Client Alert: Driving Compliance: Car Tech and Data Protection FAQs

Date : May 20, 2020

Vehicle technology (often called car tech) is becoming increasingly sophisticated, with GPS trackers, inbuilt software, in-car cameras and other devices and apps gathering large amounts of data about numerous aspects of a driver's driving habits and life more generally. Information is also collected about passengers and other road users. In data protection terms this data, together with other information such as the car registration number and serial number, is likely to be personal data to the extent that it can be linked back to an individual.

This data is then shared amongst the various players that make up this dynamic sector, such as dealerships, financiers, car hire companies, insurers, vehicle and device manufacturers. The data is also of wider interest to others, including travel companies, marketers and advertisers, government planning authorities, law enforcement and anti-fraud companies.

These FAQs look at the need for the use of personal data collected to comply with data protection laws including GDPR and UK Data Protection Act 2018, and also ePrivacy laws. It focuses mainly on the legal obligations of controller and processor organisations (rather than individual drivers) in relation to the following technologies:

1. connected cars;
2. autonomous vehicles; and
3. dashcams.

Under GDPR, the relevant data protection authority (DPA) can take a range of enforcement action against organisations that infringe data protection laws, including administrative fines of up to €20 million or 4% of annual global turnover, whichever is greater. Enforcement action may also be taken under other applicable laws, such as ePrivacy laws (which are currently being reformed, with the current proposals including the introduction of GDPR-equivalent enforcement powers). The article uses some specific data protection terms which are explained here www.bit.ly/gdprwords. There is also some background to GDPR in our FAQs here www.bit.ly/gdprfaqs.

What are the issues with Connected Cars?

Connected cars are part of the Internet of Things (IoT). They involve the driver sharing data with the vehicle, such as:

1. their contact list, emails and texts (both metadata and content), if they hook up their phone to the vehicle to receive messages;
2. locations, such as home, work, favourite places for shopping and recreation and, more intrusively, places of worship or health facilities;
3. identity or security information in order to authenticate authorised vehicle usage, including biometric data, for facial recognition or fingerprint activated access systems;
4. body weight and more sensitive health data where, for example, there are special modifications or features to accommodate a disability;
5. infotainment preferences such as music and radio, which could in some instances reveal political, religious, or sexual orientation;
6. driving behaviour, such as speed and braking (recoverable through telemetry and/or the vehicle's black box following an accident), if the driver's eyes are on the road (through internal cameras or headrest sensors) and if the driver wears a seatbelt (through belt clip sensors);
7. appointments and calendar items if these are synched with the vehicle – again the data here could include special category data including data relating to health and religious persuasion;
8. details of other devices where they are synched with the vehicle including identifying details for phones and tablets added via Bluetooth, WiFi or NFC.

In turn, that data is shared with other parties and used for various purposes, including remote control and diagnostics, monitoring via a dedicated app, improving safety, notifying emergency services if the driver has an

accident, finding a parking spot and marketing of relevant products and services.

What about litigation risk?

We have already had litigation over connected cars. For example in 2005 a US appeal court looked at the lawfulness of tracking hire vehicles to enforce the hire company's terms and conditions. In that case a driver alleged that he had not been told of the presence of a tracking facility in a car he hired in 2000. The device was used to monitor his driving and he was sent 3 penalty notices by the hire company for exceeding the speed limit using data taken from the vehicle. Tracking was disclosed in the rental agreement and on the hirer's premises. The driver commenced proceedings and won his claim on the basis that the hirer's practice was deceptive. The decision was upheld on appeal.

Are there any guidelines?

The European Data Protection Board (EDPB) has developed guidelines on processing personal data in the context of connected vehicles and mobility related applications. The guidelines were put out to a public consultation that closed on 4 May 2020. The guidelines outline the applicable law, provide some general recommendations and include some helpful case studies. In particular, the guidelines highlight the need to comply with the data protection principles and to minimise the amount of data collected and stored, emphasising that constant vehicle tracking should be avoided where possible, such as where the relevant purpose could be achieved with a more limited dataset (such as mileage data). The European Automobile Manufacturers' Association (ACEA) however criticised elements of the EDPB's guidance on 15 May 2020 and also suggested that this guidance be postponed. The ACEA also says that the guidance is inconsistent with advice which has already been issued in France and Germany. 60 other individuals and organisations have also made submissions to the EDPB in connection with the guidance.

In March 2020 the Dutch Data Protection Authority (Autoriteit Persoonsgegevens (AP)) disclosed that it had contacted vehicle manufacturers to look at their compliance with data protection law. The AP asked all manufacturers of cars, commercial vehicles and trucks in the Netherlands to provide details of the personal data they process, why they process it, for how long, how they secure it and with whom they share it.

What are the security risks?

In terms of risks, smart vehicle technology increases the volume of personal information collected by the vehicle. In addition, where the vehicle has wireless links to communicate with devices and services (such as image sensor communication, Bluetooth and Wi-Fi or mobile communication technologies (e.g. 5G), there is the potential for hacking. The motives of malicious actors include tracking individuals, fraud, vehicle theft, data theft, denial of service / extortion and vehicle ID reassignment.

For instance, by accessing the servers of a cloud-based platform at the back-end of an app, an authorised hacker was able to see the vehicle's location, access the personal data of the app's users, and remotely control vehicle functions, such as opening doors and stalling engines.

Manufacturers are having to come up with novel ways to overcome security threats, such as 'bug bounties' – incentives offered to hackers and researchers who find and report security vulnerabilities in their products. For example, in March 2019, Tesla awarded a car to researchers at Pwn2Own (a hacking contest at the CanSec West conference in Vancouver), for demonstrating a vulnerability against the in-car web browser. Tesla quickly issued a software update to address this.

As the number of connected vehicles on the roads has increased, so has the number of automotive cyber-security incidents. Having strong security protections is therefore imperative.

GDPR Article 32 sets out the relevant requirements regarding security of processing. Both controllers and processors must implement "*appropriate technical and organisational measures to ensure a level of security appropriate to the risk*" to individuals' rights, in particular as regards the risk of personal data breaches. Specific

measures may include, amongst other things, encryption of personal data and regular penetration and resilience testing.

Industry standards such as relevant ISO and SAE standards are important benchmarks for setting consistent policies for addressing risk assessment and threat analysis in this context. The 5StarS project is carrying out research and developing an assurance framework for assessing vehicle cyber security.

In addition to data protection laws, ePrivacy laws (including the EU Directive on Privacy and Electronic Communications (2002/58/EC) and local laws implementing this, e.g. the UK's Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR)) may also need to be complied with. Note that the Directive / PECR apply to data on electronic communications networks more broadly than just personal data.

One important consequence of this is that, whilst consent may not necessarily be required under the GDPR (if another legal basis such as 'legitimate interests' can be relied on instead), consent may still be required under ePrivacy laws. Consent might be harder than it sounds – for example some car companies take a data protection consent when they hand a new car over but how can that be binding on other drivers or someone who buys the car second-hand?

Where data is collected from a connected vehicle via a publicly available communications service, (e.g. a GPS tracker runs off a mobile network) consent may be needed under PECR to place and read data from a connected vehicle or a device that is connected to it. The limited exceptions to this are where the information is accessed:

1. for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or
2. when this is strictly necessary to provide an online service that the user has requested (e.g. a geo-location based theft recovery service).

What about Autonomous Vehicles?

Autonomous vehicles allow for some aspects of safety critical control functions to be performed without direct driver input.

In a vehicle with some automated critical control functions, personal data will be collected and processed in a similar way, and similar privacy considerations will apply, as in relation to connected cars above for owner and passenger information, location tracking, marketing and sensor data etc. As well, privacy issues may arise in relation to the voice recognition and control system of the autonomous vehicle. Initial research – such as the innovative work being done at Jaguar Land Rover - has also focused on the health and well being of all of the occupants of the vehicle.

In addition, the research and development that is going into designing the autonomous cars of the future is leveraging a wealth of personal data on driver behaviour. This use will need to comply with the data protection principles and have a valid legal basis. It is important that individuals have been told up front that their data will be used for this specific purpose and, where possible, anonymised data is used. We've seen that transparency has been a key feature of many cases in the first 2 years of GDPR and it will be key to fulfilling legal obligations in the world of autonomous vehicles.

What about Dashcams?

Dashcams can record video of those individuals in the vehicle (such as in a bus or a taxi) and/or of the road outside. Some systems record both audio and video, and some video only. Video images and audio recordings where individuals are identifiable are personal data.

Dashcams are most commonly used for recording traffic so that the footage can be provided to law enforcement and/or insurers in the event of an accident. As such, this can provide details on the location and activities of any individuals who are visible to the vehicle at a given point in time.

Dashcams are also being used to aid the development of autonomous driving technology, with video data powering AI-driven automated object recognition in order to train the system to accurately identify pedestrians, other vehicles, objects and other hazards. Some next generation dashcams are strictly not dashcams in the traditional sense – for example they may be mounted on the exterior of the vehicle to read traffic signs or sense lane movement. This may increase transparency issues as those inside the car might not be aware of their existence.

Video data may also be combined with other data from other technologies, such as facial recognition algorithms, resulting in high volumes of potentially intrusive personal data being processed about individuals.

In the UK the Information Commissioner's Office's CCTV Code of Practice and in Ireland the Data Protection Commission's Guidance for Drivers on use of "Dash Cams" provide guidance on use of dashcams. We've looked at some of this guidance already and have some tips for compliance here https://bit.ly/cctvlaw.

The Irish guidance explains that, where a dashcam is used in a commercial non-personal context, such as by chauffeurs, ride-sharing companies, taxis, buses or couriers, the operators (including potentially drivers, and/or employers, insurers or others involved in the decision to utilise the dashcam) will be caught by data protection law. Video data that captures events in a public space, even where the camera itself is located on private property, will not be exempted from the GDPR by reason of the household / personal exemption. This means that an individual who uses a dashcam whilst their vehicle is on the road will generally be considered a data controller and as such would be subject to data protection laws.

The ICO guidance emphasises that continuous recording, particularly involving audio as well as video, should be avoided unless there is a strong justification for this.

Both regulators recognise that, in terms of transparency, it may be a challenge to provide all individuals captured by dashcam footage and in-car audio with the required privacy information. They recommend using a "layered" approach, with the most important information displayed on a highly visible sign (e.g. a sticker on the outside of the vehicle) alerting individuals that a dashcam is being used, and providing a way to obtain further information (e.g. a QR code that can be scanned with a smartphone, linking to an online privacy notice setting out the required information).

Video recordings should be securely stored, and access should be restricted to authorised individuals and handled in accordance with data retention policies. In this regard, controllers need to be aware of, and limit, who has access to the camera and any storage devices on which recordings are stored.

What about Subject Access Requests?

GDPR creates or extends a number of rights available to individuals in connection with their data. You can find out more about these rights in our GDPR FAQs here www.bit.ly/gdprfaqs. As with CCTV, subject access requests (SARs) can be burdensome if there is a large volume of data being processed and organisations will need to put proper procedures in place to deal with these requests. They will also need to have proper processes to deal with requests from third parties including people involved in traffic accidents, law enforcement or a spouse going through a divorce.

What about Employees?

If you, as an employer, make a vehicle available to your employees then be aware that additional compliance considerations could apply. One of the first cases we handled (in 2004) related to an employer who wanted to use data from earth moving machinery to assess the productivity and performance of employees. This type of processing can be especially problematical as consent is unlikely to work with employees and, in some cases, works councils may need to be informed or consulted. In some US states tracking employees may be prohibited unless certain conditions are met.

Compliance Checklist

Below are some of the key compliance obligations under relevant data protection laws, which organisations processing personal data using connected or autonomous vehicle technologies, or recordings using a dashcam in a commercial context or in a public area, will need to comply with:

1. **DPIAs** – Do a data protection impact assessment (DPIA) to identify and mitigate privacy risks. This is often mandatory when rolling out new technologies or technologies that involve large-scale monitoring, particularly on an organisational basis. We have a short film on how to do DPIAs here http://bit.ly/faceraid.
2. **Data protection by default and by design** – Design all technology with privacy in mind. Settings should default to the most privacy-protective option.
3. **Accountability** – Ensure that the use of these technologies is supported by clear policies and procedures.
4. **Controller/processor status** – Identify which players are data controllers (joint or independent) and data processors for each relevant data processing activity.
5. **Transparency** – Provide clear and transparent information about processing of individuals' personal data using these technologies, including details of the data controller, your purposes for processing personal data, retention periods, and with whom it will be shared. The level of detail and how this is presented should be appropriate to the specific technology being used. E.g. this could be done in the vehicle sale or lease contract, relevant services agreement, the vehicle's maintenance manual or via the on-board computer (particularly where 'just in time' information is required) and / or by use of highly visible stickers and QR codes.
6. **Data minimisation and retention** – Collect only the minimum data that you need to in order to fulfil the purpose you have collected this for and retain this only for the minimum period necessary for this purpose. This will generally mean avoiding collecting real-time location data or continuous video recording. Consider also using anonymised data where possible.
7. **Accuracy and control** – Where appropriate, include functions that give individuals control over updates to and deletion of their data.
8. **Purpose limitation** – Ensure that personal data that is collected for a specific purpose is not used for any incompatible purpose. Examples given by the European Data Protection Supervisor (EDPS) include not taking data originally collected for maintenance purposes and allowing this to be used by insurance companies to: enrich driver profiles; calculate custom pricing; offer driving behaviour-based insurance policies; or investigate liability in road traffic accidents.
9. **Security** – Ensure that there are robust protections for security and access control to safeguard against data loss or unauthorised access to personal data. Protections should be included to ensure that individual driver data is protected where the same vehicle is shared between multiple users.
10. **Lawful processing** – Ensure that a valid legal basis can be established for all processing activities (unless an exemption applies). If you're relying on consent, this must generally allow for individuals to turn on their own settings to activate personal data processing, and there must be an easy way for individuals to withdraw consent. If legitimate interests is relied on, carry out a legitimate interests assessment (LIA) whereby the organisation's business interests are balanced against the rights of the individual.
11. **Sensitive or criminal data** – Ensure that an additional condition for processing special categories of personal data or criminal data can be met if this type of data is being processed. This will be necessary if, for example, location data reveals a person's religion or sexual orientation, or if a finance company wants to carry out fraud tracing activities.
12. **Third parties and data sharing** – Ensure that all: data sharing with other third party controllers has a valid legal basis and is documented in a data sharing agreement that sets out each party's respective responsibilities; processing by third party processors is documented in a contract that contains the legally-prescribed data processing terms; proper systems are in place to deal with third party requests including requests for data from law enforcement authorities.
13. **Data subject rights** – Ensure that data subject rights are given effect to, including rights of access and rights to object to processing on the basis of legitimate interests. For example, if a data subject requests a copy of a dashcam video recording this should be provided promptly and generally within one month at the latest (unless an exemption applies). However, when providing this recording it may need to be redacted to remove data of a third party.
14. **Consent** - Finally, to comply with the ePrivacy Directive / PECR, organisations that access data from a connected or autonomous vehicle via a publicly available communications service will need to look at consent. They may need to obtain consent to access data collected in the vehicle where required – this

consent will need to be obtained to the GDPR standard. This is the case irrespective of which legal basis is being relied on under GDPR.

For more details of Cordery's work in the automotive sector and details of recent projects please visit https://www.corderycompliance.com/automotive/

For more information please contact Katherine Eyres or Jonathan Armstrong who are lawyers with Cordery in London where their focus is on compliance issues.

The 2005 US case referred to in these FAQs is James Turner v. American Car Rental, Inc.

Details of Jaguar Land Rover's studies are here https://bit.ly/3g2HGCH.

The EDPB consultation is here - https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-12020-processing-personal-data-context_en.

Office: +44 (0)207 075 1784

jonathan.armstrong

Office: +4

katherine