



SOUTHERN FEDERATION of MODEL ENGINEERING SOCIETIES

Formed from the Federation established in 1970 by Model Engineers for Model Engineers
A Company Limited by Guarantee in England and Wales No. 9002737
www.sfmes.co.uk

It is real, it is here, it will bite from May 25 on- wards IT IS General Data Protection Regulations

**"I SUPPOSE I'LL BE THE ONE
TO MENTION THE ELEPHANT
IN THE ROOM"**

 **software** AG



Cartoon courtesy of *Software AG* via Google

Visit the Southern Federation website section "Understanding the Law"
And then go down to "Data Protection"
www.sfmes.co.uk

Editor: David Goyder Tel: 023 8042 1201 newslettereditor@sfmes.co.uk

Views and comments expressed in this publication are not necessarily those of the Southern Federation of Model Engineering Societies

EDITORIAL

This is less of a newsletter and more a service to members in our recognition that many members just do not use a computer, do not have access to a computer or just plain don't like them!

Additionally, as Dr Martin Baker notes early in his introduction, "...new laws have given rise to people establishing overzealous interpretations and hence overzealous and onerous guidance.

We have knowledge already that some less well informed societies are relying on 'old Joe', it doesn't apply to us, without realising the consequences of not seeing the elephant.

The penalties are money ones, and a lot too, so ignoring the elephant could become expensive as in bankrupting a society. We know of an instance where

members are on the verge of writing to officers to say, "we are making you aware of the law that you refuse to follow and any fines our society receives will be your personal responsibility". That would hurt.

So, the Southern Federation's contribution is to provide guidance so you can do your own research (DYOR), discover how to be lawful, find out what you do not have to do and what you are obliged to do under the law.

We wish you a safe and speedy conclusion to your efforts and remind you that the Southern Federation personnel who have researched the matter thoroughly may be able to guide you to the source of knowledge.

David Goyder, Newsletter Editor

What we have for you

The imposition of GDPR requires that many of us who are officers of Societies to learn an awful lot in an area where we are less than familiar. Few of us are lawyers and fewer of us read government regulations for the fun of it. Much better a model engineering magazine!

This one off news supplement has as its purpose to make member societies aware of the scope of information that the Southern Federation team has prepared as a guide to allow us to comply with these regulations.

First of all we go through the "Common Myths". There will always be the 'expert' who was told by his mate that it does not apply to us. If in doubt read the myths!

After the myths, we present the suggested "Check List". This will take you through what to look at and perhaps act upon. It is exactly as it is in the web site

Next we have the questionnaire overview. Well worth using the questionnaire to see what it turns up

for your society.

Then we reprint the introduction prepared some time ago and shown is the last regular newsletter.

And you will help your fellow members if those who are computer literate to print this off for those who are less comfortable in the computing world so that your committees may make informed decisions and stay compliant with the law.

And just to show you it is real, a nursery was inspected and observations were, "USB sticks and laptops were not always encrypted" or, "Paper files were not always stored securely when not in use during the day".

We are not immune because we are model engineers!

GDPR Team

Southern Federation of Model Engineering Societies

Understand "Legitimate Interest"

An important consideration in law is when the data you hold is your **legitimate interest** or right by way of **contract**. Data in these categories do not require consent and the person cannot require its removal. Membership is an example of right by contract.

Common Myths on GDPR

Beware

As with Child Protection and with Health and Safety, new laws have given rise to people establishing overzealous interpretations and hence overzealous and onerous guidance. The following lists common misconceptions in relation to our Affiliated Societies to what is required under the law and is based on either the wording of the law itself or from guidance from the Information Commissioner's Office (ICO).

Myth: We are a small group: not even a registered company, so it doesn't apply to us.

There is no small size exclusion in the law: you are either holding personal data for your own personal purposes (which is exempt) or you have data for your group, such as the list of its members. But the provisions you need to make are not onerous either if your affairs in the eyes of data protection law and use of data fall entirely in the areas that do not need approval from people for you to keep their data. Being a small organisation in the eyes of the law **and** keeping within reasonable boundaries means that some detailed record keeping is not required.



Image courtesy GDPR in Schools Limited © 2018

Myth: Must appoint a Data Protection Officer (DPO)

The law does not require such an appointment although that is a way to satisfy the law. All is required is that you have identified and recorded the name of a person who takes lead responsibility for data protection and that the person has agreed to do so.

That person does not have to be on your management

group/board/committee but if not then it is desirable (but not a legal requirement) that there should be a specific role on the committee to whom that person reports.

The ICO considers these as two different approaches (DPO and person with lead responsibility) as both acceptable means to comply with the law. These two may be distinguished loosely along the lines of professional and amateur experience level.

There are cases where a formally appointed DPO is required by law, but this will not apply to most affiliated societies. We recommend that you do not call a person your DPO unless you are required to have appointed one by law.

If a person ceases to perform that function (e.g. extended sickness or resignation) then you must establish a replacement promptly.

The SFMES recommends you avoid calling the person responsible your DPO as the term may under certain circumstances carry with it a presumption of higher duty, authority and accountability. You may consider using the title Data Protection Compliance Leader



Image by Fox Studios via Vox WiFi Gear and Google

Myth: Must register your use of data

Registration is only required under specific criteria of the data you use. Most Societies affiliated to Southern Federation of Model Engineering Societies will not need to register.

More Common Myths on GDPR

As a general rule for our Affiliates, you do not need to consider if you need to register if the use of data is solely for membership suppliers and customers contact details, you are not a charity and are not doing anything that might be considered marketing.

If you need to see the full set of rules then you should refer to the UK Information Commissioners' Office

Myth: Must have explicit approval of data owner's use.

There are several categories of data that an undertaking such as club or society can hold without requiring the consent of the owner because your society has a **Legitimate Interest** in holding the data. By following sensible limitations to your use of data, many affiliated societies of the Federation will never need to ask their contacts for permission to hold data - and hence in turn will not need to keep a register of approvals. However they should still have a general statement on their use of data should a person or the ICO enquire.



Image courtesy Work Environments Cartoons and Comics

Myth: You must remove data if the data owner requires that to be done

Myth: You must remove data when a person resigns, is written off or passes away

Myth: There are strict time frames after which you must remove data

Myth: Because of the changes of the law you now need to write/contact to everyone about data protection

Have a look at the other “Myths” in the page in the Southern Federation website. Once signed in to the members area, go down to “Understanding the Law” and then, “Common Myths”.

Myth: The rules only applies to society computers and websites

Myth: You have to get permission to share your member data with the Southern Federation of Model Engineering Societies

Myth: We have to declare and process our sharing of boiler test records with the SFMES

Myth: I can take a copy of club data home or copy onto my own computer or mobile

Myth: You have to remove data when people die



GDPR Regulations Do Not Apply To Deceased Persons

GDPR Citation (27) states;

"(27) This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons."

*An important consideration in law is when the data you hold is your **legitimate interest**. Data is this category does not require consent and the person cannot require its removal.*

General Data Protection Regulations (GDPR)

Applies To

All Affiliated Societies of the Federation regardless of size

Synopsis

Provide an abridged summary of steps to take and outline of the process of using the questionnaire to help with those tasks

A small society with under 10 volunteers should not be spending more than 4 hours in total on these tasks. Very large societies with complex affairs may need to spend more than 100 hours or more.

- decide who is going to be responsible for Data Protection
- ask your committee to approve the appointment and choose the job title



- perform an information audit of systems where personal data is held
 - ◇ club computer facilities
 - ◇ club day to day physical records
 - ◇ club archives
 - ◇ officer and manager computer facilities
 - ◇ officer and manager day to day records
 - ◇ office and manager club archives
 - ◇ previous incumbent's data
- identify the data you share with others, and in which country their computer or records systems reside
 - ◇ privileged sharing with regulatory body's, government departments including police, solicitors, auditors
 - ◇ legitimate interest where to share data

with others in order to perform your functions as a society

- ◇ data requiring consent (we recommend strongly that you do not share data in this category)
- if you conduct business (including website or email service provision) involving transfer of data outside the EU, you must get written contractual agreement to comply with the UK law or more to another supplier
- determine the processing you need to perform (e.g., membership, health and safety, marketing (avoid if possible))



- determine how long you need to keep data after it is last used - examples
 - ◇ 1 year for credit card sales
 - ◇ 100 years for boiler certificates
 - ◇ 8 years for finance
 - ◇ 2 years for critical computer operational logs
 - ◇ 3 months for short term computer operational logs
 - ◇ company statutory register of members must be kept forever
- determine if you need to register with the ICO - most societies should aim to ensure that their affairs do not require them to register
- if you hold more data than is your **legitimate interest** either
 - ◇ destroy it and record that you have done so
 - ◇ obtain **consent** for you to keep it if there is no prior consent, the consent was not properly presented (e.g. opt out box), or the consent was not recorded properly at the time
- if you hold the data in several different systems, decide how you will keep them in synch
- assess your security arrangement for data in all locations identified by the audit
- decide the tools you need to extract data to comply with information requests (noting that you must support electronic response for all data)

General Data Protection Regulations (GDPR)

- if there is request for you to remove or amend data, you must determine how that will be done assuredly across all your system **if you assess the request as being lawfully enforceable**



- establish how you will verify the true identity of

someone requesting data access, track requests and record what responses you gave

- establish your policy documents for how you manage personal data and what you advise people as to your use of their data
- establish your procedures for
 - ◇ controlling the obtaining personal data records and synchronisation of that data across systems - your own and others
 - ◇ the removal of data once no longer required for lawful purpose
 - ◇ handling request for disclosure
- monitor and review on a regular basis (e.g. annually) and ensure the review is approved and documented by your committee

General Data Protection Regulations - Questionnaire Overview

Applies To

All Affiliated Societies of the Federation regardless of size

Synopsis

Introduces the SFMES questionnaire and outlines how you can use it. You should have an initial position within about 15 minutes.

The questionnaire is one means of generating your basic documents. Societies are different and the needs are varied. So you will still need to consider the results you get from the reports generated by the questionnaire as your starter for 10. The larger the society and the more complex its affairs leads to greater need for customisation.

Starting by reference to the results of your information audit, the questionnaire produces:

- Your policy statement
- Your public declaration advising people about the data you handle
- an action plan to progress next steps

According to your log on details we hold, you will be able to work on the questionnaire private to those members of your Society that may log on. We will not share your answers with anyone, but SFMES managers may view your answers for systems support and when you ask for assistance

You have the ability make comment on the sections and these comments are shared with all other people using the questionnaire.

As you respond to the questionnaire, further questions related to your answers will appear. When you have answered all questions the system decides are relevant for you, you can view and export the outputs generated, or just print them directly.

You, and others from your society who can log on, can come back again later and make further changes. In particular you can elect to edit any part of the generated result so it matches the needs of your Society.

Eventually you can confirm a version as approved - thereafter if you continue to make changes the changes will be marked against a new version number.

You may leave the results on the system for ever or delete them at your convenience. If you leave the answers and customisations on the system, please ensure that details are kept up to date. The questionnaire results will be deleted automatically after your society ceases its affiliation with the Federation.

The questionnaire is implemented by an application called **Document Realiser**. The SFMES has provided a document definition within that facility to create the questionnaire and generate the outputs required.

Introduction to managing the General Data Protection Regulations (GDPR)

By Southern Federation Secretary Peter Squire and Martin Baker

Please note this is a direct copy from the website resource for member societies to be found in full at

https://www.sfmes.co.uk/public/?_instant=1524821766664

From the level of correspondence received over the last few months, it is clear that GDPR has been exercising the minds, patience, tolerance and time, of individuals involved with the running of clubs and societies.

Since the December 2017 Newsletter there has been a steady trickle of information (I use the word 'trickle' carefully) from the Information Commissioners Office (ICO) about GDPR, and in particular what it may mean to medium, small and micro businesses. I have lost count of the number of phone calls that I have made to the ICO Helpline, to be told "watch our website for information about that" The GDPR is clearly aimed at business who process data for sales and marketing purposes. We have all read of recent breaches in data security, and the implications it has had on some individuals.

Here we are now less than a month away from implementation, and the ICO has not finalised the exemptions for small and recreational organisations, such as village hall committees, bowls' and cricket clubs.

The ICO Working Party 29 is, at the time of writing this, still deliberating about medium, small and micro businesses and the guidance we can offer at this time is our estimate of what is reasonable until the recommendations of WP29 are adopted and published.

Currently the ICO website states;

Please note

The Article 29 Working Party (WP29) is currently considering the scope of the exemption from documentation of processing activities for small and medium-sized organisations.

WP29 includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

If necessary, we will update this guidance to reflect the outcome of WP29's discussions.

In the December newsletter, I stated,

"You should start by appointing a Data Protection Officer (DPO), which does not have to be a

committee post but should at least have a designated report to a committee member."

This attracted a fair amount of criticism at the time from over burdened committees who were already finding it difficult to find someone to help run the club. It was at that time the best information available, but this is an area where the ICO statements have become clearer.

*Under the GDPR, you **must** appoint a DPO if:*

- you are a public authority (except for courts acting in their judicial capacity);*
- your core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking); or*
- your core activities consist of large scale processing of special categories of data or data relating to criminal convictions and offences.*

This applies to both controllers and processors. You can appoint a DPO if you wish, even if you aren't required to. If you decide to voluntarily appoint a DPO you should be aware that the same requirements of the position and tasks apply had the appointment been mandatory.

There are therefore cases where a formally appointed DPO is required by law, but this will not apply to most affiliated societies. SFMES recommends you identify someone as responsible for producing a data protection policy, but also recommends that you avoid calling the person responsible your 'DPO' as the term may under certain circumstances carry with it a presumption of higher duty, authority and accountability. You may consider using the title Data Protection Compliance Leader which is more appropriate to the skills and authorities in a model engineering society.

As with Child Protection, Safeguarding and Health and Safety, new laws have given rise to people establishing overzealous interpretations and hence overzealous and onerous guidance and piles of paperwork. Using the ICO website to determine the data protection requirements for a small organisation will lead to many hours of work, and a pile of un-necessary paperwork. Unfortunately there is no 'one size fits all' process or statement that can be universally applied across model engineering

Introduction to managing the General Data Protection Regulations (GDPR) cont'd

clubs and societies.

The following outlines the major measures required **by law** and identifies relaxations often omitted from ICO headlines and other commercial documentation, that will ease the burden on affiliated Societies.

The ICO has not finalised the exemptions for small organisations such as our Affiliates. So the following guidance is our estimate of what is reasonable until the recommendations of their working group WP29 is adopted.

Caveat

The following is aimed at Societies undertaking Model Engineering as a hobby activity and does not cover activities outside that scope.

Background

The guidance within this section is drawn from GDPR Articles 30 and 32 and from the ICO. These contain important relaxations relevant to model engineering societies often not found in headline documentation issued by the ICO and others.

If you make use of these relaxations, you must ensure that they really apply to you and that means apart from anything else, reading and understanding this lot and making sure it applies to your Society.

Who needs to document their processing activities? [GDPR Article 30]

There are two important watersheds in Article 30, when you have less than 250 employees (most Societies) and when you have less than 9 (a few Societies)

Unless you have more than 250 employees you do not have to keep records of processing or the data you control.

If you have less than 250 employees, you only need to document processing activities that:

- are not occasional; or
- could result in a risk to the rights and freedoms of individuals; or
- involve the processing of special categories of data or criminal conviction and offence data.

Although there is no lawful basis to do so in the context of most of our affiliated societies, the ICO provides general advice nonetheless where certain data is kept. The Federation considers the following as a guideline for small societies and a recommendation for larger societies, those that

keep their data on third party systems such as the internet or who have credit/debit card payment services

- who manages your data protection activities
- what you keep and use it for (typically for the purposes of administering your membership, finances and health and safety)
- your policy including access rights and for how long different data is kept
- where or who keeps / processes your data
- your security measures including breach detection and handling

Note that records of consent are only required if your use of data is in a class of activity that requires consent - such as marketing and then that consent only has to be given by those to whom you market. Most Societies will be able to position their activities so they do not need to ask for consent.

Where a Society undertakes any activities for which there are more controls, documentation is likely to be obligatory; and the measures needed to be taken are more complex (and beyond the scope of our recommendations). Some of these categories include

- marketing
- automated decisions (including writing off members who do not pay their subscriptions - but an automated system can ask a human if it is OK to proceed)
- exchange of data to organisations in the UK or elsewhere within Europe that is not part of your normal trading business of contacting each other
- exchange of data outside of the EU (including use of websites hosted outside the EU)
- about sex offenders and people with other criminal records

Security Measures [GDPR Article 32]

The law requires you and your data processors to implement appropriate technical and organisational measures to ensure a level of security.

Noting that affiliated Societies are small and with limited financial resources, the law does not oblige you to have state of the art security measures. You may take into account the following in deciding what to do.

- costs in relation to your level of turnover and

Introduction to managing the General Data Protection Regulations (GDPR) cont'd

available funds

- the use to which you are putting the data
- the likely risk to the data subjects if there were a security breach
- the extent to which the data is already in the public domain (such as electoral registers)

There are some base obligations that will be seen to apply everywhere

- you need to control access to the data to a sufficient level that you know if a breach has occurred.
- The means that this security at the least is achieved by passwords for electronic systems or by numbered or otherwise controlled keys that are not readily copied for physical copy

This means for paper and other physical filing; that the data must be under appropriate lock and key (the key can be electronic or physical). If data of different classes is available under the same lock and key, some other measure (such as prominent labelling) is used to minimise accidental inappropriate access.

For electronic data, that a password of a reasonable strength is required distinct for each individual in order to access the data - the consequences of which are.

- every computer, including those at home of your members used for Society data, with must have a password of reasonable strength to gain access to it - you cannot just open up the machine and use it - this includes mobiles if data is stored on them such as in a phone directory
- computer systems must have a log on system with timeout, and must not transmit any password in plain text over external communications such as the internet

The law does not mandate that your website has to use any encryption standard - and for many Societies the need is not substantive. That said, the general trend in expectations (not the law) is that websites with personal data should use the https:// secure protocol and have appropriate controls for upload, download and backup.

If you do not use a website and share data, then if you use email to send files between each other then you must verify that the email transmission is secure end to end - and for the lay person that is easier

said than done - or use a tool to encrypt the file. Special consideration needs to be taken for memory sticks and removable hard disks which must be secure, either by means of technology or by strict procedures to keep them under lock and key.

Information Audit

This means you need to understand what you are doing in relation to personal data. Only once you understand what you are doing are you then able to ensure that the policies and procedures you put in place are appropriate

We provide you with two spreadsheets for recording your audit which are based on ones provided by the ICO, you should be able to open then in Excel or Open Office. These both are pre-filled in as a starting point for a typical Society. These have been simplified to span only those matters likely to be relevant to a Society; you may find that you can use them as they stand. If you are unsure about these simplifications then please refer to the IC website and use their originals.

Remember that the scope of the audit covers

- paper based files at your society
- paper based files at your members' homes - and every such member has to be recorded individually !!!!
- society computers
- third party computers and websites
- members personal computers that hold society information including contact lists
- backups
- development systems

Before documenting the result of your information audit, assess whether it may be simpler in some cases to cease past practices of allowing members to keep their own records of your business data.

Policy Documents

You should prepare the following directly yourself or by using the **questionnaire** available from the left menu:

- an internal statement of your policy including procedures and review intervals/criteria
- a declaration you may give to people saying to them what data you will keep
- a plan of action to ensure transition to compliance and to keep it that way

Introduction to managing the General Data Protection Regulations (GDPR) cont'd

Our Questionnaire

An option for you is to use our questionnaire online. Very quickly it will provide a good start for smaller societies to the basic documentation you need to have.

The questionnaire will ask about matters determined from your information audit. That is something you have to do but we have pre-populated the audit registers templates available on the web with some standard entries. It is down to you to do the rest.

Once complete, you can generate your policy statement, the data subject declaration and the plan of action tailored to the answers you give.

You can also share, forum style, comments with other people about parts of the questionnaire and you can modify the generated outputs to vary wording or cover additional circumstances.

These outputs can be downloaded in html format. That format will open in Microsoft Word, Open Office etc, or used directly in your own website.

Society officers are the only people who can edit or see the questionnaire for their Society. If your data protection lead manager is not already an officer on the website, then with their consent you can add them to the list of officers so they can perform the task themselves.

You will find the Data Protection section of the website within **Understanding the Law** from the left menu at <https://www.sfmes.co.uk> You have to be logged on to see this section.

Peter Squire, Secretary

Martin Baker, IT Manager & Treasurer

SOUTHERN FEDERATION MES COMMITTEE

Chairman	Bob Polley
Vice Chairman	Mike Chrisp
Secretary	Peter Squire
Treasurer & IT Manager	Martin Baker
Membership Secretary	David Goyder
Boiler Registrar	David Mayall
Safety Officer	Robert Walker
Newsletter Editor	David Goyder
Member	Paul Naylor
Events and Awards	Mike Chrisp
President	Brent Hudson
Vice President	Ivan Hurst

INSURANCE CLAIMS AND INCIDENTS

All claims and reports of incidents should be notified in the first instance to Walker Midgley.

FEDERATION INSURANCE BUSINESS Managed by Walker Midgley Insurance Ltd

www.sfmes.co.uk