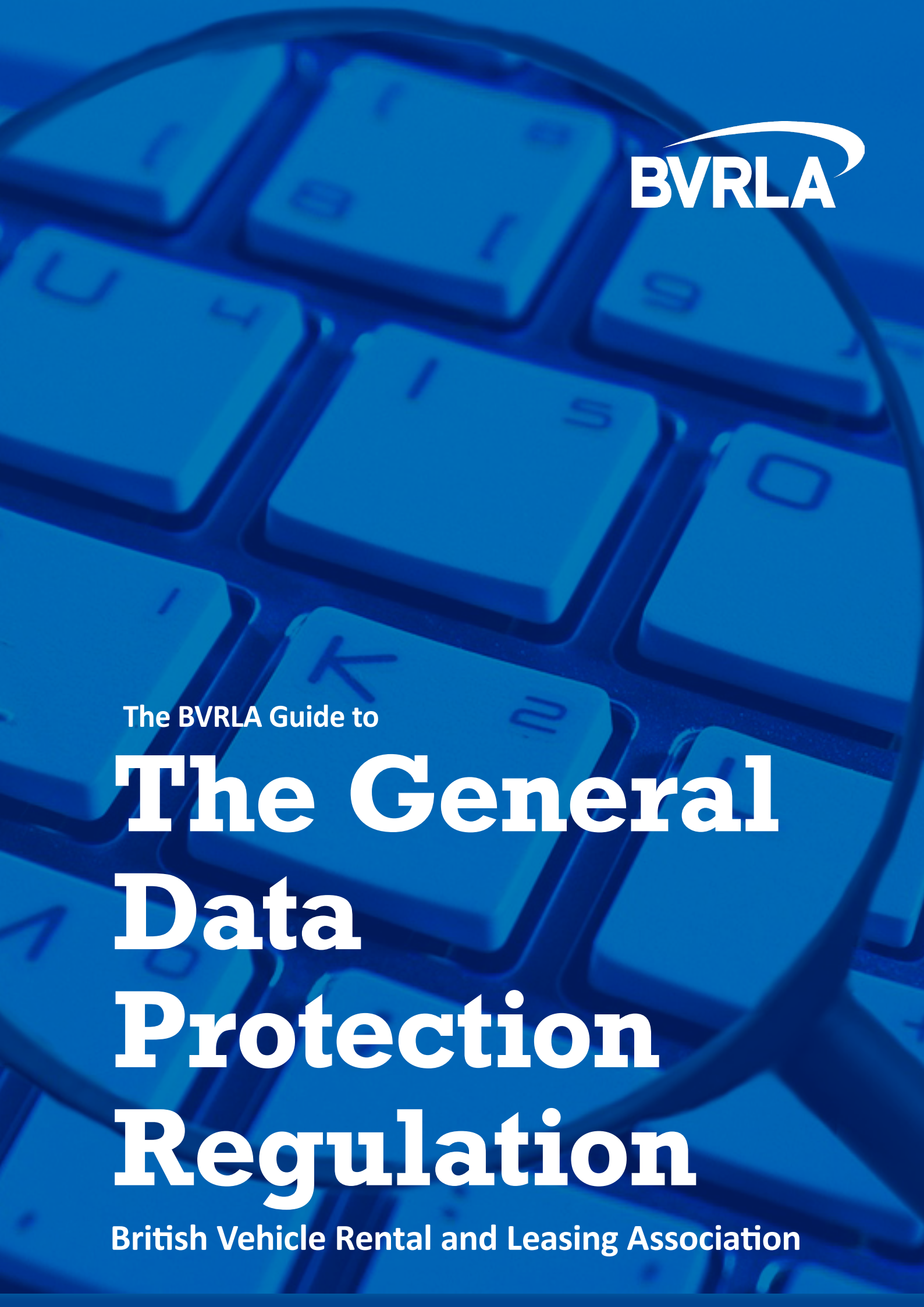


BVRLA

The BVRLA Guide to

The General Data Protection Regulation

British Vehicle Rental and Leasing Association

BVRLA Guide to the General Data Protection Regulation – March 2018

Table of Contents

Introduction

This guide highlights the key themes of the General Data Protection Regulation (GDPR) to help members understand the new legal framework. It explains the similarities with the existing UK Data Protection Act 1998 (DPA) and describes some of the new and different requirements. It is for those who have been tasked at looking at data protection within their business. It also includes practical advice for all BVRLA members.

The GDPR will apply in the UK from 25 May 2018. The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

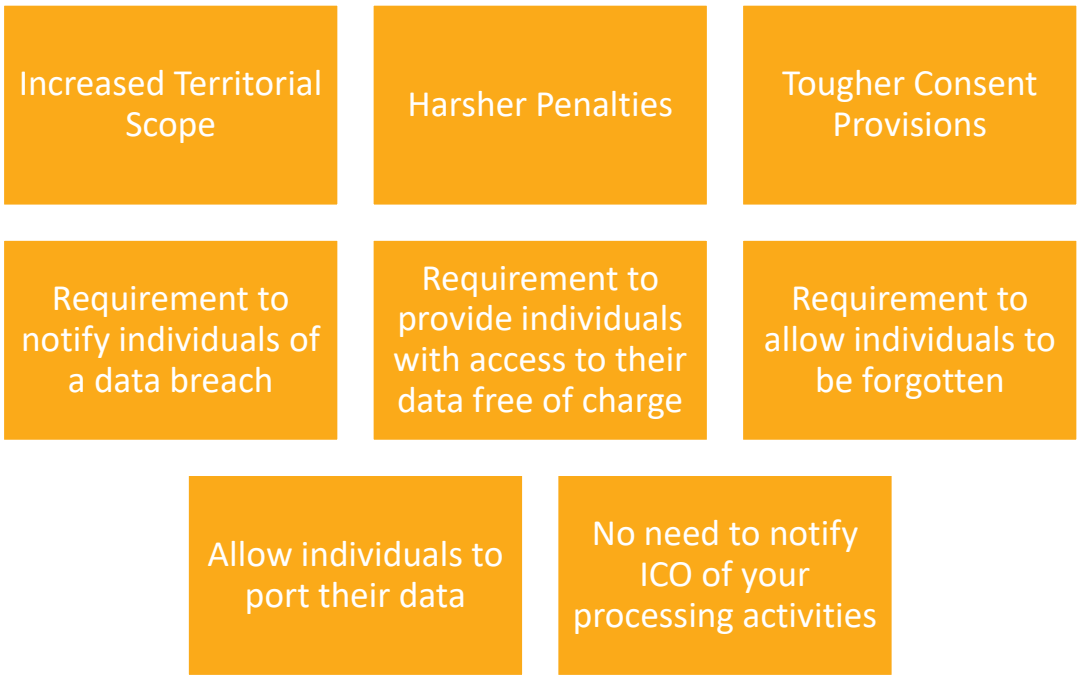
Acknowledgments

The BVRLA would like to thank Richard Humphreys at Blake Morgan for his contributions to the Guide. If members require tailored advice Richard can be contacted:

BLAKE MORGAN

DDI: 01865 254243 ■ M: 07702 217921 ■ F: 0844 620 3403 ■ E: Richard.Humphreys@blakemorgan.co.uk
6 New Street Square, London, EC4A 3DJ ■ T: +44 (0) 20 7405 2000 ■ DX 445 LDE ■ www.blakemorgan.co.uk

Overview of the key changes introduced by GDPR



The Changes in Detail

Who does the GDPR apply to?

The GDPR applies to 'controllers' and 'processors'. The definitions are broadly the same as under the DPA – ie the controller says how and why personal data is processed and the processor acts on the

controller's behalf. If you are currently subject to the DPA, it is likely that you will also be subject to the GDPR.

If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have significantly more legal liability if you are responsible for a breach. These obligations for processors are a new requirement under the GDPR.

However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR.

There is still be an exemption from the regulation for processing personal data for the prevention or detection of crime. This is important for members who may be approached by the Police to release data regarding who has rented or leased a vehicle or data from a tachograph, tracking or telematics device. Provided you are satisfied the request is genuine then the data can be released. This was previously known as a section 29 request under the Data Protection Act. Under the Data Protection Bill, currently going through Parliament the exemption is in Schedule 2, section 2 and states:

"Crime and taxation: general

2(1)The listed GDPR provisions do not apply to personal data processed for any of the following purposes—

(a)the prevention or detection of crime,

(b)the apprehension or prosecution of offenders, or

(c)the assessment or collection of a tax or duty or an imposition of a similar nature,"

Personal data

Like the DPA, the GDPR applies to 'personal data'. However, the GDPR's definition is more detailed and makes it clear that information such as an online identifier – eg an IP address – can be personal data. The more expansive definition provides for a wide range of personal identifiers to constitute personal data, reflecting changes in technology and the way organisations collect information about people.

For most organisations, keeping HR records, customer lists, or contact details etc, the change to the definition should make little practical difference. You can assume that if you hold information that falls within the scope of the DPA, it will also fall within the scope of the GDPR.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This is wider than the DPA's definition and could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – eg taking identifying fields within a database and replacing them with artificial identifiers, or pseudonyms. – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Special category data

Special category data is personal data which the GDPR says is more sensitive, and so needs more protection, this is similar to sensitive personal data. It includes: processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

In the main it is unlikely that members will be processing special category data, however, if leasing companies or brokers are advised of an issue regarding someone's health during a lease agreement, e.g. a customer is unable to pay due to ill health the recording of this information means you are processing special category data. More information is available here if needed.

Processing conditions

Lawfulness of processing conditions	Practical Example
6(1)(a) – Consent of the data subject	It would also apply where you are planning on marketing your services to a customer who is not necessarily in a contract with you.
6(1)(b) – Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract	This would apply to leasing brokers who have to forward customer's details to funders to enable performance of the contract. This would also apply to rental companies who have entered into a contract with a customer to provide them with a vehicle.
6(1)(c) – Processing is necessary for compliance with a legal obligation	This could apply when a rental company needs to identify the driver of a vehicle to the Police following notification of a speeding fine.
6(1)(d) – Processing is necessary to protect the vital interests of a data subject or another person	
6(1)(e) – Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller	
6(1)(f) – Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject	This could apply to customers who you are putting on the BVRLA's RISC database or where you are recording information with a credit reference agency.

Consent

Consent under the GDPR must be a freely given, specific, informed and unambiguous indication of the individual's wishes. There must be some form of clear affirmative action – or in other words, a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. Consent must also be separate from other terms and conditions, and you will need to provide simple ways

for people to withdraw consent. Public authorities and employers will need to take particular care to ensure that consent is freely given.

Consent has to be verifiable, and individuals generally have more rights where you rely on consent to process their data.

Remember that you can rely on other processing conditions (see above table) apart from consent – for example, where processing is necessary for the purposes of your organisation's or a third party's legitimate interests.

You are not required to automatically 'repaper' or refresh all existing DPA consents in preparation for the GDPR. But if you rely on individuals' consent to process their data, make sure it will meet the GDPR standard on being specific, granular, clear, prominent, opt-in, properly documented and easily withdrawn. If not, alter your consent mechanisms and seek fresh GDPR-compliant consent, or find an alternative to consent.

Consent must be specific and informed. You must as a minimum include:

- the name of your organisation and the names of any third parties who will rely on the consent – consent for categories of third-party organisations will not be specific enough;
- why you want the data (the purposes of the processing);
- what you will do with the data (the processing activities); and
- that people can withdraw their consent at any time. It is good practice to tell them how to withdraw consent.

Data protection breaches

The GDPR introduces a duty on all organisations to report certain types of data breach to the Information Commissioner's Office (ICO), and in some cases, to individuals. You only have to notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals, if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you will also have to notify those concerned directly in most cases.

You should put procedures in place to effectively detect, report and investigate a personal data breach. You may wish to assess the types of personal data you hold and document where you would be required to notify the ICO or affected individuals if a breach occurred. Larger organisations will need to develop policies and procedures for managing data breaches. Failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

For members this could include details such as bank details or credit card details being stolen by a rogue employee or system hackers or an employee steeling a customer database and selling the information.

Subject access requests

When an individual request that you provide them with the personal data you are holding there are a number of new requirements:

- in most cases you cannot charge someone to access their data (the current regulation allows a £10 charge to be made)
- You will have a month to comply (currently 40 days)
- You can refuse or charge for requests that are manifestly unfounded or excessive
- If you refuse a request, you must tell the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy. You must do this without undue delay and at the latest, within one month

Members may wish to review their current procedures on subject access request to ensure compliance with the above.

The BVRLA handles subject access request for the RISC database in line with these new requirements.

Privacy notices

Being transparent and providing accessible information to individuals about how you will use their personal data is a key element of the Data Protection Act 1998 (DPA) and the EU General Data Protection Regulation (GDPR). The most common way to provide this information is in a privacy notice.

Under the GDPR there are some additional things you will have to tell people. For example, you will need to explain your lawful basis for processing their data, your data retention periods and that individuals have a right to complain to the Information Commissioners Office (ICO) if they think there is a problem with the way you are handling their data. The GDPR requires the information to be provided in concise, easy to understand and clear language. Consider:

- What information is being collected?
- Who is collecting it?
- How is it collected?
- Why is it being collected?
- How will it be used?
- Who will it be shared with?
- What will be the effect of this on the individuals concerned?
- Is the intended use likely to cause individuals to object or complain?

You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

More information on privacy notices is available here.

Individual's rights (including right to be forgotten and data portability)

The GDPR includes the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability

- The right to object
- The right not to be subject to automated decision-making including profiling

You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data, or, provide data electronically and in a commonly used format

On the whole, the rights individuals will enjoy under the GDPR are the same as those under the DPA but with some significant enhancements. If you are geared up to give individuals their rights now, then the transition to the GDPR should be relatively easy. This is a good time to check your procedures and to work out how you would react if someone asks to have their personal data deleted, for example. Would your systems help you to locate and delete the data? Who will make the decisions about deletion?

The right to data portability is new. It only applies:

- To personal data an individual has provided to a controller;
- Where the processing is based on the individual's consent or for the performance of a contract; and
- When processing is carried out by automated means

You should consider whether you need to revise your procedures and make any changes. You will need to provide the personal data in a structured commonly used and machine readable form, you must respond without undue delay, and within one month and provide the information free of charge.

Members will need to consider how easy it is to extract data including potentially transaction data from their system to an individual.

Right to Erasure (Right to be forgotten)

The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

When does the right to erasure apply?

The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (ie otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

Under the GDPR, this right is not limited to processing that causes unwarranted and substantial damage or distress. However, if the processing does cause damage or distress, this is likely to make the case for erasure stronger.

Data protection officers

It is unlikely that members will need to formally designate a Data Protection Officer (DPO), one is needed if you are:

- A public authority (except for courts acting in their judicial capacity)
- An organisation that carries out the regular and systematic monitoring of individuals on a large scale
- An organisation that carries out the large-scale processing of special categories of data, such as health records, or information about criminal convictions

A DPO:

- Must be an expert in data protection law
- Cannot be a member of the Senior Leadership Team, Head of HR, Head of IT or anyone that has a say in the processing of data
- Reports to the highest level of management, or, the Board of Directors
- Can be an outsourced consultant

However, members may still wish to designate someone to take responsibility for data protection compliance. You will need to assess where this role will sit within your organisation's structure and governance arrangements.

It is most important that someone in your organisation, or an external data protection advisor, takes proper responsibility for your data protection compliance and has the knowledge, support and authority to carry out their role effectively. This is also important for members who are regulated by the Financial Conduct Authority (FCA) as the FCA requires governance and oversight of all aspects of the business, including data protection compliance. A DPO therefore provides a solution for this.

Data protection impact assessments

It has always been good practice to adopt a privacy by design approach and to carry out a Privacy Impact Assessment (PIA) as part of this. However, the GDPR makes privacy by design an express legal requirement, under the term 'data protection by design and by default'. It also makes PIAs, referred to as 'Data Protection Impact Assessments' or DPIAs, mandatory in certain circumstances. A DPIA is required in situations where data processing is likely to result in high risk to individuals, for example:

- Where a new technology is being deployed
- Where a profiling operation is likely to significantly affect individuals
- Where there is processing on a large scale[1] of the special categories of data

If a DPIA indicates that the data processing is high risk, and you cannot sufficiently address those risks, you will be required to consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR. You should therefore start to assess the situations where it will be necessary to conduct a DPIA. Who will do it? Who else needs to be involved? Will the process be

[1] There is no definition of large scale but the Article 29 Working Party advise you take into account:

a) the number of data subjects concerned, either as a specific number or as a proportion of the relevant population;
b) the volume of data and/or the range of different data items being processed;
c) the duration, or permanence, of the data processing activity;
d) the geographical extent of the processing activity

run centrally or locally? You should also familiarise yourself now with the guidance the ICO has produced on PIAs as well as guidance from the Article 29 Working Party and work out how to implement them in your organisation. This guidance shows how PIAs can link to other organisational processes such as risk management and project management.

As mentioned above those members who are FCA compliant may want to consider which of their procedures requires a data protection impact assessment from a governance and compliance perspective to ensure they are able to demonstrate

Penalties

The penalties under GDPR are significantly higher, there are two bands of fines depending on what part of GDPR is breached:

- Up to the higher of 2% of global annual turnover or 10 million Euro
- Up to the higher of 4% of global annual turnover or 20 million Euro
- Global annual turnover could be taken to mean turnover of the group

Registration

When the new data protection legislation comes into effect next year there will no longer be a requirement to notify the ICO annually. However, a provision in the Digital Economy Act means it will remain a legal requirement for data controllers to pay the ICO a data protection fee. These fees will be used to fund the ICO's data protection work. As now, any money the ICO receives in fines will be passed directly back to the Government. The new model will go live on 1 April 2018. The fees will range from £55 to £1000 depending on turnover and number of staff.

Industry Specific Advice

Penalty Charge Notices and Parking Charge Notices

Where a member receives a penalty charge notice, parking charge notice, or any other request for the driver details, for example, speeding, littering etc you will need to make sure your contract allows you to share details of the driver with the authorities or companies who issue the notice or penalty apart from where there is a statutory obligation to notify.

As part of your contract you could use the following wording:

"If we receive a notification from the Police, local authority or private parking company that a penalty, parking charge notice or any other offence has been committed whilst the vehicle was on hire/lease to you we will, where possible, provide your details to the authority/company issuing the penalty, notice or offence."

Emergency situations

When the Police are investigating serious or fatal road accidents there is no need to ensure consent has been received to release personal data.

There is a BVRLA, Association of Chief Police Officers and Association of Car Fleet Operators statement of best practice which covers the release of driver details in an emergency situation. The best practice stipulates that following a request for driver information, it should be possible to identity who is the driver of most company cars as quickly as possible and, in any event, within a

maximum suggested timescale of between 12-48 hours. To view the best practice statement in full click here.

CCTV or surveillance systems in branches, car parks or offices

Members who use CCTV or any kind of recording equipment on their sites may wish to review the following to ensure compliance:

Subject access requests – ensure that the design of your surveillance system allows you to easily locate and extract personal data in response to subject access requests. They should also be designed to allow for the redaction of third party data where this is deemed necessary.

Retention periods – there are no minimum or maximum retention periods which apply to all systems or footage. Rather, retention should reflect the organisation's purposes for recording information. The retention period should be informed by the purpose for which the information is collected and how long it is needed to achieve this purpose. It should not be kept for longer than is necessary and should be the shortest period necessary to serve your own purpose.

Advising of the existence of recording equipment – You must let people know when they are in an area where a surveillance system is in operation. The most effective way of doing this is by using prominently placed signs at the entrance to the surveillance system's zone and reinforcing this with further signs inside the area. Clear and prominent signs are particularly important where the surveillance systems are very discreet, or in locations where people might not expect to be under surveillance. As a general rule, signs should be more prominent and frequent in areas where people are less likely to expect that they will be monitored by a surveillance system.

If audio recording is being used, this should be stated explicitly and prominently. It should also be clearly stated if audio recording is used for a different or further purpose than visual recording.

Signs should:

- be clearly visible and readable;
- contain details of the organisation operating the system, the purpose for using the surveillance system and who to contact about the scheme (where these things are not obvious to those being monitored);
- include basic contact details such as a simple website address, telephone number or email contact; and be an appropriate size depending on context.

Signs do not need to say who is operating the system if this is obvious. If a surveillance system is installed within a rental branch, for example, it will be obvious that the branch is responsible, however if the equipment is at the entrance to a private car park where the vehicle is to be returned it may not be so obvious.

All staff should know what to do or who to contact if an individual makes an enquiry about the surveillance system.

More information is available here.

Retention of customer details including credit card information

Members who use 3rd party suppliers for their IT systems will want to ensure the supplier is GDPR compliance and that the systems are robust and secured. If there is a data breach with a 3rd party

supplier and your customer data is compromised the responsibility is yours. You will need to make sure your contracts indemnify you against this risk as well.

You also need to review how long you keep information such as customer details and their credit card information. Factors to consider with this include:

- Road traffic offences can be issued up to 6 months after the offence date
- Invoices and rental agreements have to be kept for 7 years for accounts and auditing purposes (this does not necessarily include the credit card details)
- 3rd party insurance claims can be issued up to 3 years after the accident

Key actions to take:

- ✓ Check how compliant your 3rd party suppliers are with GDPR, this could be done through a questionnaire or you may wish to be less formal and meet them
- ✓ Ensure your agreement with your 3rd party supplier includes protection for data protection breaches
- ✓ Review how long you keep customer data and make sure your system reflects any changes you wish to make in this area. It could be that there is an archive function which doesn't allow access to the data but it can be retrieved if necessary.
- ✓ Consider implementing a regular review process for any 3rd party suppliers who are holding your customer's data

Those members who are regulated by the Financial Conduct Authority will need to make sure they are compliant with the FCA's outsourcing rules as well in this area.

Marketing

Where you are marketing to individuals you need to carefully consider how you obtained the individual's contact details and are you relying on their consent to send the information or is it necessary for the performance of the contract. If you are relying on consent consider carefully how you record the consent. The below table looks at some common areas where both of these could be applicable:

Activity	Data Protection Interpretation	Action
Customer goes on your website and signs up for marketing information to be sent to them	They need to give their consent for you to market to them. This cannot be through a pre-ticked box	Check wording on your website including your privacy notice
Customer calls the branch and enquires about booking a vehicle	They need to give their consent for you to market to them. However, you can still email a copy of a quote for the enquiry.	Consider how you obtain the consent for marketing and make the customer aware of your privacy notice
Customer makes a booking on your website	It is necessary for the performance of the contract for the customer's details to be retained. You could also use the contract as a way of gaining	Review your privacy notice and booking process along with consent from the customer to send marketing information.

	consent for future marketing campaigns	

Sample clauses

Example for marketing information

We would like to send you information about our services, special offers and the latest information from (insert rental company name) by email, post, SMS, phone and other electronic means. We'll always treat your details with the utmost care and will never sell them to other companies for marketing purposes.

- ☐ Yes please, I would like to hear about your services and offers.
- ☐ No thanks, I do not want to hear about your services and offers.

Example for a booking

Thanks for making a booking with us in order for us to perform your booking we will store your details for X years in case there is a motor insurance claim, road traffic offence or parking charge notice. We would like to send you information about our services, special offers and the latest information from (insert rental company name) by email, post, SMS, phone and other electronic means. We'll always treat your details with the utmost care and will never sell them to other companies for marketing purposes.

- ☐ Yes please, I would like to hear about your services and offers.
- ☐ No thanks, I do not want to hear about your services and offers.

Example in a rental/lease agreement

By entering into this rental agreement you agree that we can process and store your personal information in connection with this agreement including data collected from the vehicle. We may use your information to analyse statistics, for market research, credit control and to protect our assets.

You agree that if you break the terms of this rental agreement we can pass your personal information to credit-reference agencies, debt collectors, the police, local authorities, councils, private parking companies or any other relevant organisation. We can also give this information to the British Vehicle Rental and Leasing Association (BVRLA), which can share your personal information with its members to prevent crime and protect their assets, as allowed under the Data Protection Act.

RISC

For those members who use the RISC database it is very important that your rental agreement includes the above clause regarding sharing data with the BVRLA. RISC is the BVRLA's risk management tool for rental and leasing companies. It allows businesses to qualify their customers

when hiring out vehicles. RISC contains information that can help in preventing, detecting and controlling fraud and other losses.

Under the new GDPR regulations if the customer has not agreed to you sharing the data with us and you put the customer on RISC and they become aware that they did not agree for you to share the data with BVRLA they can demand that their details are deleted from the database and we would have to comply with the request.

The BVRLA's provider of RISC is GDPR compliant and has secure processes and procedures in place to protect data which you put on RISC.

Sales Process for leasing brokers

Leasing brokers will need to make it very clear that personal data submitted to them will be shared with lenders or a panel of lenders. This should be a contractual requirement rather than a consent point alternatively it could be that the data is shared for legitimate interests. For example:

"In order for you to obtain finance we will need to share your personal data with funders to allow them to check your eligibility for finance. They will submit your data to credit reference agencies to verify your identity and perform a credit check."

Renewal and retention process

Provided you have made it clear in your privacy notice or contract that you will be making contact towards the end of the lease this should be sufficient.

For leasing brokers it is more likely that this should be contained in your privacy notice. For leasing companies it is more likely to be a contractual obligation as you need to ensure the customer is aware of the return conditions.

Contacting drivers during a lease

It may be necessary to contact the driver of the vehicle whilst it is on lease to advise on vehicle recalls, that an MOT is due or a service is required.

Where the vehicle is on an agreement with a driver there should be something within your contract regarding contacting the driver while the vehicle is on lease. For example:

"From time to time while the vehicle is on lease to you we may contact you via text message, telephone, email or post regarding: servicing, vehicle condition, vehicle recalls and when an MOT is due on the vehicle."

If the vehicle is on lease to a company you may have details of the driver and have been asked by the company to make direct contact with the driver. If this is the case you will need to make sure that the company has made it clear that they will be sharing the personal data of the driver with the leasing company and that you will be contacting them regarding: servicing, vehicle condition, vehicle recalls and when an MOT is due on the vehicle

You may wish to make this part of your master hire agreement with the company.

Delivery of a vehicle

Agreement 1 – Contractual obligation between the member and the employer to inform of the release of employee's personal data.

In some cases, for example, to arrange delivery of a new vehicle, it may be necessary to release the customer data to the motor dealer to facilitate the delivery of the vehicle to your customer.

If you are sharing personal data, such as the individual employee's details who is taking possession of the vehicle, then you or your customer (i.e. the employer) must have obtained consent for the personal data to be shared.

Agreement 2 – Indemnity clause between the member and the employer

As you are delegating your responsibility of obtaining consent on to your customer, you may wish to consider including an indemnity clause should the customer fail to adhere with these requirements.

"As the provider of vehicles for your company car fleet we will need to contact your employees from time to time regarding, delivery, servicing, vehicle recalls, MOTs and other matters relating to the safe operation of the vehicle. To ensure this is done in a compliant manner we would advise that this should be a contractual term as part of the agreement to provide a company car to the employee. We cannot be held accountable if this personal data is shared with us without this clause present"

Agreement 3 – Agreement between the dealer and the manufacturer as to how the customer's data is used.

Where personal data is shared with a third party, such as a motor dealer or manufacturer, it is vital that you state clearly what purpose the data will be used for. There will need to be an agreement between the member and the dealer to facilitate this.

For example, the motor dealer must only use the data for the purpose of delivering the vehicle and once this purpose has been fulfilled then the data must be destroyed and not used for any other purpose, such as sharing this information for marketing purposes etc.

As there is no regulation regarding how company data is shared. You may therefore wish to consider having a confidentiality agreement with your third party, explaining how any customer data you have provided can be used.

A sample clause for you to use with a third party, such as a motor dealer:-

"You agree to use any company or personal data provided by us for the sole purpose of arranging delivery and/or collection of motor vehicles only. This data will at all times remain our property and will be returned to us on demand. You also agree to destroy any data provided once the purpose the data was provided for has been completed. You are strictly prohibited from sharing any data we provide without our express written consent and that you will treat any such data as confidential."

Suppliers using your data

Customer data may be held or used by your appointed supplier or agent, for example, companies you use to help you arrange or carry out vehicle repairs, servicing or maintenance to your vehicles.

Members may wish to ensure that any data supplied to any supplier or agent you use which either relates to your vehicle or customer is kept confidential. You should also ensure that any such data is not shared or used outside the scope you have specified in your agreement with a supplier or agent.

Key contract terms to consider reflecting in your supplier agreement:

- ensure that your customer or vehicle data is not released by your supplier without your written consent and shall be only used or shared for purposes you have specified
- ownership of any data relating to your vehicle or customer remains your property
- ensure that your vehicle or customer data is destroyed by your supplier once the purpose it was required for has been completed.

Data collected in vehicles

Renting Vehicles with Telematics Devices

Where a vehicle is rented to a customer with a telematics device, tachograph or tracking device fitted to it the customer should be advised that the device is fitted and why it has been fitted.

If any personal data is recorded the customer will need to be advised what happens to that data after the rental and what purpose the data will be used for.

For example, if a tracking device is fitted to the vehicle the customer should be advised of this fact in the rental agreement. A sample clause could be:

'The vehicle you are renting has been fitted with a tracking device. If the vehicle is not returned to the agreed time and place we will use the data recorded on the device to recover our vehicle. All data will be deleted once the rental agreement is ended.'

Where a tachograph is fitted to a vehicle the rental company may wish to offer advice to the customer on protecting any personal data which is recorded on the tachograph. Personal data is protected on the tachograph through use of a company card which locks in the personal data stored. For more information on tachographs the BVRLA's fact sheet 558 Digital Tachographs can be accessed from the link below: 558 Digital Tachographs

Rental companies may also wish to include a disclaimer in the rental agreement for customers renting vehicles with digital tachographs installed which absolves the rental company if any data is lost due to the data not being locked correctly by the customer. A sample clause could be:

'Responsibility for protecting data held in the digital tachograph is the sole responsibility of the renter and we cannot be liable in any manner whatsoever, if the renter has not taken the necessary steps to protect the data by locking it in.'

Telematics Devices in leased vehicles

If a customer has asked for a tracking or telematics device to be fitted to the vehicle, the leasing company may wish to offer advice to customers based on the above impact assessments which should be conducted before devices are fitted. The leasing company is only responsible for devices which it has fitted or that are factory fitted on the vehicle.

Leasing companies may wish to include a disclaimer in their lease agreements regarding responsibility for personal data stored on devices when the vehicle is returned:

'Any data stored on a tachograph, tracking or telematics device should be removed prior to the end of the lease. If data is left on the device the leasing company cannot be held liable in any manner whatsoever for the loss of or use of the data.'

Leasing companies may also ensure that the customer has informed them that a tracking device or telematics device is fitted to the vehicle. This is so that if the leasing company's employees or agents

are driving the vehicle, for example to take it for a service, repair or alteration the device can be disabled. If it cannot be disabled the customer should inform the leasing company who will need to alert their employees/agents.

The leasing company may also wish to consider a liability clause where they have fitted the device, for example:

'The leasing company cannot be held liable for any faults to tachographs, tracking or telematic devices which result in loss of personal data or use of such data.'

Data collected in rental vehicles

Access to vehicle generated data is an essential business requirement for all commercial fleets as well as fleet management, leasing and rental car companies. It enables many critical enterprise functions and is foundational for enabling and sustaining long-term competitiveness.

Rental members need to consider how to ensure that an individual who rents a vehicle which has connected services does not inadvertently share their information with other individuals who rent the vehicle. It is important as if personal data is accessed the customer could hold the rental company responsible for the data protection breach in the asset they own.

The BVRLA advises the following when members are renting vehicles with connected services:

- ✓ advise the customer that it is a connected vehicle and if they connect their phone this could result in transfer of personal data to the vehicle and possibly motor manufacturers' cloud servers.
- ✓ advise the customer that it is their responsibility to erase any information that is stored in the vehicle before returning it and the rental company can assist with this if required.
- ✓ Ensure that where possible any personal data is wiped after each rental and this should be checked prior to disposal of the vehicle as well

Data collected in leased vehicles

Where data is collected in vehicles the BVRLA suggests the following principles apply:

Personal Data – In addition to the legal obligations governing the collection, processing and transmission of personal data, the motor manufacturer or its appointed agent (hereinafter called OEM) should ensure that express written consent from the driver of the vehicle has been obtained before any personal data is collected which includes but not restricted to any data collected by in-built real time connectivity devices or periodic vehicle data downloads.

Vehicle Specific Data – The vehicle owner agrees that vehicle specific data (i.e. data which relates to the maintenance and/or performance of the vehicle) may be collected and used from the vehicle(s) provided this is shared with the vehicle owner to an agreed electronic format.

Once the OEM has obtained the vehicle owner's permission to do so, the OEM will ensure that any driver or vehicle user related data is collected and stored in an anonymised form so that identity or any personal data about the driver or vehicle occupants cannot be established, unless the OEM has obtained written consent from the driver to do so.

Driver Specific Data – Provided the driver's written consent has been obtained incompliance with the national law governing data protection, the vehicle owner agrees that driver related data may be

collected and used (e.g. data obtained from the driver's use of the vehicle and connected services) subject to the following conditions being adhered to:-.

- OEM agrees to obtain the vehicle owner's prior written consent before contacting their customer, driver or hirer. If the vehicle owner receives a complaint from the driver, hirer or customer about the use of their driver specific data, you agree to immediately stop contacting the driver (through all mediums) for anything other than vehicle safety related services; and
- OEM agrees not to sell or provide access to driver or vehicle data to any third party without the vehicle owner's prior written consent or a court order (where applicable) in the case of a ex matter;
- OEM agrees to make it expressly clear in its Terms and Conditions with the driver of any vehicle owned by a BVRLA member that the OEM you may have a legal obligation to provide vehicle data to the vehicle owner

A Checklist

The following checklist is a useful starting point for your business in assessing key actions you need to take:

Business Process Analysis

1. Where is personal data gathered?
2. Where and how is personal data stored?
3. Where and how is personal data transmitted…..outside of the EEA?
4. To which third parties is personal data given?

Technical Analysis

5. Have you conducted technical testing of IT systems to instances of personal data?

This should include checking the robustness of systems or getting confirmation from suppliers on the robustness of systems,

Third parties and personal data

6. Do you have a written contract with suitable provisions for 3rd parties who you share data with?
7. Have you assessed the security measures taken by the third party to safeguard personal data?
8. Have you reviewed the personal data provided and ensure it is only what is needed for the job? Hint…. Minimise!

The above should be completed before any personal data is handed over.

Privacy policy and consents

9. Have you updated your Privacy Policy?
10. Have you put in place Data Processing Notices?

Consent

11. Is it fully informed, freely given and capable of withdrawal?
12. Have you removed any pre-ticked boxes?
13. Have you got records of who has given consent on your database today?

Subject access requests

14. Where is your personal data stored?
15. Do you need a web-page/portal for requests?
16. Have you established a robust process to respond in time to requests?
17. Do you have a system of record keeping for requests?

Data in cars

18. Do you check whether any personal data is left in a car at the end of a rental or lease?
19. Do you know how to delete data from your cars?
20. Are your agreements reflective of the fact that your vehicles are fitted with trackers?

Ongoing compliance

21. Have you got a procedure in place to regularly check compliance with GDPR?
22. Have you got a procedure for regularly checking your system is not liable to security breaches?

