MotorVise (Automotive) Ltd GDPR Update

May 2018

Overview

- Introduction
- Background to GDPR
- Legitimate Interest vs Consent
- Data Management Ecosystem
- Rights & Obligations
- Customer channels & actions
- Suppliers
- IT & housekeeping
- Training
- Summary

Background to GDPR

- GDPR will replace the Data Protection Act (DPA) from 25 May 2018.
- Applies to Data Controllers (e.g. you as dealers) and Data Processors (e.g. anyone who works with your data on your behalf) of data.
- Places greater emphasis on the documentation that Data Controllers must keep to demonstrate accountability – accountability is the most significant addition.
- Like DPA it applies to personal data, however the GDPR definition is more detailed and makes it clear that information such as an IP address can be personal data.
- Companies are required to have a comprehensive but proportionate governance measure.
- Penalties can be severe for breaches – this could be up to €20 million or 4% of your turnover.
- In the past, our industry's aggressive marketing culture may have prioritised our interest over that of customers.

Lawful Basis for Processing

1. Contract

- Where a customer or employee has entered, or is in the process of entering, into a contract with you, personal data may be processed if it is necessary for performance of the contract or is in order to take steps at the request of the data subject prior to entering into a contract.

Lawful Basis for Processing

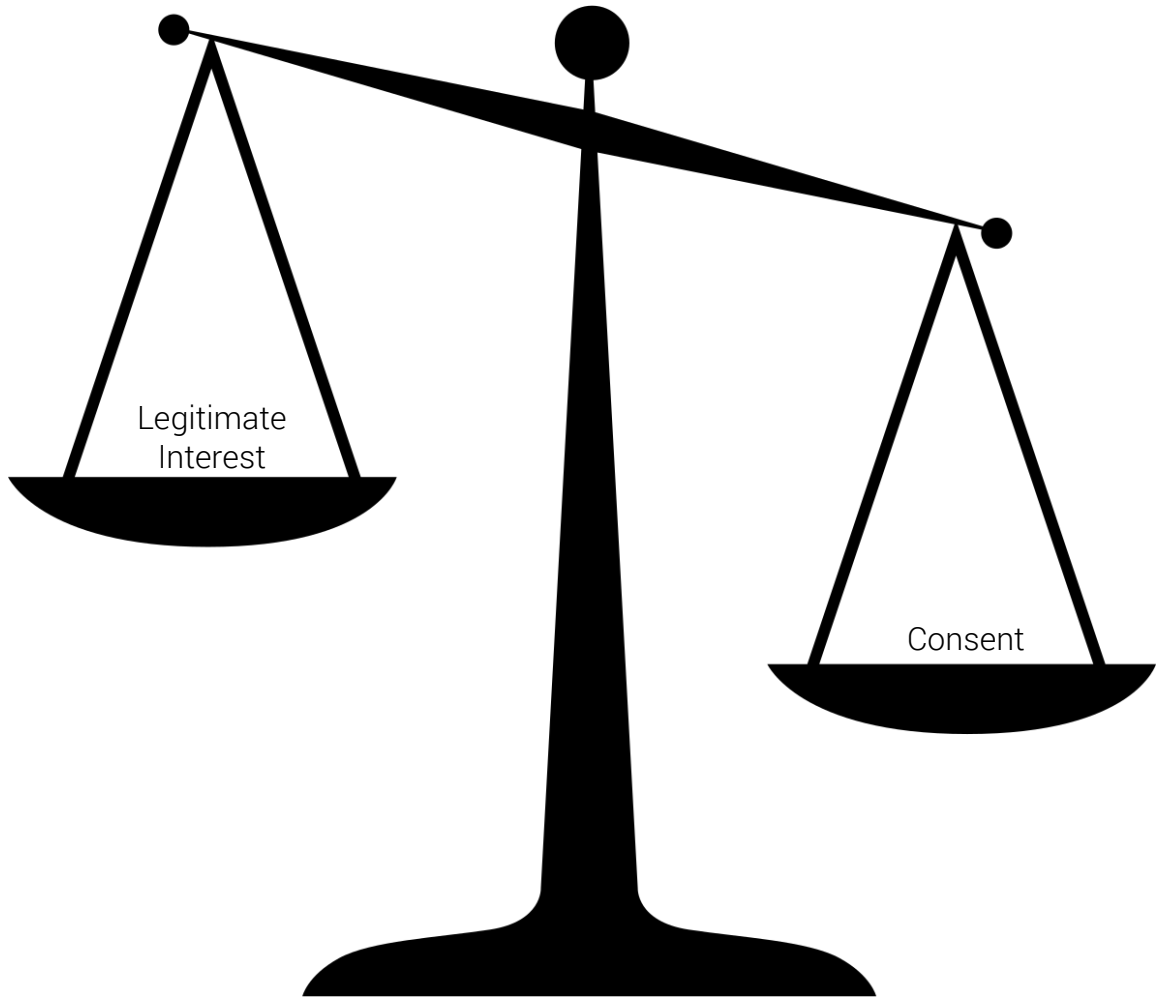
2. Legal Obligations

- Employee records must be kept for 7 years. This is for HMRC records, VAT records, money laundering, tax, national insurance, national interest etc.

Lawful Basis for Processing

3. Marketing

- Consent or Legitimate Interest – it's your choice!
- We recommend Legitimate Interest.



Lawful Basis for Processing (Marketing)

Consent

- In circumstances where a person makes a freely given, informed and specific choice to allow you to process their data, consent will be the lawful basis under which their data is processed.
- As existing customer data will be processed under Legitimate Interest, Consent will be predominantly exercised for non-employees who have not, as a minimum, entered sale negotiations with the business.

Legitimate Interest

- Non-employees who have completed or negotiated a sale with you may have their personal data processed for the purposes of the Legitimate Interests pursued by you or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.
- To balance the data subject's fundamental rights and freedoms with your commercial interest, the data subject will be informed that they may receive marketing communications for similar products and services at the point of enquiry or purchase, and will be given the ability to opt-out of further processing at any subsequent point in the relationship by visiting your website.
- They may also call you or contact your Group Data Controller who will complete the on-line opt-out for them.

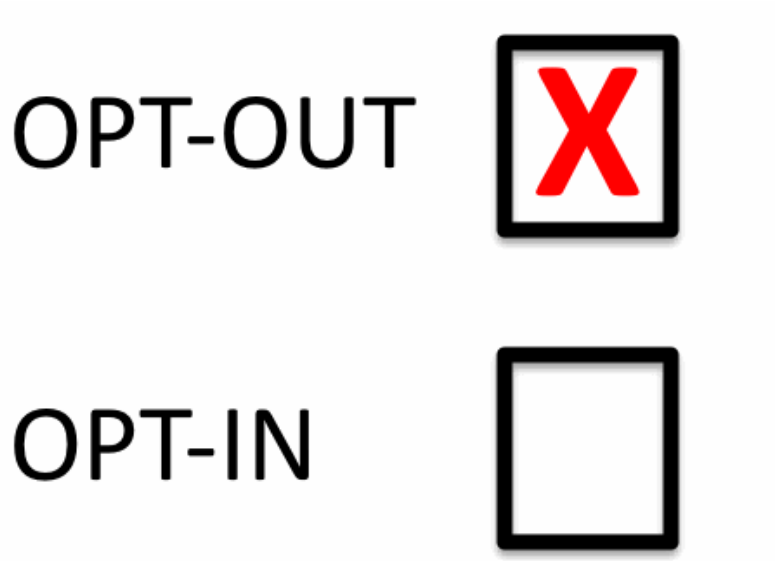
Legitimate Interest

If you use Legitimate Interest as your lawful basis for processing (marketing):

- If a customer asks to opt out, you MUST comply.
- At the point of every purchase / transaction, customers must be reminded of how you use their data and be given an opportunity to opt out.
- Your Dealer Management System (DMS) will be the primary source of customer records.
- Initially, only your contact centre and CRM team should amend preferences of customers on the DMS.
- To make your life simple, visit www.dealerwebsite.co.uk/optout to opt customers out. All information gathered from this page should be sent directly to the CRM team for validation and action.

Legitimate Interest

- The most important thing to remember is that if a customer asks to opt out, you MUST do it. This must be done within 28 days of receiving their request.



GDPR Considerations

External consultant	House-keeping	Training	Data sharing
Complaints/Breaches	HR	Subject Access Requests (SARs)	Consent
Legitimate Interest	Marketing	IT	Databases

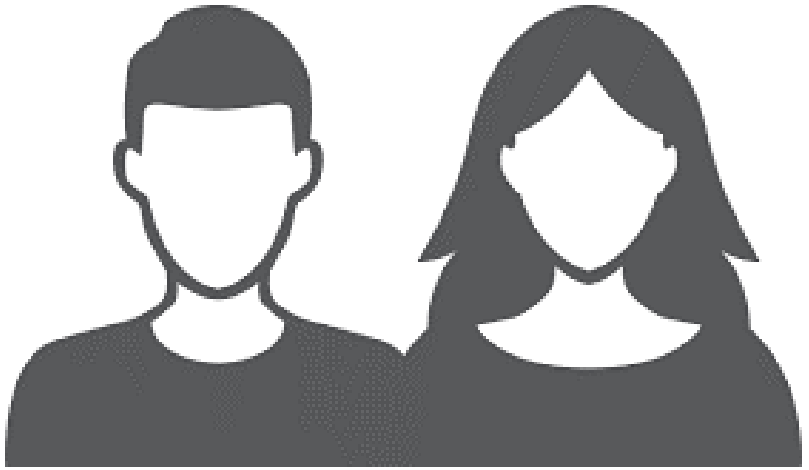
Key Roles

The data controller is the company. Within the company you have:

- Group Employee Data Controller (company)
- Group Customer Data Controller (named individual)
- Data Processors (e.g. MotorVise events)
- Data Subject (customers and employees)
- A Data Protection Officer is not required as you are not a public authority and do not process special categories of data and do not perform systematic monitoring of individuals.

Types of Customers

- B2B vs B2C
- Existing sales and service - franchise
- Existing sales and service - non-franchise
- Existing parts customers
- Existing fleet customers
- Leads (negotiation / time limits)



Customer Rights

Customers have the right to:

- A copy of their data
- Rectification of their data
- Erasure of their data (in some cases)
- Object to us or restrict the processing of their data

Note:

Customers have additional legal rights that you must be sensitive and responsive to.

Your Employee Obligations

- Employees should be aware that, under GDPR, they are personally accountable for your actions and can be held criminally liable if they knowingly, or recklessly, breach it.
- Any serious breach of data protection regulations should also be regarded as misconduct and be dealt with under your company's disciplinary procedures.
- If an employee accesses another employee's personal records, without authority, this constitutes a gross misconduct offence and could lead to their summary dismissal.
- Any breach should be reported immediately to your Group Employee Data Controller. The breach will also need to be reported to the Regulator within 72 hours. Failure to report breaches to the ICO will invoke fines, and the person responsible for the delay will be personally liable.

Your Employee Obligations

In relation to personal information:

- If, as part of their job duties and responsibilities, an employee collects personal information about other employees, clients or customers, they must comply with this policy.
- This includes ensuring the information is processed in accordance with GDPR, is only processed for the purposes for which it is held, is kept secure and is not kept for longer than necessary.

They must also comply with the following guidelines at all times:

- They must not disclose confidential personal information to anyone except the Data Subject (unless prior written consent has been given). Particularly, it should not be;
  - given to someone from the same family,
  - passed to any other unauthorised third party,
  - placed on the company's website,
  - posted on the internet in any form.

Your Employee Obligations

Your employees should:

- Be aware that those seeking information sometimes use deception in order to gain access to it.
- Always verify the identity of the data subject and the legitimacy of the request, particularly before releasing personal information e.g. by telephone.
- Strictly follow the company's requirements when they are provided with code words or passwords to be used before releasing personal information.
- Only transmit personal information between locations by fax or e-mail if a secure network is in place, e.g. a confidential fax machine, or encryption is used for e-mail.
- Forward any requests for personal information about another employee to the Group Employee Data Controller who is responsible for dealing with such requests.
- Ensure any personal data is kept securely (i.e. where an unauthorised individual finds it impossible to access this data), either in a locked filing cabinet or if computerised, it is password protected so that it is protected from unintended destruction or change and is not seen by unauthorised persons.

Your Employee Obligations

- NOT access another employee's records without authority as this will be treated as gross misconduct and is a criminal offence.
- NOT write down (in electronic or hard copy form) opinions or facts concerning a Data Subject which it would be inappropriate to share with that Data Subject.
- NOT remove personal information from the workplace with the intention of processing it elsewhere unless this is necessary to enable them to carry out their job duties and has been authorised by their line manager.
- Ensure that when working on personal information as part of their job duties when away from their workplace, and with the authorisation of their line manager, they continue to comply with GDPR.
- Ensure that hard copy personal information is disposed of securely.
- Remember GDPR compliance is their personal responsibility. If they have any questions or concerns about the interpretation of these rules, they should contact the relevant Group Data Controller immediately.

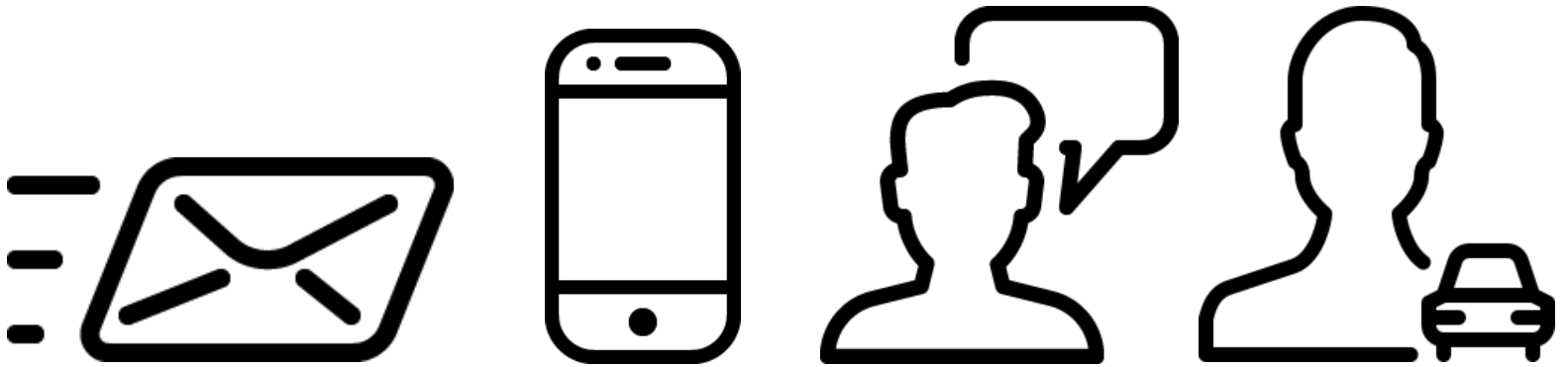
Employee Rights

Employees have the right:

- To be informed. Employers are obliged to provide transparency as to how personal data will be used.
- Of access.
- To rectification of data that is inaccurate or incomplete.
- To be forgotten under certain circumstances.
- To block or suppress processing of personal data.
- To data portability which allows employees to obtain and reuse their personal data for their own purposes across different services under certain circumstances.

Customer Channels

- Contact centre
- Service counter
- Sales enquiry / walk-in
- Sales order
- Parts
- Websites



Contact Centre GDPR Opt-Out Compliance

- Every time the contact centre make an outgoing call, or take an incoming call, they should make the following statement:

  "As an existing/new customer just before we continue, due to new regulations we need to inform you how we process your data. You can find full information on this at www.dealershipwebsite.co.uk/transparency. I can confirm we will market to you based on a Legitimate Interest basis but you may opt out at any time by visiting www.dealershipwebsite.co.uk/optout, or I can do this for you now. Is this all OK?"

- If a customer chooses to opt out of all contact methods you must explain that this will mean you cannot contact them about important safety recalls, MOT and service reminders or other services. Ask if they are absolutely sure they want to opt out of the contact methods.
- We do not believe you need distinguish between sales and service communications. We would recommend you only ask your customers to opt out of all or none.
- Most customers will want to receive service and MOT reminders and by default they will also receive sales communications.

Service Counter GDPR Opt-Out Compliance

- Service Advisors should draw customers' attention to the new section at the bottom of the job card:

  'We take your privacy seriously and will only use your personal information to administer your account and to provide the products and services you have requested from us. From time to time we would like to contact you with details of service, MOT reminders and other safety related items that your vehicle may need, and replacement of your vehicle. We will market to you on a legitimate interest basis, for full details on how we use your data visit www.dealershipwebsite.co.uk/transparency. You may opt out at any time at www.dealershipwebsite.co.uk/optout or your Service Advisor can do this for you.'

- Service Advisors should NOT amend customer preferences using DMS, and should use www.dealershipwebsite.co.uk/optout.

Sales Enquiry/Walk-In GDPR Opt-Out Compliance

Non face-to-face and sales showroom visits

- It is important that all sales enquiries have the statement below read out to them and that the customer is given the opportunity to opt out. A final reminder to opt out is given once the customer orders from you in the form of a similar statement at the bottom of the order form:

  'We take your privacy seriously and will only use your personal information to administer your account and to provide the products and services you have requested from us. We will market to you on a legitimate interest basis, for full details on how we use your data and your rights visit www.dealershipwebsite.co.uk/transparency. You may opt out at any time at www.dealershipwebsite.co.uk/optout. We can do this for you.'

Parts GDPR Opt-Out Compliance

- It is important that all parts enquiries have the statement below read out to them and that the customer is given the opportunity to opt out. A final reminder to opt out is given once the customer orders from you in the form of similar statement at the bottom of the order form:

  'We take your privacy seriously and will only use your personal information to administer your account and to provide the products and services you have requested from us. We will market to you on a legitimate interest basis, for full details on how we use your data and your rights visit www.dealershipwebsite.co.uk/transparency. You may opt out at any time at www.dealershipwebsite.co.uk/optout. We can do this for you.'

Website Enquiries GDPR Opt-Out Compliance

- When a customer enquires via a website form they should see the following statement:

  ‘We take your privacy seriously and will only use your personal information to administer your account and to provide the products and services you have requested from us. You can see how we process your data and understand your rights at www.dealershipwebsite.co.uk/transparency. By submitting your contact data in the form above you consent to us processing your personal data, in accordance with our Data Privacy Notice, and contacting you via these methods. You may opt out at any time by visiting www.dealershipwebsite.co.uk/optout.’

Outbound Sales Prospecting

- All data supplied for outbound prospecting for group marketing and events MUST be checked to ensure customers have not opted out.
- All data supplied MUST be securely destroyed within 21 days of issue.
- Leads generated from manufacturer systems and other dealership data sources MUST be checked to ensure customers have not opted out.
- Centres who need to request fresh data from your DMS for any other prospecting, should use a data request form which should be made available from the CRM team.

Supplier Due Diligence

- All third parties you share data with should receive a due diligence questionnaire.
- All suppliers should be listed on your websites, next to your privacy policy.
- All suppliers MUST sign a new data sharing agreement to ensure their data standards are the same as yours and are GDPR compliant.
- All forms received from suppliers should be forwarded to the relevant Group Data Controller.

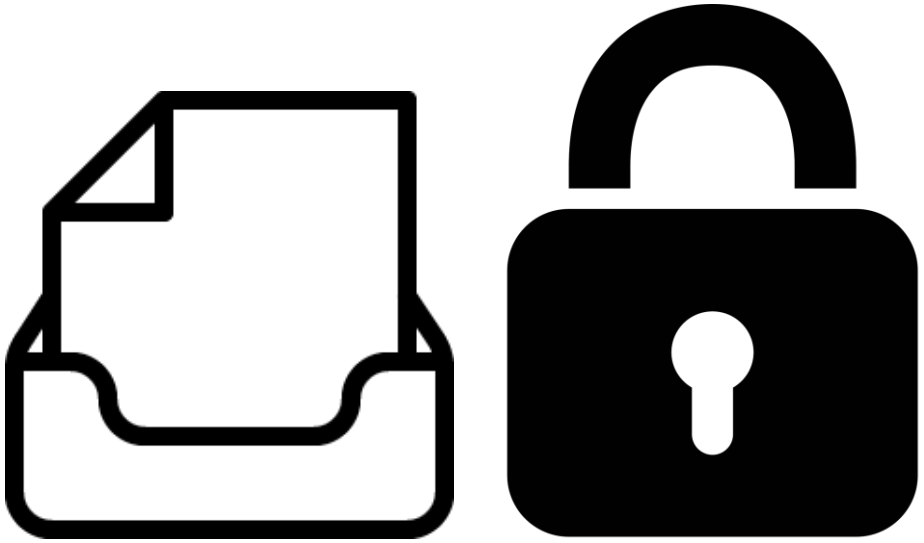
IT

- Access / control levels
- Laptops
- USB / external drives
- Email
- Company mobile phones
- Personal phones
- Restricts uploads / downloads

- Losing any IT equipment with company data / email on, must be reported immediately to the relevant Group Data Controller.
- All IT equipment with company data / email on must passcode protected.
- Personal mobile devices with company email accounts must be passcode / password protected at all times.

Housekeeping

- Security of personal data
  - Employee
  - Customer
  - Lead
- Hard copies
- Bins
- Printer / scanners
- Deal files
- Screens
- Shredding



SARs / Complaints

- Subject Access Requests (SAR) – be aware and ensure that these are handled appropriately. These may not necessarily be called SAR.
- Customers have rights to access to all internal communications and notes.
- Complaints process – escalate all complaints to the relevant person.

Training / Awareness

All these people need training:

- Directors / Senior Management
- General Managers
- Sales teams
- Aftersales team
- Parts teams
- Contact centre teams
- Technicians & non-customer/data facing teams

Email To Customers

Due to the introduction of GDPR, you are required to email all existing customers by 25th May to inform them of how you are processing their data in the future.

Example email:

'Dear <salutation> <surname>,

At <dealership name> we take your privacy seriously.

On the 25th of May the European union are imposing new legislation on the UK called the General Data Protection Regulations. As part of this legislation we need to let you know how we use your data.

You can find full information about out how we use your data at dealershipwebsite.co.uk/data

As an existing customer or someone who has enquired about making a purchase with <dealership> we will communicate with you on a Legitimate Interest basis to inform you about products and services from <dealership> that are related to your original enquiry or purchase. You may opt out of marketing communications at any time at dealershipwebsite.co.uk/optout or by speaking to one of our team or by emailing datacontroller@dealershipwebsite.co.uk with your full details including postcode and registration number.

Thank you for taking the time to read this data notice.'

Summary

- DPA to GDPR
- Legitimate Interest
- Rights of customers and employees
- Your obligations
- Complaint handling and breaches
- Most important thing: opt-out compliance
- Check prospecting data – verify opt out status in DMS
- IT & housekeeping
- Training