bynx
fleet software without boundaries

Fleet Intelligence

GDPR – setting the benchmark for a global standard for data protection

Mark Binks
Group Managing Director

New data protection rules came into force on the 25th May 2018. GDPR (General Data Protection Regulation) has received a lot of publicity over the past year but do you fully understand what it means to be "GDPR-ready" and are you ready? It's not too late, we've published this white paper to help you.

Even if local legislation does not require fleet and leasing providers to comply with GDPR, they must if they want to attract international or multinational customers in their local market.

What does GDPR involve?

While businesses will recognize many of the principles enshrined in GDPR, the regulation includes new measures and enhancements that will affect systems and processes across all business units. GDPR gives individuals enhanced rights regarding the processing of their personal data and imposes corresponding obligations on organizations that collect such data. Individuals will have the right to have their data deleted or transferred to alternative service providers, and will be able to sue for material and/or non-material damage arising from data breaches. They will also be able to participate in group litigation.

Among the changes that have come into force are:

- the introduction of data protection impact assessments
- mandatory appointment of data protection officers for certain organizations
- more stringent rules for obtaining consent to collect and use personal data
- tighter rules for data controllers and data processors
- changes to data breach disclosure requirements
- the introduction of substantial fines for failure to comply with the GDPR

For asset finance and vehicle fleet businesses, data is held in a variety of management systems: *finance, human resources, sales, marketing, operations and so on.*

Today's vehicle has become a data collection device in its own right - and some of that data could identify individuals. The proliferation of online business also means identifying details, such as names, addresses, phone numbers, biometric particulars and other attributes are being collected, stored and processed more than ever before. Then, there are the copious notes people write into the system – who knows where or what they are or who made them?

That data needs to be cleansed, secured and managed responsibly, which is what GDPR is all about. The consequences of failing to do so, or of suffering data breaches, include prosecution, fines, embarrassment, financial losses and damaged reputations.

How to be GDPR prepared

14 steps in readiness for GDPR:

1) *Awareness* – ensure decision-makers and key personnel within your organization are aware of the new laws and the impact they might have.

2) *Appoint* from within your organisation a suitably experienced data protection officer. This could be anyone, however, marketing, sales or legal personnel are usually most appropriate.

3) *Audit* - document the personal data you hold within your organization (and outside if you share it with third parties) and where it came from. An information audit is recommended for large organizations.

4) *Cleanse* - initiate a data cleanse. Delete old data or at the very least archive it securely (remember, you may be required to keep some driver details for legal reasons).

5) *Communicate* - review your current privacy notices against what is required within the new laws and make any necessary changes.

6) *Individual rights* – check procedures to ensure they cover all the rights individuals have under the new laws. This should include how you will delete personal data when necessary or when asked to do so.

7) *Employment Contracts* – review employment contracts and if you have to keep personal data for legal reasons (such as with drivers), make sure you detail this in any Contract of Employment.

8) *Access requests* – review how you will handle access requests from individuals. The rights of individuals in terms of accessing their data are being strengthened. You will need to update your procedures to meet the new timescales and you will not be able to charge for such requests in the same way you could before GDPR.

9) *Legality* – fully understand your legal basis for processing personal data. Why are you doing it? Look at the various types of data you process and why you process it. This is your legal basis for processing it. You must document this information as part of the new regulations.

10) *Consent* – review how you are seeking, obtaining and recording consent and where you need to make any changes to be compliant under GDPR.

11) *Children* – it is the responsibility of every business or organization that processes personal data to verify people's ages and gather consent from parents or guardians if they are minors. In some countries, young people can apply for provisional driving licences (as young as 15), so there could be implications. You need to at least take steps to verify a driver's age.

12) *Data breaches* – ensure you have the correct procedures in place to detect, report and investigate personal data breaches.

13) *DPIA (data protection impact assessment)* – familiarize yourself with this, alongside how and when to implement it in your organization. In the UK, further information can be found on Information Commissioner's Offices websites.

14) *International* – determine which data protection supervisory authority you come under if you operate internationally and be sure to follow their guidance.

Personal Information Management policy (PIM)

You may be surprised at the scope within which personal data permeates your business. Having a personal information management policy in place will be critical to the success of your compliance. It acts as a framework for your PIMS (Personal Information Management System) and demonstrates your commitment to compliance with data protection requirements and good data protection practice overall.

Here's what should be included in your policy:

- It should be appropriate to the purpose of the organization and provide a framework for setting PIMS objectives.
- It should encompass the whole organization.
- It should outline your commitment to satisfying any requirements applicable to your organization.
- It should include details on how you commit to continuous improvement of your PIMS.
- It should be available in documented format and communicated within the organization.

Good practice for processing information includes:

- Processing personal information only where necessary, for legal, regulatory or legitimate organizational purposes (including marketing).
- Processing only the minimum personal information required for these purposes.
- Providing clear information to persons about how their personal information can be used and by whom.
- Processing personal information fairly and lawfully.
- Maintaining a documented inventory of the categories of personal information processes by the organization.
- Keeping personal information accurate and up-to-date.
- Retaining personal information only for as long as is necessary and ensuring its timely and appropriate disposal.
- Respecting people's rights in relationship to their personal information.
- Keeping all personal information secure.
- Only transferring personal information outside of the country of origin where it can be adequately protected.
- Developing and implementing a PIMS to enable the policy to be implemented.
- Where appropriate, identifying internal and external interested parties and the degree to which they are involved in the governance of the organization's PIMS.
- Maintaining records of the processing of personal information.

PIMS (Personal Information Management System)

Every organization should implement a PIMS to support the Polity and new GDPR rules. Once established and implemented, the system should also be maintained and continually improved. This system addresses the management of personal information that might be held across a wide range of operational units and IT-based applications.

Data inventory and data flow

It's a good idea to establish a data inventory and map the flow of data throughout the organization so it's possible to know where weaknesses may lie. You need to be aware of all the **business processes that utilize personal information**, the **sources of that data** and the **categories of personal information processed**, plus the **purposes for which it can be used.** You also need to be aware of the existence of any high-risk personal information (such as a person's bank details, health or criminal records, for example).

Understand the systems and repositories of personal information, and (where applicable for international organizations) where data is transferred over international boundaries or subject to different laws, regulations, standards or frameworks.

Data Collection and Processing

The new rules are strict on how data is collected, processed and distributed around an organization, particularly across international borders. It strongly respects the rights of individuals to have authority about who collects and uses their data and how. Businesses are being mandated to provide information to individuals whose data they are collecting (or have collected), which clearly communicates **who the business is, the purpose** for which data is being collected and processed, **the types of personal information being collected, who it will be used by** and **whether it will be shared with third-parties.** It should also state where the data came from (if it was collected from a source other than the individual). If the information is being used for marketing purposes, the PIMS needs to support a process by which the individual can object, and this needs to be clearly explained. The right to object must be supported alongside the mechanism by which a person can object. Consent records must be kept, correct and up-to-date.

Planning and Control

The new rules stipulate that an organization must plan, implement and control the processes needed to meet the new requirements. This includes establishing criteria for the processes, implementing control of the processes, keeping documented information. Planned and unplanned changes must also be controlled. An organization must review the consequences of unintended changes and actively mitigate adverse effects. Control includes outsourced processes – the process may be outsourced but the business is still responsible for the data.

Securing systems and data

The GDPR data security requirements are broadly classified in to three categories:

assessment
prevention
monitoring/detection

Assessment

The first task is a security risk assessment, including a data protection impact assessment. These assessments should include a systematic evaluation of the organization's processes and their impact on the protection of personal data.

How we tested the security of **Bynx**

As part of our commitment to software quality and platform security, we recently subjected our software source code to penetration testing.

Bynx currently manages over 1 million vehicles globally and it undergoes continuous refinement so it's imperative it's well-structured, architected and contains high-standard elements. The test also looked to identify labelling discrepancies and potential licensing issues associated with open source programming.

We place a lot of emphasis on programming quality and risk remediation and stringent coding practices, quality control and testing regimes are part of our DNA.

The test concluded that **Bynx** is highly maintainable (thus low maintenance costs), robust, easy to configure, structured, agile and secure.

It also uncovered minor hidden security issues and open source vulnerabilities, which we have now fully addressed in preparation for supporting our clients through GDPR and beyond.

Because we've adopted the highest level of data security, globally and locally we deliver our customers and their clients the best level of comfort.

Prevention

The adage "prevention is better than cure" truly applies here. The GDPR emphasizes the importance of preventing security breaches and recommends several techniques, including encryption, anonymization and pseudonymization.

Anonymization is the technique of scrambling data and pseudonymization refers to the practice of reducing the 'linkability' of a data set from the original identity of the data subject. In other words, even if it did escape somehow the data set would be meaningless. These two initiatives reduce the risk of accidental or intentional data disclosure by making the information unidentifiable.

Access control should be limited to privileged users only and even they should be restricted to accessing and using personal data selectively and for defined purposes. This is referred to as fine-grained access control and can help limit unauthorized access to personal data. Minimizing the collection and retention of personal data will help reduce the burden of compliance.

By using Bynx, you'll be compliant

We have introduced new functionality that blocks and anonymizes personal identifiable information for drivers, customers, suppliers and prospects. It also enables the ability to define separate retention rules and associated processes for blocking and anonymizing this information.

Monitoring

Preventative security measures are one thing, but businesses must continually monitor to detect breaches. GDPR mandates recording and auditing all activities with respect to personal data and recommends records are maintained centrally under the responsibility of the data controller. Data processors and third parties must be prevented from tampering with or destroying these records. Auditing will also assist in the forensic analysis of a data breach. Timely notification, in the case of a data breach, is mandated under the new rules. An organization must notify the supervisory authority within 72 hours after having become aware of it. This is a major change from most current legislation.

It's important every fleet and leasing manager familiarizes him or herself with the new GDPR laws. The work involved now will pale into insignificance when compared with the amount of effort and financial resources required to correct a failure to comply - or prosecution should it come to that.

There are many sources of guidance, some are listed here:

UK Information Commissioner's Office – *https://ico.org.uk*
EU Information on GDPR – *http://bit.ly/1kidyy8*
Article 29 Working Party Development EU Guidelines – *http://bit.ly/2gs7BE2*
Data Protection Commissioner, Ireland – *http://bit.ly/2gxsWN8*

This article was originally published in Asset Finance International's Quarterly Pricing Review

If you'd like to talk to us about your fleet management business platform needs, please get in touch:

T: +44 (0) 1789 471600
W: www.bynx.com
E: sales@bynx.com

Follow us: *https://www.linkedin.com/company/bynx-europe-ltd*
https://twitter.com/BynxGlobal