The Federation of Astronomical Societies

General Data Protection Regulation (GDPR) for Astronomical Societies

Version 2.1

3rd February 2020

Document History

Date	Author(s)	Version	Comments
03-Feb-2020	Paul Daniels	2.1	A small typo correction, one small clarification, removal of parentheses from '(GDPR)' in the header and repair of the automatic date fields in the title box and header.
05-Jan-2020	Graham Bryant	2.0	Updated as post GDPS Implementation
23-Apr-2018	Graham Bryant	1.0	Document released to membership
22-Apr-2018	Paul Daniels	0.2	Documents combined and re-formatted
20-Apr-2018	Graham Bryant/ Philip Johns	0.1	Document Created

Contents

1 Introduction

On the 25th May 2018 all organisations resident and operating in Europe that collect and handle (process) personal data adopted the European General Data Protection Regulation (GDPR). Brexit will not stop or reverse the introduction of this legislation.

The GDPR regulations in their original form are vast and complex in nature. The Information Commissioners Office (ICO) has distilled those regulations into a more digestible format. Their guidelines naturally cover all forms of organisations with a variety of responsibilities both statutory and voluntary.

Many websites purporting to offer assistance to organisations can make GDPR appear daunting, complex and often worrying readers into seeking outside help with their GDPR compliance. One should not lose sight of the fact that many of these sites are selling their services, so hyping up the concerns would be part of their marketing strategy.

The guidance issued here by the Federation of Astronomical Societies is intended as an additional introductory guide only and is based on our understanding of how many astronomical societies operate. Consequently a number of aspects of the GDPR have been omitted where we consider that it has little or no relevance to the way an astronomical society operates.

For a full and detailed understanding and an outline of your legal responsibilities you must consult the ICO website or seek appropriate legal advice. A quick internet search will bring up a plethora of organisations willing to assist you but, as noted above, for a fee.

However, there is a significant amount of additional information on the Information Commissioner Office (ICO) website which should be accessed to gain a deeper understanding of GDPR[1].

The ICO is urging organisations to take a common sense approach when implementing GDPR. One of the overarching guiding principles of GDPR is openness with data subjects and their data. Openness with what you collect about individuals, openness with how you process that information and how long you keep the information and so on. Keep this in mind when implementing GDPR.

2 Background

All astronomical societies that have collected information regarding their members have always been subject to some form of Data Protection Act. GDPR strengthens the rights of the data subject. Under GDPR regulations that person, the data subject (your member) is described as a ‘natural person’.

Previously under the Data Protection Act you would have made sure that personal information was:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with your rights
- Secure
- Not transferred to other countries without adequate protection

If your society was already adhering to those Data Protection Act principles you will not be too far from being compliant with GDPR.

There are, however, some additional data subject rights within the GDPR that you need to demonstrate compliance.

3 Additional personal rights

The GDPR provides the following eight additional rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

4 Lawful basis

The GDPR states there must be a lawful reason for obtaining and processing personal data.

There are six available lawful bases for processing. No single basis is 'better' or more important than the others. Whichever basis is most appropriate for an astronomical society to use will depend on your purpose and relationship with the individual.

We have outlined all of the lawful bases for collecting data here:

- Consent
- Contract
- Legal Obligation
- Vital Interests
- Public task
- Legitimate interests

Most likely an astronomical society will obtain and process data under the heading of '**contract'**. This is the lawful basis upon which an astronomical society will obtain and process data.

When a person becomes a member of the society, it is likely they will pay a membership fee and in return they will receive services such as lectures, meetings, access to observing evenings, *etc*, *etc*. This is the '**contract**' a society will have with its member and the lawful basis upon which it obtains and processes its members' personal data.

The 'processing' that a society undertakes with their members' data is likely to be in the form of making a membership list, or some other list to organise observing events, *etc*, or in giving access to a members' area of the society's website.

If your astronomical society is a Charity and if your member is a UK taxpayer, you may wish to collect gift aid from HMRC. In these circumstances you have an additional '**legal obligation'** to provide and process personal data to HMRC when collecting that gift aid.

If there has been some criminal activity then you are obliged to cooperate with the police or other law enforcement agency. In these circumstances you may have a '**legal obligation'** to provide personal data. Some societies have involvement with vulnerable persons (adults and children). In these circumstances a few astronomical society members may wish to volunteer to help out with observing or some other activity with those vulnerable persons. In some circumstances members may be subject to a DBS check if they wish to volunteer for this type of activity. In these situations those members must give their '**consent**' for the DBS check to take place.

Unless your society's primary objective is to work with vulnerable groups of people, a member's failure to give consent in this circumstance cannot bar them from being a member of your astronomical society; failure to give consent simply means they cannot work with vulnerable people in an unsupervised manner.

5 Collecting data

It is worth considering what data your astronomical society collects from its members. Good practice will dictate that a society will collect the minimum required to provide the services it offers to members. For example, do you need to collect dates of birth? Many societies have junior rates or senior citizen rates for membership fees. A society could accept self-disclosure with the member simply stating to the astronomical society upon joining: "I am over/under XX age".

Astronomical societies should not need to collect what is considered 'sensitive data' such as ethnic origin, health status, religion, sexual orientation. There is a complete list of what is considered sensitive data on the ICO's website.

A member may volunteer ('**consent'**) some health information to you indicating they have diabetes or epilepsy, *etc*. They may do this confidentially for what they consider to be their own safety. Consider who needs to know this information and discuss with the member who they would like to have this information shared with (if at all) and how it might be recorded. *Take the common sense approach*.

Some societies may collect personal information about visitors to their meetings or observing sessions. This may include a name, and other contact details. Some societies may wish to retain this data for a short period until the event occurs or, if there has been an accident at an observing session with a member of the public, kept for a longer period. Astronomical societies should consider how long this personal information on its visitors needs to be held. Erasure at the earliest possible opportunity would be best practice.

6 Children

If you have members who are children you should be aware that they have the same rights as adults. You should also be aware that children may be less understanding of the risks regarding sharing personal data and you may need to be vigilant regarding this aspect. If you collect data by means of a 'contract' with them you need to ensure that the child understands what information they are agreeing to provide about themselves. A child aged 13 years or over can give their consent. For children under this age their legal guardian must be consulted.

7 Data erasure

The GDPR allows for data erasure or what is now being described as the 'right to be forgotten'. Unless there is a compelling reason to retain a past member's data – such as ongoing litigation or they still possess some loaned society equipment that you are trying to recover, *etc*, then the astronomical society must remove that person's data.

It is good practice to ensure all past members' data is removed once they cease to become a member of your astronomical society.

8 Society members' rights

GDPR strengthens an astronomical society member's right to know what data the society holds about them, to know what processing takes place with their personal data, to know how long that data is held, to check on its accuracy and, if wished, withdraw their consent for the society to process their data.

Society members can request that the astronomical society restrict the processing of that data. However, in practical terms, most astronomical societies will be processing the data in a rather benign manner – such as creating a membership list. However, one must be alive to the fact that some aspect of their member's personal data could become sensitive and not offered.

Such sensitive personal data might be that the address and/or contact details has changed and the member does not want those contact details known – an example might be a vulnerable female member. This should not cause an astronomical society a problem and must be accommodated. *Take a common sense approach.* One can easily see how in such circumstances the need for good data security (in both physical and human

procedures) is paramount.

When a data subject (astronomical society member) makes a data request this must be acknowledged and the requested information provided within 1 calendar month. You cannot make a charge for providing this data unless their requests are unreasonably frequent or unreasonable in the detail they ask for. ICO guidance could be sought in such circumstances.

9 Data Security

Just as with the previous Data Protection Act, the GDPR expects anyone/organisation holding personal data to do in a secure manner. Astronomical societies holding personal data on electronic devices must insist that those devices are password protected and any portable device is encrypted.

Paper copies of data must also be held securely in locked cabinets in locked rooms/buildings. Astronomical societies should consider the most secure manner of destroying such paper copies when there is no longer a need to hold this data. Shredders are useful, especially those that 'cross shred'. Placing un-shredded paper copies containing personal data in the dustbin runs the risk of data breaches and must be avoided at all costs.

Once again the basic premise on holding data, is only hold the absolute minimum and for as short a period as practicable.

10 Data Breach

Data breaches could be any of the following examples – this list is not exhaustive but illustrates to astronomical societies the variety of ways in which data breaches could occur:

- Data stolen from a laptop or similar electronic device
- Data given to a person or organisation when the person or organisation has no right to the data – this could be given unintentionally or maliciously. *This could include situations where e-mail has been sent and the sender 'copied all' rather than use the 'blind copy' facility – e-mail addresses are personal data and you have a responsibility not to share an address amongst all society members*
- Data lost – *such as a membership print out or memory stick and left on a train or meeting hall* etc.
- Data intercepted during electronic transfer (internet)
- Data erroneously deleted - *where there was no back-up copy and the astronomical society now needs to collect the data from its members once again (astronomical societies have a duty to hold their members' data securely)*

Data breaches must be reported to the ICO immediately and certainly within 72 hours. The astronomical society is under an obligation to investigate the breach and report findings within 28 days to the members affected and the ICO.

In the UK, the Information Commissioner has, to date, regulated with a 'light touch' and fines for breaches have been considered modest, up to £500k. Whilst the Information Commissioner has stated they wish to take a helpful stance in the early stages of GDPR implementation, they have indicated that they will be issuing significantly heavier fines in the future, up to €10m, for breaches of data and especially where that data is of a sensitive nature.

It is often the case within astronomical societies that certain members – often committee members – will have access to personal data and may keep such data on password protected laptops. Societies should consider local procedures for access to, or the destruction of, the data in the event of that committee member no longer holding the committee position or if they should die and the laptop passes into the hands of their executor.

11 Data Protection Officers

Many astronomical societies will have an elected governing body such as Committee, Trustees or a Council. Within such bodies there will be assigned duties such as Secretary, Treasurer, *etc*. Under GDPR, astronomical societies should consider appointing a Data Protection Officer (DPO) whose remit is to manage overall data protection and the GDPR compliance on behalf of their society. It is often useful to have a deputy in the event of the DPO being absent for whatever reason.

The DPO would be the member of the astronomical society who 'oversees' the data collection processes and processing and ensures that the astronomical society and its governing body (a committee) is complying with the regulations.

The DPO could also be the person who is contacted when there is a data subject request from within the society's membership or from people outside of the society. They must be easily contactable (often through the society's website).

12 Communication with society members

Astronomical societies should write to (not e-mail) their members and gain their consent to communicate with them. Some society members may have already received such communication in the post from national organisations. With new members this would be undertaken at the point of joining the astronomical society.

A number of societies that have begun to implement GDPR have already written individually to their members outlining the data the society holds about them and asking whether the data is correct. This ensures the current data is accurate. Within that letter, some societies have included an 'opt in' tick box requesting the right for the astronomical society to continue to make contact with its members *via* various channels of communication. Such communication channel examples may be e-mail, social media (*e.g.* Facebook), letter, text, *etc*. In such cases, multiple boxes have been used so their members may choose a number of methods of communication. An astronomical society only needs to offer methods of communication that it is able/willing to use.

In gaining consent, astronomical societies cannot resort to 'default opt in' positions with their members and assume a member will be included unless they select an 'opt out' box. This is strictly forbidden under GDPR guidance.

The returned letter can be held on file as a confirmation of the current accuracy of data and the society member's consent on how they wish the astronomical society to communicate with them.

Some societies within this process have also included a short form indicating what happens to members' data, where it is held, what processing the society does with the personal data and how long such data is retained. Again this is good practice and can be considered as given in the spirit of openness with the society's members. Additionally, this allows society members to challenge aspects of the society's practices when holding its members' personal data.

13 Data Privacy Statements

Astronomical societies are strongly urged to consider putting on their website a Data Privacy statement.

Such statements often state that the astronomical society is careful with personal data, conforms to current data legislation and, what appears frequently with such statements, the fact that the society does not give, pass or sell personal data to third parties.

Within the Data Privacy statement there should be a link to the society's Data Protection Officer where a data subject request can be made. Astronomical societies may find it useful that such requests are automatically sent *via* the website to two people in case the DPO is unavailable for a period of time (holidays *etc*.). If automated links are not possible then an address must be posted.

14 FAQs on GDPR for Astronomical Societies

Do astronomical societies have to adopt the GDPR?
The short answer is YES. All organisations that handle personal data have to be compliant with these regulations.

We are considering ignoring the GDPR and do nothing – what are the consequences?
The regulations state that organisations must be compliant if they hold personal data. If a society chooses to ignore their responsibilities they run the risk that they could be fined if there is a data breach or do not respond to a data subject request.

In a recent poll, 70% of respondents stated they are quite likely to make a data subject request at some point in the future. The consequence for an unincorporated association (which the majority of societies are in the UK) is that the responsibility for paying the fine will be the committee AND the entire membership.

We are a new society and will struggle to complete this immediately - will that be a problem?
The Information Commissioners Office (ICO) has stated that they are aware there will be some delays for some organisations and that those organisations may need more time. The ICO will expect all organisations that need to be compliant to work towards being compliant as soon as possible.

We have read that organisations need to appoint a Data Controller and a Data Processor, this seems excessive for an astronomical society, do we need both?
Guidance given to the FAS is that small organisations such as astronomical societies will only need to appoint a Data Protection Officer - that role will cover both functions. A Data Controller is someone who states what information needs to be collected and processed, the Data Processor does the processing – these are generally designed for large organisations handling a lot of personal and/or especially sensitive data. In practice the society's committee will decide both aspects and the Data Protection Officer over-sees the activity.

What is meant by 'personal data', we only collect the name and contact details of our members, is that personal data?
Any information that can be used to identify an individual is 'personal data'. So a name and address will identify someone, as can a phone number or e-mail address so both are also considered personal data.

When the earlier data protection acts were drafted in the latter part of the 20th Century, the internet was not so widespread and pervasive. The implication of having access only to bits of data about an individual is that those bits of data can be used together to identify someone and if desired, steal their identity. These data snippets form part of our 'on-line' presence which is why the GDPR was needed to secure personal information.

Rather than inform our membership of all the detail of our use of their personal information, we would like to send a quick letter off to our members saying we use their information for 'administrative purposes', is that sufficient?
Again, the short answer is NO. GDPR expects organisations to be open and transparent with the data subject. Coverall statements or jargon labelled responses are unacceptable. The ICO suggests the 'child test'. Any information sent out by an organisation should be clearly understood by a child.

How much can I rely on the FAS guidelines?
As with all information given out by the Federation of Astronomical Societies, we never purport to be the expert on the subject and the guidance should not be relied upon in a court. The guidelines have been drafted as a result of attending workshops, conferences and reviewing information on the ICO website. All information is given in good faith but societies should seek additional sources of information if they wish to better inform themselves.

The FAS will always update the astronomical community in the light of further guidance issued by the ICO and in the light of experience.

Do I have to follow the FAS guidelines?
Not at all, some astronomical societies have already begun implementing the GDPR regulations. The FAS simply wanted to draw from those societies their experiences and share with you some method of implementing the GDPR guidelines. We hoped you would not have to 're-invent the wheel' and would like to think you find them helpful.

Is there anywhere we can get additional information?
The ICO has a wealth of information on its website[2]. You can e-mail the ICO with questions and there is an on-line chat facility.

There have also been a number of workshops for the charitable and 'third sector' which societies can access and more are planned. There is usually a fee to pay for such conferences. The FAS did send a representative to such workshops and conferences to produce these FAS guidance notes for the astronomical community.

15 Step by Step Guide to Implementing GDPR

If your astronomical society collects information about your members such as name, address, e-mail, *etc*, you are collecting personal data.

The following is offered as a guide[3] only to implementing the GDPR within your astronomical society. This has been trialled and tested with some societies and demonstrated that it has proved helpful.

Throughout this process you should document your actions and decisions.

Step 1.

Select a small team of willing members from your committee. This exercise is best undertaken by a number of members who have a good understanding of how your astronomical society works.

Read the relevant documents supplied and familiarise yourselves with the ICO website and the GDPR regulations[4].

Step 2.

Undertake an audit of the type of personal data collected by your astronomical society and what your society does with it. There is a documentation form attached entitled (**Society Data Audit Tool**) which can be used to collect and display this information. Taking society member information and reformatting that into a membership list is 'processing the data'.

Many astronomical societies that have undertaken such exercises are often surprised by how much the personal data is 'processed' within their society and the purposes for which it is used.

Note:
You are not collecting the actual data your society collects but describing it on the form. For instance in the form it asks '*What data is collected?*'. You would, as an example, state: '*name, address, e-mail, phone numbers*'. You would not be stating the actual names, addresses, e-mail addresses, *etc*. of your members.

Step3.

Once you have populated the documentation form, share it amongst the full committee to ensure you have all the data needed and that it is complete and comprehensive.

You may find that some databases can be combined, restricted or deleted altogether as they are no longer relevant. You may find you collect some data that in reality is no longer required. Generally, it is a good opportunity as an astronomical society to decide what is the appropriate amount of information required from members and how it is processed and how long you retain the information.

Make an action plan to implement the changes you decide.

Step 4.

If ever your astronomical society is asked by a member to inform them what you do with their personal data – in other words one of your members makes a 'data subject request' – you will need to refer to some documentation that describes the astronomical society's data collection and processing and its rules regarding this.

This 4th step collects those processes and lays them out in an easy to see format (use the attached document entitled **Society Processing Record**). This should be periodically reviewed to ensure the society processes are still relevant.

Step 5.

It is useful to write to all members of your astronomical society describing what you are doing regarding GDPR. Many will already have heard about GDPR and, indeed, many may have been contacted by local or national organisations seeking permission to continue to communicate with them.

This is the opportunity to send to your member a copy of the data you hold about them asking for them to confirm that the information is correct. At the same time you can ask your member to 'opt in' to the various communications channels your society uses to communicate with your members.

Some societies that have already implemented the GDPR processes have also taken the opportunity to share the Society Processing Record (described in Step 4 above) to each member in the spirit of openness and for members to see what happens to their data.

Step 6.

Collect the returns, update the society's data as necessary and amend any communication channels. Experience shows that most members will want to continue to communicate with no changes.

Step 7.

Post on the astronomical society's website a Data Privacy Statement. Create a link in that statement so that members of the astronomical society or members of the public can easily make a subject data request.

Step 8.

Decide at a committee meeting how you should manage a data subject request. You could set up a test request to ensure that your processes described above and your responses are working effectively. Also decide at the committee meeting how often to review the society's data collection and processing.

References

[1] The ICO website can be found at www.ico.org.uk

[2] ICO Guide – Principles
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/

[3] ICO Guide – Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now
https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf.

[4] ICO Guide – Guide to the General Data Protection Regulation (GDPR)
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr

Society Data Audit Tool

This is an exercise to gather an understanding of what data is collected by your society, where it is stored and for what purpose.
From this list (which you should retain and repeat periodically) you should be able to draw a comprehensive list of all data collected by your society in preparation for the implementation of the GDRP.
It is advised that several members of your committee collaborate on drawing up this list.
Include anyone else who collects or 'processes' your data. You may find that you duplicate data actions within your society.

What data is collected	How is it collected	Where is it stored	What format	What purpose	Who collects data	Who requires the data	How long is data stored	Amendments to current practice

Society Processing Record

Society members' personal data is collected and is processed for the following purpose and retained:

Processing	Data Processor	For what purpose	Where stored	Who has access	Retention Period

Society Processing Record (Worked Example)

Society members' personal data is collected and is processed for the following purpose and retained:

Processing	Data Processor	For what purpose	Where stored	Who has access	Retention Period
Members' personal data processed within Primary Membership database	Membership Secretary	• Maintain list of members: • Communication with members: *Data anonymised for the following processing* • Producing statistical data for committee: • Controlling number of members joining the Society: • Producing financial projection from members subscriptions	(Society's Cloud database) Membership secretary computer (password protected)	Committee members after request to Membership secretary have access to the Cloud based membership database	Data retained only whilst the person is member of the Society. Database updated as changes to membership occurs
Processing	**Data Processor**	**For what purpose**	**Where stored**	**Who has access**	**Retention Period**
Members data (name only) processed within website to give access to members area	Webmaster	• Give members login access: • Analysis of web usage • Telescope training status: • Notification of helping with visits: • Ability to book telescope time: • Ability to post advert on the members area:	Within website Web-host company	Webmaster	Data removed when member leaves the Society

Processing	Data Processor	For what purpose	Where stored	Who has access	Retention Period
Members data (name and First Aid qualification)	Membership Secretary	Advertise to members and visitors that they are qualified First Aiders	• Website, Spreadsheet held by Membership secretary • Poster in clubroom	Poster in clubroom - all members Webmaster Chairman, Committee	Only whilst First Aid certificate remains in date. (Up to 3 years) then deleted. If member leaves before expiry, then their data is deleted
Processing	**Data Processor**	**For what purpose**	**Where stored**	**Who has access**	**Retention Period**
Members signing-in register Name and date of visit time in/out	Membership Secretary	• Monitor who is on site at observatory. • H&S • Statistical data drawn from the sign-in register	Clubroom	All members	Information deleted after one year