GDPR and the automotive industry

7 December 2017

Author: Ian Inman, Head of Privacy and Data Protection, Cox Automotive UK

Editor: Dr Shaun McGirr, Lead Data Scientist, Cox Automotive Data Solutions

Executive Summary

1. The General Data Protection Regulation (GDPR) comes into force in the UK on 25 May 2018. It builds upon existing data protection law, adding more detail to existing requirements, new rights for individuals, and new obligations on those who process personal data.

2. The GDPR provides several legitimate grounds for processing personal data. Not all processing need be based on the consent of the individual and all grounds are equally valid.

3. The maximum fine for contraventions of the GDPR is 20 million euros or 4% of global turnover. However, these fines are not mandatory and are the absolute maximum.

4. Organisations must comply with the GDPR's requirements and be seen to be compliant. It makes concepts such as privacy by design and default a legal requirement and encourages Data Protection Impact Assessments in all cases, requiring these in some cases.

5. The GDPR introduces a higher standard of consent and explicitly prohibits silence, inactivity and pre-ticked boxes as valid consent. Organisations are not required to get fresh consent if their current consents meet the GDPR standards.

6. The right to erasure, right to restrict processing and right to data portability are all new rights created by the GDPR. Dealers and Manufacturers will need to check their Dealer Management System, Customer Relationship Management systems, and any others that store personal data, to ensure they are functionally compliant.

Let us know your thoughts about the impact of GDPR at coxautodata.com/blog

What is the GDPR and why does it matter?

The General Data Protection Regulation, or GDPR, represents the biggest shake up of data protection laws for almost 20 years. It will have a profound effect on the way all businesses collect and use peoples' personal information.[1]

In many ways the GDPR simply takes the existing law and builds on it, retaining principles at the core of the current law and introducing new rights and obligations. Rumours about fines, consent, and other issues have exploded recently; the reality is, however, that many are just myths.

The GDPR also strengthens the powers of the UK Information Commissioner (the ICO) by significantly increasing the level of fines that can be levied for breaches of the law. Under current legislation, the maximum fine for serious contraventions is £500,000. Under the GDPR, breaches falling within the higher tier carry fines of up to 20 million euros or 4% of global turnover.

However, these figures are the absolute maximum that can be issued and are certainly not mandatory. Not all breaches will be met with fines and even where they are, the GDPR requires fines to be both proportionate and dissuasive. This suggests that, much as is the case now, the ICO will not be issuing maximum fines to everyone.

What is new?

The GDPR introduces several concepts that, while part of data protection terminology for some time, have never been explicitly required by legislation: Data Protection Impact Assessments (DPIAs), Privacy by Design, Privacy by Default, and the accountability principle.

Accountability

Unlike the current Data Protection Act 1998 (DPA), the GDPR makes explicit that not only must data controllers comply with the legislation's principles, they must be able to demonstrate compliance. One way you can do this is by complying with other aspects of the GDPR, such as the duty to maintain records of processing operations and ensuring you have proper, valid evidential consent.

The best way to approach compliance with this requirement is to think in terms of evidence. Could you demonstrate, either to the ICO or a tribunal or court, the measures you have in place to demonstrate how you complied with the law?

1. Find the official summary and full text of "Regulation (EU) 2016/679" here:
http://eur-lex.europa.eu/legal-content/EN/LSU/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG

Data Protection Impact Assessments (DPIAs)

Much like accountability, DPIAs are not themselves a new concept; they are now explicit within the legislation. DPIAs are currently known as Privacy Impact Assessments and the ICO Privacy Impact Assessment Code of Practice has been around much longer than the GDPR.[2]

Although explicit within the legislation, they are only mandatory where processing is likely to result in high risk to the rights and freedoms of individuals. They are, however, extremely useful tools for identifying potential data protection and privacy issues in new projects or products at an early stage. This makes mitigating those issues easier and cheaper than bolting on compliance later.

Privacy by Design & Privacy by Default

If a DPIA identifies data protection and privacy risks early in the product or project lifecycle, Privacy by Design and Default are about designing those products, projects and systems to ensure privacy and data protection compliance is factored in from the ground up. In simple terms, do your systems and products allow those who use them to comply with their GDPR obligations?

- Can you delete information in response to a request under Article 17 or to comply with your obligations in relation to data retention?
- Can you properly restrict personal data so that they are not processed in contravention of a request under Article 18?
- Are DPIAs part of your project planning and product development processes?

Of course, organisations can freely go above and beyond the basics of privacy by design and default, and new and more sophisticated methods of achieving it will no doubt be developed. For now though, don't overcomplicate things because they are not intended to be complicated.

Check that your systems enable you to comply with your obligations. Work with your suppliers to address any issues and examine your policies and procedures. Are data protection impact assessments a standard part of any new projects or products you undertake? These are all simple things you can start doing right now, which tie in with the principles of both data protection by design and default.

What else is new?

There are several other new obligations and requirements in the GDPR, more than we could cover here. In certain circumstances data processors (those who process personal data under the instruction of someone else) can be liable for regulatory action. Organisations are required, where relying on consent, to be able to demonstrate that they had consent and both data controllers and processors must retain records of processing activities.

2. Current code available here: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

The Six Principles

Where the DPA has eight principles covering areas such as fair and lawful processing, adequacy, accuracy and retention, the GDPR condenses these to six. There are no longer principles relating to overseas transfers or individuals' rights, though these requirements are now elsewhere in the GDPR, and rest assured that compliance with those requirements is still necessary!

Collecting personal data

These six principles are broadly the same as the existing principles one, two, three, four, five and seven, but with some minor tweaks in certain areas. For example, the GDPR explicitly separates the concepts of fairness and transparency. Under the DPA, the requirement to be transparent with individuals about who you are and what you do with their personal data is rolled up into the concept of fairness. However, being transparent with individuals about processing does not necessarily make it fair. Fairness is about whether the processing is generally fair and within the reasonable expectations of the individual, not just what they have been told.

In addition, the GDPR gives much clearer guidelines around what transparency means in practice. It requires privacy notices be accessible, understandable and in clear and plain language. Privacy notices written in 'legalese' and hidden away in an obscure part of a website are unlikely to suffice today; under the GDPR they certainly will not.

Managing personal data you hold

The principles still require that organisations take 'appropriate' technical and organisational security measures to protect personal data, though the GDPR provides more detail about that requirement. The principles still require personal data to be kept accurate and up to date, but now add that all reasonable steps must be taken to rectify or erase inaccurate personal data. The GDPR principles still require that personal data is fit for purpose and limited to what is necessary for those purposes, and it still requires that personal data is not retained for longer than needed. There is also a subtle nod to the concept of anonymisation within the GDPR data retention principle, which is not found in the current DPA.

The principles show how the GDPR is very much an evolution of existing data protection law. They have undergone subtle tweaks but are essentially the same principles we have had for almost twenty years.

Consent

The GDPR provides a number of grounds for processing, all of which are equally valid and none of which take precedence over the others. This means that you don't always need consent to justify processing personal data. Other conditions, such as legitimate interests, are just as valid and often more appropriate.

Generally speaking, it is advisable not to rely on consent unless there are no other appropriate bases for processing. One such example is electronic marketing, which in many cases requires the consent of the individual, leaving no other condition available: you must rely on consent.

What is consent?

Under data protection law, consent has a specific definition, which contains several criteria that must be met for consent to be valid. Consent must be:

- Freely given
- Specific
- Informed
- Unambiguous, and
- Involve a positive indication.

'Freely given' reflects that individuals must have a genuine choice. This is unlikely to be the case where there is a significant imbalance in the relationship between them and the data controller. In addition, consent is unlikely to be freely given where the provision of goods or services is conditional on consent to process personal data that is not necessary for that provision.

The requirements that consent be specific and informed are closely linked, and tied to the general transparency requirements of the principles. The GDPR says that for consent to be informed an individual must be aware, at minimum, of the identity of the controller and the purposes for processing. However, it also requires granularity of consent to different purposes. This would cover, in a marketing context, granularity as to what individuals will be marketed about and which methods of marketing communication (e.g. email, telephone) they are consenting to. Organisations seeking to rely on consent will need to consider these issues, as well as the broader requirements of clarity and accessibility, when drafting privacy notices and consent statements.

Consent requires the individual to make a choice by way of a clear affirmative action or statement. The GDPR gives a number of examples of what may constitute such an action. These include ticking a box, signing a consent form or choosing particular technical settings on a website. The GDPR also explicitly states that silence, pre-ticked boxes or inactivity are not valid consent. If any doubt existed under the DPA about the use of pre-ticked opt-in boxes, that is now gone under the GDPR.

This also means that unticked opt-out boxes are also no longer valid: the assumption is that consent is not given unless the individual has done something (i.e. given a positive indication) to indicate they consent. Pre-ticked opt-in boxes and unticked opt-out boxes fail this requirement as the individual must do something (i.e. give a positive indication) to show that they do not consent.

Individuals' Rights

The GDPR incorporates all of the rights that individuals enjoy under the current regime, though some of them work slightly differently. Importantly, the GDPR also creates new rights for individuals and here we look at what some of these mean.

Article 17 – The Right to Erasure

Also known as the right to be forgotten, this is probably the most well-known of the new rights created by the GDPR. Under the current regime there is a requirement not to keep personal data longer than necessary, but individuals have no general right to have personal data deleted.

Article 17 changes that, giving individuals the right to obtain from a data controller the erasure of personal data. However the right is not absolute, arising only in certain circumstances, and in some circumstances not at all, such as where it is necessary to process the personal data for the defence of a legal claim.

On the face of it, Article 17 seems simple: if any one of the situations set out in Article 17(1) applies and none of the circumstances in Article 17(3) apply, then an obligation to erase the personal data arises. Yet this may cause problems if, for example, you receive an objection to the processing of personal data for direct marketing purposes. This is one of the grounds where an obligation to erase would arise.

You may want to keep a record of the individual's contact details on a suppression list instead of deleting them entirely, so you know not to contact them in future. However, there is nothing in Article 17 that appears to allow for that, or for retaining the personal data even if you have another reason for doing so. It remains to be seen how this right bears out in practice.

Article 18 – The Right to Restriction of Processing

The right to restrict processing is designed to supplement other areas of data protection and so it too only arises in certain circumstances. For example, it can be exercised where the individual has disputed the accuracy of personal data and the data controller is investigating the dispute. The key thing to bear in mind is that where this right does apply, personal data can only be processed (other than being stored) when the individual consents to the processing.

The GDPR gives some examples of mechanisms to secure the restriction of processing, such as moving the data to another system, making it unavailable to users or temporarily removing published data from a website. Such restrictions must be made clear to ensure compliance.

Article 20 – The Right to Data Portability

This right is designed to complement the right of access to personal data. It applies to:

- Personal data which the individual has provided to the organisation,

- Where that personal data is processed on the basis of the consent of the individual or on a contract, and
- The processing is carried out by automated means.

In simple terms the right affords an individual the ability to receive the personal data in question 'in a structured, commonly used and machine readable format', to send that personal data to another organisation and also, potentially, directly from one organisation to another.

Further guidance from the Article 29 Working Party has made clear that the reference to personal data provided to the organisation by the individual should not be interpreted narrowly. It is not limited to information the individual supplied directly to an organisation when they signed up to receive a product or service, such as name or address. In their guidance they say that information generated by an individual using those products or services, such as search histories, website browsing histories and activity logs, will also be covered by the right.

What does all this mean for the automotive industry?

We cannot afford to bury our heads in the sand; the GDPR implementation date is just over five months away. It might seem like there is an insurmountable list of things to do, but there are some things you can and should be working on right now to get ready. GDPR compliance is achievable but it will take the correct allocation of resources, time, people and money to get there.

- Start reviewing your privacy notices and amending them to ensure they include all the information now required by Articles 13 and 14 and that they are presented in clear, accessible and understandable ways.
- Look at how you currently obtain consent to process personal data. Does it satisfy the GDPR requirements? Remember if it does, there is no need to obtain fresh consent. Of course, if it does not satisfy the requirements, you won't have valid consent from May.
- Are your systems and processes ready to deal with individuals' rights, both new and existing? Could you delete personal data upon request or restrict its processing? Review the functionality of your IT systems as early as possible, particularly bearing in mind the potential cost and time to get them changed, to ensure they allow you to comply with your obligations under GDPR. Work with your systems suppliers to ensure your systems are configured to enable you not only to comply, but to demonstrate that you comply.
- Start looking at your processes and procedures for identifying and handling data breaches. Are they sufficiently robust to enable you to identify those which might meet the requirements for mandatory reporting under the GDPR? What changes might be needed?

More information

For more about the importance of GDPR compliance in automotive, and case studies of how Dealers and Manufacturers are preparing, see pages 51-73 of Automotive Management's November 2017 issue: https://issuu.com/am_magazine/docs/am_november_2017/51

Listen to the MotorTradeRadio.com interview with Louise Wallis from the Retail Motor Industry Federation and National Franchised Dealers Association here: http://motortraderadiocom.libsyn.com/gdpr-and-its-impact-on-the-uk-motor-industry

Watch our blog for data-related webinars from Cox Automotive in early 2018: coxautodata.com/blog

If you have specific questions about this paper, please get in touch: Ian.Inman@coxauto.co.uk

Media contact: Gwen Allen, 07392 082320

Note: this is our view based on the data available to us at present. Readers should compare our findings with their own experience before making the decision that is best for their business. This technical paper does not constitute legal advice on GDPR compliance or any other matter of data protection.