What is GDPR and how does it impact my flower club?

*Please note the following is a high level summary of the basic requirements and implications and does not try to consider every possible scenario therefore you should read the official guidance to ensure you are fully compliant. Most of the following is common sense and you are probably doing most of it already.*

Please note if your Flower Club is a registered charity or has junior members these bring further requirements not covered below.

The General Data Protection Regulation (GDPR) relates to Data Protection and comes into force from 25 May 2018 and brings with it various legal requirements that you must comply with.

To help understand this the following is a list of definitions which you should read to fully understand the following guidance as this may not be what you think.

**Personal Data** – This is any information which directly relates to an individual, ie name, phone number, email address, photograph etc. This is not just digital information but all personal information including that which is recorded or stored in paper format.

**Processing** – this refers to the collection, storing and transferring of data and includes simply accessing the data, electronically or in paper format.

**Data Controller** – This is the person within an organisation that decides what data is collected, what it is used for and who it is shared with. In the case of a Flower Club the Club itself can fulfil this role.

**Data Processor** – Is anyone who processes data on the instruction of the Data Controller.

The GDPR details the procedures that are required by law and your organisation needs to be compliant to avoid breaches that could lead to fines or compensation claims made by those individuals affected. It is essential you follow best practice in terms of the following:

* How you gather information
* How securely you store information
* How you comply with requests for the information you hold
* How you can evidence the above in the event of an audit

In reality you will already do most of this and it is just a question of documenting what you already do.

**GDPR has six principles for the processing (collecting, storing and accessing) of data:**

1. It must be processed fairly, lawfully and transparently – individuals have the right to know what is being gathered and have it corrected or removed. For example a club member can request to see what data you hold, have it corrected if necessary or ask for it to be removed.
2. You should only use data for legitimated purposes specified at the time of collection and this should not be shared with third parties without permission. For example personal data held on club mailing lists to notify members about club events, membership renewal etc, should not be shared with any other club or organisation without permission from all involved.
3. Data should be limited only to what is required for the stated purpose. Usually this would be limited to name, address, telephone number and email address.
4. The personal data you hold should be accurate, kept up to date and if no longer accurate should be rectified. For example membership lists should be updated every year or when members advise of changes.
5. Personal data should only be stored for as long as it is necessary. Individuals not renewing their membership should be removed from the current list. Prior year lists should be retained for as long as stated in your privacy statement and then deleted if in electronic format or shredded if in paper format.
6. Personal data should be held in a safe and secure manner. Electronic data should be held on a password protected computer and documents password protected when emailing. Paper documents should also be held securely.

**Privacy Notice / Statement**

This should be a clear and simple statement that is available at the time an individual gives their consent to share personal data with you. At the point you collect personal data you are required to provide a Privacy Notice / Statement covering:

* The identity of the Data Controller *– ie* *the flower club*
* The purpose of collection –  *ie* *to notify members of future events, membership renewal etc*
* Confirmation you will not be sharing the data with third parties
* How long the data will be held – *ie until a request is received to have removed and for as long as considered necessary*
* Individuals rights to see what data you hold *– ie details of who to contact*
* Individuals rights to opt-out and have their data removed – *ie who to contact and confirmation data will be removed within a month of receiving the request*
* Details of consent by way of legitimate interests if formal consent is not obtained (see Consent section below)

An example of a Privacy Notice / Statement is attached as Appendix 4.

**Consent**

Legitimate interests is the most flexible lawful basis of obtaining consent, but you cannot assume it will always be appropriate for all of your processing. If you choose to rely on legitimate interests, you take on extra responsibility for ensuring people’s rights and interests are fully considered and protected.

Legitimate interests is most likely to be an appropriate basis where you use data in ways that people would reasonably expect and that have a minimal privacy impact.

You should avoid using legitimate interests if you are using personal data in ways people do not understand and would not reasonably expect, or if you think some people would object if you explained it to them.

If you want to rely on legitimate interests, you can use the three-part test below to assess whether it applies to you. This is referred to this as a legitimate interests assessment (LIA) and you should do it before you start the processing after 25 May 2018.

An LIA is a type of light-touch risk assessment based on the specific context and circumstances. It will help you ensure that your processing is lawful. Recording your LIA will also help you demonstrate compliance in line with your accountability obligations under GDPR. In most cases an LIA will be quite short, but in others there will be more to consider.

First, identify the legitimate interest(s). Consider:

* Why do you want to process the data – what are you trying to achieve?
* Who benefits from the processing? In what way?
* Are there any wider public benefits to the processing?
* How important are those benefits?
* What would the impact be if you couldn’t go ahead?
* Would your use of the data be unethical or unlawful in any way?

Second, apply the necessity test. Consider:

* Does this processing actually help to further that interest?
* Is it a reasonable way to go about it?
* Is there another less intrusive way to achieve the same result?

Third, do a balancing test. Consider the impact of your processing and whether this overrides the interest you have identified. You might find it helpful to think about the following:

* What is the nature of your relationship with the individual?
* Is any of the data particularly sensitive or private?
* Would people expect you to use their data in this way?
* Are you happy to explain it to them?
* Are some people likely to object or find it intrusive?
* What is the possible impact on the individual?
* How big an impact might it have on them?
* Are you processing children’s data?
* Are any of the individuals vulnerable in any other way?
* Can you adopt any safeguards to minimise the impact?
* Can you offer an opt-out?

You then need to make a decision about whether you still think legitimate interests is an appropriate basis. There’s no foolproof formula for the outcome of the balancing test – but you must be confident that your legitimate interests are not overridden by any risks you have identified.

Keep a record of your LIA and the outcome. There is no standard format for this, but it’s important to record your thinking to help show you have proper decision-making processes in place and to justify the outcome, the checklist in Appendix 2 may help.

Keep your LIA under review and refresh it if there is a significant change in the purpose, nature or context of the processing. You must tell people in your Privacy Notice / Statement that you are relying on legitimate interests, and explain what these interests are.

If you want to process the personal data for a new purpose, you may be able to continue processing under legitimate interests as long as your new purpose is compatible with your original purpose. You should consider conducting a new LIA, as this will help you demonstrate compatibility.

If you do not want to rely on legitimate interests then you need to obtain formal consent an example consent form is attached as Appendix 3.

**Registration**

You do not have to register if your organisation was established for not-for-profit making purposes and does not make a profit or if your organisation makes a profit for its own purposes, as long as the profit is not used to enrich others. You must:

* only process information necessary to establish or maintain membership or support
* only process information necessary to provide or administer activities for people who are members of the organisation
* only share the information with people and organisations necessary to carry out the organisation’s activities.
* only keep the information while the individual is a member or supporter or as long as necessary for member/supporter administration

You should document your compliance with the above. See appendix 5 for a simple checklist.

GDPR brings additional requirements ie if you have junior members then the above exemption may not apply. If you have your own CCTV then this exemption does not apply.

**Photography**

Images of people are considered personal data so photographing and filming at events may sometimes fall under “legitimate interests” noted above but in some cases you may need active consent from the individuals concerned to store, use or share these images.

**So what do you actually need to do:**

You must be able to demonstrate compliance.

* In most cases the Data Controller will be your Flower Club and members of your committee will be Data Processors if they collect, store or access personal data of the members either electronically or in paper format. You must identify anyone who should be included as a Data Processor..
* Understand and document what data you hold, in what format and how this is stored, when it is updated and when it is required to be destroyed – see Appendix 1 for an example document to comply with this requirement.
* You need to have a Privacy Notice / Statement which must be available when members give their personal data – see Appendix 4 for a Privacy Notice / Statement template.
* Carry out a legitimate interests assessment (see Appendix 2 for a simple checklist), once completed document your conclusion that the exemption applies. If the conclusion is the exemption does not apply you need to ensure that appropriate consents are obtained. Even if the exemption does apply you may want to obtain formal consent (see Appendix 3 for an example consent form).
* Ensure that emails are sent out as blind copies (bcc option). Failure to do so will be a breach for every email address included and members could make a complaint to the Information Commissioner’s Office.
* If you email newsletters to members all of your emails must be blind copies and include an opt-out or unsubscribe option.
* Consider if the not for profit exemption for registration applies and document your conclusion (see Appendix 5 for a simple checklist. If the exemption does not apply you must register each year and pay the appropriate fee.

**Appendix 1 - Personal Data Held**

In order to comply with GDPR, the committee of [insert name of Flower Club] need to know what personal data they hold, where they get it from and how they use it. Below is a list of questions used to identify the personal data which is being processed by the flower club. We have reviewed all databases, spreadsheets, email lists, paper documents and any other form of list or documentation which contains personal data.

*Personal data is any information that can either directly or indirectly identify a living individual*

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Document/list description** | **For what purpose is the data held?** | **What data is collected?** | **Do you have explicit consent to use the data?** | **How is the data held and what security measures are in place?** | **Who holds the data and who has access to it?** | **How long is the data kept for?** | **How is the data destroyed?** | **Is any data kept by or circulated to persons outside of the Flower Club** |
| *Club membership list* | *To provide a list of club members to enable the club to contact members regarding club activities* | *Names, addresses, email addresses, telephone numbers* | *Yes / No* | *Data Collection consent form (locked filing cabinet) and*  *Club Secretary’s Laptop (password protected)* | *Club committee* | *Until asked to be removed* | *Paper shredder and electronic deletion from laptop* | *No* |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

**Appendix 2 – Legitimate Interests Assessment**

☐ We have checked that legitimate interests is the most appropriate basis.

☐ We understand our responsibility to protect the individual’s interests.

☐ We have conducted a legitimate interests assessment (LIA) and kept a record of it, to ensure that we can justify our decision.

☐ We have identified the relevant legitimate interests.

☐  We have checked that the processing is necessary and there is no less intrusive way to achieve the same result.

☐ We have done a balancing test, and are confident that the individual’s interests do not override those legitimate interests.

☐ We only use individuals’ data in ways they would reasonably expect, unless we have a very good reason.

☐ We are not using people’s data in ways they would find intrusive or which could cause them harm, unless we have a very good reason.

☐ If we process children’s data, we take extra care to make sure we protect their interests.

☐ We have considered safeguards to reduce the impact where possible.

☐ We have considered whether we can offer an opt out.

☐ We keep our LIA under review, and repeat it if circumstances change.

☐ We include information about our legitimate interests in our Privacy Notice / Statement.

**Conclusion**

Based on the above assessment the legitimate interests requirements are met.

**Appendix 3 - Consent Form to Collect & Use Personal Information**

Under the General Data Protection Regulation (‘GDPR’) there are occasions when **[insert name of Flower Club]** must obtain your explicit consent to use your information, known as ‘Personal Data’. Personal Data includes, but is not limited to your name, address, telephone number and email address.

**[insert name of Flower Club]** would like to hold and use your information for the purposes set out below:

Please tick all relevant boxes to indicate your consent. You may consent to all of the purposes, any number of the purposes or none of the purposes. If you do not consent to **[insert name of flower Club]** using your information for the purposes listed below then we will not contact you.

**🞎** To include my contact detailsin the **[insert name of Flower Club]** membership list. The membership list is circulated to committee members of the **[insert name of Flower Club]**;

**🞎** To keep me informed of news, activities and events at **[insert name of Flower Club]**;

**🞎** To contact me with regards to specific events by **[insert name of Flower Club]**;

**🞎** [add any other use]

**[insert name of Flower Club]** will not share this data with any third parties.

I consent to **[insert name of Flower Club]** contacting me for the above purposes by:

**🞎** Post **🞎**email **🞎**phone **🞎**SMS **🞎**social media including Facebook, Twitter

Please complete your details below:

Name:

Address:

Email Address:

Phone Number:

Signature:

Date:

You can change your consent preferences or withdraw your consent completely by contacting **[insert details of who to contact, ie club secretary]**. The use of your information will cease within a month of the club receiving notification.

For full details of how **[insert name of Flower Club]** uses your information, please refer to our Privacy Statement which is available from **[Name, Address and Email Address of relevant officer]** [*if this is available on a Flower Club website, then please provide details].*

**Appendix 4 – Privacy Notice / Statement**

**1. Background**

This Privacy Notice / Statement lets you know what happens to any personal data that you give to us. This privacy notice applies to personal information processed by ……………………… Flower Club.

……………Flower Club is the Data Controller and the Committee are the Data Processors.

**Changes to this privacy notice**

We may change this privacy notice from time to time by updating this page in order to reflect changes in the law and/or our privacy practices. We encourage you to check this privacy notice for changes whenever you visit our website – https://www.

**2. What kinds of personal information about you do we process?**

Personal information that we’ll process, if relevant, includes: Personal such as title and name

* Contact details, such as address, email address and phone number

If we organise a club outing we may request all or some of the following data on the application form depending on the specific requirements of the outing:

* Your date of birth, gender and/or age
* Your nationality and passport details
* Details of your emergency contact
* Dietary requirements
* Mobility issues if accommodation is being booked

**3. What is the source of your personal information?**

We’ll collect personal information from you directly

**4. What do we use your personal data for?**

We use your personal data, including any of the personal data listed in section 1 above, for the following purposes:

* To maintain a membership list which will be used to
* Update you on club activities
* Send out membership renewal forms, nomination to the committee forms, AGM minutes and agenda
* Meeting attendance list for fire precaution purposes
* To comply with legal and regulatory obligations, requirements and guidance

**5. What are the legal grounds for our processing of your personal information (including when we share it with others)?**

We rely on the following legal basis to use your personal data:

1. Where **it is in our legitimate interests to do so**, such as:
   1. Managing our contact with you, updating your records to ensure our information is accurate and up to date
   2. Maintaining membership lists and attendance lists at club meetings for fire precaution purposes
   3. Advising you of club events and activities
   4. For any other matters directly related to the club’s activities
2. With your **explicit consent** when and if required

**6. When do we share your personal information with other organisations?**

We do share your personal information with any third parties.

**7. How and when can you withdraw your consent?**

Where we’re relying upon your consent to process personal data, you can withdraw this at any time by contacting us using the details below.

**8. What should you do if your personal information changes?**

You should tell us so that we can update our records.

**9. Do you have to provide your personal information to us?**

We’re unable to provide you with details of our activities if you do not provide certain information to us.

**10. For how long is your personal information retained by us?**

Unless we explain otherwise to you, we’ll hold your personal information based on the following criteria:

* For as long as we have reasonable business needs, such as managing our relationship with you and managing our activities
* For club outings we retain the information until the event has taken place.
* Retention periods in line with legal and regulatory requirements or guidance.

**11. What are your rights under data protection laws?**

Here is a list of the rights that all individuals have under data protection laws. They don’t apply in all circumstances.

* The right **to be informed** about the processing of your personal information
* The right to have your personal information **corrected if it is inaccurate** and to have **incomplete personal information completed**
* The right **to object** to processing of your personal information
* The right **to restrict processing** of your personal information
* The right **to have your personal information erased** (the “right to be forgotten”)
* The right to **request access** to your personal information and to obtain information about how we process it

Any breaches will be notified to Information Commissioner’s Office within 72 hours.

You have the right to complain to the Information Commissioner’s Office which enforces data protection laws: https://ico.org.uk.

**Contact Us**

If you have any questions about this privacy notice, or if you wish to exercise your rights you can contact us by contacting ……………………….

**Appendix 5 – Not for Profit Registration Exemption**

☐ We have checked that the club was established for not-for-profit making purposes

☐ We have checked it does not make a profit or if it makes a profit it is for its own purposes

☐ We have checked that any profit is not used to enrich others

☐ We have checked that we only process information necessary to establish or maintain membership or support

☐ We have checked that we only share the information with people and organisations necessary to carry out the organisation’s activities.

☐ We have checked that we only keep the information while the individual is a member or supporter or as long as necessary for member/supporter administration

☐ We have checked that we do not operate CCTV

**Conclusion**

Based on the above assessment the not for profit registration exemption applies.