers that will drive business.

Our survey results can be shared on Social Media, as well as the JudgeService website. We can also create a specific widget that dealers can include on their website and this, combined with our partnerships with *motors.co.uk*, *Autotrader* and *Trusted Dealers*, ensures that the reviews get maximum exposure.

We have been chosen by over a thousand car dealerships, and have clients ranging from the largest dealer groups in the country to the single site car dealer, because of our specialist knowledge and experience. Our knowledge will support any business in enhancing customer satisfaction, gaining competitive advantage, increasing sales and retaining existing customers.



www.judgeservice.com

Telephone: 01423 225166
Email: info@judgeservice.com

JudgeService Research Ltd
11 Cardale Court
Cardale Park
Harrogate, North Yorkshire
HG3 1RY
United Kingdom

JudgeService