masternaut

MASTERNAUT INSIGHTS

GDPR
The General Data Protection Regulation

A viewpoint for
Masternaut customers

July 2018

masternaut

Foreword

In recent months I've been approached by a number of our customers looking for insight and advice on how the new General Data Protection Regulation (GDPR) will affect them. In particular they've expressed a desire to understand how the new regulation will affect their fleet operations, what it means for their day to day business activities and how the use of telematics fits in.

First of all, despite some of the prophecies of doom that have been circulating, GDPR is an evolution in data protection and, for those organisations that were compliant under the Data Protection Act, it is really an extension of current best practice.

But that isn't to say that GDPR doesn't incorporate any substantive changes or that no action is necessary. GDPR extends the scope of data protection and brings with it some significant changes to the way in which data is defined and how organisations need to manage personal data in particular. Fleet operators do need to be aware that the data they hold, including that derived from the use of telematics, will almost certainly fall under the remit of GDPR and that they have new obligations in how they treat and manage data.

This viewpoint has been compiled in response to these requests and is designed to help Masternaut's customers make sense of GDPR, putting the changes into context and highlighting the differences that are of particular relevance to fleet operators.

I hope you will find it useful.
Djamel Souici - General Counsel, Masternaut

About the author

Djamel Souici is Group General Counsel and as the chief legal officer for Masternaut, he is responsible for all legal affairs for the company. In his role he has established a pan-European legal team and set up a network of advisory law firms to support Masternaut's business across Europe.

Djamel provides expert guidance in the areas of corporate governance, compliance, employment law, litigation, intellectual property and commercial transactions (M&A) as well as privacy and data protection.

Educated in law at Ruhr University Bochum in Germany, Djamel was admitted to the Bar Association before progressing to a career in commercial law. Prior to joining Masternaut, Djamel worked for major tech companies like Novell corporation and looks back at more than 25 years of experience in IT.

Content

5 | Data processor and data controller

5 | Scope

6 | Personal data

7 | Lawful basis for processing

7 | Consent

8 | Data protection by design and by default

8 | Records of processing activities

9 | Data protection officers

10 | Data transfers outside of the eu

11 | Fines

12 | Masternaut and GDPR

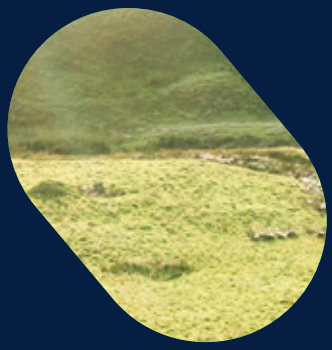
12 | ISO27001 certification

12 | Data centres

13 | Privacy by design

13 | Access to data and data portability

13 | Data protection impact assessment (DPIA)



Overview

On 25 May 2018, the **General Data Protection Regulation (GDPR)** came into force. Designed to harmonise data privacy laws across Europe, to protect the personal data of citizens of member states of the European Union (EU) and to bring data protection up to date with the digital age, the new rules are an evolution in data protection law rather than a revolution, but there are some significant changes in thinking and practice that will affect fleet operators and Masternaut customers.

Data processor and data controller

To begin with, GDPR does not change the definitions of the terms "data controller" and "data processor" and it's worth stating them again here:

- A data **controller** remains defined as the organisation "which, alone or jointly with others, determines the purposes and means of the processing of personal data". Masternaut customers would fall into this category.
- A data **processor** is the organisation that processes personal data on behalf of the controller. This definition covers cloud-based service providers such as Masternaut.

For Masternaut customers it's important to understand that, from a data protection perspective, Masternaut does not set the purpose of why personal data is being processed.

The legitimate purpose for processing personal data is solely defined by our customers, which makes the customer the data controller.

So, for the sake of clarity and in accordance with the above, Masternaut will typically act as the data processor for its customers and the customer will be seen as the data controller.

Scope

In essence, GDPR applies if the data controller or processor or the data subject (the live person) is based in the EU.

Furthermore the regulation also applies to organisations based outside the EU if they collect or process personal data relating to EU residents.

As part of the harmonisation process, a single set of rules now applies to all EU member states for data protection and an organisation with multiple establishments across Europe is only responsible for compliance with respect to the enforcing data protection authority of the organisation's main establishment.

This is a change from the former situation, where under EC/95/46 each country has its own data protection authority (the Information Commissioner's Office in the UK) and local laws apply. An organisation that operated across multiple jurisdictions was responsible to the data protection authorities in each country where it carried out business and local data protection laws applied.

GDPR is simplifying this by allowing multi-national organisations to be responsible to one data protection authority. This is possible because GDPR is not an EU directive but a regulation (see Regulation (EU)2016/679). Directives have to be transferred as law into local law (e.g. EC/95/46 is enacted in the UK under the Data Protection Act 1998) whereas a regulation becomes immediately active as binding law for all EU member states.

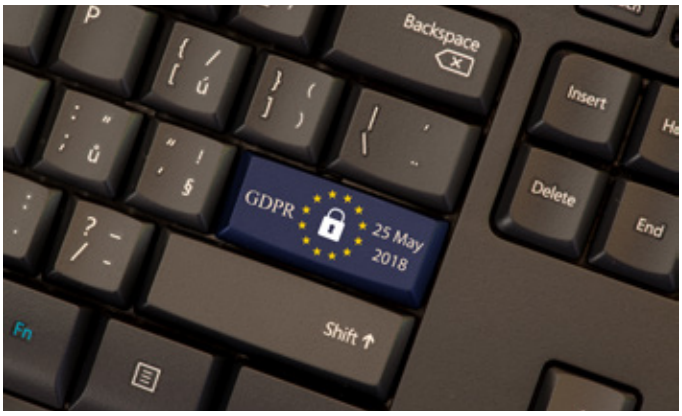
It's worth noting that in the context of **Brexit**, GDPR will remain in force in the UK even after the UK has left the EU.

Personal data

Fleet managers need to be concerned about GDPR because, as a general rule, they manage or have access to driver information that clearly falls under the umbrella of 'personal data' and thus within the scope of the regulation.

'Personal data' means data that relates to an identified or identifiable natural person (the "data subject"). For fleet managers, this will typically be the drivers.

An identifiable data subject is someone who can be identified, either directly from the data itself or indirectly by reference to an identifier like a name, an ID number, location data, a digital identifier or to one or more factors specific to the identity of that natural person.

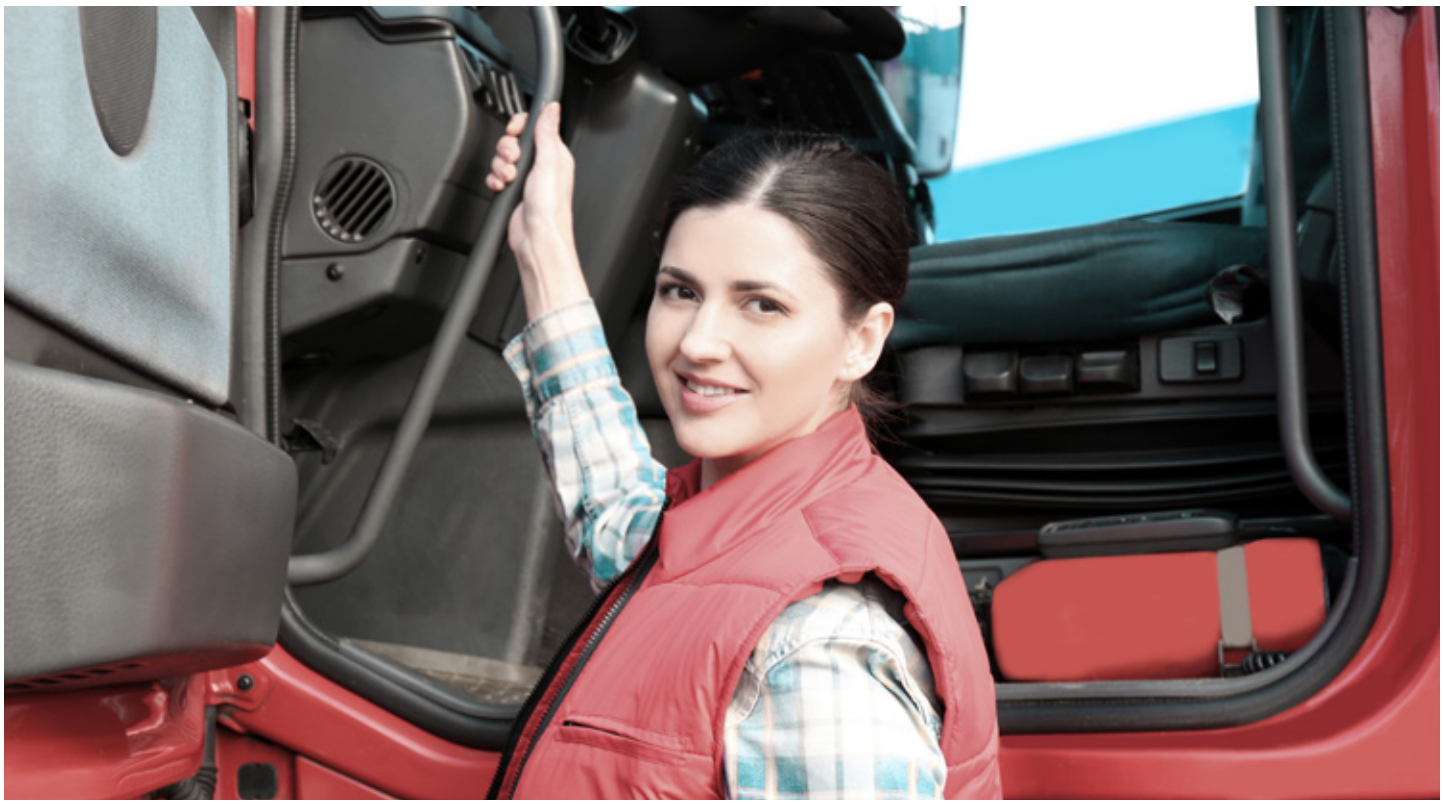


This is an important change from previous definitions and is a broad interpretation that can encompass data like the IP address of a driver's personal device, their device ID, their phone number or even a vehicle number plate. This would include data derived from a telematics system that includes identifiers that can be linked to the driver of a telematics-enabled vehicle.

GDPR requires that personal data be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes
- Adequate, relevant, and limited to what is necessary for achieving those purposes
- Accurate and kept up to date
- Stored no longer than necessary to achieve the purposes for which it was collected
- Properly secured against accidental loss, destruction or damage.

Further, GDPR places additional obligations on organisations to document their processing activities and to be able to demonstrate their compliance with the above mentioned principles.



Lawful basis for processing

Having established that personal data is being managed, there is also a need to ensure that there is a lawful basis for processing this data (which needs to be documented).

This is more important under GDPR because the basis for processing has an effect on an individual's rights. For example, processing personal data based on consent generally confers stronger rights to the individual concerned, such as the right to have their data erased.

There are, however, a number of other options available and, other than by consent, processing is lawful if it is:

- necessary for the performance of a contract with the data subject
- to comply with a legal obligation or to protect the vital interests of a data subject
- for the performance of a task carried out in the public interest
- in the exercise of official authority
- for the **legitimate interests** pursued by the controller

Most fleet operators will probably avoid gaining driver consent and instead utilise legitimate interest or the performance of a contract as the basis for processing.

Consent

Driver consent is **not** required if, for example, data is being used for payroll purposes.

If an employee is paid for driving time and telematics data is used to record these times, then **processing is covered by the contract** of employment. Such use falls under the exception of processing for the performance of a contract and driver consent is not required.

Where relying on legitimate interests, operators must ensure that the balance between the interests of the operator and the rights of drivers are considered and properly documented. Operators must also ensure that drivers would reasonably expect their data to be processed on the basis of the legitimate interests of the operator, which could include fraud prevention, security and safety, amongst others.

In the absence of a contractual or legitimate interest basis, operators may need to seek driver consent, but if this basis for processing is used, the consent has to be specific, unambiguous and freely given.

There should be clarity of purpose so that drivers know from the outset what information is being captured, why it is being collected and what will happen to it, including details of who it will be shared with. The reasons should be straightforward, e.g. " to measure, manage and reduce fuel use and CO2 emissions" would be perfectly legitimate. However, measuring speeding events is likely not a permitted purpose.

Such consent should be documented and ideally incorporated into employment, supplier and driver contracts, as well as procurement T&Cs. Building consent into these procedures should reduce the risk of future conflicts.

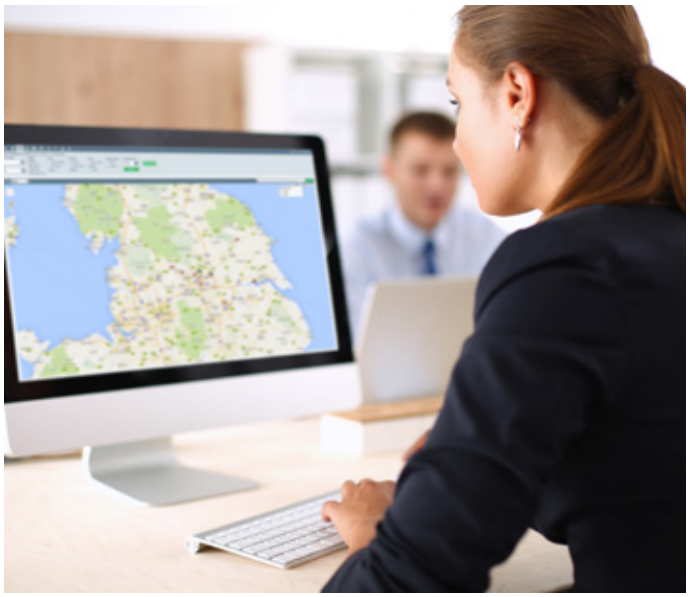
Data protection by design and by default

Under GDPR, operators will also have a general obligation to implement technical and organisational measures to show that data protection has been integrated into business as well as data processing activities.

These are measures which should meet the principles of 'data protection by design and by default'.

In essence this means that data protection measures are designed into the development of business processes in such a way so as to ensure that processing of personal data is limited to that which is necessary for the purpose for which the data was collected. And that only those within an organisation who need to access the personal data can do so.

It also includes an obligation to design processes so that measures which enhance privacy, such as the pseudonymisation of personal data, are initiated by the controller as soon as possible.



Records of processing activities

Under GDPR, fleet operators will have an obligation to provide comprehensive, clear and transparent privacy policies and, if your organisation has 250 or more employees, there's also a need to maintain internal records of processing activities.

Such records need to contain the following information:

- The name and contact details of the **data controller** and of any data protection officer
- The **purpose** of the processing
- A description of the **categories of data subjects** involved and of and the categories of personal data
- The recipient(s) of any personal data
- Whether personal data is **transferred** to third countries or international organisations
- The data **retention** times of the different categories of data
- Where possible, a general description of the technical and organisational **security mechanisms** in place to protect and secure personal data

Records must be in writing (but can be saved in electronic form) and are to be made available to the appropriate data protection authority (the Information Commissioner's Office) on request.

Data protection officers

Under the GDPR, a data protection officer (DPO) must be appointed by an organisation if the following circumstances apply:

- The organisation is a public authority (except for courts acting in their judicial capacity)
- Large scale systematic monitoring of individuals (for example, online behaviour tracking or tracking of driver behaviour across large fleets) is to be carried out
- Large scale processing of special categories of data

The role of the DPO is to:

- Inform and advise the organisation and its employees about their obligations to comply with GDPR and other data protection laws
- Monitor compliance with GDPR and other data protection laws, including managing internal data protection activities, advising on DPIAs, training staff and conducting internal audits
- Be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc)
- Report, where appropriate, data breaches to the Supervisory Authorities

If an organisation appoints a DPO, then the individual in post should:

- Report to the highest management level of the organisation – i.e. board level
- Operate independently and not be dismissed or penalised for performing their task
- Have access to adequate resources to meet their GDPR obligations.

An existing employee can be allocated the role of DPO so long as their existing duties are compatible with the duties of the DPO and do not lead to a conflict of interest. Alternatively the role can be outsourced.

Either way, although GDPR does not specify the precise credentials a data protection officer is expected to have, it does require that they should have professional experience and knowledge of data protection law. This should be proportionate to the type of processing the organisation carries out, taking into consideration the level of protection the personal data requires.

Data transfers outside of the EU

Most fleet operators contract their fleet telematics with third party organisations who then process that telematics data as a data processor on the operator's behalf. That does not absolve the operator from the responsibility to ensure that such processing is carried out lawfully.

The transfer of data across national boundaries for processing is an important case in point.

Whilst personal data pertaining to EU citizens can be processed anywhere in the EU, **GDPR sets restrictions for such processing in countries outside the EU**. These restrictions are similar to those in place under EC/95/46 but with a more complex framework of rules and exceptions.

Fleet operators need to ensure that their data is being processed in a lawful way. In the event that fleet telematics data (which is likely to be considered as personal data) is not processed within the EU, operators must ensure that the conditions laid out in GDPR that permit for the transfer of personal data out of the EU for processing are being met.

Failure of the operator, as the data controller, to ensure compliance with the rules for such transfers could leave the operator open to enforcement action and, in the event that the breach is not remedied in line with the authorities requirements, could face hefty fines.

Operators must ensure that the conditions laid out in GDPR that permit for the transfer of personal data out of the EU for processing are being met.

As a general rule, transfers of personal data to third countries (non-EU countries) or international organisations may only lawfully take place if the data controller and the data processor have fully complied with the provisions of GDPR.

Any transfer of personal data governed by EC95/46 remains valid under GDPR unless changed by the EU Commission. This means that **whitelisted** countries, which provide the same level of safeguards for personal data as the EU, remain territories in which personal data can be transferred and be processed without the consent of a data subject or of the data protection authority.

Switzerland is an example of such a whitelisted country. However, **the USA is not whitelisted**.

Data transfers outside of the EU

The status quo of a whitelisted country is subject to ongoing monitoring by the EU Commission and may change if developments in such countries indicate that the level of protection of personal data has materially altered and no longer meets the required standard.

If personal data is to be processed in non whitelisted countries, GDPR requires that appropriate safeguards are established, such as the inclusion of standard data protection clauses adopted by the EU Commission or by the data protection authorities and approved by the Commission.

The EU has yet not published approved standard data protection clauses under GDPR but provides that the model articles for data processing under EC/95/46 remain valid unless amended, replaced or repealed.

This is highly relevant for data transfers into third countries and in particular the USA, as it means that for the time being (and provided that the model articles were executed between the parties for data processing) there is a legal basis for the transfer of data when GDPR comes into force.

Fleet operators are thus well advised to continuously check the validity of their data processing agreements. If a data processing agreement becomes invalid, the fleet operator may expose himself to enforcement action and the possibility of hefty fines.

Consent of the data subject is still an appropriate basis for legal data processing outside of the EU. However, GDPR makes it clear that the data subject must 'explicitly' consent to the transfer of their personal data after having been informed of the possible risks of such a transfer.

In summary, data transfers into third countries or international organisations become more regulated under GDPR. If a fleet operator wants to avoid any risks of fines or liability or avoid complex contracts it should be confirmed by its telematics provider that its telematics data is only processed in the EU.

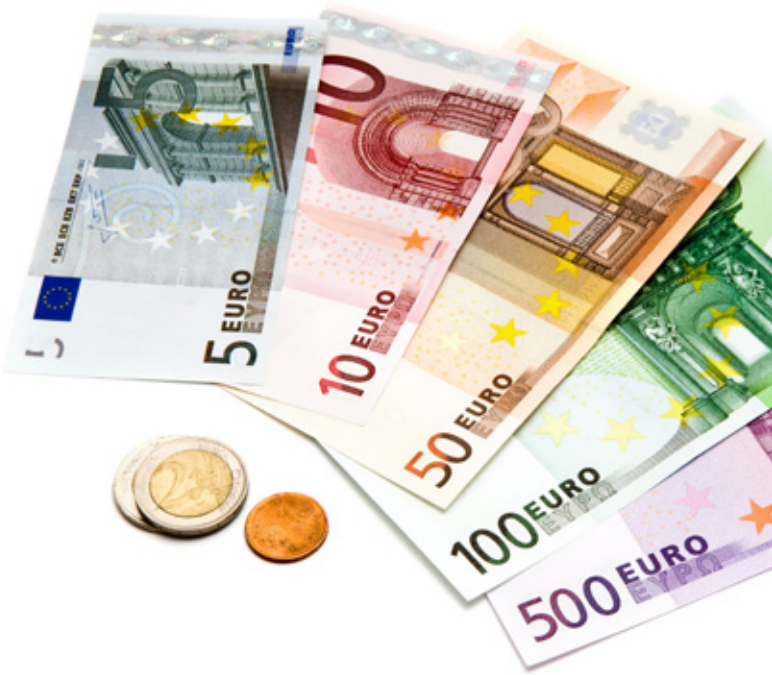
Fines

Local data protection laws have often been perceived as paper tigers, if for no other reason that a breach of the law had no painful consequences for a data controller or processor.

This has changed drastically with GDPR.

For serious breaches the data protection authorities can impose **fines of up to 20 million EURO or 4% of the worldwide annual turnover** of a company.

Likewise, fines are likely to be substantial for significant breaches of the principles for processing personal data, including consent of the data subject and for illegal transfers of personal data into third countries.



Masternaut and GDPR

Ensuring the safety and security of our customers data is a top priority for us and over recent years we've made significant investments into data protection and security. Accordingly, there were relatively few additional measures needed to meet the requirements of GDPR and we have taken all necessary steps to ensure compliance.

For a long time we have treated any data collected and processed on behalf of our customers as personal data. Likewise, we have developed organisational processes and security measures that match or exceed the requirements of the Data Protection Act 1998 and EU directive EC/95/46.

In addition to this, we have taken the following additional steps to ensure the security and safety of all our customer's data and to ensure that these meet or exceed the requirements of GDPR.

ISO27001 certification

Masternaut is formally certified to ISO 27001:2017.

ISO 27001 (also known as ISO/IEC 27001:2005) is a standardised specification for an Information Security Management System (ISMS), which is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organisation's information risk management processes.

According to GDPR, personal data is critical information that all organisations need to protect. Having certification to ISO 27001 provides our customers with confidence that we are protecting their personal data.

Of course, there are some EU GDPR requirements that are not directly covered in ISO 27001, such as supporting the rights of personal data subjects: the right to be informed, the right to have their data deleted, and data portability. But, as the implementation of ISO 27001 identifies personal data as an information security asset, most of the EU GDPR requirements will be covered.

THE BRITISH ASSESSMENT BUREAU
ISO27001

Certification No. 214521

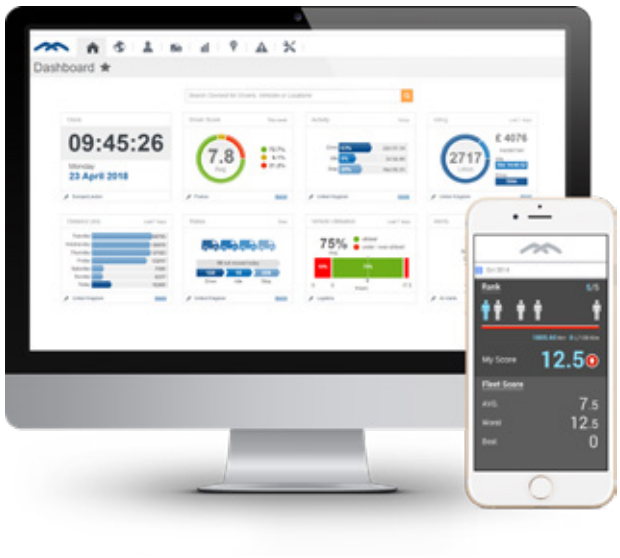
Data centres

Customer telematics data is currently processed exclusively in Masternaut's own enterprise-class data centres in France and/or the UK. No personal data is either passed to any third party cloud provider or hosted in a co-located data centre. Our data centres are secured by a full, independently tested cyber security suite, whilst physical and biometric access controls ensure that only vetted employees who have a need to work there have access.

Privacy by design

Masternaut's leading telematics platform **Masternaut Connect** implements privacy by design.

The role-based access model implemented in Connect allows administrators to set access rights and to define roles for each user, ensuring that each user only gets to see what he needs to know.



Access to data and data portability

Masternaut has structures and processes in place to process data subject information requests in response to and in co-operation with the data controller. All personal data on the Masternaut Connect platform is portable. Once the necessary authorisation process has been completed, the data can be downloaded by the customer and used for any covered purpose.

Telematics data is only processed in Masternaut's data centres either in the UK or in France. It has established logical and physical access prevention means to ensure that only employees who need to know have access to customer data.

There are appointed **Data Protection Officers** for Masternaut sites with data centres.

Data protection impact assessment (DPIA)

A general risk assessment for all information assets managed by Masternaut was carried out as part of our ISO 27001 certification process.

Under Article 35, GDPR, a DPIA is required for data controllers who process personal data using new technology, which might result in a high risk to the rights and freedoms of natural persons.

Given that Masternaut is the data processor and that none of the data collected by us or stored on the Masternaut Connect platform meets with the above criteria, there's no requirement for us to carry a DPIA. That duty rests with our customers as the data controllers. But so long as the customer does not use the data in ways which will fall under the Article 35, there is no need to undertake a DPIA.

Masternaut is confident that it is processing its customer data in a fully GDPR compliant manner.

Summary

Whilst the requirements for compliance with GDPR may seem overwhelming, much of what it contains is an extension of the current legislation and many customers may have not needed to make significant changes to ensure compliance.

However, compliance with GDPR is not optional and there are levels of complexity that aren't necessarily apparent. Fleet operators are thus well advised, in light of the revised regime regarding penalties and fines under GDPR, to take all necessary steps to comply with the new law in order to manage risks and reduce liability.

It's an obvious recommendation, but early consultation with your organisation's legal counsel is the best step, especially as they may be unfamiliar with the quantity and content of the data that fleet managers are now managing.

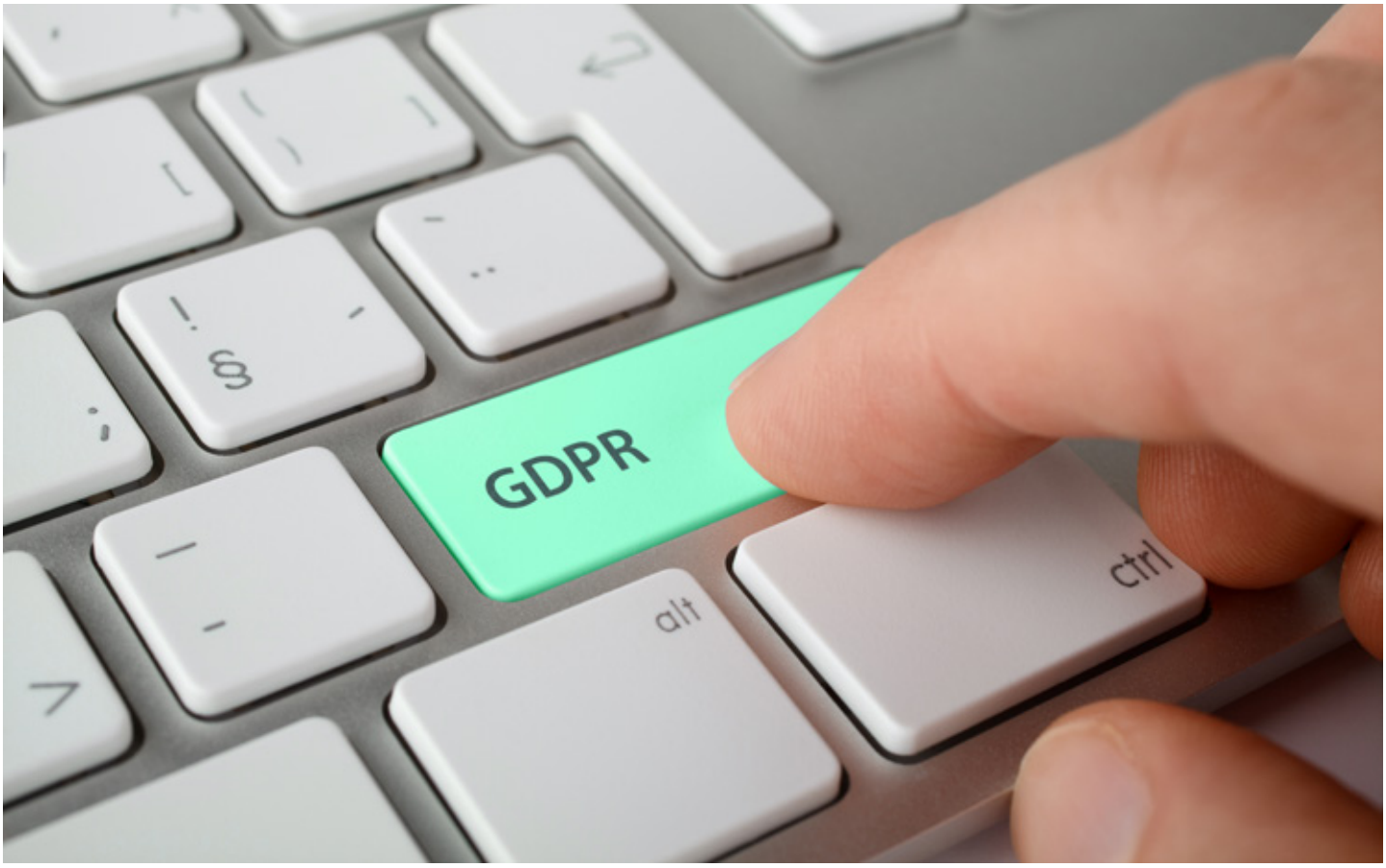
Alternatively, the Information Commissioner's Office provides excellent guidance on the implications of the GDPR as well as all other aspects of data protection. See https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

Perhaps the best advice is to take action now to ensure that you meet the requirements of this new legislation.

Disclaimer

The information contained in this viewpoint is Masternaut's interpretation of GDPR requirements as of the date of publication. Please note that not all interpretations or requirements of the GDPR are well settled and its application is both fact and context specific. The information contained in this document should not be relied upon as legal advice or to determine how GDPR applies to your business or organisation.

We encourage you to seek guidance from your legal counsel with regard to how GDPR applies specifically to your business or organisation and how to ensure compliance. This information is provided "as-is" and may be updated or changed without notice. The contents of this document may be referenced or copied and used for internal, reference purposes only.



masternaut

ABOUT MASTERNAUT

At Masternaut, we believe every business is sitting on unrealised potential. Your vehicles create oceans of data every day. Hidden in that data are insights that have the power to transform your fleet – and possibly even your business. We specialise in revealing these transformative insights so you can turn them to your advantage. From telematics devices to expert analysis, every one of our tools helps your business unlock potential.

Learn more about us at
www.masternaut.com

masternaut