Why forthcoming EU data regulations will affect global auto industry players

By **Stephen L. Tupper**

New privacy and data protection law is coming in Europe. It's a slow process, but the contours of the final regulation are becoming discernible. Enterprises that handle personal data of Europeans – and particularly US companies with operations or customers in Europe – can get a jump on the regulation by doing several things now.

The size and scope of vehicle manufacturing and related processes practically guarantees that an automotive enterprise will have European connections, making compliance with the new law critical.

Why now? Directive to regulation

The present legal structure began in 1995 when the European Union (the "EU") enacted a directive with the rather long-winded title of "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data" (which we'll call the "Data Protection Directive" for short).

The Data Protection Directive laid out the broad guidelines with which the local law of each member state of the European Economic Area (the "EEA" – all 28 of the European Union member states plus Iceland, Liechtenstein, and Norway) would have to comply. Among other objectives, the Data Protection Directive sought to require uniform minimum levels of data protection among EEA member states and allow personal data of EEA citizens to pass freely among EEA member states and certain other jurisdictions with adequate protections under local law.

But the Data Protection Directive stopped short of being a detailed regulation. Under EU law, a "directive" merely states the requirements that EEA member states must incorporate into their local law. It requires that each EEA member state government interpret the directive and enact its own law based on that interpretation. Accordingly, the Data Protection Directive left a great deal to the discretion of EEA member states. As a result, the law remains non-uniform and it's hard to predict whether a particular practice or data transfer will conform to the requirements of the law. This problem applies within the EEA, but it also raises issues for those who move personal data into and out of the protective bubble of the EEA. These issues were a problem as far back as the initial issuance of the Data Protection Directive in 1995. Today, with increased globalisation and Cloud-based computing, the stakes are even higher and the Data Protection Directive is even less adequate to the task.

Enter the General Data Protection Regulation (the "GDPR"). The GDPR will be a "regulation," which is different from a directive in that it will apply across the EEA on its own terms without the necessity that EEA member states enact their own conforming versions. It will be top-down law instead of the bottom-up approach of a directive. Political preferences aside, the regulation is more likely to provide a uniform and predictable system within which to operate.

The European Commission presented the first proposal on 25 January 2012 (designated Proposal 2012/0011). Since then – as one might expect at a table with more than 28 participants – thousands of amendments have been considered. A committee of EU lawmakers has boiled the changes down into the most recent draft as of 22 October 2013, but more work needs to be done.

Most observers who follow such things anticipate that the GDPR will be enacted in late 2015 or early 2016 and that enforcement will begin in 2017 or 2018.

Plenty of time, right? Yes…and no – for two reasons:

Firstly, it will take time to implement the changes required to comply with the regulation. Two years after enactment of the regulation is a long-ish time. But enterprises – particularly large ones – take time to change course. And that's to say nothing of getting senior management up to speed, budgeting and personnel allocations necessary to put the new compliance regime in place, and the actual time to implement those changes. Starting now is likely to make it less painful (and less expensive) when the final regulation comes out.

Secondly, many enterprises already have privacy and data protection processes that happen on a periodic (annually, biannually, etc.) basis. These include privacy impact assessment ("PIA") review, US Commerce Department Safe Harbor recertification, and other processes. Keeping the likely requirements of the GDPR in mind during these periodic processes is much less onerous than sitting down to work on GDPR compliance as a separate process of its own.

Some specific action items

Although the GDPR is far from finalised, some provisions and ideas in the draft

regulation are so popular or accepted that it is reasonable, even at this early hour, to take action. The following discussion is by no means comprehensive, but it contains several suggestions that allow enterprises to make the best of the time between finalisation and effectiveness of the GRPR:

Privacy by design: The regulation requires that data controllers and processors build privacy and data protection into nearly every business process. Although the draft GDPR does not contain specific requirements, it's more than just rhetoric. The GDPR will likely require, among other things, that data controllers and processors be able to locate a particular person's data, carry the burden of proof that the controller or processor has the legal right to process it (whether by consent or a series of hard-to-achieve exemptions), correct it, tell the data subject who else has his or her data and – shockingly to most US-centric enterprises – forget the data subject and his or her personal data at the appropriate times. Most US enterprises' systems are not set up to track the circumstances under which personal data was collected, what consents are in place, or even ensure timely deletion of personal data, and that requires a great deal of backpedalling and forensic research if the enterprise ever has to prove its compliance. It is much easier to build privacy into a process at its inception than it is to re-engineer the process later. Privacy by design is the new reality and building it in now will save cost and energy later when – by every indication – it won't be optional.

Binding corporate rules: Leaving aside the fact that uniform law will make things a little more predictable state-to-state, transfers of personal data of EEA citizens out of the EEA will not get any easier under the GDPR. If your enterprise is using a combination of Standard Contractual Clauses, US Safe Harbor, and other means to comply, now is a good time to consider establishing so-called "binding corporate rules" ("BCRs"). BCRs are not easy to implement and they take time and money, as well as involvement with data protection authorities ("DPAs") in the EU. But, for many enterprises, the GDPR will be the event that tips the scales in favour of BCRs. And it's reasonable to think that many enterprises will think the same thing after the regulation comes out, resulting in a rush of BCR applicants. It's already a slow process and being a part of a rush in 2016 or 2017 won't make the process any easier. If you're on the fence about BCRs or if you think that you might implement them any time in the next three years, now – well before the rush – is a great time to consider them.

Cloud computing: European lawmakers care deeply about where personal data goes. They worry that, if data ends up in a jurisdiction without European-style protections, both private parties and units of government will use the information in ways not permitted by EEA law. Events such as allegations that the NSA tapped German Chancellor Angela Merkel's cellular phone or information revealed by Edward Snowden about the US National Security Agency's surveillance programmes give apparent weight to those worries. Cloud computing, on the other hand, works, in large part, because data can be stored and/or processed in virtual environments that transcend (even defy) international borders. Additionally, most Cloud services are provided by specialised vendors and not by the enterprise itself. Enterprises should take the opportunity now to evaluate where data goes and whether it is in the enterprise's hands or the hands of a vendor. And the additional compliance obligations brought on by the GDPR will create a need to address those issues in vendor contracts (be they limitations on geographic locations, obligations that match the GDPR, allocation of liability for failures to comply, or otherwise). Acting now is particularly helpful because the average contract with a Cloud vendor or other IT vendor will expire or come up for renewal during the time between now and the final GDPR. Getting a head start on including the appropriate obligations and allocating liability gives an enterprise a greater opportunity to include more of its vendor contracts. And, at the very least, any new or renewal vendor agreement should include a provision that requires the vendor to come to the table and negotiate in good faith if EEA law changes and the change needs to be covered by the agreement.

Staff: The GDPR requires that almost every substantial enterprise (presently pegged at processing the personal data of more than 5,000 data subjects in any 12-month period) or any enterprise whose core activities involve processing personal data must appoint and empower a data protection officer (a "DPO"). The DPO will have several particular duties and the DPO's contact information is likely to be required. It should go without saying that nearly every enterprise should have a person in this role regardless of the impending GDPR, but looking at job descriptions (and employee indemnification for the DPO) now will avoid having to do it later.

Data breach response plan: The draft GDPR requires that an enterprise that suffers a data breach must notify both the data subject and each DPA, in some cases within 24 hours. Although this provision has the benefit of making data breach reporting law uniform across the EEA (unlike the US, which has more than 45 separate state data breach notification laws with no uniform federal law on the horizon), obligations will become specific and timing will be imposed. The next review of an enterprise's data breach response plan should include consideration of the GDPR requirements.

The stakes are high

The stakes are high for those who run afoul of the GDPR. The initial draft began with penalties of up to a fine up to the greater of €1m (about US$1.12m) or 2% of the offender's global annual revenues. (Yes, you read that correctly.) A later committee amendment upped the penalties to the greater of €100m (about US$112m) or 5% of global annual revenues. (Yes, you read that correctly as well.) The largest fine to date has been €150,000 (about US$167,000) levied against Google by the French DPA. The fine was the maximum available under applicable law and it is reasonable to think that DPAs will reach into that higher range.

The final GDPR is a long way off, but the key concepts are becoming clear and enterprises that begin acting now have the opportunity to save time, money, and energy on the way to compliance.

Stephen L. Tupper heads the Dykema law firm's Privacy, Data Security, and E-Commerce practice team