FEDERATION of British Historic Vehicle Clubs

Yesterday's Vehicles on Tomorrow's Roads

GDPR Guide

Originally commissioned by and presented with compliments of the Federation of British Historic Vehicle Clubs June 2018

Reviewed and updated by Nettitude April 2021

NETTITUDE

EXCELLENCE AS STANDARD

GDPR Guide

CREST

CHECK
IT Health Check Service

PCI Security Standards Council™

NETTITUDE

EXCELLENCE AS STANDARD

Report Contents

NETTITUDE

Update: April 2021

It is nearly three years since the General Data Protection Regulation was introduced and the Federation thought it would be useful to ask Nettitude, the original authors of this booklet to provide an update.

Introduction

The General Data Protection Regulation (GDPR) is designed to balance the need for businesses and customers' data information to flow freely, and the need to protect the rights of the individual. As an officer within a historic vehicle club, you need to be aware of the legal requirements of the GDPR so you can ensure your organisation is compliant.

Within this document, you will get a refresh of what GDPR means to you so you can grow your understanding of protecting personal data and be able to handle data in the digital economy appropriately in an ever more complex digital environment.

The key concepts of GDPR are including (but not limited to) the natural person, personal data, data controllers and processors, and legitimate interests of living individuals. There are legal bases for processing, including consent, legitimate interests and contracts.

There have been some big data breaches since the inception of the GDPR in 2018. British Airways were fined £19m for a widespread credit card breach where personal data was involved and Marriott International fined £17m for failing to protect personal data at the adequate level.

In the final section, we give some 'tips and tricks' describing how to mitigate these risks associated with the handling and processing of data, third party contracts and transfers and the roles and responsibilities regarding Data Protection in the workplace.

Data Protection doesn't just apply to technical, online e-commerce companies; it applies to the handling of any personal data within your organisation. Just because it is a historic vehicle club, there is a lot of personal data which needs to be handled with care!

Updates to GDPR since 2018 and the impact of Brexit

The main question that many people have asked since the United Kingdom departed from the jurisdictional control of the EU is, will GDPR apply after Brexit?

The answer is yes, GDPR will continue to apply after the EU transition period has ended. While GDPR rules were initially drafted and passed by the European Union on 25th May 2018 (2016/678), it is still applicable to any organisation who handles data related to residents living in the EU – which will likely include many UK companies. The UK adopted this legislation on the same day where it was named as 'Data Protection Act 2018' which replaced the Data Protection Act 1998.

Further, many aspects of the EU GDPR were converted exclusively into UK law on the 1st January 2021, under the title 'UK GDPR'. This means that you will need to continue to follow the regulation regarding data protection for your customers, members and subscribers.

What changes will there be to GDPR?

While GDPR will continue to apply, there are some changes from when the Act was transferred to the UK. The first is the control the UK government has over the GDPR framework it abides by and as from 1st January 2021 the UK now has the powers to review and amend the regulatory rules as required. Any changes made will impact UK GDPR only.

In terms of the actual laws, there will be relatively few amendments made to the data protection rules. The Data protection exit regulations were created in 2019, ahead of the Brexit deadline, which makes some technical adjustments to GDPR law, so they fit into a UK-only context.

The Information Commissioner's Office (ICO), who currently uphold information rights in the country, will continue to oversee data protection after the EU transition period. There has been an agreement with the UK and the EU with the process of data sharing that allow for the free and unhindered movement of data so long as the appropriate technical measures are in place.

Despite Brexit and the end of the transition period, historic vehicle clubs should continue with their existing practices regarding data. The only area that may change is for those organisations who need to process data from those living in the EU (such as if you serve EU members) or need to arrange the transfer of data between the two sides. The reason for this is that if there was an issue, you may be investigated not only by the UK GDPR but also the EU GDPR regulations…thankfully they are 99% similar (unless you are dealing with law enforcement issues)

Can I still send and receive data from the EU?

The government has previously said it will not restrict the flow of data between the UK and EU where it is required. However, there will be adaptions to how this takes place. The ICO has a temporary 'adequacy of transfer' agreement with the EU but this is not seen as a permanent solution at this stage.

The UK is currently awaiting an adequacy ruling from the European Economic Area. This will determine whether the UK's GDPR protocol is deemed adequate for EU data to be processed under it. If it passes the adequacy review, it will allow the free movement of data between the two sides. Data covered by an adequacy ruling will be classed as a 'restricted transfer', due to each side using different GPDR rules.

If you are receiving data from the EU or other approved 'third countries' (that is, those countries which have had their data protection deemed adequate by the EEA) from 1st January 2021, you will need to have an alternative transfer mechanism to send data. An example of this could include having Standard Contractual Clauses (SCCs) agreed with your EU counterparts, which will be the route most enterprises need to take. With this, a contract will be put in place between you and the other organisation, using EU terms. You can find out if this is the best practice for you using the ICO's interactive tool , or if alternative provisions should be made.

11 out of 12 recognised 'third countries' have already been deemed adequate by the EEA for their data protection has stated they will allow unrestricted transfer with the UK. This means that data can continue to be transferred freely with these countries from 2021. Further data processing agreements with other countries will take place, along with prospective data sharing agreements with the United States and the replacement for the 'EU-US Privacy Shield.'

What action does my historic vehicle club need to take?

As it stands, you only need to take action if your historic vehicle club passes data to and from the EU member states. If you already comply with GDPR and do not need to transfer or receive data from the EU, you will not need to make any amendments to your current business practices.

If you do send data to the EU, you may need to adjust your privacy notices so that it correctly informs individuals how their data will be handled and moved. You may also need to discuss with the relevant EEA organisations with which you transfer data to come to an arrangement regarding how this will be done moving forward. As part of this, any clauses or contracts required will need to be created and signed prior to 1st January 2021. These are known as 'model clauses' and it would be prudent to seek professional advice to ensure you're on the 'right' side of the law.

If your vehicle club is UK-based, and you are collecting personal data, you will be classed as a data controller. As you will be monitoring or using the data of EEA citizens; you may also need to appoint appropriate representatives to represent you in a member state where you will be collecting data from.

What you need to do to maintain UK GDPR

As the explanation for the changes to the UK GDPR have been described now the UK has left the regulatory control of the EU, below is a short list of actions which need to be taken to ensure that the adherence and the maintenance to the GDPR can be maintained;

DSAR – Data Subject Access Request

This had existed before the Data Protection Act 2018 but the new legislation requires a more comprehensive keeping of records. The old Data Protection Act allowed for a small charge to be levied to the Data Subject (usually £10) but with this legislation this cannot be done unless the request is unduly large or persistent and can be open to interpretation! The requirements of the DSAR are listed below;

- Confirmation that you process their personal data.
- Access to their personal information.
- Your lawful basis for processing their data.
- The period for which you'll store their data (or the criteria you'll use to determine that period, e.g., "as long as you're a customer").
- Any relevant information about how the data was obtained.
- Any relevant information about automated decision-making and profiling.
- The names of any third parties you share their information with.

Data Subjects do not need a reason to submit a DSAR. The data subjects can request to see their data at any time; even if they could be identified by the historic vehicle they own (e.g. VIN or V5C data). Historic vehicle clubs may only ask questions on the data subject that helps to verify the subject's identity and help them locate the requested information.

DPIA – Data Privacy Impact Assessment

A Data Protection Impact Assessment (DPIA) is required under the GDPR any time you begin a new project that is likely to involve "a high risk" to other people's personal information.

While it is clear a DPIA is required by law under certain conditions, it is unhelpfully light on specifics required. To help clarify the situation, here are some scenarios that would require a DPIA:

- If you're using new technologies;
- If you're tracking people's location or behaviour;
- If you're systematically monitoring a publicly accessible place on a large scale;
- If you're processing personal data related to "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";
- If your data processing is used to make automated decisions about people that could have legal (or similarly significant) effects;
- If you're processing children's data;
- If the data you're processing could result in physical harm to the data subjects if it is leaked

In other cases, where the high-risk standard is not met, it may still be prudent to conduct a DPIA to minimise your liability and ensure best practices for data security and privacy are being followed in your historic vehicle club.

Cookies

To a non-technical audience, these aren't biscuits! Cookies are small text files that are stored on your end-user's web browsers, Chrome, Internet explorer etc. What is often misunderstood are that cookies most often contain an identifier (known as a "Cookie ID") that is in itself considered personal data under the GDPR. This means that when you have a website, under GDPR, cookie IDs are considered personal data.

The effect of this is that it is a unique ID that allows your website to remember the individual user and their preferences and settings, when they return to your website. This means that it identifies the personal identity of the user and should be considered.

Consent

Gaining consent of the data subject is crucial to the correct operation of personal data within the Data Protection Act. "Freely given" consent essentially means you have not cornered the data subject into agreeing to you using their data. For one thing, that means you cannot require consent to data processing as a condition of using the service. They need to be able to say no.

The one exception is if you need some piece of data from someone to provide them the service in which you offer as a historic vehicle club. For example, you may need their credit card information to process their subscription or order.

Also, if you you want an end user's email address for marketing purposes, you must give the user an opportunity to confirm or decline for each service you offer.

If you have more than one reason to conduct a data processing activity, you must obtain consent from the end user for all those purposes. So, if you store phone numbers for both marketing and identity verification purposes, you must obtain consent for each purpose.

Third Party contracts and data transfers

Finally, it is essential that you research the security practices of any potential third party and agree in writing to the measures it will take to secure its systems. This can be done when you sign up to their service. This is especially important as under the UK GDPR, the data processor holds the same liability as the data controller. This means you cannot shift the liability and risk of personal data processing to a third party and not think any more of it!

As a result, it is necessary that the proposed contract must also state that your third parties take the following into account:

- Will act only on your documented instructions;
- Will not contract a sub-processor without your prior approval; and
- Will delete or return all personal data to you when the contract ends.

Remember if you collect personal data from a living person, you are responsible for it until you cease to do business with them and this includes outsourcing efforts.

Original Report: June 2018

EXECUTIVE SUMMARY

Federation of British Historic Vehicle Clubs engaged Nettitude to deliver a GDPR (General Data Protection Regulation) guide specific to member Clubs in order to support their efforts to comply with the regulation in readiness for 25th May 2018.

The engagement was to provide a breakdown of issues clubs might encounter, explanations around the 12 Steps to GDPR compliance and a Q&A session for common scenarios that might occur.

It must be understood that the scenarios listed and answers provided are not an exhaustive list of all issues historic vehicle clubs will encounter, so further engagements with Nettitude may be required in order to cover specifics pertinent to a specific club.

INTRODUCTION

The engagement follows a GDPR Awareness presentation delivered by Nettitude. Nettitude consultant Ron Williams has experience with the operation of vehicle clubs so has constructed this guide based on that knowledge and as a Subject Matter Expert (SME) of GDPR. All clubs should be aware that GDPR is intended to bring a more secure platform everywhere Personal Data is handled. Following the guidance can result not only in providing increased security but also offering streamlined processes by removing some of the speculative guesswork behind various administration activities appropriate to operating a historic vehicle club. Try to imagine Personal Data as your car keys. Think of all the questions you'd ask before handing your keys over to a stranger. Substitute in Personal Data and you've got the correct frame of mind to tackle GDPR.

GDPR Overview

Regardless of the UK's status as a member of the European Union (EU), it is clear that the UK will adopt GDPR for a number of reasons:

- The UK will still be a member of the EU as of 25th May 2018;
- The UK government has stated that GDPR will be adopted. The Data Protection Bill, published September 2017, sets new standards for protecting general data, in accordance with the GDPR;
- UK businesses that wish to process the personal data of EU residents would be required to adopt the principles of GDPR regardless of the UK's EU membership status.

The Information Commissioner's Office (ICO) has published a 12-step guide[1] to assist with the implementation of GDPR, and continues to release guidance and clarifications on GDPR on a regular basis.

Nettitude has aligned their approach and recommendations made to Federation of British Historic Vehicle Clubs, with the guidance provided by the ICO in order to ensure alignment to the main cornerstones of GDPR.

For a more detailed explanation of the key differences between GDPR and the existing Data Protection Act, refer to Appendix A – Differences between GDPR and DPA.

Differences between GDPR and DPA

GDPR applies to both Data Processors and Data Controllers (previously only Data Controllers were in scope for DPA). However, Data Processors would normally be acting via commercial agreements from a Data Controller, these would include Data Protection principles.

GDPR introduces some new items which are considered Personal Data (PD) as the definition has been expanded to include any data which can potentially be used to identify a living person. GDPR also bring a concept of "Security of Processing", which suggests that personal data should either be encrypted or go through a process of pseudonymisation - part of this is the concept of appropriate technical and organisational measures.

Other differences are shown below in the table below.

[1] https://ico.org.uk/media/for-organisations/documents/1624219/preparing-for-the-gdpr-12-steps.pdf

GDPR	DPA	Impact
Privacy by design – Privacy impact assessment (PIAs) for all projects and initiatives	PIAs should be conducted for new projects – not currently a requirement	PIAs are mandatory for all new projects and initiatives impacting privacy
Consent – opt-in for all data collections with clear and concise privacy notices	PECR (Privacy and Electronic Communications Regulations) requires opt-in but the DPA currently does not Privacy notices are required at all points of data collection	Requirement for opt-in for all data collection Privacy notices must be prominent and in plain English
Responsibility and accountability – notification requirements to include data retention and contact details	Annual notification to the ICO for data processing	Additional requirements for notification on an annual basis
Data breaches – mandatory notification within 72 hours	Notification is encouraged but not required	All data breaches must be reported to the relevant SA within 72 hours
Fines – up to €20m or 4% annual global turnover	Fines are currently up to £500,000 or 1% of annual turnover	Significant increase in potential fines for breaches or non-compliance
Right to erasure – removal of all records (including web presence) for a data subject	No current requirement to remove all data related to an individual	Systems must be reviewed and developed to allow deletion of specific records as needed
Data portability – ability to transfer data between electronic systems	No current requirement to provide ease of transfer between systems	New systems must be developed with portability as a requirement

Table 1 – GDPR vs DPA

12 STEPS GUIDE

Information Held

Have a look at the information you are requiring from members. Most clubs are pretty good at this now and only acquire minimal information – enough to perform the function of the club. That is the important phrase – enough information to perform the function of the club. Standard information collected, for a historic vehicle club, would be along the lines of the following:

- Name
- Address
- Telephone Number
- Email address
- Vehicles – Make and model

The reasoning for the above would be to provide club services to the individual – send magazine, send emails etc.

If you are requiring Date of Birth (DOB), Sex or Religion, you need to be extremely clear in your reasoning for acquiring that data. For example: clubs that loosely provided a reason for DOB and Sex on the basis that providing activities at club events was based on this data. It would be more than likely to require a separate consent field for those datasets. However, if you are trying to catalogue member age groups, simply provide tick boxes with a set of age ranges.

Perhaps the most important document regarding the Information you Hold is the retention document. All Personal Data should have a shelf life, and that should be documented with reasoning as to why you have chosen that length. Think of it as a service schedule for your car – a fan belt needs replacing after 12 months because the rubber cracks, but the cam chain is for the life of the vehicle because it is always lubricated.

Privacy Notices

A privacy notice tells the members how their data is going to be used. This needn't be complex and a statement of fact will suffice. An example below:

We use your data for the purposes of running the historic vehicle club. This involves:

- Organising Track days
- Communicating Member events
- Internet based forum
- Etc

Individuals Rights

There are a number of rights an individual has under GDPR:

- 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; and
- the right not to be subject to automated decision-making including profiling

To summarise the above: 'The individual can do whatever they want with the data you hold providing there are no laws or legislation that says otherwise.'

The most important right is the right to erasure or, as it is commonly known, the Right to be Forgotten. Make sure there is a process that covers an individual requesting the Right to be Forgotten even if it means terminating their membership.

Subject Access Requests

Everyone has the right to know what information an organisation has referring to them. This is referred to as a Subject Access Request (SAR). You have 30 days to respond to a SAR and cannot charge for it. You should have a policy in place that identifies who is responsible for managing this request and what steps are involved in order to complete it.

Lawful Basis for Processing Personal Data

Simply put, the purpose of a historic vehicle club is to 'Provide a service for members supporting their vehicle and providing vehicle based activities.' Should the club offer more than this, it should be fully publicised to the members.

Consent vs Legitimate interests

This is perhaps the largest issue that will cause confusion amongst vehicle clubs. A club is there to provide a service to its members and as such, as long as you are doing that, there is no limit to what you can send your members. Let's go through a couple of examples below:

Craftsman's Auto Parts has just manufactured a new stock of uprated carb jets for the Dellorto that 20% of the member base run. These jets are always in demand and Craftsman's serves several clubs. Some of your members are signed up to marketing emails, some not, but you know the club will want to know about this. This is a Legitimate Interest. The communication to members should provide the detail of the situation. An example would be as follows:

Dear members,

A new batch of Dellorto carb jets have become available from Craftsman's. If you would like more information, please feel free to contact the club or deal with Craftsman's directly.

Thanks

Admin Team

This isn't a marketing email as no values or offers are being made, just an alert to something that is rarely available. Let's look at how it could be a marketing email:

Dear members,

Craftsman's have a new batch of Dellorto carb jets in and they are offering them to our members at 30% off if you place an order in the next 48 hours. Just contact them on 01234 567890 and quote the 'NSH30%NOW' code word to get your discount.

Thanks

Admin Team

The distinction between a legitimate update to members and a marketing email is clear. The legitimate interests are a statement of fact with the crucial information only. It becomes a marketing message when offers/stipulations are included.

There is no limit to the amount of Legitimate Interests messages you can send. If the message/content has a genuine purpose for the value of members, send away, but don't see this as an opportunity to spam your members with needless information. As club administrators, you should know how to differentiate.

Children

Several vehicle clubs do have a child membership scheme. A child, according to the ICO, is someone under the age of 13. 13 or over are classed as adults so can provide their own consent etc. Now, it might be wise to have a line in your privacy policy stating 'We do not accept any members under the age of 13. Should you join the club and it is found that you are under the age of 13, we will immediately delete your account.' However, if you do have a child membership scheme, it is imperative that you attain parental/legal guardian consent for that child to be a member.

Data Breaches

This is very much dependant on the systems at use and the volume of data that is under control. GDPR is expecting appropriate controls based on organisation size so specialised hardware won't be required for a small club consisting of 300 members whereas it will for a large club consisting of tens of thousands of members. It must be understood that a little goes a long way. Should you be a small club, a decent Anti-Virus (Think McAfee, Symantec, Sophos etc) solution on your admin teams'

PCs and having a password to log on, is a large way to compliance for the data breaches section. Sending emails with password protected ZIP attachments containing member data and keeping the member data to a 'Need to know' basis only. The security solution complexity should be scaled with the amount of members being served.

Data Protection Impact Assessments (DPIA)

DPIAs primary purpose is to force the Personal Data administrators to account for risk with relation to changes in the way you collect, manage, store and process personaldata. In the context of data collected for club purposes, a spreadsheet keeping a log of changes that involve personal data is all that is essentially required. Again, the more complex the systems, the more thorough the solution for change management should be.

Data Protection Officers (DPO)

Whilst you aren't required to have a DPO, it is worth considering appointing a single point of contact and authority.

International

Should you operate in other countries, specifically those outside of the EU, then you are subject to their laws and legislation as primary and superseding those rules in GDPR.

SCENARIO Q&A

Q) How should clubs word privacy notices/policies?

A) They should be worded as matter of fact. Explain what the data is being used for and that it will be kept safe

Q) Where should privacy notices appear? Is it sufficient for these to appear in club magazines/newsletters and/or on club websites and/or in membership application forms?

A) The Privacy Policy/notices should be at any point where a prospective member can join the club

Q) Does joining a club imply that new members have given a club permission to contact them? Or: What permissions do clubs need to ask from a new member to enable them to be contacted, for marketing and general club update purposes?

A) Joining a club is what the prospective member is trying to do. As such, liaising with an individual regarding club matters is absolutely fine and expected as per legitimate interests. This can be listed in T&Cs for joining and should be identified in your privacy policy for what data you take and for what purpose.

Marketing is a separate entity. You cannot send marketing emails unless a user has explicitly signed up via an opt in process to receive them. The definition of marketing communications is often specific to each individual club.

Q) Do clubs need to gain new specific permission from existing members, in order to contact them about club shop and/or product updates from club sponsors e.g. Classic vehicle insurance providers.

A) Put simply – if you don't have a method of proving consent for this, you cannot continue to send marketing communications.

Q) What is the best means of getting members to opt into receiving these communications, letter, email, checkbox?

A) Entirely down to the club and what each club thinks will satisfy their constraints. A check box is fine, although email and letters are valid. It depends on what systems are setup to process the consent.

Q) What is the best practise for gathering people's data at events, are physical sign up forms GDPR compliant or should clubs start transitioning to iPads etc?

A) This will again depend on how the club is set up. Any of those methods are acceptable. However, it would be recommended that a single method is prioritised as to prevent 'loose' data from being forgotten about.

Q) When gathering information from a member for a database what information is strictly necessary and what information would just be good to know? For example, members' age, email, contact number, bank details would be necessary. But would it also be good to know a members gender, vehicle type and profession?

A) You can only gather information that you need. If you don't need it you cannot store it without having explicit consent. Date of birth would be a good example. The club may want to categorise

the age of owners by having Date of Birth, but it isn't needed to provide services. As such consent from each member would be required to store it along with the reason it is being stored. An optional replacement, would be to have age groups – 18-25, 26-35, 36-50, 50+ etc.

Q) Event Photography Scenario: At a large national event a club would like to take photos of their vehicles on the display stand. Members of the public walk freely around each vehicle and often sit in them. The club has a small sign on their stand which reads "Photographs may be taken and later distributed on our Facebook page and magazine". Is this enough warning? Or does the club need to ask everyone visiting the stand to sign a waiver form?

A) This depends. If it is in a public place (such as a car park, beach, pier etc) there are no stipulations – the club can freely take photos without having to worry. However, at a show where people have paid to get in, this is a tricky situation. If the photograph isolates a subject where they can be easily identified, a consent form is required. This will usually be for a posed photo so shouldn't be a problem. It might be worth checking with the show organisers to see how they have worded entry rules for guests.

Q) Is using BCC for mass club emails safe and GDPR compliant?

A) Yes. BCC is ideal as it is preventing mail information leaking.

Q) For "lapsed members" (members who have not renewed but more due to forgetfulness rather than actively deciding to leave), how long can a club still contact them via email in the hopes of prompting them to renew?

A) It can't unless they have signed up to marketing. The best thing to do would be to remind them that their membership is coming to a close 7 days before it does so. Language is important in these communications, so just be factual and concise:

Dear Member,

Your membership is set to end in 7 days time on 01/01/2020. If you wish to continue your membership with us, please contact the membership team on 01234 567890 or membership@carclub.net

Q) For members who have opted out of receiving general marketing communications, will the club need to produce a duplicate E-Newsletter which does not contain shop and club affiliate updates?

A) Absolutely. It's worth noting that the language 'Opted out' is a misnomer. 'Not opted in' would be the correct language/action

Q) Will my club be held accountable if an external provider (i.e. online payment provider) has a data breach?

A) Possibly. Due diligence on suppliers is a requirement (article 28). If you are using a data processor who has glaring security issues and you haven't performed adequate due diligence, expect to be fined should a breach occur.

Q) Do members have to give their consent for their details to be shared with external providers?

A) This would depend on what it is they're doing. If they are hosting the club database, then no. If you are sharing it with a vehicle dealership so they can offer new vehicles to them, then yes.

Q) Track Day Scenario: Club 1 is organising a joint track day for its members and has invited two other clubs, following the days racing Club 1 would like to commemorate the day with a race day booklet. This printed booklet will contain the results of the day along with the names, cars and times of each driver and which club they are associated with. Club 1 would like to also share the booklet with the other two clubs who attended. Is this sharing of information GDPR compliant or would Club 1 have to ask the permission of each attendee before sharing the booklet?

A) There are two ways to go about it:

- Include in the T&Cs that you will be doing this and that you shouldn't accept/pay for the track day if you are unhappy with it
- Attenuate the name. Surname only along with the vehicle model would be enough pseudo-anonymisation.

Q) Volunteer Scenario: A large vehicle club is organising a weekend event showcasing old and unusual vehicles. To help run the event, a large amount of members have volunteered to work alongside the club's paid staff. In order to deliver a great event, club officials will need to create a culture of shared information amongst the club staff and volunteers. How can the club staff share important personal data with the volunteers safely to mitigate against a possible data breach?

A) This should be performed on a least privilege basis. If individuals don't need to know, they shouldn't. Volunteers will fall under the same remit as paid staff and should be required to sign and accept contractual agreements, just like staff, if they are getting access to personal data. How the data breach mitigation steps are created would be on a case by case basis per club.

Q) Reposting of old content Scenario: A club has recently uploaded its entire back-issue catalogue of club magazines dating back to 1990, within the "Members Only" area of their website. Within these E-Magazines is old information such as names, email addresses and phone numbers of past and current club/regional officials. How does this comply with GDPR? Will the club have to manually remove each line of information or only do so to selected lines if a Right to be Forgotten Requests is filled?

A) The older the content, the less chance the information is accurate anyway. It would also depend on what type of addresses they were – business or personal. In most circumstances this would fall under public domain so no redacting required.

Q) How can club personnel share members' personal data to regional officers (RO) – is sharing a copied excel file ok?

A) Yes this is fine. However you should look to send personal data encrypted. You should require that the RO have fundamental security on their machines and require them to remove all club data when stepping down. Ideally they would access data through a portal, but this isn't required.

Q) Will GDPR impact clubs keeping members' data for archiving purposes?

A) Massively. Retention policies will be required for all data with reasoning behind the lengths of retention. Historical archiving is allowed, but you must be clear as to why it is being performed. For a vehicle club this will most likely be all about the vehicle, so the club can redact the owner information.

Q) How long should clubs keep hold of data after a member has left and/or died?

A) This is arbitrary in relation to the length you feel is required through your retention policy or law/legislation.

Q) Club Office Scenario: To join this vehicle club you must fill out and return a physical membership form to the club office, this form is then filed and stored away. Is having paper copies of member's personal details, a thing of the past, should everything now be digital?

A) Not required, but it is beneficial. Anything relating to an individual should be kept in one place and one record as it allows less data corruption and easy completion of any Subject Access requests and Right to be Forgotten etc. Your retention policy will apply equally to paper copies of data and digital records.

Q) In order to ensure that the processing of personal data is "fair and lawful" (first data protection principle) my understanding is that one of number of conditions needs to be complied with. In the opinion of the seminar presenters are classic vehicle clubs able to operate under the "legitimate interests" condition or do they need to obtain consent from members to the processing of their personal data?

A) Yes they are legitimate. As long as their information is used in an appropriate way and that the information gathered is required for club activities.

Q) Is the answer to the question above different according to whether clubs make members personal data available to third parties such as insurance providers and parts suppliers for marketing purposes or simply use such data themselves?

A) Yes. They must separately opt in to be sent communications about anything other than club business.

Q) Are third parties engaged by clubs to print and/distribute club magazines/newsletters to be regarded as data processors? What arrangements should clubs put in place with such third parties to ensure compliance with data protection legislation?

A) Absolutely. These are Data processors. Due diligence should be performed on a risk analysis basis with all data processors.

Q) Can local area officials use club data for promoting the club?

A) Yes, but they cannot broadcast this data.

Q) Where clubs have overseas sections can they make available data relating to members in particular countries to the club organisers in the countries concerned? Is the answer to this question different depending on whether the countries are EU members?

A) If the country is a member of the EU, it too will follow GDPR. However, local legislation applies and that should be applied with over and above the sanctions imposed by GDPR.