Quartix
Real-Time Vehicle Tracking

GDPR Guide

Introduction to GDPR Compliance for Fleet Managers

The General Data Protection Regulation (GDPR) is the biggest change in how businesses handle personal data since the introduction of the Data Protection Act in 1998. It dramatically increases personal rights around consent, collection, usage, storage and access to personal data, whether that of consumers or employees.

GDPR impacts companies using vehicle tracking and telematics systems, as it is deemed to be 'collecting and storing personal data'. Vehicle tracking can improve operational performance and reduce costs, but fleet managers need to ensure the correct processes and documentation are in place to comply with the new legislation. This guide is an introduction to GDPR, based on current industry interpretations. However, companies are advised to seek their own legal advice, as Quartix is not a law firm.

When does it become law and what are the penalties?

Companies need to comply by 25 May 2018. Failure to meet GDPR's terms will be punishable by stiff penalties – businesses can be fined €20 million or up to 4% of global annual turnover, whichever is the greater.

The UK is leaving the EU, do we still need to worry about GDPR?

Yes. Although it is EU legislation, the UK Government has said it is likely to implement similar rules, and any company doing business in the EU post-Brexit will need to be compliant with GDPR.

What is 'personal data'?

GDPR makes clear that personal data includes online identifiers and location data – meaning that IP addresses and mobile device IDs are all personal and must be protected accordingly. All of these will now be subject to the same data protection requirements as every other type of personal data.

GDPR in a nutshell

Key Principles	
Lawfulness, fairness and transparency	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject
Purpose	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
Solely collecting data you need	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
Accuracy	Personal data shall be accurate and, where necessary, kept up to date
Storage limitation	Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
Integrity and confidentiality	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
Accountability	The controller shall be responsible for, and be able to demonstrate compliance with the GDPR

Key Rights:

- The right to be informed – *the right to know what personal data is being used for*
- The right of access – *the right to view this data*
- The right to rectification – *the right to correct errors in personal data*
- The right to erasure – *the right to ask for data to be removed*
- The right to restrict processing – *the right to restrict how a company uses personal data*
- The right to data portability – *the right to receive personal data in an electronic form*
- The right to object - *the right to ask a company to stop using personal data*
- Rights to prevent decisions being made solely based on automated processing and profiling of personal data

Key Roles:

1. The Data Controller – the fleet operator
2. The Data Processor – the system provider
3. The Data Subject – the driver

Three areas to focus on

Companies need to look at all the ways they collect, store, and process personal data. When it comes to handling telematics data involving drivers, these are the three areas companies should focus on:

1. Consent or Legitimate Interest

Companies have two options when it comes to justifying the collection and management of personal data. They can either gain consent from drivers or make a case based on legitimate interest.

Option 1: Consent

Consent must be freely given, specific, informed and unambiguous. Companies will need to prove that they have received consent and that drivers understand what data is being collected and why. If drivers do not give consent, or withdraw it later, the tracking would need to be removed.

Option 2: Legitimate Interest

An alternative is to use a justification of legitimate interest, i.e. it is essential to business operations or to prevent fraudulent activities. Examples of legitimate interest could include:

- Preventing unauthorised fuel claims in relation to mileage travelled
- Monitoring vehicles to prevent theft
- Unauthorised and unsafe out of hours use of vehicles
- Duties of care to protect staff, including driver safety, and lone workers
- A need to track working hours against timesheets to ensure drivers comply with working time directives

This needs to be specific and documented – simply stating the need to check on 'good and 'bad' drivers may not be sufficient. To show legitimate interest, companies must conduct a risk assessment that balances the rights of the data subject against the interests of the business.

2. Transparency

GDPR also provides staff with the right to access any personal data held on them quickly and easily. This includes any telematics data where they are identifiable as the driver of a vehicle. They will also have the right to ask to change any errors and to erase personal data if required.

3. Security

The GDPR increases requirements to protect personal data. It will compel all organisations to report any data breach that "is likely to result in a risk to people's rights and freedoms", to their relevant supervisory authority (the Information Commissioner's Office in the UK), as well as notifying the individuals affected. This all has to happen within 72 hours of the breach being discovered, and failing to notify the authorities can result in significant fines.

It is important to bear in mind that this doesn't just cover personal data being lost or stolen by hackers – it also covers access by those that are not authorised to view it as part of their role. Data, therefore, needs to be stored securely and organisations have to look at how they grant permissions to view information internally.

Quartix
Real-Time Vehicle Tracking

GDPR Guide

Quartix and GDPR

Quartix has always followed industry best practices and legislation (such as the Data Protection Act).

- All our data is processed within ISO 27001 certified datacentres in the UK.
- Quartix is certified under the UK Government Cyber Essentials scheme for IT security and continually review best practices and standards to keep up to date.

While compliance is a matter for individual organisations, who are the 'data controllers' under GDPR, Quartix, as the 'data processor', is fully committed to helping our customers meet GDPR needs and we are working towards compliance with the General Data Protection Regulations by the deadline on 25th May 2018.

Key features of our system designed to assist with GDPR compliance:

1. Access to data and potential rectification

Quartix customers have self-service access to their data and can easily make recent data available to drivers, if required. This reduces the time, effort and resources required to deal with any driver requests for the personal information held on them.

2. Security and auditability

Data has always been protected in Quartix, both within vehicle units and in our secure data centres. Customers' access permissions to data can be set at a granular level, allowing them to restrict the information that specific employees can view. Any changes to vehicle and driver data made through our web application are automatically recorded, providing an audit trail to support compliance.

3. Access to data

Under GDPR, customers and individual 'data subjects' have the rights to access and request changes to the data concerning them. Quartix will refer any such request from an individual 'data subject' to the customer as the 'data controller'. Customers will have the option to request extracts of the data concerning their vehicles and / or have it removed from the system.

Quartix
Real-Time Vehicle Tracking

GDPR Guide

Checklist - questions to consider

If a company is collecting and using telematics data (the data controller), responsibility needs to be upheld for the personal data collected. To help achieve compliance, start by asking these questions:

1. Is there someone in the company who is responsible for data protection, and overall GDPR compliance? If so, do they know about driver data and have they included it in their GDPR compliance planning?
2. What telematics/driver data is currently held? Has the business documented what this is, justified why the company holds it and how it is collected/used/stored?
3. Has the company decided whether it will get driver consent or documented the legitimate interest for collecting driver data?
4. Is there a process in place to give drivers access to information?
5. Have new GDPR processes been communicated to drivers and those that work with their data so that everyone is aware of their rights and responsibilities?
6. How long does the business need to keep telematics data for? Quartix securely stores telematics information as part of its service. Retention time is set by customers and should depend on its usage. For example, if it's just 'total shift time', used to enable staff to be paid, it would be different to storing driving style information that builds over time. Be clear about how long data is being stored and why.
7. Are there breach notification processes in place?
8. Are there mechanisms in place to safeguard the Key Rights of drivers?

Additional Resources

For an official overview of GDPR visit the Information Commissioner's Office (ICO) website at

https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

For information on how GDPR affects employment contracts:
http://www.shoosmiths.co.uk/client-resources/legal-updates/hr-gdpr-changing-employment-contracts-and-policies-13115.aspx

For information on the UK Government Cyber Essentials scheme for IT security:
https://www.cyberessentials.ncsc.gov.uk/

About Quartix

Quartix has delivered real-time vehicle-tracking and telematics solutions to small and mid-size fleets for over 16 years. Businesses choose Quartix because we offer cost-efficient solutions that are easy-to-use from installation through reporting. Over 10,000 companies are using Quartix solutions to gain actionable insight into vehicle movements, engine usage, driver behaviour, and fuel consumption.

If you have any queries on GDPR and vehicle tracking please speak to your Quartix contact or email us at support@quartix.net

Disclaimer