

GET READY FOR D-DAY

The forthcoming General Data Protection Regulation (GDPR) will shake up the way personal data is collected, stored and used. *Andrew Don* reports on what it means for fleets

May 25, 2018, is D-Day – or 'Data Day' – when the General Data Protection Regulation (GDPR) takes effect. It will not be phased in; it will be implemented in one big bang. The GDPR has been referred to as 'the Data Protection Act on steroids' – and for good reason.

Breach the GDPR and the maximum penalty will be a €20 million (£17.9m) fine or 4% of total global turnover for the previous year, whichever is the highest.

This is a gargantuan increase from the current £500,000 maximum for breach of the Data Protection Act 1998.

If you think data protection is a bore or GDPR does not concern you, you'd better think again. The rights of the individual are at the heart of it. That means every employee on a company's data base – fleet very much included.

The UK is committed to embracing this European legislation, Brexit or no, and the new Data Protection Bill that is going through Parliament encapsulates the GDPR.

It is a juggernaut that is coming your way and everyone, including fleet decision-makers, needs to be prepared.

THE LAW

The GDPR, or Regulation (EU) 2016/679, to give it its more formal title, builds on existing data protection legislation with a particular focus on digitalisation and technology.

£17.9m
maximum penalty for breach of GDPR regulations

£500,000
current maximum penalty under Data Protection Act

It covers 'the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repeals Directive 95/46/EC (General Data Protection Regulation)'.

In the UK, it reforms the eight data protection 'principles' in the Data Protection Act 1998 and introduces new principles of transparency and accountability with a company's ability to prove consent a significant pillar of the new regime.

The regulation aims to give individuals greater control over their personal data and this includes the right to request their data is edited or even erased.

It also introduces a duty to report certain types of breach to the Information Commissioner's Office (ICO) and, in some cases, to individuals within a set time.

The issue of consent for personal data to be captured and used for more than just contact is one of the trickier areas according to Paula Tighe, director of information governance at legal firm Wright Hassall.

"Individuals must give clear consent for their data to be used, but must be allowed to revoke consent easily at any time," she says.

"If you change the way you want to use the data, you must obtain a new consent."

Consent must be implicit and attempts to obtain or confirm consent will help mitigate problems at the hands of the ICO.

Sue O'Connell, compliance manager at FleetCheck, says it may be that existing consents will need to be refreshed if



they are not in line with the GDPR standards. Records will have to be up to date, so regular reviews will be essential.

MONUMENTAL CHANGE FOR FLEETS

So what does all this have to do with fleets? Caroline Sandall, director of ESE Consulting and deputy chairman of fleet operators association ACFO, says the GDPR will fundamentally change the way fleets interact with drivers.

Sandall, who believes the GDPR has been "a little underplayed" in terms of its impact on fleet, says: "A lot of news items have focused on telematics data and the more obvious data things, when actually what is really critical is making sure you can absolutely prove that drivers understand what is happening to their data and that you maintain a robust audit trail to show this."

Drivers need to understand their obligations, and a tick-box exercise of 'I have read and understood the policy' will not stand up to scrutiny.

"This is a monumental change for HR to deliver, or for smaller companies, or a wider group of people because you've got to ensure drivers know what they are signing up to when they have a company car," says Sandall.

"You need to think about how you need to change your processes to adapt to that. If you've got a paper process, it's how you capture that consent because at some point, somebody will get audited and probably found wanting, and the fines relating to this are substantial."



"You need to think about how you need to change your processes"

Caroline Sandall, ACFO

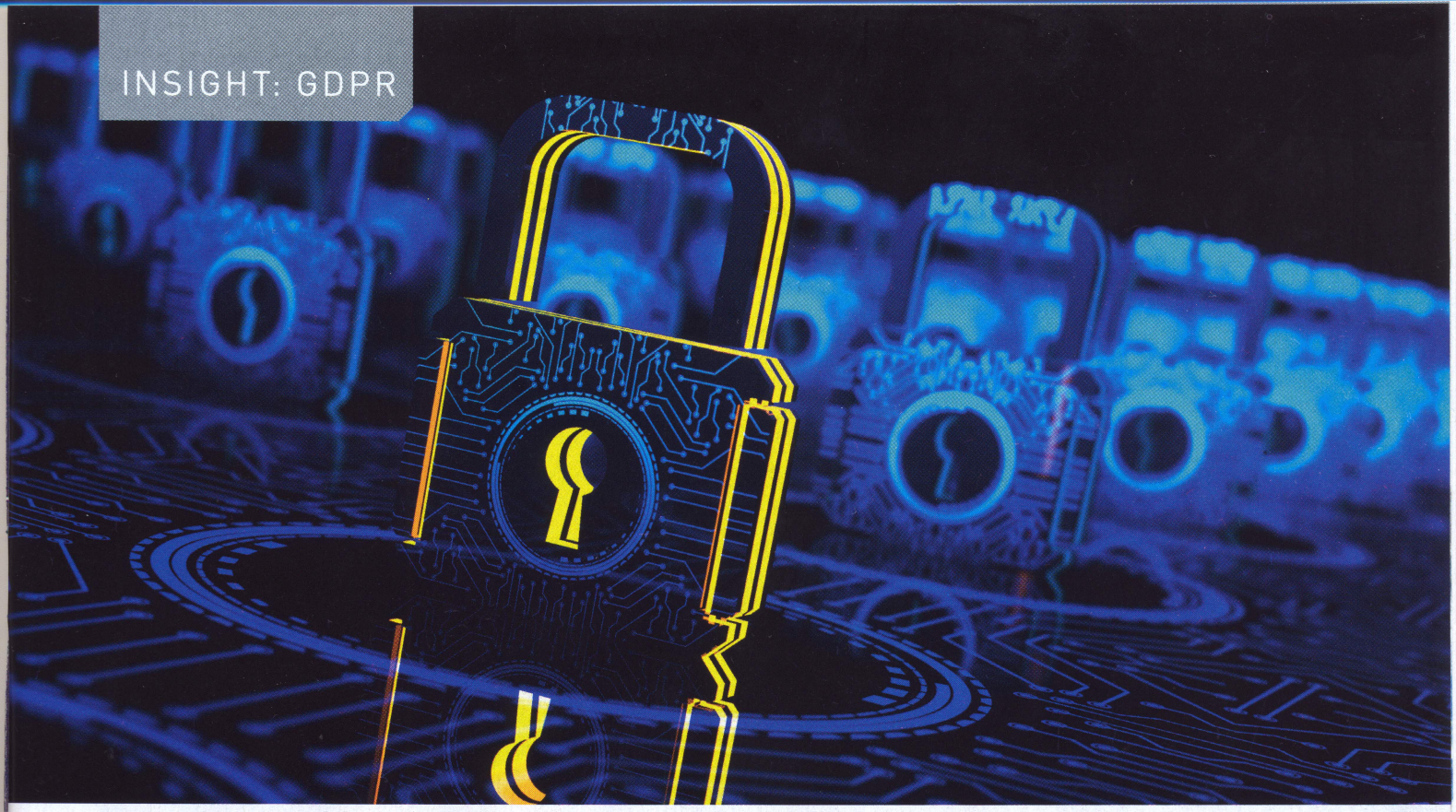
Data held by fleet operators which could be affected by GDPR includes:

- Name, date of birth, age, address.
- Phone/mobile numbers, emergency contact details.
- Medical conditions relating to ability to drive.
- Location information while working and potentially outside working hours if using a company vehicle (telematics).
- Driving behaviour (speed, acceleration, 'aggressiveness' of driving) – the speed information could be handed to authorities in the future for prosecution.
- Potential in-car CCTV for insurance protection which may include in-cab camera so includes personal video footage.
- Any related HR data handled during driver management; performance and disciplinary data.

PRIVACY IMPACT ASSESSMENT

Tighe says businesses should undertake a privacy impact assessment (PIA) before beginning any project involving personal data where data processing could pose a significant risk to individuals because of the technology used, or the scale of the processing.

"These assessments will help you and the regulator decide the likely effects on the indi-



vidual if their data is lost or stolen and should form part of your ongoing processes," says Tighe. "Ensure you have a robust process for making the assessments and then record it, along with the outcome – a PIA is a simple step towards compliance, with the emphasis on what you do, rather than on what you say you will do."

O'Connell of FleetCheck says it is essential to start planning for GDPR compliance now.

"Fleet managers need to make sure that decision-makers and key personnel in their organisation are made aware that the law is changing and that they appreciate the impact this is likely to have," she says.

"Companies should also make sure the right procedures are in place to detect, report and investigate a personal data breach."

PROTECTION REGISTER

A data protection register is one of the best ways to protect an organisation against claims of a data breach.

This document records all the actions you are taking to achieve compliance – the single most important step small- and medium-sized enterprises (SMEs) can take towards getting it right by May.

It shows you have understood there is a need for change and what steps you are taking.

Tighe says: "Without a record of what you're doing, the ICO will assume you are doing nothing, which is bad. By starting your register and keeping it up to date with all the actions undertaken, you are doing something, which is good."

WHERE RESPONSIBILITY LIES

Responsibilities for data protection are set at a much higher level than fleet manager and are HR/legal functions. However, data protection issues encompass the fleet manager's role among every other business role and awareness of the law among all employees is essential.

One of the most effective ways of ensuring compliance is for an organisation to recruit a dedicated data protection officer to oversee data-handling processes – especially where businesses deal with personal data on a large scale.

It is not just electronically-held data that can pose a problem, according to Tighe. Fleets need to consider written records because they are also covered by the regulations. This means they will have to ensure all staff are trained on the correct handling of personal data, important when telematics data is accessed and added on by line managers

"Organisations that can prove they have made an effort to comply, even if they are not fully compliant with every aspect of the GDPR from the word go, will fare better than those who cannot," says Tighe.



"A PIA puts the emphasis on what you do rather than what you say you will do"

Paula Tighe, Wright Hassall

BIG DATA

Big data enables fleet managers to understand in real-time vehicle performance and driver behaviour but the explosion in available information means employers must be vigilant in complying with the GDPR.

The legislation will have a significant impact particularly for the fleet introduction of internet-connected cars.

The ICO has already undertaken initial work with the Society of Motor Manufacturers and Traders (SMMT) and the British Vehicle Rental and Leasing Association (BVRLA) to develop its understanding of the data protection privacy risks arising from the deployment of connected and automated vehicle technology.

Martin Evans, managing director at Jaama and an ICFM director, says: "Much can be achieved with big data to enable fleet managers to make informed decisions by understanding driver behaviour and vehicle performance and utilisation.

"But the flipside of that is fleet managers being mindful of businesses holding large volumes of data, which will contain information deemed personal under GDPR."

Evans says fleet managers are worried: "Understanding and embracing big data is important but it is also vital for businesses to protect themselves."

He warns fleet operators could find themselves capturing so much big data that a failure to act on the information obtained could prove to be counterproductive in terms of ensuring compliance with, for example, road traffic and health and safety legislation.

"It is therefore vital that businesses have in place good systems that will take vehicle and driver information and digest it," adds Evans.

"In turn, that will enable fleet managers to make informed decisions as they will have an holistic picture."

A roundtable discussion at a Fleet Industry Advisory Group (FIAG) workshop last autumn found agreement among delegates that telematics systems provided a wealth of data but information collected must be used responsibly and drivers informed of the use to which it is being put.

"Businesses must be clear about what data they are gathering and why, where it is going and how it is being used and gain people's consent," says Alex Ktorides, head of ethics and risk and a partner at law firm Gordon Dadds.

This means updating contracts of employment, employee terms and conditions and codes of conduct and he suggests that anonymising data will be a very effective tool.

If information is personal and identifies who a person is and how that employee is using their car and their behaviour then it impacts on their privacy and requires sign-off.

"There is huge value in gathering data, but that must be balanced against people having a right to privacy. Employers must put people's rights at the forefront and show good governance and gain consent," Ktorides says.

Anthony Monaghan, who leads the transportation and engineering practice at global insurance broker and risk adviser Marsh, stresses that consent cannot be inferred from silence, pre-ticked boxes or inactivity.

"Under the GDPR, where an organisation relies on consent as the legal basis for using an individual's personal data, that consent must be freely given, specific, informed and an unambiguous indication of the individual's wishes, meaning that consent has to be a positive opt-in."

PA Consulting Group has its own assessment methodology, which allows organisations to benchmark where they currently are against the various dimensions of the regulation.

Charles Ford, a fleet specialist at PA Consulting Group and member of the ICFM, says: "Potential areas that fleet organisations will need to address include remediating high-risk processes and IT that hold and process personal information; updating consent notices; updating policies and standards; increasing staff awareness and training; and dealing with third party contracts to ensure compliance."

Both the fleet organisation and third-party suppliers are equally liable under GDPR, Ford points out.

THIRD-PARTY SUPPLIERS

Dirk Schlimm, executive vice-president at telematics provider Geotab, points out that if fleet managers use a third-party to monitor and manage vehicles and drivers, they need to ensure the fleet management system enables GDPR-compliant fleet management – for example, a privacy mode feature and data minimisation.

They also need to ensure suppliers comply with the GDPR in terms of how they process data they receive from the fleet manager.

Key obligations for the supplier are to follow the fleet manager's instructions for data processing, to put in place technical and organisational measures to keep data secure, and to have proper data-related documentation in place.

"Fleet managers should keep an inventory of all the vendors that have access to data, whether and to what extent data is being transferred outside the EU, and have clarity on rationale for processing personal data, such as legitimate purpose and/or consent," says Schlimm.

TRANSPARENCY

If fleet managers do not comply with the new regulation and adopt adequately secure systems to properly manage policy and consent, their employer could face the maximum penalty, warns Charlotte Ebutt, a solicitor in the technology and media team at Royds Withy King.

Businesses need to be as transparent as possible in respect of how they are using personal data and be aware of the rights that individuals now have.

"Data protection is not a subject to be taken lightly," Ebutt says.

The huge penalties could have disastrous effects on not only company finances, but reputation too.

TOP GDPR TIPS

- **Ensure people throughout the business are aware of the GDPR.**
- **Promote a culture of shared responsibility which lies with everyone who handles and processes data – not just data controllers.**
- **Map and document what personal data you hold relating to your drivers, including telematics data.**
- **Weigh up what data you hold, how you will use it and including security procedures, data that manufacturers collect and share.**
- **Document how you intend to use the data and who you will share it with and communicate this to drivers.**
- **Check and amend current procedures to ensure they cover all the rights individuals have under the GDPR.**
- **Make sure you have an audit trail around the notices and consent that you ask for.**
- **Be prepared for drivers requesting to see their data and have systems in place to facilitate this.**
- **Designate someone in your company to take responsibility for data protection compliance.**

Source: Anthony Monaghan, Marsh

